DEFENSE INFORMATION SYSTEMS AGENCY

JOINT INTEROPERABILITY TEST COMMAND
FORT HUACHUCA, ARIZONA

DEPARTMENT OF DEFENSE INTERNET PROTOCOL VERSION 6 GENERIC TEST PLAN VERSION 4

MAY 2009

DEPARTMENT OF DEFENSE
INTERNET PROTOCOL
VERSION 6
GENERIC TEST PLAN
VERSION 4

MAY 2009

Submitted by:

Alvin M. Slarve
Chief
Integrated Communications
Systems Branch

Approved by:

for RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

Prepared Under the Direction of:

Donald L. Hann
Joint Interoperability Test Command
Fort Huachuca, Arizona

(This page intentionally left blank.)

EXECUTIVE SUMMARY

The Internet Protocol (IP) Version 6 (IPv6) is the next generation of the IP protocol with virtually inexhaustible address space that allows improved security, extended routing capabilities, and IP mobility. All products purchased in support of Department of Defense (DoD) networks must be IPv6 capable. The Joint Interoperability Test Command (JITC), DoD, and non-DoD agencies will use this plan to test the IPv6 capabilities of both commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) network devices.

The source requirement document, DoD IPv6 Standard Profiles for IPv6 Capable Products, identifies six product classes for IPv6 network devices: Host/Workstation, Network Appliance/Simple Server, Advanced Server, Router, Layer-3 Switch, and Information Assurance Device. Testers will select the applicable procedures in this plan based on the type of device as specified in the vendor's Letter of Conformance and the device specific capabilities.

Conformance testing will consist of automated test equipment that provides controlled data inputs to elicit a response from a device under test and evaluate that response in accordance with the requirements in the corresponding IPv6 Request for Comment. The procedures exhaustively exercise a manufacturer's IPv6 protocol implementation within a device. Functional categories include: IPv6 Base Requirements, IP Security, Transition Mechanisms, Quality of Service, Mobility, Bandwidth Limited Networks, Network Management, Routing, Automatic Configuration, Server, Host, Router, Layer-3 Switch, and Information Assurance Device.

For interoperability testing, testers will place the device in a network that simulates the environment of the Defense Information Systems Network (DISN) IP Core Network. The test network contains a representative sample of the network equipment currently in use, while utilizing the same dynamic routing protocols currently native to the DISN IP Core Network. Data traffic will be generated and transmitted across the network to assess the device's capability to effectively pass IPv6 traffic and perform other IPv6-related functions in a realistic operational environment. A sample of the capabilities evaluated is auto discovery, addressing, multicast, device mobility, network mobility, encryption, and tunneling. Some of the network connection technologies are Ethernet, Fiber Optic Digital Data Interface, Asynchronous Transfer Mode, Attached Resource Computing Network, and Frame Relay.

A set of procedures is also included to characterize the operational performance of IPv6 devices.

The JITC conducts certification testing for COTS and GOTS equipment for placement on the DoD IPv6 Capable Product Registry. The DoD IPv6 Capable Product Registry will be used by program managers to select IPv6 capable products that will meet operational requirements for transition to IPv6 as the primary DoD network communication protocol.

(This page intentionally left blank.)

TABLE OF CONTENTS

Page

APPENDICES

LIST OF FIGURES

TABLE OF CONTENTS (continued)

Page

LIST OF TABLES

INTRODUCTION

The Department of Defense (DoD) set two objectives for Internet Protocol (IP) Version 6 (IPv6) in Fiscal Year 2008: further expansion of IPv6 transition efforts, and all products purchased in support of DoD networks must be IPv6 capable. The Joint Interoperability Test Command (JITC) under the direction of the Assistant Secretary of Defense, Networks and Information Integration, and the DoD IPv6 Transition Office will utilize the DoD IPv6 Generic Test Plan (GTP) Version 4 to test the IPv6 capabilities of both commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) products used by the DoD.

The generic nature of the DoD IPv6 GTP allows DoD and non-DoD testers to execute procedures with minimal adaptation to local infrastructure. The DoD IPv6 GTP presents a collection of generic test procedures that best test the mandatory requirements found within the DoD IPv6 Standard Profiles for IPv6 Capable Products Version 3.0 document.

For a device to be "IPv6 capable" and placed on the DoD IPv6 Capable Product Registry, it must conform to the Requests for Comments (RFCs) mandated within the DoD IPv6 Standard Profiles for IPv6 Capable Products and be tested to verify protocol functionality and interoperability using the DoD IPv6 GTP. Once JITC certifies a device as IPv6 capable, it will be placed on the DoD IPv6 Capable Product Registry.

FUNCTIONAL DESCRIPTION

The IP is a network protocol used to transport data across Defense Information Systems Network (DISN). The IPv6 is the next generation of the IP protocol and is a critical enabler in achieving the DoD's vision for global, net-centric operations. The primary factors for DoD transition to IPv6 are the advanced feature sets made possible by the virtually inexhaustible address space that IPv6 offers. These features include end-to-end connectivity, improved security, extended routing capabilities, and IP mobility.

The DoD IPv6 Standard Profiles for IPv6 Capable Products identifies IPv6 protocol functional categories and sub categories that must be tested for a device to be certified as IPv6 capable.

IPv6 Base Requirements

- Basic IPv6 specification and addressing formats
- Path Maximum Transmission Unit Discovery for efficient bandwidth utilization
- Stateless Address Auto configuration for IPv6 address assignment by non-stateful means
- Neighbor Discovery for auto-discovery of other nodes and routers
- Internet Control Message Protocol for network and path control, error messages, and troubleshooting

- Uniform Resource Identifier: General Syntax to access resources

IP Security (IPSec) Profile

- Basic Security Architecture for IPSec
- IPSec Authentication Header and Encapsulating Security Payload for tunneling and transporting encrypted traffic
- Public Key Infrastructure management for network resource access control
- Authentication, Authorization, and Accounting services for administration and access control
- Cryptographic Message Syntax for encrypted traffic
- Secure e-mail certificate handling for message validation

Transition Mechanisms

- Transition mechanisms for IPv6 hosts and routers
- Generic packet tunneling for routing

Quality of Service

- Resource ReSerVation Protocol for Traffic Engineering (TE)
- Differentiated Services for TE
- Per-Hop Behaviors for defining policies and priorities for packets
- Header Compression for locating priority field bits

Mobility

- Definitions of managed objects for IPv6 mobility support
- Mobility support for both IP Version 4 (IPv4) and IPv6

Bandwidth Limited Networks

These requirements are currently optional and are not required for any device type.

Network Management

- Domain Name System (DNS) definitions for Quad-A name/address resolution
- DNS Security for safekeeping name/address resolution services
- Dynamic Host Configuration Protocol for stateful address auto-configuration
- Management Information Base for remote network management
- Simple Network Management Protocol for IPv6

Routing

A router is either an Exterior Router or an Interior Router. Router products may include both capabilities.

Automatic Configuration

A device's product class will determine which method of automatic configuration is appropriate. The two types of automatic configuration are Stateless Address Auto-configuration (SLAAC) and Dynamic Host Configuration Protocol Version 6 (DHCPv6). Every device under test must perform either SLAAC or DHCPv6.

The DoD IPv6 Standard Profiles for IPv6 Capable Products further defines product classes for IPv6 network devices.

- Host
- Network Appliance or Simple Server
- Advanced Server
- Router
- Layer-3 Switch
- Information Assurance Device

TEST BACKGROUND

The DoD IPv6 GTP is a modular, scalable test plan designed to evaluate a device or system through conformance, performance, and interoperability testing. The DoD IPv6 GTP Version 4 also provides generic test procedures to allow the JITC to certify a device as IPv6 capable and place it on the DoD IPv6 Capable Product Registry.

The DoD IPv6 GTP allows DoD or non-DoD test organizations to test in accordance with requirements in the DoD IPv6 Standard Profiles for IPv6 Capable Products. Test case procedures may require slight adjustments to better suit the requirements as related to the product class and device under test.

TEST PURPOSE

Testing will determine the RFC conformance, performance, and interoperability of IPv6 capable COTS and GOTS equipment.

REQUIREMENTS

The DoD IPv6 Standard Profiles for IPv6 Capable Products is the source requirement document addressed in the DoD IPv6 GTP. Only the "MUST" RFC requirements from the DoD IPv6 Standard Profiles for IPv6 Capable Products document are tested. However, vendors may request additional testing based on their device's

capabilities. Refer to Appendix F for a complete list of product class requirements and see Table 1 for detailed device requirements and a listing of all test cases related to the required RFC based on their product class. For all other RFC requirements considered emerging or optional for the DoD IPv6 Capable Product Registry test process, refer to the DoD IPv6 Standard Profiles for IPv6 Capable Products document.

Table 1. IPv6 Capable Device to Test Case Matrix for DoD IPv6 Capable Product Registry Testing

RFC	RFC Title	Test Case	Product Class						Effective Date	Comment
			Host/ WS	Network App or Simple Server	Advanced Server	Router	L3 Switch	IA Device		
IPv6 Base										
2460	Internet Protocol, Version 6 (IPv6) Protocol Specification	C.1.2	M	M	M	M	M	M	Current	
5095	Deprecation of Type 0 Routing Headers in IIPv6		M	M	M	M	M	M	7/2009	
4443	Internet Control Message Protocol (ICMPv6)	C.1.14	M	M	M	M	M	M	Current	
2461	Neighbor Discovery for IPv6	C.1.3	M	M	M	M	M	M	Current	
4861									7/2009	
2462	IPv6 Stateless Address Auto configuration	C.1.4	M	M	M	M	M	M	Current	Note 1
4862									7/2009	
1981	Path MTU Discovery for IPv6	C.1.1	M	S	M	M	M	M	Current	
4291	IPv6 Addressing Architecture	C.1.13	M	M	M	M	M	M	Current	
4007	Scoped Address Architecture	C.1.11	M	M	M	M	M	M	Current	
4193	Unique Local IPv6 Unicast Addresses	C.1.12	O	O	O	O	O	O	Current	
2710	Multicast Listener Discovery for IPv6	C.1.8	M	M	M	M	M	M	Current	
3810	MLDv2 for IPv6	C.1.10	M	S+	M	M	S+	S+	Current	Note 2
2464	IPv6 over Ethernet	C.1.5	CM	CM	CM	CM	CM	CM	Current	Note 3
2492	IPv6 over ATM	C.4.2	CM	CM	CM	CM	CM	CM	Current	Note 3
2472	IPv6 over PPP	C.1.7	CM	CM	CM	CM	CM	CM	Current	Note 3
5072									7/2009	
3572	IPv6 over MAPOS	C.1.9	CM	CM	CM	CM	CM	CM	Current	Note 3
2467	IPv6 over FDDI	C.1.6	CM	CM	CM	CM	CM	CM	Current	Note 3
2491	IPv6 over NBMA	C.4.1	CM	CM	CM	CM	CM	CM	Current	Note 3
2497	IPv6 over ARCnet	C.4.3	CM	CM	CM	CM	CM	CM	Current	Note 3
2590	IPv6 over Frame Relay	C.4.4	CM	CM	CM	CM	CM	CM	Current	Note 3
3146	IPv6 over IEEE 1394 Networks	C.4.5	CM	CM	CM	CM	CM	CM	Current	Note 3
4338	IPv6, IPv4, and ARP Packets over Fibre Channel	C.4.6	CM	CM	CM	CM	CM	CM	Current	Note 3
4944	Transmission of IPv6 Packets Over IEEE 802.15.4 Networks		CM	CM	CM	CM	CM	CM	7/2009	
IPSec										
4301	Security Architecture for Internet Protocol	C.2.1	M	S+	M	M	S+	CM	Current	
4302	IP Authentication Header	C.2.2	S	S	S	CM	S	CS	Current	

Table 1. IPv6 Capable Device to Test Case Matrix for DoD IPv6 Capable Product Registry Testing (continued)

RFC	RFC Title	Test Case	Product Class						Effective Date	Comment
			Host/ WS	Network App or Simple Server	Advanced Server	Router	L3 Switch	IA Device		
4303	IP Encapsulating Security Payload	C.2.3 C.2.8	M	S+	M	M	S+	CM	Current	
4308 [VPN-B]	Cryptographic Suites for Ipsec	C.2.7	M	S+	M	M	S+	CM	7/2009	
4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C.2.4 C.2.8	M	S+	M	M	S+	CM	Current	
4835									7/2009	
4869	Suite B Cryptographic Suites for Ipsec		M	S+	M	M	S+	CM	7/2009	
IEEE 802.1-2007i	Standard for Information Technology Part 11 – Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 6 MAC Security Enhancements		CS	CS	CS	CS	CS	CS	Current	
2401	Security Architecture for the Internet Protocol		CM	CS+	CM	CM	CS+	CM	Current	Note 4
2406	Ipsec Encapsulating Security Payload (ESP)		CM	CS+	CM	CM	CS+	CM	Current	Note 4
2402	Ipsec Authenticating Header (AH)		CM	CS+	CM	CM	CS+	CM	Current	Note 4
3971	Secure Neighbor Discovery		S	S	S	S	S	S	Current	
3972	Cryptographically Generated Addresses		S	S	S	S	S	S	Current	
3041	Privacy Extensions for Stateless Address Auto configuration in IPv6	C.3.7	S+ CM	S	CM	S+	S	S	Current	
4941									7/2009	
4306	Internet Key Exchange Version 2 (IKEv2) Protocol	C.2.5	M	S+	M	M	S+	CM	7/2010	
4307	Cryptographic Algorithms for Internet Key Exchange Version 2 (IKEv2)	C.2.6	M	S+	M	M	S+	CM	7/2010	
2407	The Internet IP Security Domain of Interpretation for ISAKMP		CM	CS+	CM	CM	CS+	CM	Current	Note 5
2408	Internet Security Association and Key Management Protocol (ISAKMP)		CM	CS+	CM	CM	CS+	CM	Current	Note 5
2409	The Internet Key Exchange (IKE)		CM	CS+	CM	CM	CS+	CM	Current	Note 5
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)		CM	CS+	CM	CM	CS+	CM	Current	Note 5

Table 1. IPv6 Capable Device to Test Case Matrix for DoD IPv6 Capable Product Registry Testing (continued)

RFC	RFC Title	Test Case	Product Class						Effective Date	Comment
			Host/ WS	Network App or Simple Server	Advanced Server	Router	L3 Switch	IA Device		
4304	Extended Sequence Number (ESN) Addendum to Ipsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)		CS	CS	CS	CS	CS	CS	7/2009	Note 5
Transition Mechanisms										
4213	Transition Mechanisms for IPv6 Hosts and Routers [Dual Stack]	C.3.18	CM Note 6	S	CM Note 6	M Note 6	CM Note 6 Note 7	S	Current	
4213	Transition Mechanisms for IPv6 Hosts and Routers [manual tunnels]			N/R				N/R	Current	
4213	Transition Mechanisms for IPv6 Hosts and Routers [Translation and other methods]		O	O	O	O	O	O	Current	
2766	Network Address Translation-Protocol Translation (NAT-PT)		SN	SN	SN	SN	SN	SN	Current	
3053	IPv6 Tunnel Broker		CM	CS	CM	CM	CM	N/R	Current	
4798	Connecting IPv6 Islands over IPv4 MPLS using IPv6 Provider Edge (6PE) routers		N/R	N/R	N/R	CS	CS	N/R	Current	
Quality of Service										
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	C.3.3	O	O	O	M	O Note 7	N/R	Current	
3168	The Addition of Explicit Congestion Notification (ECN) to IP		O	O	O	S	O	N/R	Current	
2205	Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification		O	O	O	S+	O	N/R	Current	
2207	RSVP Extensions for IPSEC Data Flows		O	O	O	S+	O	N/R	Current	
2210	The Use of RSVP with IETF Integrated Services		O	O	O	S+	O	N/R	Current	
2750	RSVP Extensions for Policy Control		O	O	O	S+	O	N/R	Current	
3175	Aggregation of RSVP for IPv4 and IPv6 Reservations		O	O	O	O	O	N/R	Current	
3181	Signaled Preemption Priority Policy Object		O	O	O	O	O	N/R	Current	
2961	RSVP Refresh Overhead Reduction Extension		O	O	O	O	O	N/R	Current	

Table 1. IPv6 Capable Device to Test Case Matrix for DoD IPv6 Capable Product Registry Testing (continued)

RFC	RFC Title	Test Case	Product Class						Effective Date	Comment
			Host/ WS	Network App or Simple Server	Advanced Server	Router	L3 Switch	IA Device		
4495	A Resource Reservation Protocol (RSVP) Extension for the Reduction of Bandwidth of a Reservation Flow		O	O	O	O	O	N/R	Current	
2998	A Framework for Integrated Services Operation over DiffServ Networks		O	O	O	O	O	N/R	Current	
2996	Format of the RSVP DCLASS Object		O	O	O	O	O	N/R	Current	
2746	RSVP Operation Over IP Tunnels		O	O	O	O	O	N/R	Current	
3182	Identity Representation for RSVP		O	O	O	O	O	N/R	Current	
2872	Application and Sub Application Identity Policy Element for Use with RSVP		O	O	O	O	O	N/R	Current	
2747	RSVP Cryptographic Authentication		O	O	O	O	O	N/R	Current	
Mobility										
3775	Mobility Support in IPv6	C.3.14	CM	CS	CM (sect 9)	CM Note 8	N/R	N/R	Current	
3776	Using Ipsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents	C.3.15	CM	CS	N/R	CM Note 8	N/R	N/R	Current	
4877	Mobile IPv6 Operation with IKEv2 and the Revised Ipsec Architecture		CM	CS	N/R	CM Note 8	N/R	N/R	7/2010	
4282	The Network Access Identifier		CS+	CS	N/R	CS+ Note 8	N/R	N/R	Current	
4283	Mobile Node Identifier for Option for IPv6		CS+	CS	N/R	CS+ Note 8	N/R	N/R	Current	
3963	Network Mobility (NEMO) Basic Support Protocol	C.3.16	N/R	N/R	N/R	CM	N/R	N/R	Current	
Bandwidth Limited Networks										
3095	Robust Header Compression (RoHC)		O	O	O	O	O	N/R	Current	
4815	Corrections and Clarification to RFC 3095		O	O	O	O	O	N/R	Current	
4995	RoHC Framework		O	O	O	O	O	N/R	Current	
4996	RoHC: A profile for TCP/IP		O	O	O	O	O	N/R	Current	
3241	RoHC over PPP		O	O	O	O	O	N/R	Current	
3843	RoHC: A Compression Profile for IP		O	O	O	O	O	N/R	Current	
4362	RoHC: A Link-Layer Assisted Profile for IP/UDP/RTP		O	O	O	O	O	N/R	Current	
2507	IP Header Compression		O	O	O	O	O	N/R	Current	
2508	Compressing IP/UDP/RTP Headers for Low-Speed Serial Links		O	O	O	O	O	N/R	Current	
3173	IP Payload Compression		O	O	O	O	O	N/R	Current	

Table 1. IPv6 Capable Device to Test Case Matrix for DoD IPv6 Capable Product Registry Testing (continued)

RFC	RFC Title	Test Case	Product Class						Effective Date	Comment
			Host/ WS	Network App or Simple Server	Advanced Server	Router	L3 Switch	IA Device		
Network Management										
3411	An Architecture for Describing Simple Network Management Protocol Version 3 (SNMPv3)	C.3.9	N/R	N/R	N/R	M	CM Note 10	N/R	Current	Note 9
3412	Message Processing and Dispatching for the SNMP	C.3.10	N/R	N/R	N/R	M	CM Note 10	N/R	Current	Note 9
3413	SNMP Applications	C.3.11	N/R	N/R	N/R	M	CM Note 10	N/R	Current	Note 9
N/A	SNMP over IPv6	N/A	N/R	N/R	N/R	S+	S+	N/R	7/2010	
3595	Textual Conventions for IPv6 Flow Label	C.3.21	N/R	N/R	N/R	M	CM Note 10	N/R	Current	Note 9
4022	Management Information Base for the Transmission Control Protocol	C.3.21	N/R	N/R	N/R	M	CM Note 10	N/R	Current	Note 9
4113	Management Information Base for the User Datagram Protocol	C.3.21	N/R	N/R	N/R	M	CM Note 10	N/R	Current	Note 9
4087	IP Tunnel MIB	C.3.21	N/R	N/R	N/R	S	S Note 10	N/R	Current	Note 9
4293	Management Information Base (MIB) for IP	C.3.21	N/R	N/R	N/R	M	CM Note 10	N/R	Current	Note 9
4295	Mobile IP Management MIB	C.3.21	N/R	N/R	N/R	CM	CM Note 10	N/R	Current	Note 9
4807	Ipsec Security Policy Database Configuration	C.3.21	N/R	N/R	N/R	CM	CM Note 10	N/R	Current	Note 9
4292	IP Forwarding Table MIB	C.3.21	N/R	N/R	N/R	M	CM Note 10	N/R	Current	Note 9
4601	Protocol Independent Multicast – Sparse Mode (PIM-SM)	C.3.21	N/R	N/R	N/R	CS+	N/R	N/R	Current	
3973	Protocol Independent Multicast – Dense Mode	C.3.21	N/R	N/R	N/R	CS+	N/R	N/R	Current	
Routing										
2740	OSPF for IPv6 (OSPFv3)	C.3.5	N/R	N/R	N/R	CM Note 11	CM Note 9	N/R	Current	
4552	Authentication/Confidentiality for OSPFv3		N/R	N/R	N/R	CM Note 11	CM Note 9	N/R	Current	
4271	A Border Gate Protocol (BGP-4)	C.3.19	N/R	N/R	N/R	CM Note 12	CM Note 7	N/R	Current	
1772	Application of the Border Gateway Protocol in the Internet	C.3.1	N/R	N/R	N/R	CM Note 12	CM Note 7	N/R	Current	
2545	Use of BGP-4 Multi-Protocol Extensions for IPv6 Inter-Domain Routing	C.3.4	N/R	N/R	N/R	CM Note 12	CM Note 7	N/R	Current	

Table 1. IPv6 Capable Device to Test Case Matrix for DoD IPv6 Capable Product Registry Testing (continued)

RFC	RFC Title	Test Case	Product Class						Effective Date	Comment
			Host/ WS	Network App or Simple Server	Advanced Server	Router	L3 Switch	IA Device		
2858 4760	Multi-Protocol Extensions for BGP-4	C.3.20	N/R	N/R	N/R	CM Note 12	CM Note 7	N/R	Current 7/2009	
Automatic Configuration										
2462 4862	IPv6 Stateless Address Auto configuration (SLAAC)	C.1.4	M Note 1	M Note 1	N/R	M Note 13	N/R	N/R	Current 7/2009	
3315	DHCPv6 [client]	C.3.8							Current	
3315	DHCPv6 [server]	C.3.8	N/R	CM	CM	CM	N/R	N/R	7/2009	
	DHCPv6 [Relay Agent]	C.3.8		N/R	N/R		CM			
3769	IPv6 Prefix Delegation		N/R	CM	CM	CM	N/R	N/R	7/2009	
3633	IPv6 Prefix Options for DHCPv6		N/R	CM	CM	CM	N/R	N/R	7/2009	
N/A	[disable autoconfiguration]		M	M	M	M	M	M	Current	
5175	Extensions to Router Advertisement Flags		CS+	CS+	CS+	CS+	CS+	CS+	7/2009	
Server										
959	File Transfer Protocol		N/R	O	O	N/R	N/R	N/R	Current	
2428	FTP Extensions for IPv6 and NAT		N/R	O	O	N/R	N/R	N/R	Current	
2821	Simple Mail Transfer Protocol (SMTP)		N/R	O	O	N/R	N/R	N/R	Current	
2911	Internet Printing Protocol		N/R	O	O	N/R	N/R	N/R	Current	
3162	RADIUS (Remote Authentication Dial-In User Service) and IPv6		N/R	O	O	N/R	N/R	CM	Current	
4330	Simple Network Time Protocol (SNTP)		N/R	O	O	N/R	N/R	N/R	Current	
3226	DNS Security and IPv6 A6 Aware Server/Resolver Message Size Requirements		N/R	O	O	N/R	N/R	N/R	Current	
3261	Session Initiation Protocol (SIP)		N/R	O	O	N/R	N/R	N/R	Current	
3596	DNS Extensions to Support IPv6		N/R	O	O	N/R	N/R	N/R	Current	
3053	IPv6 Tunnel Broker		N/R	O	O	N/R	N/R	N/R	Current	
Host										
3484 [Sec 2.1]	Default Address Selection for IPv6 [Policy Table]		S+	S	S+	N/R	N/R	N/R	Current	
3484 [rest of RFC]	Default Address Selection for IPv6		M	S	M	N/R	N/R	N/R	Current	
3596 resolver	DNS Extensions to Support IPv6		M	S	M	N/R	N/R	N/R	Current	

Table 1. IPv6 Capable Device to Test Case Matrix for DoD IPv6 Capable Product Registry Testing (continued)

RFC	RFC Title	Test Case	Product Class						Effective Date	Comment
			Host/ WS	Network App or Simple Server	Advanced Server	Router	L3 Switch	IA Device		
3986	Uniform Resource Identifier (URI): Generic Syntax		M	S	M	N/R	N/R	N/R	Current	
Router										
2784	Generic Router Encapsulation (GRE)		N/R	N/R	N/R	CM	N/R	N/R	Current	
2473	Generic Packet Tunneling in IPv6		N/R	N/R	N/R	CM Note 11	N/R	N/R	Current	
L3 Switch										
4541	Considerations for IGMP and MLD Snooping Switches		N/R	N/R	N/R	N/R	CS	N/R	Current	
IA Device										
3585	IPsec Configuration Policy Information Model		N/R	N/R	N/R	N/R	N/R	CS+	Current	
3586	IP Security Policy Requirements		N/R	N/R	N/R	N/R	N/R	CS+	Current	

NOTES:

1. The device must implement one of the automatic configuration mechanisms SLAAC or DHCPv6. However, all nodes MUST perform duplicate address detection and automatically generated link-local address regardless of automatic address configuration method.
2. All Layer-3 Switches implementing MLDv2 MUST perform the modes of “router” and “listener,” as annotated in RFC 3810.
3. The device must be conformant to at least one of the Connection Technologies protocols.
4. IPSec Fallback requirements only apply to a product that MUST support IPSec that does not currently support IPSec RFC 4301.
5. Products with IKEv2 implementation MAY also include a fall-back to IKEv1; products without IKEv2 MUST at least meet the IKEv1 requirements.
6. MUST implement Dual Stack or Tunneling to meet the requirement to carry both IPv4 and IPv6 traffic.
7. The device must be conformant if it functions as an External System Node.
8. The device must be conformant if it functions as a Home Agent.
9. The device must be conformant if it functions as an Interior System Node.
10. The device must be conformant if it functions as a Managed Switch.
11. The device must be conformant if it functions as an Interior Router.
12. The device must be conformant if it functions as an External Router.
13. MUST support Router requirements for SLAAC.

LEGEND:

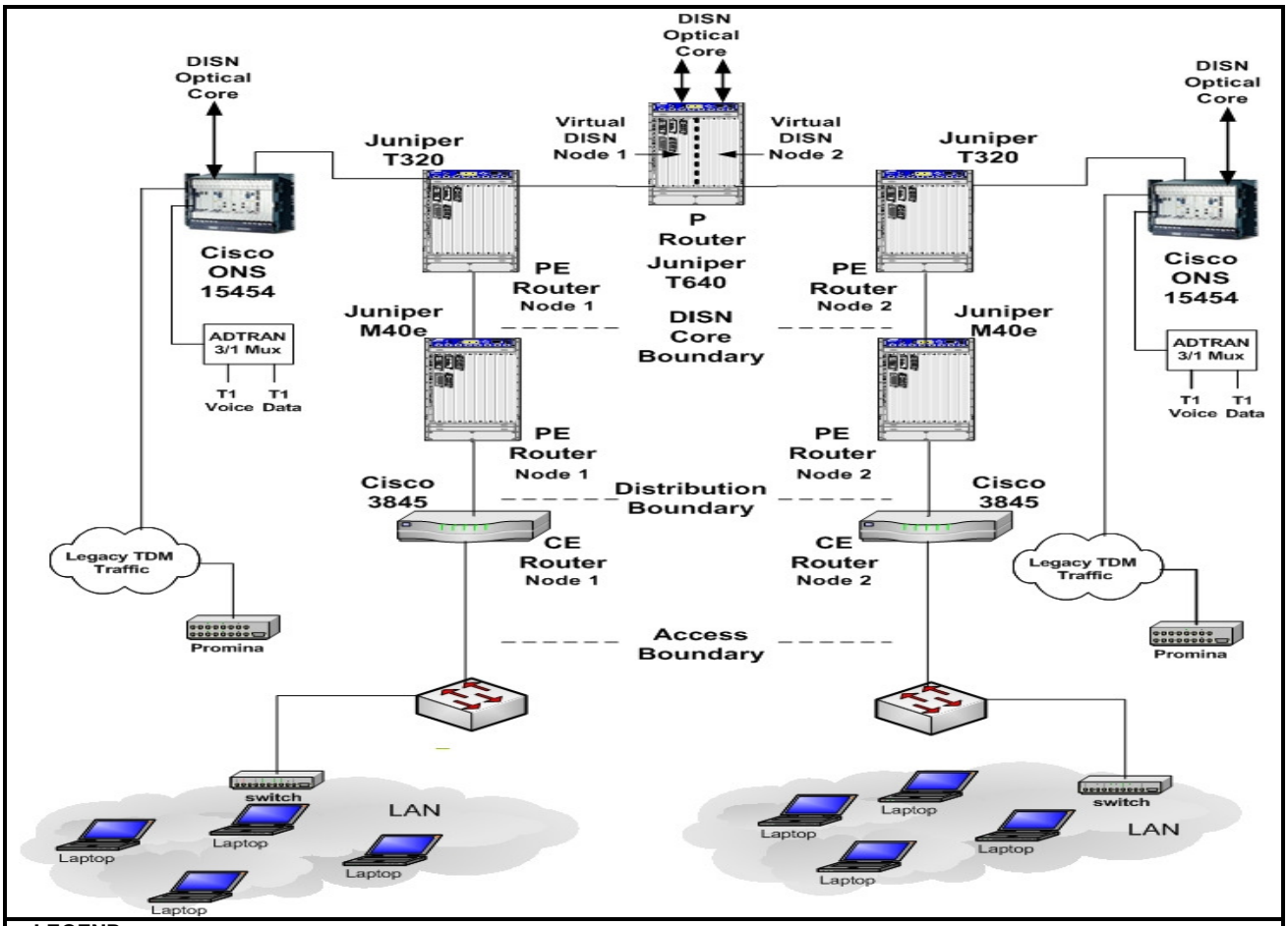
A6	IPv6 Address Record	MIB	Management Information Base
App	Appliance	MLD	Multicast Listener Discovery
ARCnet	Attached Resource Computer Network	MLDv2	MLD Version 2
ARP	Address Resolution Protocol	MPLS	Multi-protocol Label Switching
ATM	Asynchronous Transfer Mode	MTU	Maximum Transmission Unit
BGP-4	Border Gateway Protocol Version 4	N/A	Not Applicable
CM	Conditional Must	N/R	No Requirement
CS	Conditional Should	NAT	Network Address Translation
CS+	Conditional Should Plus	NBMA	Non-Broadcast Multi-Access Network
DHCP	Dynamic Host Configuration Protocol	O	Optional
DHCPv6	DHCP Version 6	OSPF	Opened Shortest Path First
DiffServ	Differentiated Services	OSPFv3	OSPF Version 3
DNS	Domain Name Service	PPP	Point-to-Point Protocol

Table 1. IPv6 Capable Device to Test Case Matrix for DoD IPv6 Capable Product Registry Testing (continued)

DoD	Department of Defense	RADIUS	Remote Authentication Dial-In User Service
FDDI	Fiberoptic Digital Data Interface	RFC	Request for Comment
FTP	File Transfer Protocol	RoHC	Robust Header Compression
IA	Information Assurance	RSVP	Resource ReSerVation Protocol
IEEE	Institute of Electrical and Electronic Engineers, Inc.	RTP	Real-Time Transport Protocol
IETF	Internet Engineering Task Force	S	Should
IGMP	Internet Group Multicast Protocol	S+	Should Plus
IKE	Internet Key Exchange	SDH	Synchronous Digital Hierarchy
IKEv1	IKE Version 1	Sect	Section
IKEv2	IKE Version 2	SLAAC	Stateless Address Auto-configuration
IP	Internet Protocol	SN	Should Not
IPSec	Internet Protocol Security	SNMP	Simple Network Management Protocol
IPv4	Internet Protocol Version 4	SONET	Synchronous Optical Network
IPv6	Internet Protocol Version 6	TCP	Transmission Control Protocol
ISAKMP	Internet Security Association and Key Management Protocol	UDP	User Datagram Protocol
L3	Layer-3	V	Version
M	Must	VPN-B	Virtual Private Network Suite B
MAC	Media Access Control	WS	Workstation
MAPOS	Multiple Access Protocol Over SONET/SDH		

SCOPE

A vital component of the DoD IPv6 Capable Product Registry test process is JITC's interoperability testing. The JITC conducts interoperability testing across a test network simulating two DISN IP Core Nodes engineered specifically to emulate the DISN IP Core topology. Interoperability testing in such a manner yields a high degree of certainty that the risks posed by untested, and possibly unstable, implementations of IPv6 in equipment accessing the DISN network have been minimized. The JITC will execute a series of test cases according to the "MUST" requirements of a device's Product Class, to assess its interoperability and functionality across two simulated DISN IP Core Nodes, as depicted in Figure 1.



LEGEND:

CE	Customer Edge	ONS	Optical Network System
DISN	Defense Information Systems Network	P	Provider
IP	Internet Protocol	PE	Provider Edge
LAN	Local Area Network	TDM	Time Division Multiplexer
MUX	Multiplexer		

Figure 1. Simulated DISN IP Core Test Network

The JITC conducts interoperability testing of IPv6 capable devices using the procedures in Appendix C. Appendix D is used to test the performance of devices and networks under test.

The test environment will consist of interfaces, network hardware, operating systems software, and application software components configured to test IPv6 and dual stack IPv4/IPv6 capabilities in a converged DISN IP Core environment.

The successful completion of the IPv6 capable testing process (i.e., conformance, interoperability, and performance testing) will signify that the device is IPv6 capable and JITC will certify the device for placement on the DoD IPv6 Capable Product Registry. The DoD IPv6 Capable Product Registry will be used by program managers to select IPv6 capable products that will meet the operational requirements for transition to IPv6 as the primary DoD network communication protocol.

METHODOLOGY

The tester may adapt test procedures, as necessary, to accommodate the device under test and its functionality within the network environment. The DoD IPv6 GTP contains test procedures for the following:

- Conformance - the process of testing that determines if an implementation conforms to a specification.
- Interoperability - the ability to exchange and use information, usually across several heterogeneous networks (analyzed by a conditional yes or no response).
- Performance - testing conducted to evaluate the compliance of a system or component with specified performance requirements (analyzed by measurable metrics).

All testing involving traffic generation will include a combination of IPv4 and IPv6 traffic to emulate single and dual-protocol environments.

The detailed conformance and interoperability test procedures are in Appendix C. Performance testing is not required for devices, but vendors may request performance testing. Detailed performance procedures are in Appendix D. Table 1 lists all RFCs and their corresponding test cases. Each test case can test to any product class.

APPENDIX A

ACRONYMS

ABR	Area Border Routers
AH	Authentication Header
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
AS	Autonomous System
ATM	Asynchronous Transfer Mode
BDR	Backup Designated Router
BGP	Border Gateway Protocol
BGP-4	BGP Version 4
BGP4+	BGP Multi-protocol Extensions
BR	Border Router
CIDR	Classless Inter-Domain Routing
CN	Correspondent Node
CoA	Care of Address
COTS	Commercial off the Shelf
DAD	Duplicate Address Detection
DiffServ	Differentiated Services
DISN	Defense Information Systems Network
DHCP	Dynamic Host Configuration Protocol
DHCPv6	DHCP Version 6
DISA	Defense Information Systems Agency
DISR	DoD Information Technology Standards Registry
DNS	Domain Name Service
DoD	Department of Defense
DR	Designated Router
DSCP	Differentiated Services Code Point
DUT	Device Under Test
eBGP	External BGP
ESP	Encapsulating Security Payload
FDDI	Fiber Optic Digital Data Interface
FN	Foreign Network
FTP	File Transfer Protocol
GOTS	Government off the Shelf
GRE	Generic Route Encapsulation

GTP	Generic Test Plan
HA	Home Agent
HMAC	Hash Message Authentication Code
HN	Home Network
HTM	HyperText Markup
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
IATP	Information Assurance Test Plan
iBGP	Internal BGP
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol for IPv6
ID	Identification
IDS	Intrusion Detection Systems
IEEE	Institute of Electrical and Electronic Engineers, Inc.
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IKEv1	IKE Version 1
IKEv2	IKE Version 2
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IPv6CP	IPv6 Control Protocol
IPX	Internetwork Packet Exchange
ISAKMP	Internet Security Association and Key Management Protocol
JITC	Joint Interoperability Test Command
LAN	Local Area Network
LCP	Link Control Protocol
LSA	Link State Advertisements
MAC	Media Access Control
MAPOS	Multiple Access Protocol Over SONET/SDH
MIB	Management Information Base
MLD	Multicast Listener Discovery
MLDv2	MLD Version 2
MN	Mobile Node
MODP	Modern Programming Practice
MR	Mobile Router
MTU	Maximum Transmission Unit

N/A	Not Applicable
NBMA	Non-Broadcast Multi-Access
NCP	Network Control Protocols
NEMO	Network Mobility
NLP	Network Layer Protocols
NLRI	Network Layer Reachability Information
NMS	Network Management System
NSA	National Security Agency
OID	Object Identifiers
OS	Operating System
OSPF	Open Shortest Path First
OSPFv3	OSPF Version 3
PC	Personal Computer
PHB	Per-hop behaviors
PMTU	Path Maximum Transmission Unit
PPP	Point-to-Point Protocol
QoS	Quality of Service
RFC	Request for Comment
RTSP	Real-Time Streaming Protocol
SA	Security Associations
SDH	Synchronous Digital Hierarchy
SLAAC	Stateless Address Auto-configuration
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNMPv3	SNMP Version 3
SONET	Synchronous Optical Network
TCP	Transmission Control Protocol
TE	Traffic Engineering
TGA	Traffic Generator/Analyzer
TN	Test Node
ToS	Type of Service
UDP	User Datagram Protocol
UI	User Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Language

VLC	VideoLAN Client
WAN	Wide Area Network

APPENDIX B

DETAILED REQUIREMENTS

Table B-1. IPv6 Capable Device Requirements for Testing

RFC	RFC Title	Product Class						Effective Date	Comment
		Host	Network App or Simple Server	Advanced Server	Router	L3 Switch	IA Device		
IPv6 Base									
2460	Internet Protocol, Version 6 (IPv6) Protocol Specification	M	M	M	M	M	M	Current	
5095	Deprecation of Type 0 Routing Headers in IPv6	M	M	M	M	M	M	7/2009	
4443	Internet Control Message Protocol (ICMPv6)	M	M	M	M	M	M	Current	
2461 4861	Neighbor Discovery for IPv6	M	M	M	M	M	M	Current 7/2009	
2462 4862	IPv6 Stateless Address Auto configuration	M	M	M	M	M	M	Current 7/2009	Note 1
1981	Path MTU Discovery for IPv6	M	S	M	M	M	M	Current	
4291	IPv6 Addressing Architecture	M	M	M	M	M	M	Current	
4007	Scoped Address Architecture	M	M	M	M	M	M	Current	
4193	Unique Local IPv6 Unicast Addresses	O	O	O	O	O	O	Current	
2710	Multicast Listener Discovery for IPv6	M	M	M	M	M	M	Current	
3810	MLDv2 for IPv6	M	S+	M	M	S+	S+	Current	Note 2
2464	IPv6 over Ethernet	CM	CM	CM	CM	CM	CM	Current	Note 3
2492	IPv6 over ATM	CM	CM	CM	CM	CM	CM	Current	Note 3
2472 5072	IPv6 over PPP	CM	CM	CM	CM	CM	CM	Current 7/2009	Note 3
3572	IPv6 over MAPOS	CM	CM	CM	CM	CM	CM	Current	Note 3
2467	IPv6 over FDDI	CM	CM	CM	CM	CM	CM	Current	Note 3
2491	IPv6 over NBMA	CM	CM	CM	CM	CM	CM	Current	Note 3
2497	IPv6 over ARCnet	CM	CM	CM	CM	CM	CM	Current	Note 3
2590	IPv6 over Frame Relay	CM	CM	CM	CM	CM	CM	Current	Note 3
3146	IPv6 over IEEE 1394 Networks	CM	CM	CM	CM	CM	CM	Current	Note 3
4338	IPv6, IPv4, and ARP Packets over Fibre Channel	CM	CM	CM	CM	CM	CM	Current	Note 3
4944	Transmission of IPv6 Packets Over IEEE 802.15.4 Networks	CM	CM	CM	CM	CM	CM	7/2009	
IPSec									
4301	Security Architecture for Internet Protocol	M	S+	M	M	S+	CM	Current	
4302	IP Authentication Header	S	S	S	CM	S	CS	Current	

Table B-1. IPv6 Capable Device Requirements for Testing (continued)

RFC	RFC Title	Product Class						Effective Date	Comment
		Host	Network App or Simple Server	Advanced Server	Router	L3 Switch	IA Device		
4303	IP Encapsulating Security Payload	M	S+	M	M	S+	CM	Current	
4308 [VPN-B]	Cryptographic Suites for IPsec	M	S+	M	M	S+	CM	7/2009	
4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	M	S+	M	M	S+	CM	Current	
4835								7/2009	
4869	Suite B Cryptographic Suites for IPsec	M	S+	M	M	S+	CM	7/2009	
IEEE 802.1-2007i	Standard for Information Technology Part 11 – Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 6 MAC Security Enhancements	CS	CS	CS	CS	CS	CS	Current	
2401	Security Architecture for the Internet Protocol	CM	CS+	CM	CM	CS+	CM	Current	Note 4
2406	IPsec Encapsulating Security Payload (ESP)	CM	CS+	CM	CM	CS+	CM	Current	Note 4
2402	IPsec Authenticating Header (AH)	CM	CS+	CM	CM	CS+	CM	Current	Note 4
3971	Secure Neighbor Discovery	S	S	S	S	S	S	Current	
3972	Cryptographically Generated Addresses	S	S	S	S	S	S	Current	
3041	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	S+ CM	S	CM	S+	S	S	Current	
4941								7/2009	
4306	Internet Key Exchange Version 2 (IKEv2) Protocol	M	S+	M	M	S+	CM	7/2010	
4307	Cryptographic Algorithms for Internet Key Exchange Version 2 (IKEv2)	M	S+	M	M	S+	CM	7/2010	
2407	The Internet IP Security Domain of Interpretation for ISAKMP	CM	CS+	CM	CM	CS+	CM	Current	Note 5
2408	Internet Security Association and Key Management Protocol (ISAKMP)	CM	CS+	CM	CM	CS+	CM	Current	Note 5
2409	The Internet Key Exchange (IKE)	CM	CS+	CM	CM	CS+	CM	Current	Note 5
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	CM	CS+	CM	CM	CS+	CM	Current	Note 5

Table B-1. IPv6 Capable Device Requirements for Testing (continued)

RFC	RFC Title	Product Class						Effective Date	Comment
		Host	Network App or Simple Server	Advanced Server	Router	L3 Switch	IA Device		
4304	Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)	CS	CS	CS	CS	CS	CS	7/2009	Note 5
Transition Mechanisms									
4213	Transition Mechanisms for IPv6 Hosts and Routers [Dual Stack]	CM Note 6	S	CM Note 6	M Note 6	CM Note 6 Note 7	S	Current	
4213	Transition Mechanisms for IPv6 Hosts and Routers [manual tunnels]		N/R				N/R	Current	
4213	Transition Mechanisms for IPv6 Hosts and Routers [Translation and other methods]	O	O	O	O	O	O	Current	
2766	Network Address Translation- Protocol Translation (NAT-PT)	SN	SN	SN	SN	SN	SN	Current	
3053	IPv6 Tunnel Broker	CM	CS	CM	CM	CM	N/R	Current	
4798	Connecting IPv6 Islands over IPv4 MPLS using IPV6 Provider Edge (6PE) routers	N/R	N/R	N/R	CS	CS	N/R	Current	
Quality of Service									
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	O	O	O	M	O Note 7	N/R	Current	
3168	The Addition of Explicit Congestion Notification (ECN) to IP	O	O	O	S	O	N/R	Current	
2205	Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification	O	O	O	S+	O	N/R	Current	
2207	RSVP Extensions for IPSEC Data Flows	O	O	O	S+	O	N/R	Current	
2210	The Use of RSVP with IETF Integrated Services	O	O	O	S+	O	N/R	Current	
2750	RSVP Extensions for Policy Control	O	O	O	S+	O	N/R	Current	
3175	Aggregation of RSVP for IPv4 and IPv6 Reservations	O	O	O	O	O	N/R	Current	
3181	Signaled Preemption Priority Policy Object	O	O	O	O	O	N/R	Current	
2961	RSVP Refresh Overhead Reduction Extension	O	O	O	O	O	N/R	Current	

Table B-1. IPv6 Capable Device Requirements for Testing (continued)

RFC	RFC Title	Product Class						Effective Date	Comment
		Host	Network App or Simple Server	Advanced Server	Router	L3 Switch	IA Device		
4495	A Resource Reservation Protocol (RSVP) Extension for the Reduction of Bandwidth of a Reservation Flow	O	O	O	O	O	N/R	Current	
2998	A Framework for Integrated Services Operation over DiffServ Networks	O	O	O	O	O	N/R	Current	
2996	Format of the RSVP DCLASS Object	O	O	O	O	O	N/R	Current	
2746	RSVP Operation Over IP Tunnels	O	O	O	O	O	N/R	Current	
3182	Identity Representation for RSVP	O	O	O	O	O	N/R	Current	
2872	Application and Sub Application Identity Policy Element for Use with RSVP	O	O	O	O	O	N/R	Current	
2747	RSVP Cryptographic Authentication	O	O	O	O	O	N/R	Current	
Mobility									
3775	Mobility Support in IPv6	CM	CS	CM (sect 9)	CM Note 8	N/R	N/R	Current	
3776	Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents	CM	CS	N/R	CM Note 8	N/R	N/R	Current	
4877	Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture	CM	CS	N/R	CM Note 8	N/R	N/R	7/2010	
4282	The Network Access Identifier	CS+	CS	N/R	CS+ Note 8	N/R	N/R	Current	
4283	Mobile Node Identifier for Option for IPv6	CS+	CS	N/R	CS+ Note 8	N/R	N/R	Current	
3963	Network Mobility (NEMO) Basic Support Protocol	N/R	N/R	N/R	CM	N/R	N/R	Current	
Bandwidth Limited Networks									
3095	Robust Header Compression (RoHC)	O	O	O	O	O	N/R	Current	
4815	Corrections and Clarification to RFC 3095	O	O	O	O	O	N/R	Current	
4995	RoHC Framework	O	O	O	O	O	N/R	Current	
4996	RoHC: A profile for TCP/IP	O	O	O	O	O	N/R	Current	
3241	RoHC over PPP	O	O	O	O	O	N/R	Current	
3843	RoHC: A Compression Profile for IP	O	O	O	O	O	N/R	Current	
4362	RoHC: A Link-Layer Assisted Profile for IP/UDP/RTP	O	O	O	O	O	N/R	Current	
2507	IP Header Compression	O	O	O	O	O	N/R	Current	
2508	Compressing IP/UDP/RTP Headers for Low-Speed Serial Links	O	O	O	O	O	N/R	Current	
3173	IP Payload Compression	O	O	O	O	O	N/R	Current	

Table B-1. IPv6 Capable Device Requirements for Testing (continued)

RFC	RFC Title	Product Class						Effective Date	Comment
		Host	Network App or Simple Server	Advanced Server	Router	L3 Switch	IA Device		
Network Management									
3411	An Architecture for Describing Simple Network Management Protocol Version 3 (SNMPv3)	N/R	N/R	N/R	M	CM Note 10	N/R	Current	Note 9
3412	Message Processing and Dispatching for the SNMP	N/R	N/R	N/R	M	CM Note 10	N/R	Current	Note 9
3413	SNMP Applications	N/R	N/R	N/R	M	CM Note 10	N/R	Current	Note 9
N/A	SNMP over IPv6	N/R	N/R	N/R	S+	S+	N/R	7/2010	
3595	Textual Conventions for IPv6 Flow Label	N/R	N/R	N/R	M	CM Note 10	N/R	Current	Note 9
4022	Management Information Base for the Transmission Control Protocol	N/R	N/R	N/R	M	CM Note 10	N/R	Current	Note 9
4113	Management Information Base for the User Datagram Protocol	N/R	N/R	N/R	M	CM Note 10	N/R	Current	Note 9
4087	IP Tunnel MIB	N/R	N/R	N/R	S	S Note 10	N/R	Current	Note 9
4293	Management Information Base (MIB) for IP	N/R	N/R	N/R	M	CM Note 10	N/R	Current	Note 9
4295	Mobile IP Management MIB	N/R	N/R	N/R	CM	CM Note 10	N/R	Current	Note 9
4807	IPsec Security Policy Database Configuration	N/R	N/R	N/R	CM	CM Note 10	N/R	Current	Note 9
4292	IP Forwarding Table MIB	N/R	N/R	N/R	M	CM Note 10	N/R	Current	Note 9
4601	Protocol Independent Multicast – Sparse Mode (PIM-SM)	N/R	N/R	N/R	CS+	N/R	N/R	Current	
3973	Protocol Independent Multicast – Dense Mode	N/R	N/R	N/R	CS+	N/R	N/R	Current	
Routing									
2740	OSPF for IPv6 (OSPFv3)	N/R	N/R	N/R	CM Note 11	CM Note 9	N/R	Current	
4552	Authentication/Confidentiality for OSPFv3	N/R	N/R	N/R	CM Note 11	CM Note 9	N/R	Current	
4271	A Border Gate Protocol (BGP-4)	N/R	N/R	N/R	CM Note 12	CM Note 7	N/R	Current	
1772	Application of the Border Gateway Protocol in the Internet	N/R	N/R	N/R	CM Note 12	CM Note 7	N/R	Current	
2545	Use of BGP-4 Multi-Protocol Extensions for IPv6 Inter-Domain Routing	N/R	N/R	N/R	CM Note 12	CM Note 7	N/R	Current	

Table B-1. IPv6 Capable Device Requirements for Testing (continued)

RFC	RFC Title	Product Class						Effective Date	Comment
		Host	Network App or Simple Server	Advanced Server	Router	L3 Switch	IA Device		
2858 4760	Multi-Protocol Extensions for BGP-4	N/R	N/R	N/R	CM Note 12	CM Note 7	N/R	Current 7/2009	
Automatic Configuration									
2462 4862 3315	IPv6 Stateless Address Auto configuration (SLAAC) DHCPv6 [client]	M Note 1	M Note 1	N/R	M Note 13	N/R	N/R	Current 7/2009 Current	
3315	DHCPv6 [server] DHCPv6 [Relay Agent]	N/R	CM N/R	CM N/R	CM	N/R CM	N/R	7/2009	
3769	IPv6 Prefix Delegation	N/R	CM	CM	CM	N/R	N/R	7/2009	
3633	IPv6 Prefix Options for DHCPv6	N/R	CM	CM	CM	N/R	N/R	7/2009	
N/A	[disable autoconfiguration]	M	M	M	M	M	M	Current	
5175	Extensions to Router Advertisement Flags	CS+	CS+	CS+	CS+	CS+	CS+	7/2009	
Server									
959	File Transfer Protocol	N/R	O	O	N/R	N/R	N/R	Current	
2428	FTP Extensions for IPv6 and NAT	N/R	O	O	N/R	N/R	N/R	Current	
2821	Simple Mail Transfer Protocol (SMTP)	N/R	O	O	N/R	N/R	N/R	Current	
2911	Internet Printing Protocol	N/R	O	O	N/R	N/R	N/R	Current	
3162	RADIUS (Remote Authentication Dial-In User Service) and IPv6	N/R	O	O	N/R	N/R	CM	Current	
4330	Simple Network Time Protocol (SNTP)	N/R	O	O	N/R	N/R	N/R	Current	
3226	DNS Security and IPv6 A6 Aware Server/Resolver Message Size Requirements	N/R	O	O	N/R	N/R	N/R	Current	
3261	Session Initiation Protocol (SIP)	N/R	O	O	N/R	N/R	N/R	Current	
3596	DNS Extensions to Support IPv6	N/R	O	O	N/R	N/R	N/R	Current	
3053	IPv6 Tunnel Broker	N/R	O	O	N/R	N/R	N/R	Current	
Host									
3484 [Sec 2.1]	Default Address Selection for IPv6 [Policy Table]	S+	S	S+	N/R	N/R	N/R	Current	
3484 [rest of RFC]	Default Address Selection for IPv6	M	S	M	N/R	N/R	N/R	Current	
3596 resolver	DNS Extensions to Support IPv6	M	S	M	N/R	N/R	N/R	Current	

Table B-1. IPv6 Capable Device Requirements for Testing (continued)

RFC	RFC Title	Product Class						Effective Date	Comment
		Host	Network App or Simple Server	Advanced Server	Router	L3 Switch	IA Device		
3986	Uniform Resource Identifier (URI): Generic Syntax	M	S	M	N/R	N/R	N/R	Current	
Router									
2784	Generic Router Encapsulation (GRE)	N/R	N/R	N/R	CM	N/R	N/R	Current	
2473	Generic Packet Tunneling in IPv6	N/R	N/R	N/R	CM Note 11	N/R	N/R	Current	
L3 Switch									
4541	Considerations for IGMP and MLD Snooping Switches	N/R	N/R	N/R	N/R	CS	N/R	Current	
IA Device									
3585	IPsec Configuration Policy Information Model	N/R	N/R	N/R	N/R	N/R	CS+	Current	
3586	IP Security Policy Requirements	N/R	N/R	N/R	N/R	N/R	CS+	Current	

NOTES:

1. The device must implement one of the automatic configuration mechanisms SLAAC or DHCPv6. However, all nodes MUST perform duplicate address detection and automatically generated link-local address regardless of automatic address configuration method.
2. All Layer-3 Switches implementing MLDv2 MUST perform the modes of “router” and “listener,” as annotated in RFC 3810.
3. The device must be conformant to at least one of the Connection Technologies protocols.
4. IPSec Fallback requirements only apply to a product that MUST support IPSec that does not currently support IPSec RFC 4301.
5. Products with IKEv2 implementation MAY also include a fall-back to IKEv1; products without IKEv2 MUST at least meet the IKEv1 requirements.
6. MUST implement Dual Stack or Tunneling to meet the requirement to carry both IPv4 and IPv6 traffic.
7. The device must be conformant if it functions as an External System Node.
8. The device must be conformant if it functions as a Home Agent.
9. The device must be conformant if it functions as an Interior System Node.
10. The device must be conformant if it functions as a Managed Switch.
11. The device must be conformant if it functions as an Interior Router.
12. The device must be conformant if it functions as an External Router.
13. MUST support Router requirements for SLAAC.

LEGEND:

A6	IPv6 Address Record	MAPOS	Multiple Access Protocol Over SONET/SDH
App	Appliance	MIB	Management Information Base
ARCnet	Attached Resource Computer Network	MLD	Multicast Listener Discovery
ARP	Address Resolution Protocol	MLDv2	MLD Version 2
ATM	Asynchronous Transfer Mode	MPLS	Multi-protocol Label Switching
BGP-4	Border Gateway Protocol Version 4	MTU	Maximum Transmission Unit
CM	Conditional Must	N/A	Not Applicable
CS	Conditional Should	N/R	No Requirement
CS+	Conditional Should Plus	NAT	Network Address Translation
DHCP	Dynamic Host Configuration Protocol	NBMA	Non-Broadcast Multi-Access Network
DHCPv6	DHCP Version 6	O	Optional
DiffServ	Differentiated Services	OSPF	Opened Shortest Path First
DNS	Domain Name Service	OSPFv3	OSPF Version 3
DoD	Department of Defense	PPP	Point-to-Point Protocol

Table B-1. IPv6 Capable Device Requirements for Testing (continued)

FDDI	Fiberoptic Digital Data Interface	RADIUS	Remote Authentication Dial-In User Service
FTP	File Transfer Protocol	RFC	Request for Comment
IA	Information Assurance	RoHC	Robust Header Compression
IEEE	Institute of Electrical and Electronic Engineers, Inc.	RSVP	Resource ReSerVation Protocol
IETF	Internet Engineering Task Force	RTP	Real-Time Transport Protocol
IGMP	Internet Group Multicast Protocol	S	Should
IKE	Internet Key Exchange	S+	Should Plus
IKEv1	IKE Version 1	SDH	Synchronous Digital Hierarchy
IKEv2	IKE Version 2	Sect	Section
IP	Internet Protocol	SLAAC	Stateless Address Auto-configuration
IPSec	Internet Protocol Security	SN	Should Not
IPv4	Internet Protocol Version 4	SNMP	Simple Network Management Protocol
IPv6	Internet Protocol Version 6	SONET	Synchronous Optical Network
ISAKMP	Internet Security Association and Key Management Protocol	TCP	Transmission Control Protocol
LAN	Local Area Network	UDP	User Datagram Protocol
L3	Layer-3	V	Version
M	Must	VPN-B	Virtual Private Network Suite B
MAC	Media Access Control	WS	Workstation

(This page intentionally left blank.)

APPENDIX C

CONFORMANCE AND INTEROPERABILITY TESTING

Conformance: compares a device's attributes to Request for Comments (RFCs).

The criteria and procedures for conformance testing are identical. The only difference is the RFC that is to be tested. The following are criteria and procedures for conformance testing:

Criteria: The device will conform to all MUST requirements found in the RFC.

Test Procedure: The tester will configure the network as shown in Figure E-1 and complete the following:

- Verify configuration of the Traffic Generator/Analyzer (TGA) and the software test suite
- Verify configuration of the device and the Tool Command Language script (if required by test suite)
- Document the configurations of all variable items in the test set
- Initiate the test suite
- Interact with the test suite and device, as necessary, for successful testing
- Complete the test suite
- Reference the RFC and examine results for variances from expected conformance
- Document the results

Interoperability: determines a device's ability to work/communicate with other products in a heterogeneous environment.

The Joint Interoperability Test Command (JITC) will configure interoperability testing using the network depicted in Figure E-8.

A MUST requirement will be defined by the terms MUST, REQUIRED, or SHALL. The definition is an absolute requirement of the specification. The following test cases are MUST requirements for all Internet Protocol (IP) Version 6 (IPv6) capable devices.

Annex 1, IPv6 Base Requirements

C.1.1	RFC 1981:	Path Maximum Transmission Unit Discovery for IPv6
C.1.2	RFC 2460:	IPv6 Specification
C.1.3	RFC 2461/4861:	Neighbor Discovery for IPv6
C.1.4	RFC 2462/4862:	IPv6 Stateless Address Auto-configuration
C.1.5	RFC 2464:	Transmission of IPv6 Packets over Ethernet Networks

C.1.6	RFC 2467:	Transmission of IPv6 Packets over Fiber Optic Digital Data Interface Networks
C.1.7	RFC 2472/5072:	IPv6 over Point-to-Point Protocol
C.1.8	RFC 2710:	Multicast Listener Discovery (MLD) for IPv6
C.1.9	RFC 3572:	IPv6 over Multiple Access Protocol over Synchronous Optical Network/Synchronous Digital Hierarchy (MAPOS)
C.1.10	RFC 3810:	MLD Version 2 (MLDv2) for IPv6
C.1.11	RFC 4007:	IPv6 Scoped Address Architecture
C.1.12	RFC 4193:	Unique Local IPv6 Unicast Addresses
C.1.13	RFC 4291:	IPv6 Addressing Architecture
C.1.14	RFC 4443:	Internet Control Message Protocol for the IPv6 Specification

Annex 2, IP Security (IPSec) Profile Requirements

C.2.1	RFC 4301:	Security Architecture for the IP
C.2.2	RFC 4302:	IP Authentication Header (AH)
C.2.3	RFC 4303:	IP Encapsulating Security Payload (ESP)
C.2.4	RFC 4305:	Cryptographic Algorithm Implementation Requirements for ESP and AH
C.2.5	RFC 4306:	The Internet Key Exchange (IKE) Version 2 (IKEv2)
C.2.6	RFC 4307:	Cryptographic Algorithms for Use in the IKEv2
C.2.7	RFC 4308:	Cryptographic Suites for IPSec
C.2.8	RFC 4308	Suite B Cryptographic Suites for IPSec
C.2.9		IPSec Encryption Algorithms

Annex 3, Other Required RFCs

C.3.1	RFC 1772:	Application of the Border Gateway Protocol (BGP) in the Internet
C.3.2	RFC 2473:	Generic Packet Tunneling in IPv6 Specification
C.3.3	RFC 2474:	Definition of the DiffServ Field in the IP Version 4 (IPv4) and IPv6 Headers
C.3.4	RFC 2545:	Use of BGP Version 4 (BGP-4) Multi-protocol Extensions for IPv6 Inter-Domain Routing
C.3.5	RFC 2740:	Open Shortest Path First for IPv6 (OSPFv3)
C.3.6	RFC 2784:	Generic Routing Encapsulation
C.3.7	RFC 3041/4941:	Privacy Extensions for Stateless Address Auto configuration in IPv6
C.3.8	RFC 3315:	Dynamic Host Configuration Protocol for IPv6
C.3.9	RFC 3411:	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
C.3.10	RFC 3412:	Message Processing and Dispatching for the SNMP
C.3.11	RFC 3413:	SNMP Applications
C.3.12	RFC 3484:	Default Address Selection for IPv6
C.3.13	RFC 3596:	Domain Name Service Extensions to Support IPv6
C.3.14	RFC 3775:	Mobility Support in IPv6

C.3.15	RFC 3776:	Using IPSec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents
C.3.16	RFC 3963:	Network Mobility Basic Support Protocol
C.3.17	RFC 3986:	Uniform Resource Identifier: Generic Syntax
C.3.18	RFC 4213:	Transition Mechanisms for IPv6 Host and Routers
C.3.19	RFC 4271:	A BGP-4
C.3.20	RFC 4760/2858:	Multi-protocol Extensions for BGP-4
C.3.21	MIB RFCs:	Network Management: Management Information Base (MIB)

Annex 4, Optional Connection Technologies

C.4.1	RFC 2491:	IPv6 Over Non-Broadcast Multiple Access Networks
C.4.2	RFC 2492:	IPv6 over Asynchronous Transfer Mode Networks January 1999
C.4.3	RFC 2497:	Transmission of IPv6 Packets over ARCnet Networks
C.4.4	RFC 2590:	Transmission of IPv6 Packets over Frame Relay Networks Specification
C.4.5	RFC 3146:	Transmission of IPv6 over Institute of Electrical and Electronic Engineers 1394 Networks
C.4.6	RFC 4338:	Transmission of IPv6, IPv4, and Address Resolution Protocol Packets over Fiber Channel
C.4.7	RFC 4302:	IP Authentication Header (AH)

Annex 5, National Security Agency (NSA) IPv6 Information Assurance (IA) Test Plan (IATP) Procedures

C.5.1 NSA IPv6 IATP, Annex 1, Firewalls
C.5.2 NSA IPv6 IATP, Annex 3, Intrusion Protection/Detection Systems

(This page intentionally left blank.)

APPENDIX C, ANNEX 1

INTERNET PROTOCOL VERSION 6 BASE REQUIREMENTS

C.1.1

Request for Comments (RFC) 1981: Path Maximum Transmission Unit (PMTU) Discovery for Internet Protocol (IP) Version 6 (IPv6)

References: RFC 1981

Resource Requirements:

Hardware: Traffic Generator/Analyzer (TGA)
Software: Ixia IxANVL Test Suite IPv6 Advanced, Spirent AX4000 Conformance Test Suite #404677, Agilent N2X Test Suite #N5701A-001, or equivalent

Conformance Test

Purpose: To determine if the device under test (DUT) conforms to RFC 1981.

Background: The PMTU Discovery for IPv6 is necessary for proper IPv6 implementations. A source node initially assumes that the PMTU of a path is the (known) Maximum Transmission Unit (MTU) of the first hop in the path. If any of the packets sent on that path are too large to be forwarded by some node along the path, that node will discard them and return Internet Control Message Protocol (ICMP) Version 6 (ICMPv6) Type 2 Packet Too Big messages. Upon receipt of such a message, the source node reduces its assumed PMTU for the path based on the MTU of the constricting hop as reported in the Packet Too Big message. See page C-1 for criteria and procedures.

Interoperability Test

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Purpose: To determine if the DUT can successfully participate in PMTU discovery in a heterogeneous environment.

Criteria: If the DUT is a:

- Router or Layer-3 Switch - upon receipt of a packet larger than the MTU setting placed on the physical interface, will issue a “Packet Too Big” message. If packets continue to be received larger than the MTU state, the router will then drop the traffic.
- Host - upon receipt of a “Packet Too Big” message from its local router, the Host will fragment its packets and continue to transmit packets to the local router. Periodically, the Host will re-size its packets until an optimal condition is met.
- When a “Packet Too Big” message is received, it is implied that a packet was dropped by the node that sent the ICMP message. This necessitates that the originating node retransmit the dropped packets.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Set the PMTU of the border routers on both sides of the network to 1280.
- Decide on a source and destination side of the test network.
- Transmit a datagram of 1518 Kilobits from the source Host or TGA across the network to the destination Host/TGA.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Observe the packet captures taken before the source-side border router and after the source-side border router to determine if the source-side border router is issuing a "packet to large" message and the source-side Host is reducing its packet size accordingly.
- Record the results and archive all packet captures and screen shots.

Expected Results: A “Packet Too Big” message should be issued by the source-side router, and as a result, the source-side Host will reduce its packet size below the router’s MTU setting. The Host will then increase its packet size until an optimal setting has been reached in accordance with the source-side router.

C.1.2

RFC 2460: IPv6 Specification

References: RFC 2460 (Dependent on RFCs 1981, 4301, and 4443)

Resource Requirements:

Hardware: TGA
Software: Ixia IxANVL Test Suite IPv6 Core, Spirent AX4000 Conformance Test Suite #404677, Agilent N2X Test Suite #N5701A-001, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 2460.

Background: The RFC 2460 is the base specification of the IPv6 protocol. It specifies a number of parameters that enable successful completion of IPv6 traffic addressing and control. See page C-1 for criteria and procedures.

Interoperability Test

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Purpose: To determine if the DUT sends properly formatted IPv6 packets.

Criteria: The DUT will be able to properly form and send IPv6 packets.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Initiate ICMPv6 Echo Requests from the DUT to the global address of Host 2.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Observe Host 2 with a traffic analyzer to determine if the request is received and a return Echo Reply datagram is sent.
- Observe the DUT with a traffic analyzer to determine if the Echo Reply sent by Host 2 is received and processed.
- Record the results and archive all packet captures and screen shots.

- Evaluate the packet to determine that it includes the following **IPv6 General Packet Headers**, in the correct order:
  - Version = 6
  - Traffic Class
  - Flow Label
  - Payload Length
  - Next Header
  - Hop Limit
  - Source Address
  - Destination Address
- A full implementation of IPv6 includes implementation of the following Extension Headers:
  - Hop-by-Hop Header
  - Routing (Type 0)
  - Fragment
  - Destination Options
  - Authentication
  - Encapsulating Security Payload
- There are 9 possible IPv6 Extension Headers. When using more than one, it is recommended that they appear in the following order:
  - IPv6 Headers
  - Hop-by-Hop Header
  - Destination Options Header
  - Routing Header
  - Fragment Header
  - Authentication Header (if implementing IP Security (IPSec))
  - Encapsulating Security Payload Header (if implementing IPSec)
  - Destination Options Header
  - Upper-layer Header
- Evaluate the packet to determine that it includes the above Extension Headers, in the correct order.

Expected Results: A successful test result is one of the correctly formed IPv6 packets in the following:

- Eight items in the IPv6 General Header.
- Nine possible items in the Extension Header.

Special Note in regards to what type of a device should initiate the response of a – "Message to Big" message.

Note: It is possible, though unusual, for a device with multiple interfaces to be configured to forward non-self-destined packets arriving from some set (fewer than all) of its interfaces and to discard non-self-destined packets arriving from its other interfaces. Such a device must obey the protocol requirements for routers when receiving packets from, and interacting with neighbors over, the former (forwarding)

interfaces. It must obey the protocol requirements for hosts when receiving packets from, and interacting with neighbors over, the latter (non-forwarding) interfaces.

If an intermediate node processes a Routing header of a received packet and determines the packet is to be forwarded onto a link whose link MTU is less than the size of the packet, the node must discard the packet and send an ICMP Packet Too Big message to the packet's Source Address.

C.1.3

RFC 2461/4861: Neighbor Discovery for IPv6

References: RFC 2461/4861

Resource Requirements:

Hardware: TGA
Software: Ixia IxANVL Test Suite IPv6 Advanced, Spirent AX4000 Conformance Test Suite #404677, Agilent N2X Test Suite #N5701A-001, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 2461/4861.

Background: The RFC 2461/4861 specifies the neighbor discovery function that emulates address resolution protocol in IPv4. It is necessary for implementing neighbor solicitations and neighbor advertisements within IPv6. The IPv6 nodes on the same link use Neighbor Discovery to discover each other's presence, to determine each other's link-layer addresses, to find routers, and to maintain reachability information about the paths to active neighbors. See page C-1 for criteria and procedures.

Interoperability Test 1

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Purpose: To determine if the DUT properly sends ICMPv6 Type 1 (Destination Unreachable) messages when destinations addresses are unavailable.

Background: There are a number of different reasons why a destination may be unreachable. When a datagram cannot be delivered, recovery from this condition normally falls to higher-layer protocols like Transmission Control Protocol (TCP), which will detect the miscommunication and re-send the lost datagram's. In some situations, such as a datagram dropped due to router congestion, this is sufficient. However, in other cases, a datagram may not be delivered due to an inherent problem with how it is being sent. For example, the source may have specified an invalid destination address, which means even if resent many times, the datagram will never get to its intended recipient.

Criteria: The DUT will receive a Destination Unreachable ICMP message for each packet that fails to reach the intended target specified in the destination address of the IPv6 header.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Transmit a datagram from either a Host or TGA to a destination address of a non-existent address found on Subnet 2.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark) to determine if the packet is forwarded or discarded.
- Observe the device with the TGA or the network taps to determine if it returns an ICMPv6 Type 1, Destination Unreachable message, to the source address of the discarded datagram.
- Record the results and archive all packet captures and screen shots.

Expected Results: The source address should receive a Destination Unreachable message for all discarded packets.

Many of these ICMP types have a "code" field. The following lists the types with their assigned code fields.

Type	Name	Reference
1	Destination Unreachable	[RFC 4443]
	Code:	
	0 - no route to destination	
	1 - communication with destination administratively prohibited	
	2 - beyond scope of source address	[RFC 4443]
	3 - address unreachable	
	4 - port unreachable	
	5 - source address failed ingress/egress policy	[RFC 4443]
	6 - reject route to destination	[RFC 4443]

Interoperability Test 2

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IP Packet Analyzer

Purpose: To determine if a Host can detect that its neighbor is no longer reachable, so that it may fail-over and elect another default router.

Background:

Communication to or through a neighbor may fail for numerous reasons at any time, including hardware failure, or a hot-swap of an interface card. If the destination has failed, no recovery is possible and communication fails. However, if it is a node in the path that has failed, recovery may be possible.

A node actively tracks the reachability state for the neighbors to which it is sending packets. Neighbor Unreachability Detection is used for all paths between hosts and neighboring nodes, including Host-to-Host, Host-to-router, and router-to-Host communication. Neighbor Unreachability Detection may also be used between routers, but it is not required if an equivalent mechanism is available, for example, as part of the routing protocols.

When a path to a neighbor appears to be failing, the specific recovery procedure depends on how the neighbor is being used. If the neighbor is the ultimate destination, address resolution should be performed again. If the neighbor is a router, attempting to switch to another router would be appropriate.

Criteria: The DUT will perform a Neighbor Unreachability Detection and determine if its current default connection is functioning properly. If the determination is made that the neighbor is unreachable, the DUT will switch to a new gateway to continue communication.

Test Procedure: The tester will configure the network as shown in Figure E-2 and complete the following:

- Transmit a continuous ICMPv6 Ping from Client/Host 1 to the global address of Server 1.
- Disconnect the cable connection between Host 1 and the router (default gateway) that Host 1 uses as a first hop in step 1.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark) to observe the results of the disconnection.
- Record the results and archive all packet captures and screen shots.
- Allow time for Host 1 to determine that its first hop in step 2 is unreachable.
- Continue to monitor the packet exchange to observe whether a new default gateway is utilized.
- Continue to monitor the packet exchange to observe the results of the reconnection.
- Record the results and archive all packet captures and screen shots.

Expected Results: Host 1 should perform Neighbor Unreachability Detection and determine that its first hop is no longer available. It should then switch over to its new gateway, possibly receiving a new IPv6 address in the process.

C.1.4

RFC 2462/4862: IPv6 Stateless Address Auto-configuration

References: RFC 2462

Resource Requirements:

Hardware: TGA
Software: Ixia IxANVL Test Suite IPv6 Advanced, Spirent AX4000 Conformance Test Suite #404677, Agilent N2X Test Suite #N5701A-002, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 4862/2462.

Background: The RFC 4862/2462 specifies how a Host auto-configures its interfaces in IPv6. These steps include determining whether the source of addressing should be stateless or stateful, whether the information obtained should be solely the address or include other information, and Duplicate Address Detection (DAD). IPv6 Stateless Address Auto-configuration allows a Host to connect to a network segment, auto-configure an IPv6 address, and start communicating with other nodes without having registered or authenticating itself with the local site. One stage of this process is DAD. This is the means by which a newly arrived Host to the subnet does not infringe upon other already established and communicating hosts. See page C-1 for criteria and procedures.

Interoperability Test 1: Basic Stateless Address Auto-configuration Function

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Purpose: To determine if the device can successfully participate in address auto-configuration and communicate with different vendor equipment.

Background: The IPv6 Stateless Address Auto-configuration allows a Host to connect to a network segment, auto-configure an IPv6 address, and start communicating with other nodes without having registered or authenticating itself with the local site. One stage of this process is DAD. This is the means by which a newly arrived Host to the subnet does not infringe upon other already established and communicating hosts.

Criteria: The DUT will generate an IPv6 unicast address using the prefix of the DUT's default gateway and the Extended Unique Identifier-64 address of the DUT.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark) to observe the network traffic found on a link-local network.
- Connect Client/Host 1 to the network and observe the neighbor discovery communication process that goes on between Host 1 and all the other nodes on the network.
- Record the results and archive all packet captures and screen shots.

Expected Results: Client/Host 1 should connect to the network and send out a router solicitation for a router subnet prefix. Upon receiving the prefix, Host 1 should determine its first candidate address and send it via neighbor discovery to the link-local network. If no other nodes on the network possess the proffered address, then Host 1 should assign it to its main network interface.

Interoperability Test 2: Test of Duplicate Address Detection

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Purpose: To determine if the device can successfully participate in DAD and communicate with different vendor equipment.

Background: The IPv6 Stateless Address Auto-configuration allows a Host to connect to a network segment, auto-configure an IPv6 address, and start communicating with other nodes without having registered or authenticating itself with the local site. One stage of this process is DAD. This is the means by which a newly arrived Host to the subnet does not infringe upon other already established and communicating hosts.

Criteria: The DUT will correctly configure (or not configure an address) based on a duplicate address being on the network.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark) to observe the network traffic found on a link-local network.
- Connect Client/Host 1, as the DUT, to the network and observe the neighbor discovery communication process that goes on between Host 1 and all the other nodes on the network.

- Connect Client/Host 2 to the same network segment. Manually configure the same EUI-64 address of Client/Host 1 on the network interface.
- Restart the network interface of Client/Host 1.
- Record the results and archive all packet captures and screen shots.

Expected Results: Upon restarting Client/Host 1's network interface, it should connect to the network and send out a router solicitation for a router subnet prefix. Upon receiving the prefix, Host 1 should determine its first candidate address and send it via neighbor discovery to the link-local network. Client 1 should detect that Client 2 has it's auto configured address. One of the two following expected results will be acceptable:

- Client 1 will not configure an address until Client 2 releases the address.
- Client 1 will reconfigure its address with a new EUI-64 automatically configured address.

Interoperability Test 3: Disable Auto-configuration

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Purpose: To determine if the device can successfully disable auto-configuration. The DAD and link-local automatic generation should still be active.

Background: The IPv6 Stateless Address Auto-configuration allows a Host to connect to a network segment, auto-configure an IPv6 address, and start communicating with other nodes without having registered or authenticating itself with the local site. One stage of this process is DAD. This is the means by which a newly arrived Host to the subnet does not infringe upon other already established and communicating hosts.

Criteria: Stateless address auto-configuration will be disabled on the DUT correctly.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark) to observe the network traffic found on a link-local network.
- Connect Client/Host 1, as the DUT, to the network and observe the neighbor discovery communication process that goes on between Host 1 and all the other nodes on the network.
- Disable address auto-configuration.
- Restart the network interface.
- Record the results and archive all packet captures and screen shots.

Expected Results: Upon restarting Client/Host 1's network interface, it should continue to automatically participate in DAD as well as automatically generating link-local addresses.

C.1.5

RFC 2464: Transmission of IPv6 Packets over Ethernet Networks

References: RFC 2464

Resource Requirements:

Hardware: TGA
Software: Ixia IxANVL Test Suite IPv6 Core, Spirent AX4000 Conformance Test Suite #404687, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 2464.

Background: When messages are transmitted on an Ethernet network, the frame format for transmission of IPv6 packets and the method of forming IPv6 link-local addresses and statelessly auto-configured addresses are in use. This includes specific content of the Source/Target Link-Layer Address option used in Router Solicitation, Router Advertisement, Neighbor Solicitation, Neighbor Advertisement, and Redirect messages. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT can send properly formatted IPv6 packets over a Layer-2 Ethernet (EthernetV2) protocol link.

References: RFC 2464

Resource Requirements:

Hardware: TGA

Background: All address types, (link-local, unicast, multicast) should be able to be sent over an Ethernet network from one Host to at least one other Host.

Criteria: The DUT will send properly formatted IPv6 packets over a Layer-2 Ethernet topology network to a remote Host. The remote Host must be able to receive and process these packets for the test to be a success.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Ensure the network topology is an Ethernet network utilizing either a version of the Institute of Electrical and Electronic Engineers, Inc. (IEEE) 802.3 or native EthernetV2. This is determined by capturing some packets with Wireshark and examining them to check for the Layer-2 protocol.
- Configure a unique IPv6 unicast address on the DUT and the remote Host.
- Launch Wireshark.
- Send traffic across the Ethernet segment from the DUT to the remote Host.
- Capture traffic to show that IPv6 traffic is running across the Layer-2 Ethernet protocol.
- Record the results and archive all packet captures and screen shots.

Expected Results: The devices should be able to communicate with the remote Host using IPv6 formatted packets running across an Ethernet segment.

C.1.6

RFC 2467: Transmission of IPv6 Packets over Fiber Optic Digital Data Interface (FDDI) Networks

References: RFC 2467

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 2467.

Background: This RFC specifies the frame format for transmission of IPv6 packets and the method of forming IPv6 link-local addresses and statelessly auto-configured addresses on FDDI networks. It also specifies the content of the Source/Target Link-Layer Address option used in Router Solicitation, Router Advertisement, Neighbor Solicitation, Neighbor Advertisement and Redirect messages when those messages are transmitted on an FDDI network. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT can send properly formatted IPv6 packets over a Layer-2 FDDI protocol link.

References: RFC 2467

Resource Requirements:

Hardware: TGA

Background: All address types, (i.e., link-local, unicast, multicast) should be able to be sent over a FDDI network from one Host to another Host.

Criteria: The DUT will send properly formatted IPv6 packets over a Layer-2 FDDI topology network to a remote Host. The remote Host must be able to receive and process these packets for the test to be a success.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Ensure the network topology is a FDDI network. This can be determined by capturing some packets with Wireshark and examining them to check the Layer-2 protocol.
- Configure a unique IPv6 unicast address on the DUT and the remote Host.
- Launch Wireshark.
- Send traffic across the FDDI segment from the DUT to the remote Host.
- Capture traffic to show that IPv6 traffic is running across the Layer-2 FDDI protocol.
- Record the results and archive all packet captures and screen shots.

Expected Results: The devices should be able to communicate with the remote Host using IPv6 formatted packets running across a FDDI segment.

C.1.7

RFC 2472/5072: IPv6 over Point-to-Point Protocol (PPP)

References: RFC 2472 and 5072

Resource Requirements:

Hardware: TGA, three routers with serial port connections, and two workstations
Software: Ixia IxANVL Test Suite #IPv6 Core or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 2472.

Background:

Configuring, enabling, and disabling the IPv6 protocol modules on both ends of the point-to-point link is the responsibility of IPv6 Control Protocol (IPv6CP). The IPv6CP uses the same packet exchange mechanism as the Link Control Protocol (LCP). The IPv6CP packets may not be exchanged until PPP has reached the Network Layer Protocol (NLP) phase. The IPv6CP packets received before this phase is reached should be silently discarded. The IPv6CP is the same as the LCP with the following exceptions:

- Data Link Layer Protocol Field
- Code Field
- Timeouts
- Configuration Option Types.

To provide a method for transporting multi-protocol datagrams over point-to-point links, connections will be established, configured, and tested using TCP. The PPP routers will be able to pass datagrams through multiple asynchronous links or different multiplexed links. Dial-up asynchronous links or leased synchronous links are also commonly used with this protocol. Quality is provided by use of Link Quality Monitoring. The use of two defining procedures is the preferred method for test. The LCP packets must be sent by each end of the PPP to configure and establish a link. After the link is established, the PPP must send Network Control Protocols (NCP) packets to choose and configure NLP. The link will remain open until LCP or NCP terminates the session or there is a loss of power.

Before any IPv6 packets may be communicated, PPP must reach the NLP phase and the IPv6CP must reach the opened state.

The IPv6CP is responsible for configuring, enabling, and disabling the IPv6 protocol modules on both ends of the point-to-point link. The IPv6CP uses the same

packet exchange mechanism as the LCP. The IPv6CP packets may not be exchanged until PPP has reached the NLP phase. The IPv6CP packets received before this phase is reached should be silently discarded. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT is able to:

- Establish a data connection across a serial link.
- Establish a PPP connection with a proper extensible LCP.
- Establish NCP are able to establish and configure different NLP.

Reference: RFC 2472

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: The device will establish a PPP data connection across a serial link using extensible LCP options to various equipment types. For security, the data connection will successfully identify peer connections.

Test Procedure: Configure the routers as shown in Figure E-2. Each router should be configured to use PPP protocol on the serial links between routers.

Part A:

- Establish operational network using serial connections with PPP encapsulation between two routers under test.
- Two Personal Computers (PCs) will be placed on opposite sides of the network and a continuous Ping test will be performed between the PCs for a minimum of 5 minutes.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- The number and percent of failed Ping tests will be recorded.
- The link cable between routers will be disconnected and it will be verified that the line protocol on the circuit goes down.
- Record the results and archive all packet captures and screen shots.

Part B:

- One of the two routers in Part A will be replaced with an IPv6 certified router outside the manufacturer/family group of the router under test, and configured for a serial PPP connection.
- Two PCs will be placed on opposite sides of the network and a continuous Ping test will be performed between the PCs for a minimum of 5 minutes.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- The link cable between routers will be disconnected and it will be verified that the line protocol on the circuit goes down.
- Record the results and archive all packet captures and screen shots.

Part C:

- Change the encapsulation method on router A to an alternate encapsulation than the previous test.
- Verify that the link connection to the router changes to a protocol state of down and that all Ping tests across the network subsequently fail.

Expected Results:

In Parts A and B, the link between routers will establish and the Ping tests should show a 100 percent completion rate. When the cable is disconnected the router should detect the protocol as down and all packets should fail as undeliverable.

In Part C, the link between routers will not establish and Ping tests should show a 100 percent failure rate. The routers should show the protocol as down and traffic will not pass between the routers.

C.1.8

RFC 2710: Multicast Listener Discovery (MLD) for IPv6

References: RFC 2710

Resource Requirements:

Hardware: Router and PC
Software: Wireshark, Video Local Area Network (LAN) Client (VLC) Media Player 0.8.6.

Conformance Test

Purpose: To determine if the DUT conforms to RFC 2710.

Background: This RFC specifies the protocol used by an IPv6 router to discover the presence of multicast listeners (that is, 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 MLD is derived from the Internet Group Management Protocol (IGMP) Version 3. One important difference to note is that MLD uses ICMPv6 (IP Protocol 58) message types, rather than IGMP (IP Protocol 2) message types. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT properly sends MLD messages to all available multicast clients.

References: RFC 2710

Resource Requirements:

Hardware: TGA

Criteria: The DUT will be able to send and receive properly formatted MLD packets.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Enable Multicast routing on target routers.
- Configure Router A as the perimeter router (typically the closest router to the source).
- Complete the configuration of IPv6 multicast on each router.
- Enable IPv6 on the at least one Workstation per side of the network.

- Install IPv6 Capable Streaming Video Player, VLC Media Player 0.8.6 (This product is capable of serving IPv6 Multicast video) on a workstation on the “Video Source” Subnet.
- Install IPv6 Capable Streaming Video Player, VLC Media Player 0.8.6 on at least one workstation per subnet to receive Multicast traffic (this player is capable of performing server and client functions).
- Launch the VLC Streaming Video Player (when distributing Multicast traffic the software is functioning as a Server).
- Launch the VLC Streaming Video Player listening for the appropriate Multicast network traffic.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Launch Wireshark and observe the packet traffic to determine if MLD messages are sent between the router and PC.
- Record the results and archive all packet captures and screen shots.

Expected Results: The router should generate MLD Version 2 (MLDv2) queries, these queries will then be broadcast to all Multicast enabled nodes across the network. The Host should send back an MLDv2 response if listening for a Multicast group being advertised. The Host should start playing Multicast video provided the Multicast address of the server and client are the same.

C.1.9

RFC 3572: IPv6 over Multiple Access Protocol over Synchronous Optical NETwork (SONET)/Synchronous Digital Hierarchy (SDH) (MAPOS)

References: RFC 3572

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 3572.

Background: The MAPOS is a high-speed Link-Layer Protocol that provides multiple access capability over a SONET/SDH. This RFC specifies the frame format for encapsulating an IPv6 datagram in a MAPOS frame. It also specifies the method of forming IPv6 interface identifiers, the method of detecting duplicate addresses, and the format of the Source/Target Link-Layer Addresses option field used in IPv6 Neighbor Discovery messages. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT can send properly formatted IPv6 packets over a Layer-2 SONET protocol link.

References: RFC 3572

Resource Requirements:

Hardware: TGA

Criteria: The DUT will send properly formatted IPv6 packets over a Layer-2 SONET topology network to a remote Host. The remote Host must be able to receive and process these packets for the test to be a success.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).

- Ensure the network topology is a SONET network. This can be determined by capturing some packets with Wireshark and examining them to check the Layer-2 protocol.
- Configure a unique IPv6 unicast address on the DUT and the remote Host.
- Launch Wireshark.
- Send traffic across the SONET segment from the DUT to the remote Host.
- Capture traffic to show that IPv6 traffic is running across the Layer-2 SONET protocol.
- Record the results and archive all packet captures and screen shots.

Expected Results: The device should communicate with the remote Host using IPv6 formatted packets running across a SONET segment.

C.1.10

RFC 3810: MLDv2 for IPv6

References: RFC 3810

Resource Requirements:

Hardware: Two Routers, Two PCs (Source and Receiver)
Software: Wireshark, VLC Media Player 0.8.6.

Conformance Test

Purpose: Purpose: To determine if the DUT conforms to RFC 3810

Background:

The MLD 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 of interest to those neighboring nodes.

The differences between MLD Version 1 (MLDv1) and MLDv2 are most suitably tested at the RFC Conformance level. From an interoperability standpoint, the MLDv2 protocol, when compared to MLDv1, adds support for "source filtering," i.e., the ability for a node to report interest in listening to packets *only* from specific source addresses (as required to support Source-Specific Multicast (RFC 3569)), or from *all but* specific source addresses, sent to a particular multicast address. The MLDv2 is designed to be interoperable with MLDv1. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT properly sends MLDv2 messages to all available multicast clients.

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer, VLC Media Player 0.8.6.

Criteria: The DUT will be able to send and receive properly formatted MLDv2 packets.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Enable Multicast routing on target routers.

- Configure Router A as the perimeter router (typically the closest router to the source).
- Complete the configuration of IPv6 multicast on each router.
- Enable IPv6 on the at least one Workstation per side of the network.
- Install IPv6 Capable Streaming Video Player, VLC Media Player 0.8.6 (This product is capable of serving IPv6 Multicast video) on a workstation on the "Video Source" Subnet.
- Install IPv6 Capable Streaming Video Player, VLC Media Player 0.8.6 on at least one workstation per subnet to receive Multicast traffic. This player is capable of performing server and client functions.
- Launch the VLC Streaming Video Player (when distributing Multicast traffic it is functioning as a Server).
- Launch the VLC Streaming Video Player listening for the appropriate Multicast network traffic.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Launch Wireshark and observe the packet traffic to determine if MLDv2 messages are sent between the router and PC.
- Record the results and archive all packet captures and screen shots.

Expected Results: The router should generate MLDv2 queries, these queries will then be broadcast to all Multicast enabled nodes across the network. The Host should send back an MLDv2 response if listening for a Multicast group being advertised. The Host should start playing Multicast video provided the Multicast address of the server and client are the same.

C.1.11

RFC 4007: IPv6 Scoped Address Architecture

References: RFC 4007

Resource Requirements:

Hardware: TGA
Software: Ixia IxANVL Test Suite IPv6 Advanced, Spirent AX4000 Conformance Test Suite #404677, Agilent N2X Test Suite #N5701A-002, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 4007.

Background: The IPv6 includes support for addresses of different scope; that is, both global and non-global (e.g., link-local) addresses. Although non-global addressing has been introduced operationally in the IPv4 Internet, both in the use of private address space and with administratively scoped multicast addresses, the design of IPv6 formally incorporates the notion of address scope into its base architecture. This RFC specifies the architectural characteristics, expected behavior, textual representation, and usage of IPv6 addresses of different scopes. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT forwards traffic to the appropriate scope and not outside to another.

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: The DUT will limit the transmission of IPv6 packets to the same scope as the type of source address. For example, packets generated by a link-local address will stay on the local subnet. Packets generated by a multicast address will go to those hosts subscribing to that multicast group only.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Configure the DUT for general IPv6 functionality.
- Ensure device can create a link-local address.
- Configure a Multicast address.

- Generate traffic destined for the above addresses.
- Record the results.

Expected Results: The packets should only be sent to recipients in the correct scopes. In the case of a link-local address, only other neighbors on the same link should receive the traffic. For a multicast packet, only subscribers to that multicast group which corresponds to the multicast link should receive the traffic.

C.1.12

RFC 4193: Unique Local IPv6 Unicast Addresses

References: RFC 4193

Resource Requirements:

Hardware: TGA
Software: Ixia IxANVL Test Suite IPv6 Advanced, Spirent AX4000 Conformance Test Suite #404677, Agilent N2X Test Suite #N5701A-002, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 4193.

Background:

This RFC defines an IPv6 unicast address format that is globally unique and is intended for local communications. These addresses are called Unique Local IPv6 Unicast Addresses. They are not expected to be routable on the global Internet. They are routable inside of a more limited area such as a site. They may also be routed between a limited set of sites. Local IPv6 unicast addresses have the following characteristics:

- Globally unique prefix (with high probability of uniqueness).
- Well-known prefix to allow for easy filtering at site boundaries.
- Allow sites to be combined or privately interconnected without creating any address conflicts or requiring renumbering of interfaces that use these prefixes.
- Internet Service Provider independent and can be used for communications inside of a site without having any permanent or intermittent Internet connectivity.
- If accidentally leaked outside of a site via routing or Domain Name Service (DNS), there is no conflict with any other addresses.
- In practice, applications may treat these addresses like global scoped addresses.

This RFC defines the format of Local IPv6 addresses, how to allocate them, and usage considerations including routing, site border routers, DNS, application support, Virtual Private Network usage, and guidelines for how to use for local communication inside a site. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT can communicate using a unique local IPv6 unicast address.

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: Devices should be able to communicate with each other via a unique local IPv6 unicast address.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Configure a unique Local IPv6 Unicast Address for each interface on the network.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Pass traffic between the interfaces.
- Launch Wireshark and observe the packet traffic to determine that the interfaces are communicating via the Unique Local IPv6 Unicast Address.
- If testing a router, create an Access Control Lists to ensure the router does not forward Unique Local IPv6 Unicast Addresses out to the Global Domain.
- Record the results, and archive all packet captures and screen shots.

Expected Results: The DUTs should be able to communicate with each other via the unique local IPv6 unicast address. These DUTs should be able to pass traffic without interference from other devices on the network.

C.1.13

RFC 4291: IPv6 Addressing Architecture

References: RFC 4291 (Dependent on RFCs 1981, 2460, 4301, 4302, 4303, 4305, 4308, and 4443)

Resource Requirements:

Hardware: TGA

Conformance Test

Purpose: To determine if the DUT conforms to RFC 4291.

Background: This specification defines the addressing architecture of the IPv6 protocol. It includes the basic formats for the various types of IPv6 addresses (unicast, anycast, and multicast). See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT sends properly formatted IPv6 packets.

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: The DUT will be able to communicate properly using IPv6.

Test Procedure: The tester will establish a network topology as shown in Figures E-2 (in Part A) and E-4 (in Part B) and complete the following:

Part A: Unicast Addressing Test

- Initiate ICMPv6 Echo Requests from the DUT to the Unicast global address of Host 2.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Observe Host 2 with a traffic analyzer to determine if the request is received and a return Echo Reply datagram is sent.
- Observe the DUT with a traffic analyzer to determine if the Echo Reply sent by Host 2 is received and processed.

- Bring up a network configuration menu on the DUT and record the IPv6 link-local and site-local addresses.
- Make a screen shot of the network configuration menu.
- Record the results and archive all packet captures and screen shots.

Part B: Anycast Addressing Test

Purpose: Evaluate the packet to determine that it correctly forms the IPv6 anycast packet. The anycast addressing structure allows for any device with the configured anycast address to respond. This function allows for multiple devices to share the same address.

Part B Limitations: The DUT in this test procedure must be a Subnet Router; otherwise, this procedure is not required.

Part B Test procedure:

- Configure Router A (DUT) and Router B, and Router C as shown in Figure E-4.
- Ensure DUT has automatically configured an anycast address.
- Disable the physical interface of Router C.
- Initiate ICMPv6 Echo Requests from the DUT to the anycast.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Observe Router B with a traffic analyzer to determine if the request is received and a return Echo Reply datagram is sent.
- Observe the DUT with a traffic analyzer to determine if the Echo Reply sent by Router B is received and processed.
- Repeat the previous steps substituting Router A, B, and C as the DUT.
- Record the results and archive all packet captures and screen shots.

Part C: Multicast Addressing Test

Purpose: Evaluate the packet to determine that it correctly forms the IPv6 multicast packet

Part C Test procedure:

- Initiate ICMPv6 Echo Requests from the DUT to the multicast global address of Host 2. Host 2 in this test procedure can be the gateway router in Figure E-2.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).

- Observe Host 2 with a traffic analyzer to determine if the request is received and a return Echo Reply datagram is sent.
- Observe the DUT with a traffic analyzer to determine if the Echo Reply sent by Host 2 is received and processed.
- Record the results and archive all packet captures and screen shots.

Expected Results: The expected results will be generated from the completion of each of the three parts in the test procedure. Each result will contain an expected result for unicast, anycast and multicast address formats.

Part A: Unicast Addressing Expected Result: Analyze packet capture result with each of the following elements:

- Must have a 128-bit Node Address length.
- Must contain a Modified EUI-64 format.
- The Unspecified Address must not be used (e.g., 0:0:0:0:0:0:0:0).
- DUT must contain a link-local unicast Loop-back address in the following form:
  - 0:0:0:0:0:0:0:1 or ::1.
- The DUT must contain a Global Unicast Address is used according to Section 2.5.4 in RFC 4291.
  - Global Routing Prefix = 64 bits.
  - EUI-64 suffix = 64 bits
- Each HOST must have the unicast address pre-defined structure in Section 2.8 of RFC 4291:
  - Link-local address.
  - Any additional automatic or manual unicast address.
  - The Loopback Address.

Part B: Anycast Addressing Expected Result: Analyze packet capture result with each of the following elements:

- Must have the same addressing format as a global unicast address.
- In order to pass this test procedure, each router must reply with the ICMPv6 application to the same anycast address.

Part C: Multicast Addressing Expected Result: Analyze packet capture result with each of the following elements:

- Must have a 128-bit Node Address length.
- The first 8 bits of the address format must contain the binary equivalent to “FF.”
- The “flag” bit must conform to the “0RPT” formatting.
- The “scope” bit must conform to Section 2.7 of RFC 4291.
- The last 112 bits of the address field must represent the correct group ID.

- Each HOST must have the multicast address pre-defined structure in Section 2.8 of RFC 4291:
  - All Nodes, All Routers, and Solicited-Node Addresses.
- Each ROUTER must have the multicast address pre-defined structure in Section 2.8 of RFC 4291:
  - All Routers Addresses.

C.1.14

RFC 4443: ICMPv6 Specification

References: RFCs 1981, 2460, 2461, 2462, and 4443

Resource Requirements:

Hardware: TGA, or PC Workstations
Software: Ixia IxANVL Test Suite IPv6 Core, Agilent N2X Test Suite #N5701A-001, Wireshark, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 4443.

Background: This RFC identifies ICMP messages for the IPv6 protocol. It includes message format and identifies two types of messages: error and informational. The RFC 4443 stipulates every node MUST implement an ICMPv6 Echo responder function that receives Echo Requests and sends corresponding Echo Replies. A node should also implement an application-layer interface for sending Echo Requests and receiving Echo Replies, for diagnostic purposes. In addition, the source address of the replying node must be the same as the destination address of the Echo Request datagram. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT interoperates using ICMPv6.

Resource Requirements:

Hardware: TGA
Criteria: The device will initialize on a network with a proper IPv6 address and be able to initiate and process ICMPv6 messages on both local and remote subnets 100 percent for all parts of the test.
Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

Part A: Link-Local Unicast

- Initiate ICMPv6 Echo Requests from Host 1 to the IPv6 link-local address of Host 2.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).

- Observe Host 2 with a traffic analyzer to determine if the request is received and a return Echo Reply (ICMPv6 Type 129) datagram is sent.
- Observe Host 1 with a traffic analyzer to determine if the Echo Reply sent by Host 2 is received and processed.
- Initiate ICMPv6 Echo Requests from Host 2 to the link-local address of Host 1.
- Observe Host 1 with a traffic analyzer to determine if the request is received and a return Echo Reply datagram is sent.
- Observe Host 2 with a traffic analyzer to determine if the Echo Reply sent by Host 2 is received and processed.
- Record the results and archive all packet captures and screen shots.

Part B: Link-Local Unicast to off-link

- Initiate ICMPv6 Echo Requests from Host 1 to the link-local address of Host 3.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Observe Host 3 with a traffic analyzer to determine if the request is received and a return Echo Reply datagram is sent.
- Observe Host 1 with a traffic analyzer to determine if the Layer-3 router replies to the link-local Echo Request from Host 1.
- Record the results and archive all packet captures and screen shots.

Part C: Global Unicast

- Initiate ICMPv6 Echo Requests from Host 1 to the global address of Host 2.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Observe Host 2 with a traffic analyzer to determine if the request is received and a return Echo Reply datagram is sent.
- Observe Host 1 with a traffic analyzer to determine if the Echo Reply sent by Host 2 is received and processed.
- Initiate ICMPv6 Echo Requests from Host 2 to the global address of Host 1.
- Observe Host 1 with a traffic analyzer to determine if the request is received and a return Echo Reply datagram is sent.
- Observe Host 2 with a traffic analyzer to determine if the Echo Reply sent by Host 2 is received and processed.
- Record the results and archive all packet captures and screen shots.

Part D: Global Unicast to off-link

- Transmit ICMPv6 Echo Requests from Host 1 to the global address of Host 3.

- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Observe Host 3 with a traffic analyzer to determine if the request is received and a return Echo Reply datagram is sent.
- Observe Host 1 with a traffic analyzer to determine if it receives the reply and processes it.
- Record the results and archive all packet captures and screen shots.

Part E: All-Nodes Multicast

- Initiate an ICMPv6 Echo Request from Host 1 to the all-nodes link-local scope multicast address, FF02::1.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Observe Host 2 with a traffic analyzer to determine if the request is received and a return Echo Reply datagram is sent.
- Observe Host 1 with a traffic analyzer to determine if an Echo Reply sent by Host 2 is received and processed.
- Initiate ICMPv6 Echo Requests from Host 2 to the all-nodes link-local scope multicast address, FF02::1.
- Observe Host 1 with a traffic analyzer to determine if the request is received and a return Echo Reply datagram is sent.
- Record the results and archive all packet captures and screen shots.

Part F: All-Routers Multicast

- Initiate an ICMPv6 Echo Request from Host 1 to the all-routers link-local scope multicast address, FF02::2.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Observe Host 2 with a traffic analyzer to determine if a reply is sent for the request.
- Observe the router with a traffic analyzer to determine if the request is received and a return Echo Reply datagram is sent.
- Observe Host 1 with a traffic analyzer to determine if the Echo Reply sent by the router is received and processed.
- Record the results and archive all packet captures and screen shots.

Expected Results:

In Part A, Hosts 1 and 2 will be able to send, receive, and process ICMPv6 Type 128 and 129 packets from each other. Examination of the packets will reveal the source address of each Type 129 datagram to be the same as the preceding Type 128-destination datagram.

In Part B, Hosts 1 and 2 will be able to send, receive, and process ICMPv6 Type 128 and 129 packets from each other though a Layer-3 router. Examination of the packets will reveal the source address of each Type 129 datagram to be the same as the preceding Type 128-destination address datagram.

In Part C, Hosts 1 and 2 will be able to send, receive, and process ICMPv6 Type 128 and 129 packets from each other. Examination of the packets will reveal the source address of each Type 129 datagram to be the same as the preceding Type 128-destination address datagram.

In Part D, Hosts 1 and 3 will be able to send, receive, and process ICMPv6 Type 128 and 129 packets from each other. Examination of the packets will reveal the source address of each Type 129 datagram to be the same as the preceding Type 128-destination datagram.

In Part E, Host 2 will respond with a proper ICMPv6 Type 129 packet.

In Part F, Host 2 will not reply to the multicast, but the routers will. Host 1 will receive the Echo Reply from the routers and process the ICMP messages.

(This page intentionally left blank.)

APPENDIX C, ANNEX 2

INTERNET PROTOCOL SECURITY PROFILE REQUIREMENTS

C.2.1

RFC 4301: Security Architecture for the Internet Protocol (IP)

References: Request for Comments (RFCs) 2401, 4301, 4303, 4305, 4306, 4307, and 4308

Resource Requirements:

Hardware: Traffic Generator/Analyzer (TGA)
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test

Purpose: To determine if the device under test (DUT) conforms to RFC 4301.

Background: This RFC specifies the base architecture for IP Security (IPSec)-compliant systems. It describes how to provide a set of security services for traffic at the IP layer, in both the IP Version 4 (IPv4) and IP Version 6 (IPv6) environments. The set of security services offered includes access control, connectionless integrity, data origin authentication, detection and rejection of replays (a form of partial sequence integrity), confidentiality (via encryption), and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection in a standard fashion for all protocols that may be carried over IP including the IP itself. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT is IPSec compatible.

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

References: RFCs 2401 and 4301

Criteria: Interoperability testing of RFC 4301 is considered complete upon the successful interoperability testing of RFCs 4303, 4305, 4606, 4307, and 4308. At which

point the DUT will have demonstrated that it has incorporated the appropriate security mechanisms to prevent unauthorized access.

Test Procedure: N/A

C.2.2

RFC 4302: IP Authentication Header (AH)

References: RFCs 2402 and 4302

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 4302.

Background:

The IP AH is used to provide connectionless integrity and data origin authentication for IP datagrams, hereafter referred to as just integrity, and to provide protection against replays. The latter optional service may be selected by the receiver when a Security Associations (SA) is established. The protocol default requires the sender to increment the sequence number used for anti-replay, but the service is effective only if the receiver checks the sequence number. However, to make use of the Extended Sequence Number feature in an interoperable fashion, AH does impose a requirement on SA management protocols to be able to negotiate this new feature.

The AH provides authentication for as much of the IP header as possible, as well as for next level protocol data. However, some IP header fields may change in transit and the value of these fields, when the packet arrives at the receiver, may not be predictable by the sender. The values of such fields cannot be protected by AH. Thus, the protection provided to the IP header by AH is piecemeal.

The AH may be applied alone, in combination with the IP Encapsulating Security Payload (ESP), or in a nested fashion. Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a Host. The ESP may be used to provide the same anti-replay and similar integrity services, and it also provides a confidentiality (encryption) service. The primary difference between the integrity provided by ESP and AH is the extent of the coverage. Specifically, ESP does not protect any IP header fields unless those fields are encapsulated by ESP (e.g., via use of tunnel mode). See page C-1 for criteria and procedures.

Interoperability Test

Use Test C.2.9 at the end of this section.

C.2.3

RFC 4303: IP ESP

References: RFCs 2406, 4303, 4305, and 4308

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 4303.

Background: The ESP header is designed to provide a mix of security services in IPv4 and IPv6. The ESP may be applied alone, in combination with AH, or in a nested fashion. Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a Host. See page C-1 for criteria and procedures.

Interoperability Test

Use Test C.2.9 at the end of this section.

C.2.4

RFC 4305: Cryptographic Algorithm Implementation Requirements for ESP and AH

References: RFCs 4109, 4303, 4305, and 4308

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 4305.

Background: The IPSec series of protocols makes use of various cryptographic algorithms in order to provide security services. The ESP and the AH provide two mechanisms for protecting data being sent over an IPSec SA. 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 mandatory-to-implement algorithms for ESP and AH as well as specifying algorithms that should be implemented because they may be promoted to mandatory at some future time. See page C-1 for criteria and procedures.

Interoperability Test

Use Test C.2.9 at the end of this section.

C.2.5

RFC 4306: The Internet Key Exchange (IKE) Version 2 (IKEv2)

References: RFCs 4306 and 4307

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 4306.

Background:

This RFC describes IKEv2 protocol. The IKE is a component of IPSec used for performing mutual authentication and establishing and maintaining SAs. The IPSec provides confidentiality, data integrity, access control, and data source authentication to IP datagrams. These services are provided by maintaining shared state between the source and the sink of an IP datagram. This state defines, among other things, the specific services provided to the datagram, which cryptographic algorithms will be used to provide the services, and the keys used as input to the cryptographic algorithms. Establishing this shared state in a manual fashion does not scale well. Therefore, a protocol to establish this state dynamically is needed. The IKEv2 is the update to 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.

All IKEv2 implementations MUST be able to send, receive, and process IKE messages that are up to 1280 bytes long, and they SHOULD be able to send, receive, and process messages that are up to 3000 bytes long. See page C-1 for criteria and procedures.

Interoperability Test 1

Purpose: To determine if the DUT can communicate using IKEv2 and required encryption algorithms.

Note: This test satisfies the interoperability testing of RFC 4306 and 4307 if successfully completed.

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: The DUT will be able to successfully establish an IKEv2 connection utilizing all of the required algorithms. The DUT will be able to communicate over the established IKEv2 connections using IPv6.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Configure the DUT and the remote Host with a basic IPv6 configuration.
- Configure IKEv2 on both the DUT and remote Host.
- During this test, the required algorithms for IKEv2 will be changed and tested.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Monitor the packet capture to ensure the IKEv2 key exchange took place successfully.
- Send an Internet Control Message Protocol (ICMP) echo request from the DUT to the remote Host to ensure the IKEv2 connection is working correctly.
- Change the encryption algorithms on both the DUT and remote Host to test all required algorithms and repeat the ICMP test. Required algorithms are:
  - Encrypted Payload Algorithms - Must implement 3DES-CBC for confidentiality and HMAC-SHA1 for Integrity.
  - Diffie-Hellman Groups - Must implement Group 2.
  - IKEv2 Transform Type 1 Algorithms - Must implement ENCR_3DES.
  - IKEv2 Transform Type 2 Algorithms - Must implement PRF_HMAC_SHA1.
  - IKEv2 Transform Type 3 Algorithms - Must Implement AUTH_HMAC_SHA1_96.
- Record the results and archive all packet captures and screen shots.

Expected Results: The devices should be able to communicate with each other utilizing an IKEv2 connection. The tester should be able to observe the key exchanges, and observe packets being transmitted while encrypted with the different required encryption algorithms.

Note: If testing RFCs 2408 and 2409 use the following test procedures.

Interoperability Test 2

Purpose: To determine if the DUT can support IKE Version 1 (IKEv1).

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: The DUT will create an SA with a neighboring peer by correctly exchanging key information. Only those hosts configured with the correct IPSec settings will be able to communicate with the DUT. Hosts with incorrect IPSec settings should not be able to communicate with DUT.

Test Procedure: The tester will configure the network as shown in Figure E-2 and complete the following:

- Configure the DUT and the remote Host with a basic IPv6 configuration.
- Establish basic connectivity between the devices.
- Configure the DUT and remote Host to share keys between them using IKE.
- Document the configurations of all variable items in the IPSec configuration.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Observe the packets to ensure the key exchange takes place.
- Send an ICMP echo request from the DUT to the remote Host to ensure the IKEv1 connection is working correctly.
- Observe the packets to ensure packets are being transmitted and received.
- Document the results.

Expected Results: The tester will monitor a successful key exchange in Wireshark between the DUT and the remote Host and verify successful communication between end points.

C.2.6

RFC 4307: Cryptographic Algorithms for Use in the IKEv2

References: RFC 4307

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 4307.

NOTE: This test satisfies the interoperability testing of RFC 4306 and 4307, if successfully completed.

Background: For IKEv2 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. The IPSec series of protocols makes use of various cryptographic algorithms to provide security services. The IKE and IKEv2 provide 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. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT can communicate using IKEv2 and required encryption algorithms.

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: The DUT will be able to successfully establish an IKEv2 connection utilizing all of the required algorithms. The DUT will be able to communicate over the established IKEv2 connections using IPv6.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Configure the DUT and the remote Host with a basic IPv6 configuration.
- Configure IKEv2 on both the DUT and remote Host.
- During this test, the required algorithms for IKEv2 will be changed and tested.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Monitor the packet capture to ensure the IKEv2 key exchange took place successfully.
- Send an ICMP echo request from the DUT to the remote Host to ensure the IKEv2 connection is working correctly.
- Change the encryption algorithms on both the DUT and remote Host to test all required algorithms and repeat the ICMP test. Required algorithms are:
    - Encrypted Payload Algorithms - Must implement 3DES-CBC for confidentiality and HMAC-SHA1 for Integrity.
    - Diffie-Hellman Groups - Must implement Group 2.
    - IKEv2 Transform Type 1 Algorithms - Must implement ENCR_3DES.
    - IKEv2 Transform Type 2 Algorithms - Must implement PRF_HMAC_SHA1.
    - IKEv2 Transform Type 3 Algorithms - Must Implement AUTH_HMAC_SHA1_96.
- Record the results and archive all packet captures and screen shots.

Expected Results: The devices should be able to communicate with each other utilizing an IKEv2 connection. The tester should be able to observe the key exchanges and observe packets being transmitted while encrypted with the different required encryption algorithms.

Note: If testing RFC 4109, Security Algorithms for IKEv1 - Use Test C.2.9 at the end of this section.

C.2.7

RFC 4308: Cryptographic Suites for IPSec

References: RFCs 4109, 4303, 4305, and 4308

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 4308.

Background: These suites should not be considered extensions to IPSec, IKE, and IKEv2, but instead administrative methods for describing sets of configurations. The IPSec, IKE, and IKEv2 protocols rely on security algorithms to provide privacy and authentication between the initiator and responder. There are many such algorithms available, and two IPSec systems cannot interoperate unless they are using the same algorithms. This RFC specifies optional suites of algorithms and attributes that can be used to simplify the administration of IPSec when used in manual keying mode, with IKEv1 or with IKEv2. See page C-1 for criteria and procedures.

Interoperability Test

Use Test C.2.9 at the end of this section.

C.2.8

RFC 4869: Suite B Cryptographic Suites for IPSec

"Informational Only" – The RFC memo provides information for the Internet community. It does not specify an Internet standard of any kind.

References: RFCs 4109, 4303, 4305, and 4308

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test - **NONE**

Purpose: To Introduce the National Security Agency's (NSA's) new cryptographic suite

Background:

This document proposes four optional cryptographic user interface (UI) suites for IPSec, similar to the two suites specified in RFC 4308. The four new suites provide compatibility with the United States National Security Agency's Suite B specifications.

Each of the following UI suites provides choices for ESP (see RFC 4303) and for IKEv1 and IKEv2 (see RFC 2409 and RFC 4306). The four suites are differentiated by the choice of cryptographic algorithm strengths and a choice of whether the Encapsulating Security Payload (ESP) is to provide both confidentiality and integrity or integrity only. The suite names are based on the Advanced Encryption Standard (AES) mode and AES key length specified for ESP. The IPSec implementations that use these UI suites SHOULD use the suite names listed here. The IPSec implementations SHOULD NOT use names different than those listed here for the suites that are described and MUST NOT use the names listed here for suites that do not match these values. These requirements are necessary for interoperability.

New UI Suites: Identifier Defined in:

- Suite-B-GCM-128 RFC 4869
- Suite-B-GCM-256 RFC 4869
- Suite-B-GMAC-128 RFC 4869
- Suite-B-GMAC-256 RFC 4869

C.2.9

Interoperability Test - IPSec Encryption Algorithms

Purpose: To determine if the DUT can communicate using required IPSec encryption algorithms.

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: The DUT will be able to successfully establish IPSec utilizing all of the required encryption and authentication algorithms. The DUT will be able to communicate over the established IPSec links using IPv6.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Configure the DUT and the remote Host with a basic IPv6 configuration.
- Configure IPSec on both the DUT and remote Host (During this test, the available algorithms for both ESP and AH will be tested).
- The IPSec requirements to be tested for IKEv1 are:
  - Triple DES for encryption MUST be supported.
  - SHA-1 for hashing and HMAC functions MUST be supported.
  - Pre-shared secrets for authentication MUST be supported.
  - Diffie-Hellman Modern Programming Practice (MODP) Group 2 (discrete log 1024 bits) MUST be supported.
- The IPSec requirements to be tested for IKEv2 are:
  - Encrypted Payload Algorithms:
    - Must implement 3DES-CBC for confidentiality.
    - Must implement HMAC-SHA1 for Integrity.
  - Diffie-Hellman Groups Must implement Group 2.
  - IKEv2 Transform Type 1 Algorithms Must implement ENCR_3DES.
  - IKEv2 Transform Type 2 Algorithms Must implement PRF_HMAC_SHA1.
  - IKEv2 Transform Type 3 Algorithms Must Implement AUTH_HMAC_SHA1_96.
  - Pre-shared secrets for authentication MUST be supported.
  - Diffie-Hellman Modern Programming Practice (MODP) Group 2 (discrete log 1024 bits) MUST be supported.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Send an ICMP echo request from the DUT to the remote Host to ensure the IPSec protocol is working correctly.

- Change the encryption algorithms on both the DUT and remote Host to test all required algorithms and repeat the ICMP test.
    - ESP Encryption Algorithms - Must Implement Null Encryption and 3DES-CBC.
    - ESP Authentication Algorithms - Must Implement Null Authentication and HMAC-SHA1-96.
    - AH - Must Implement HMAC-SHA1-96.
    - Diffie-Hellman Groups - Must Implement DH Group 2.
    - Pre Shared Keys - Must Implement Pre Shared Keys.
- Record the results and archive all packet captures and screen shots.

Expected Results: The DUTs should be able to communicate with each other using IPSec to encrypt the data. The tester should be able to observe the key exchanges and observe packets being transmitted while encrypted.

Note: There are two encryption algorithms and two authentication algorithms that must be tested for ESP. They can be used however the tester wants and do not have to match each other (i.e., Null encryption algorithm with HMAC-SHA1-96). There is one algorithm for AH. The DH Group 2 is Diffie-Hellman MODP Group 2, another type of IPSec encryption.

APPENDIX C, ANNEX 3

OTHER REQUIRED REQUEST FOR COMMENTS

C.3.1

Request for Comments (RFC) 1772: Application of the Border Gateway Protocol (BGP) in the Internet

References: RFCs 1771, 1772, 2464, 2545, and 4760

Resource Requirements:

Hardware: Traffic Generator/Analyzer (TGA)
Software: There are no automated conformance test suites available at this time. These procedures are included for clarity and completeness. When a conformance test suite for this RFC becomes available, this section will be completed. Spirent TeraRouterTester or equivalent.

Conformance Test

Purpose: To determine if the device under test (DUT) conforms to RFC 1772.

Background:

The BGP is an inter-Autonomous System (AS) routing protocol. Based on performance, preference, and policy constraints, the network reachability information exchanged via BGP provides sufficient information to detect routing loops and enforce routing decisions. Enforcing routing policies based on configuration information, BGP exchanges routing information containing full AS paths. The policies will include: policy-based distribution of routing information, policy-based packet filtering/forwarding, and policy-based dynamic allocation of network resources (e.g., bandwidth, buffers).

The BGP4+ is the primary routing protocol used to exchange routing information between AS. When two routers are sharing routing information and are in different ASs, the routers are referred to as external peers. Various router types will be used in both internal and external peer configurations. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT can support both internal and external BGP Multi-protocol Extensions (BGP4+) sessions with various router types. This will be determined by whether the DUT can process advertised BGP4+ routes and correctly determine the most desirable path for incoming packets from various equipment manufacturers.

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: Internet Protocol (IP) version 6 (IPv6) Capable Packet Analyzer

Criteria: The device will pass advertised routes back to port A on the TGA based upon the preference of routes obtained from the TGA off ports B and C. The device must have equivalent performance independent of connected vendor platforms.

Test Procedure: The tester will establish a network topology as shown in Figure E-4 with the removable routing loop cable disconnected and complete the following:

Part A: External BGP (eBGP) Peer Establishment

- Configure routers A, B, and C to advertise a unique set of routes.
- Configure routers A, B, and C to be eBGP peers (each with a different AS#).
  - Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
  - Capture the routing table and BGP4+ neighbor database (peering associations) on each of these routers.
  - Install the temporary routing loop from Figure E-4 and wait 3 minutes.
  - Capture the routing table and BGP4+ neighbor database (peering associations) on each of these routers along with routing loop information.
  - Reestablish the network topology as shown in Figure E-4 with the temporary routing loop cable disconnected.
  - Capture the routing table and BGP4+ neighbor database (peering associations) on each of these routers along with routing loop information.
  - Issuing the commands:
    - Show IPv6 route (Cisco) - will yield a complete listing of all routes along with a designator for how it was learned.
    - Show route (Juniper) - will yield a complete listing of all routes IP Version 4 (IPv4) and IPv6 along with a designator for how it was learned.

Part B: Internal BGP (iBGP) Peer Establishment

- Configure routers A, B, and C to advertise unique sets of routes.
- Configure routers A and B to be iBGP peers.
- Configure routers B and C to be eBGP peers.
- Capture the routing table and BGP4+ neighbor database (peering associations) on each of these three routers.

- Issuing the commands:
  - Show IPv6 route (Cisco) - will yield a complete listing of all routes along with a designator for how it was learned.
  - Show route (Juniper) - will yield a complete listing of all routes IPv4 and IPv6 along with a designator for how it was learned.

Part C: iBGP Peer Establishment with Redistribution

- Configure routers A, B, and C to advertise unique sets of routes.
- Configure routers A and B to be iBGP peers.
- Configure routers A and B to be running Open Shortest Path First (OSPF) with redistribution of routes from BGP.
- Configure routers B and C to be eBGP peers.
- Capture the routing table and BGP4+ neighbor database (peering associations) on each of these three routers.
- Install the temporary routing loop from Figure E-4 and wait 3 minutes.
- Capture the routing table and BGP4+ neighbor database on each of these routers along with routing loop information.
- Issuing the commands:
  - Show IPv6 route (Cisco) - will yield a complete listing of all routes along with a designator for how it was learned.
  - Show route (Juniper) - will yield a complete listing of all routes IPv4 and IPv6 along with a designator for how it was learned.

Expected Results: The routing tables should reflect both the eBGP and the iBGP peering relationships configured on each device. By following the route tables, discern which routes were chosen due to a more favorable metric count and correctly determine the most desirable path.

C.3.2

RFC 2473: Generic Packet Tunneling in IPv6 Specification

References: RFCs 2473 and 4213

Resource Requirements:

Hardware: TGA and IPv6 Test Bed
Software: Spirent AX4000 Conformance Test Suite #404679, Agilent N2X Test Suite #N5701A-002, or equivalent, Network operating systems utilizing IPv6

Conformance Test

Purpose: To determine if the DUT conforms to RFC 2473, Generic Packet Tunneling in IPv6 Specification.

Background:

The RFC 2473 defines the model and generic mechanisms for IPv6 encapsulation of IP packets, such as IPv6 and IPv4. The model and mechanisms can be applied to other protocol packets such as AppleTalk, Internetwork Packet Exchange, Connectionless Network Protocol, and/or others.

Generic tunnels are utilized to encapsulate one version of IP traffic at the source and transport that traffic to its final destination unbeknownst to the networks native version of IP. Once at the destination, the traffic is then un-encapsulated to reveal its original form.

The IPv6 tunneling is a technique for establishing a "virtual link" between two IPv6 nodes for transmitting data packets as payloads of IPv6 packets. From the point of view of the two nodes, this "virtual link," called an IPv6 tunnel, appears as a point-to-point link on which IPv6 acts like a link-layer protocol. The two IPv6 nodes play specific roles. One node encapsulates original packets received from other nodes or from itself and forwards the resulting tunnel packets through the tunnel. The other node decapsulates the received tunnel packets and forwards the resulting original packets towards their destinations, possibly itself. The encapsulator node is called the tunnel entry-point node, and it is the source of the tunnel packets. The decapsulator node is called the tunnel exit-point, and it is the destination of the tunnel packets. See page C-1 for criteria and procedures.

Interoperability Test 1

Purpose: To determine if the DUT interoperates utilizing Generic Packet Tunneling techniques and the automatic tunneling mechanism using IPv6 to IPv4.

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: The device will be capable of supporting manually configured tunnels and passing network traffic from end-to-end undetected by the native transport protocol.

Test Procedure: The tester will configure the network as shown in Figure E-2 and complete the following:

- Configure the test bed with each Local Area Network (LAN) segment utilizing pure IPv6 traffic.
- Configure the Wide Area Network (WAN) link between the two routers to be an IPv4 segment.
- Configure the routers to generate a 6 to 4 tunnel across IPv4 segments.
- Send an Internet Control Message Protocol (ICMP) message from Host 1 through the router tunnel to Host 2.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Continue to monitor the packet exchange to observe whether a new default router is selected.
- From Host 1, access a File Transfer Protocol (FTP) site that exists through the routers. This will ensure that the tunnel can pass upper layer protocols.
- Observe with the TGA the results of the protocol transfers.
- Continue to monitor the packet exchange with Wireshark to observe that Generic Route Encapsulation (GRE) is being used within the tunnel, and that the ICMP Version 6 (ICMPv6) packets (payload) are not visible.
- Record the results and archive all packet captures and screen shots.

Expected Results: All transfers should complete with a 100 percent success rate.

Interoperability Test 2

Purpose: To determine if a router can successfully tunnel IPv6 traffic.

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: The DUT must be able to establish a tunnel between to IPv4 interfaces and send IPv6 traffic between those two interfaces.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Configure the DUT and the distant end router with the following configuration:
  - Configure a point-to-point IPv6 link between the two routers.
  - Configure the end hosts to use IPv4 and configure an IPv4 default gateway on each router.
  - Configure either static routes or a routing protocol to pass routes between the two routers.
- Establish a tunnel between the two routers. This tunnel will transport IPv4 traffic over an IPv6 connection. If traffic is to be sent in both directions, a tunnel must be created in each direction that traffic will be sent.
- Send an ICMP message from Host 1 through the router tunnel to Host 2.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Continue to monitor the packet exchange to observe whether a new default router is selected.
- From Host 1, access an FTP site that exists through the routers. This will ensure that the tunnel can pass upper layer protocols.
- Record the results and archive all packet captures and screen shots.

Expected Results: The two routers should be able to create a tunnel between them. The routers should be able to forward traffic that is not IPv6 over this tunnel to a distant end Host.

C.3.3

RFC 2474: Definition of the Differentiated Services (DiffServ) Field in the IPv4 and IPv6 Headers

References: RFC 2474

Resource Requirements:

Hardware: TGA
Software: Telcordia Test Suite #802111 or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 2474.

Background:

The DiffServ enhancements to the IP are intended to enable scalable service discrimination in the Internet without the need for per-flow state and signaling at every hop. A variety of services may be built from a small, well-defined set of building blocks that are deployed in network nodes. The services may be either end-to-end or intra-domain; it includes both those that can satisfy quantitative performance requirements (e.g., peak bandwidth) and those based on relative performance (e.g., "class" differentiation). Services can be constructed by a combination of:

- Setting bits in an IP header field at network boundaries (autonomous system boundaries, internal administrative boundaries, or hosts).
- Using those bits to determine how the nodes inside the network forward packets.
- Conditioning the marked packets at network boundaries in accordance with the requirements or rules of each service.

The requirements or rules of each service must be set through administrative policy mechanisms that are outside the scope of RFC 2474. A DiffServ-compliant network node includes a classifier that selects packets based on the value of the DiffServ field, along with buffer management and packet scheduling mechanisms capable of delivering the specific packet forwarding treatment indicated by the DiffServ field value. Setting of the DiffServ field and conditioning of the temporal behavior of marked packets need only be performed at network boundaries and may vary in complexity.

The RFC 2474 defines the DiffServ field. In IPv4, it defines the layout of the Type-of-Service octet in IPv6 and the Traffic Class octet. In addition, a base set of packet forwarding treatments, or per-hop behaviors (PHB), is defined. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT can generate a random unique interface identifier.

References: RFC 2474

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: The DUT will correctly implement DiffServ and be able to communicate with another device of a different manufacturer.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Establish a base IPv6 configuration on the DUT.
- Establish a base IPv6 configuration on another router of a different manufacturer.
- Enable DiffServ on both routers.
- Configure DiffServ to use the default PHB with a precedence of 5.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Pass traffic in both directions between the routers.
- Continue to monitor the packet exchange to observe whether a new default router is selected.
- Examine the packet captures to ensure the DiffServ bits in the IPv6 Header are set the same.

Expected Results: The DUT and the opposing router should pass the same type of traffic using the same DiffServ configuration. After examination of the IPv6 header, determine that the DiffServ bits are set the same in both sets of pack captures.

C.3.4

RFC 2545: Use of BGP4+ for IPv6 Inter-domain Routing

References: RFCs 1771, 1772, 2464, 2545, and 4760

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404683, Agilent N2X Test Suite #N5704A-001, Spirent TeraRoutingTester, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 2545.

Background:

The RFC 2545 describes two BGP attributes, MP_REACH_NLRI and MP_UNREACH_NLRI, that can be used to announce and withdraw the announcement of reach ability information. The RFC defines how systems should make use of these attributes for conveying IPv6 routing information. It is sometimes necessary to announce a next hop attribute that consists of a global address and a link-local address when BGP4+ is used to convey IPv6 reach ability information for Inter-domain routing.

The BGP4+ is the primary routing protocol used to exchange routing information between ASs. When two routers are sharing routing information, and are in different ASs, the routers are referred to as external peers. Various router types will be used in both internal and external peer configurations. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT can support both internal and external BGP4+ sessions with various router types. This will be determined by whether the DUT can process advertised BGP4+ routes and correctly determine the most desirable path for incoming packets from various equipment manufacturers. To look at the next hop attribute that consists of a global address and a link-local address when BGP4+ is used to convey IPv6 reach ability information for Inter-domain routing.

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: The routing tables should reflect both the eBGP and the iBGP peering relationships configured on each device. By following the route tables, discern which routes were chosen due to a more favorable metric count and correctly determine the most desirable path was taken.

Test Procedure: The tester will establish a network topology as shown in Figure E-4 with the removable routing loop cable disconnected and complete the following:

Part A: External BGP (eBGP) Peer Establishment

- Configure routers A, B, and C to advertise a unique set of routes.
- Configure routers A, B, and C to be eBGP peers (each with a different AS#).
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Capture the routing table and BGP4+ neighbor database (peering associations) on each of these routers.
- Install the temporary routing loop from Figure E-4 and wait 3 minutes.
- Capture the routing table and BGP4+ neighbor database (peering associations) on each of these routers along with routing loop information.
- Reestablish the network topology as shown in Figure E-4 with the temporary routing loop cable disconnected.
- Capture the routing table and BGP4+ neighbor database (peering associations) on each of these routers along with routing loop information.
- Issuing the commands:
  - Show IPv6 route (Cisco) - will yield a complete listing of all routes along with a designator for how it was learned.
  - Show route (Juniper) - will yield a complete listing of all routes IP Version 4 (IPv4) and IPv6 along with a designator for how it was learned.

Part B: Internal BGP (iBGP) Peer Establishment

- Configure routers A, B, and C to advertise unique sets of routes.
- Configure routers A and B to be iBGP peers.
- Configure routers B and C to be eBGP peers.
- Capture the routing table and BGP4+ neighbor database (peering associations) on each of these three routers.
- Issuing the commands:
  - Show IPv6 route (Cisco) - will yield a complete listing of all routes along with a designator for how it was learned.
  - Show route (Juniper) - will yield a complete listing of all routes IPv4 and IPv6 along with a designator for how it was learned.

Part C: iBGP Peer Establishment with Redistribution

- Configure routers A, B, and C to advertise unique sets of routes.

- Configure routers A and B to be iBGP peers.
- Configure routers A and B to be running OSPF with redistribution of routes from BGP.
- Configure routers B and C to be eBGP peers.
- Capture the routing table and BGP4+ neighbor database (peering associations) on each of these three routers.
- Install the temporary routing loop from Figure E-4 and wait 3 minutes.
- Capture the routing table and BGP4+ neighbor database on each of these routers along with routing loop information.
- Issuing the commands:
    - Show IPv6 route (Cisco) - will yield a complete listing of all routes along with a designator for how it was learned.
    - Show route (Juniper) - will yield a complete listing of all routes IPv4 and IPv6 along with a designator for how it was learned.

Expected Results: The routing tables should reflect both the eBGP and the iBGP peering relationships configured on each device. By following the route tables, discern which routes were chosen due to a more favorable metric count and correctly determine the most desirable path was taken.

C.3.5

RFC 2740: Open Shortest Path for IPv6 (OSPFv3)

References: RFC 2740 (soon to be 5340)

Resource Requirements:

Hardware: TGA, three OSPFv3 capable routers and two workstations
Software: Ixia IxANVL Test Suite #OSPFv3, Spirent AX4000 Conformance Test Suite #404685, Agilent N2X Test Suite #N5702A-001, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 2740 (soon to be 5340).

Background:

To support IPv6 there are some modifications to OSPF. Due to changes in protocol semantics between IPv4 and IPv6 and to handle the increased address size of IPv6, some changes have been necessary. The fundamental mechanisms of OSPF (flooding, Designated Router (DR) election, OSPF area support, Shortest Path First algorithms) remain unchanged. However, addressing semantics have been removed from OSPF packets and the basic Link State Advertisements (LSA). New LSA have been created to carry IPv6 addresses and prefixes. The OSPF now runs on a per-link basis, instead of on a per-IP-subnet basis. The flooding scope for LSA has been generalized. Instead of relying on IPv6's AH and ESP, authentication has been removed from the OSPF protocol. All of OSPF protocol for IPv4's optional capabilities, including on-demand circuit support, Not-So-Stubby-Area, and the multicast extensions to OSPF are supported in OSPF for IPv6.

The differences with RFC 2740 are described in section 3 of the RFC. These protocol additions and changes are backward compatible to the obsolete RFC. The following additions were only partially specified in RFC 2740 and are further clarified in section 4; Support for Multiple Interfaces on the Same Link; Deprecation of MOSPF for IPv6; NSSA Specification; Stub Area Unknown LSA Flooding Restriction Deprecated; Link LAS Suppression; and LSA Options and Prefix Options Updates. All references to IPv6 site-local addresses have been removed.

On a multi-access link, the Area Identification (ID) (*HelloInterval* and *RouterDead Interval*) defined in an incoming Hello packet should match the configuration of the receiving interface. Otherwise, the Hello packet should be dropped and the sender should not be accepted as a neighbor. The Hello Protocol is essential to the election of the DR and Backup Designated Router (BDR) for a given link. When a router's interface first becomes functional, it checks to see whether there is currently a DR for

the network. If a DR is present, the new router accepts that DR regardless of its Router Priority.

The OSPF routers use link-state protocols to send routing information to all nodes in an inter-network by calculating the shortest path to each node based on the topography of the Internetwork constructed by each node. Each router sends that portion of the routing table that describes the state of its own links and the complete routing structure (topography).

Each router maintains a database that describes the topology of the area. Each OSPF router has an identical topological database so that all routers in the area have a consistent view of the network. All routers maintain summarized topologies of other areas within an AS. Each router distributes information about its local state by flooding LSA throughout the area. When the area topology changes, OSPF ensures the contents of all routers' topological databases converge quickly. This test determines the equipment string can recognize a change in the topology and route packets accordingly.

In OSPF, every area within the AS is required to have a connection to the backbone area. In some instances, it is not possible for an area to have a direct connection through one of its Area Border Routers (ABRs). The solution to this problem is the use of a virtual link as defined in RFC 5340. A virtual link allows an ABR to connect to the backbone area by traversing a non-backbone area that does have a connection to the backbone. See page C-1 for criteria and procedures.

Implementations involving authentication and conforming to this specification MUST support authentication for OSPFv3. To provide authentication to OSPFv3, implementations MUST support ESP and MAY support AH.

If ESP in transport mode is used, it will only provide authentication to OSPFv3 protocol packets excluding the IPv6 header, extension headers, and options.

If AH in transport mode is used, it will provide authentication to OSPFv3 protocol packets, selected portions of IPv6 header, selected portions of extension headers, and selected options.

When OSPFv3 authentication is enabled:

- OSPFv3 packets that are not protected with AH or ESP MUST be silently discarded.
- OSPFv3 packets that fail the authentication checks MUST be silently discarded.

Interoperability Test

Purpose: To determine the DUTs in a mixed network are able to interoperate using OSPF.

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: The device will recognize changes to both local and distant links and react to synchronize routing databases with every network topology change regardless of manufacturer. The Hello Protocol is essential to the election of the DR and BDR for a given link. The device will perform designated router determination and election and support virtual links to OSPF Area 0 on every test iteration.

Test Procedure: The tester will configure the routers as shown in Figure E-4. Each router should be configured with the same Area ID: a *HelloInterval* of 10 and a *RouterDeadInterval* of 40 and complete the following:

Part A: Hello Mismatch, Different *HelloInterval*

- Configure all three routers to have the same Area ID and *RouterDeadInterval.*
- Configure router A to have a different *HelloInterval* (20 instead of 10) than Routers B and C.
- Enable OSPF Version 3 (OSPFv3) on the router interfaces that are intended to interact with OSPF.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Continue to monitor the packet exchange to observe the transmitted traffic on all links.
- Transmit stateful application traffic from Host 1 to Host 3.
- Record the results and archive all packet captures and screen shots.

Part B: Synchronizing databases

- Configure router B to have a higher Router Priority than router A and C.
- Enable OSPFv3 on all routers beginning with router B, then A, followed lastly by router C.
- Enable OSPFv3 on the router interfaces that are intended to interact with OSPF.
- Configure all 3 routers to have the same Area ID, a *HelloInterval* of 10 and a *RouterDeadInterval* of 40.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Continue to monitor the packet exchange to observe the transmitted traffic on all links.

- Transmit stateful application traffic from Host 1 to Host 3.
- Record the results and archive all packet captures and screen shots.

Part C: DR failure

- Configure router B to have a higher Router Priority than router A and C.
- Enable OSPFv3 on all routers beginning with router B, then A, followed lastly by router C.
- Enable OSPFv3 on the router interfaces that are intended to interact with OSPF.
- Configure all 3 routers to have the same Area ID, a *HelloInterval* of 10, and a *RouterDeadInterval* of 40.
- Disable OSPFv3 on router B.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Continue to monitor the packet exchange to observe the transmitted traffic on all links.
- Transmit stateful application traffic from Host 1 to Host 3.
- Record the results and archive all packet captures and screen shots.

Part D: BDR failure

- Configure router B to have a higher Router Priority than router A and a lower Router Priority than router C.
- Enable OSPFv3 on all routers beginning with router C, then B, followed lastly by router A.
- Disable OSPFv3 on router B.
- Transmit traffic from Host 1 to Host 3.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Continue to monitor the packet exchange to observe the transmitted traffic on all links.
- Transmit stateful application traffic from Host 1 to Host 3.
- Record the results and archive all packet captures and screen shots.

Part E: High Priority Latecomer

- Configure router A to have a higher Router Priority than router B and C.
- Enable OSPFv3 on all routers beginning with router C, then B, followed lastly by router A.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).

- Continue to monitor the packet exchange to observe the transmitted traffic on all links.
- Transmit stateful application traffic from Host 1 to Host 3.
- Record the results and archive all packet captures and screen shots.

Expected Results:

In Part A, router A will not become OSPF neighbors with routers B and C. Routers B and C will become neighbors and synchronize databases. Traffic will not be transmitted from Host 1 to Host 3.

In Part B, all routers will become neighbors and synchronize their databases. Router B will be elected the DR, and traffic will be transmitted from Host 1 to Host 3.

In Part C, all routers will become neighbors and synchronize databases. Router B will be elected the DR, and router A will be the BDR. When OSPF is disabled on router B, router A will promote itself to the DR and router C will become the BDR. Traffic will be transmitted from Host 1 to Host 3.

In Part D, all routers will become neighbors and synchronize databases. Router C will be elected the DR, and router B will be the BDR. When OSPF is disabled on router B, router A will promote itself to the BDR. Traffic will be transmitted from Host 1 to Host 3.

In Part E, all routers will become neighbors and synchronize their databases. Router C will be elected the DR, router B will be elected BDR, and router A will assume the role of DR Other. Traffic will be transmitted from Host 1 to Host 3.

C.3.6

RFC 2784: Generic Route Encapsulation

References: RFCs 2684 and 2784

Resource Requirements:

Hardware: TGA, three Bandwidth Constrained Links capable routers, and two Host workstations
Software: There are no automated conformance test suites available at this time. These procedures are included for clarity and completeness. When a conformance test suite for this RFC becomes available, this section will be completed.

Conformance Test

Purpose: To determine if the DUT conforms to RFC 2784.

Background:

The GRE is a protocol for encapsulation of an arbitrary Network Layer Protocol (NLP) over another arbitrary NLP when a system has a payload packet that needs to be encapsulated and delivered to some destination. The payload will first be encapsulated in a GRE packet. The GRE packet can then be encapsulated in some other delivery protocol and then forwarded. The concept of this protocol is to provide a simple, general purpose mechanism which reduces the problem of encapsulation from its current n^2 size to a more manageable size.

Logic Link Control Encapsulation allows multiplexing of multiple protocols over a single Asynchronous Transfer Mode (ATM) virtual connection whereas Virtual Connection Multiplexing assumes that each protocol is carried over a separate ATM virtual connection. This specification is intended for use in implementations that use ATM networks to carry multi-protocol traffic among hosts, routers, and bridges, which are ATM end systems. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine that the data link is established, configured, and tested with extensible Link Control Protocol (LCP) defined by Point-to-Point Protocol (PPP); to determine the Quality Control Configuration; to periodically verify the identity of a peer connection with a 3-way handshake; and to ensure Network Control Protocols are able to establish and configure different NLPs.

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: The device will utilize GRE to enable different protocol datagram's to traverse IPv6 networks.

Test Procedure: The tester will establish a network topology as shown in Figure E-4 and complete the following:

Part A: ATM Encapsulation

- Configure the three routers each with the ATM protocol.
- Enable virtual connections on all routers.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Continue to monitor the packet exchange to observe the transmitted traffic on all links.
- Transmit stateful application traffic from Host 1 to Host 3.
- Record the results and archive all packet captures and screen shots.

Part B: GRE Encapsulation

- Configure routers A and D to perform GRE.
- Enable router B to be an IPv6 capable router.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Continue to monitor the packet exchange to observe the transmitted traffic on all links.
- Transmit stateful application traffic from Host 1 to Host 3.
- Record the results and archive all packet captures and screen shots.

Expected Results:

In Part A, router A will encapsulate the IPv6 packet in ATM cells and send it through routers B and D. The packets will then be extracted from the cells and reassembled. Voice and video will pass across the network.

In Part B, router A will encapsulate the IPv6 packets in a GRE tunnel. The packet will be extracted at router D. The IPv6 data should not be recognizable at router B. Voice and video will pass across the network.

C.3.7

RFC 3041/4941: Privacy Extensions for Stateless Address Auto-configuration in IPv6

References: RFC 3041 and 4941

Resource Requirements:

Hardware: TGA
Software: There are no automated conformance test suites available at this time. These procedures are included for clarity and completeness. When a conformance test suite for this RFC becomes available, this section will be completed.

Conformance Test

Purpose: To determine if the DUT conforms to RFC 3041.

Background:

Nodes use IPv6 stateless address auto-configuration to generate addresses without the necessity of a Dynamic Host Configuration Protocol (DHCP) server. Some types of network interfaces come with an embedded Institute of Electrical and Electronic Engineers, Inc., (IEEE) Identifier (i.e., a link-layer Media Access Control (MAC) address), and in those cases stateless address auto-configuration uses the IEEE identifier to generate a 64-bit interface identifier. Combining a network prefix with a unique identifier forms the IPv6 address. This RFC discusses concerns associated with the embedding of non-changing interface identifiers within IPv6 addresses and describes extensions to stateless address auto-configuration that can help mitigate those concerns for individual users and in environments where such concerns are significant.

On interfaces that contain embedded IEEE Identifiers, the interface identifier is typically derived from it. On other types, the interface identifier is generated through other means, for example, via random number generation. The RFC 3041 describes an extension to IPv6 stateless address auto-configuration for interfaces whose interface identifier is derived from an IEEE Identifier. Use of the extension causes nodes to generate global-scope addresses from interface identifiers that change over time, even in cases where the interface contains an embedded IEEE Identifier. Changing the interface identifier (and the global-scope addresses generated from it) over time makes it more difficult for eavesdroppers and other information collectors to identify when different addresses used in different transactions actually correspond to the same node.
See page C-1 for criteria and procedures.

Interoperability Test

Most network interfaces come with an embedded IEEE Identifier (i.e., a link-layer MAC address), and in those cases stateless address auto-configuration uses the IEEE identifier to generate a 64 bit interface identifier. This interface identifier is appended to the link-local network prefix as well as the router provided network prefix.

Purpose: To determine if the DUT can:

- Utilize the IEEE interface identifier MAC address and combine it with a router supplied network prefix and form an IPv6 Stateless Address Auto-configuration address or
- Generate a random interface identifier to be used with a router supplied network prefix and form an IPv6 Stateless Address Auto-configuration address.

References: RFC 3041

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: The RFC 3041 is written as a Theoretical discussion of the need for Privacy Extensions for Stateless Address Auto-configuration in IPv6. At this time, there are absolutely no MUST requirements associated with this RFC. The tester will verify that the DUT is capable of using a unique IPv6 interface identifier that has been automatically configured by one of the following methods:

- Stateless address auto-configuration by using the embedded IEEE Identifier (i.e., a link-layer MAC address) to generate a 64 bit interface identifier and combining it with the router provided network prefix.
- Random address occurrence (when Stable Storage Is Present): The following algorithm assumes the presence of a 64-bit "history value" that is used as input in generating a randomized interface identifier. The very first time the system boots (i.e., out-of-the-box) a random value should be generated using techniques that help ensure the initial value is hard to guess. Whenever a new interface identifier is generated, a value generated by the computation is saved in the history value for the next iteration of the algorithm.
- The initial history value Random address occurrence (when no Stable Storage Is Present): In the absence of stable storage, no history value will be available across system restarts to generate a pseudo-random sequence of interface identifiers. Consequently, there will be no history of unique identifiers from which to calculate the next random identifier.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and verify that one of the methods of Privacy Extensions for Stateless Address Auto-configuration in IPv6 has occurred and complete the following:

- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- If possible, remove any IPv6 address on the Network Interface Card.
- Reboot DUT and continue to monitor the packet exchange to observe whether one of the three criteria stated above are met.
- Record the results and archive all packet captures and screen shots.

Expected Results: The device should use the interface identifier MAC address or generate a random interface identifier to be used with the router supplied network prefix to form an IPv6 address.

C.3.8

RFC 3315: DHCP for IPv6 (DHCPv6)

References: RFC 3315

Resource Requirements:

Hardware: TGA
Software: Agilent N2X Test Suite #N5701A-002, a client or server-based DHCP for IPv6 implementation, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 3315.

Background: The RFC 3315 enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes. It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility. This protocol is a stateful counterpart to RFC 2462/4862, IPv6 Stateless Address Auto-configuration and can be used separately or concurrently with the latter to obtain configuration parameters. See page C-1 for criteria and procedures.

Note: Local Router settings:

M---------1-bit "Managed address configuration" flag. When set, it indicates that addresses are available via Dynamic Host Configuration Protocol (DHCPv6). If the M flag is set, the O flag is redundant and can be ignored, because DHCPv6 will return all available configuration information.
O---------1-bit "Other configuration" flag. When set, it indicates that other configuration information is available via DHCPv6. Examples of such information are DNS-related information or information on other servers within the network.

Note: If neither M nor O flags are set, this indicates that no information is available via DHCPv6.

Interoperability Test

Purpose: To determine if the DUT can interoperate and successfully negotiate an IPv6 stateful address auto-configuration transaction.

References: RFC 3315

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring and a router with “managed” and “other options” flags enabled
or
Software: IPv6 Capable Packet Analyzer

Criteria: The DUT will successfully negotiate IPv6 stateful address auto-configuration transactions.

Test Procedure: The tester will configure the network as shown in Figure E-2 and complete the following:

- Install a DHCPv6 server or client, as required.
- From the Client/Host 1, initiate a DHCP request.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Continue to monitor the packet exchange to observe that the appropriate client/server interactions occur.
- Listen on User Datagram Protocol (UDP) port 546 on the Client/Host 1 subnet to verify the appropriate client messages are sent and received.
- Listen on UDP port 547 on the Server 1 subnet to verify the appropriate server messages are sent and received:
    - Solicit Message: Client sends to locate a DHCP server.
    - Advertise Message: A server sends an Advertise message to indicate that it is available for DHCP service (this is sent only as a response to a Solicit message received from a client).
    - Request Message: A client sends a Request message to request configuration parameters, including IP addresses, from a specific server.
    - Confirm Message: A client sends a Confirm message to any available server to determine whether the addresses it was assigned are still appropriate to the link to which the client is connected.
    - Renew Message: A client sends a Renew message to the server that originally provided the client’s addresses and configuration parameters to extend the lifetimes on the addresses assigned to the client and to update other configuration parameters.
    - Rebind Message: A client sends a Rebind message to any available server to extend the lifetimes on the addresses assigned to the client and to update other configuration parameters (this message is sent after a client receives no response to a Renew message).
    - Decline Messages: A client sends a Decline message to a server to indicate the client has determined that one or more addresses assigned by the server are already in use on the link to which the client is connected.

- Release Message: A client sends a Decline message to a server to indicate the client has determined that one or more addresses assigned by the server are already in use on the link to which the client is connected.
- Reply Message: A server sends a Reply message containing assigned addresses and configuration parameters in response to a Solicit, Request, Renew, Rebind message received from a client. A server sends a Reply message containing configuration parameters in response to an Information-request message. A server sends a Reply message in response to a Confirm message confirming or denying that the addresses assigned to the client are appropriate to the link, which the client is connected. A server sends a Reply message to acknowledge receipt of a Release or Decline message.
- (Optional) Reconfigure Message: A server sends a Reconfigure message to a client to inform the client the server has new or updated configuration parameters, and the client is to initiate a Renew/Reply or Information-request/Reply transaction with the server to receive the updated information.
- Information-request Message: A client sends an Information-request message to a server to request configuration parameters without the assignment of any IP addresses to the client.
- (Mandatory only if testing a relay agent) Relay-forward Message: A relay agent sends a Relay-forward message to relay messages to servers, either directly or through another relay agent (the received message, either a client message or a Relay-forward message from another relay agent, is encapsulated in an option in the Relay-forward message).

- Manipulate the Client/Host 1 subnet to cause duplicate addresses to occur.
- Monitor the packet exchange to observe that the appropriate client/server interactions occur.
- Record the results and archive all packet captures and screen shots.

Expected Results: Depending on the type of message and the direction of the transaction, the client/server must respond with the proper control message. If the device being tested is a network infrastructure device, it must be capable of multicast (the method DHCP messages are sent) and not inhibit the flow of DHCP control information across the network segments. Upon completion of the DHCP information handshake, the device under test should pull an IPv6 address and any optional information also being distributed.

C.3.9

RFC 3411: An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks

References: RFC 2466, and 3411 and 4113

Resource Requirements:

Hardware: TGA
Software: There are no automated conformance test suites available at this time. These procedures are included for clarity and completeness. When a conformance test suite for this RFC becomes available, this section will be completed; a client-based IPv6 SNMP-based Network Management System (NMS) implementation.

Conformance Test

Purpose: To determine if the DUT conforms to RFC 3411.

Background: The RFC 3411 describes architecture for describing SNMP Management Frameworks. The architecture is designed to be modular to allow the evolution of the SNMP protocol standards over time. The major architectural change incorporated in SNMP Version 3 (SNMPv3) is that of User authentication. Other major portions of the architecture are an SNMP engine containing a Message Processing Subsystem, a Security Subsystem and an Access Control Subsystem, and possibly multiple SNMP applications, which provide specific functional processing of management data. See page C-1 for criteria and procedures.

Interoperability Test

The industry has been slow to implement IPv6 NMS, and as a result, there have been no IPv6 capable NMSs identified as of yet. The Use of SNMPv3 Conformance Test software performs many of the functions expected of an IPv6 NMS application. Because of this point, Procedure 1 satisfies the interoperability test requirements of RFCs 3411, 3412, and 3413.

Purpose: To determine if the DUT can interoperate using SNMPv3.

References: RFC 2466, 3411, and 4113

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer, SNMP SimpleTesterPro

Criteria: The DUT will successfully facilitate management of network products using SNMPv3.

Test Procedure: The tester will configure the network as shown in Figure E-2 and complete one of the following procedures:

Procedure 1:

Using a SNMPv3 testing application available from SimpleSoft, Silver Creek, or other industry peer (in this case Simple Soft), perform the following:

- Install SNMPv3 testing application on an appropriate Host workstation.
- Configure the DUT for SNMPv3.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Continue to monitor the packet exchange to observe that SNMPv3 Authentication policies were negotiated properly.
- Open up the Simple Tester Pro program.
- Click on the “Get Variables to Test” icon (fourth from the right).
- Type in the IPv6 address of the DUT in the Agent IP Address box.
- Click on the Settings box.
- Select which version of SNMP to run.
- Select public from the Read Community drop down box.
- Select private from the Write Community drop down box.
- Check both IPv4 and IPv6 boxes in IP Version section.
- When using SNMPv3 click on the SNMPv3 tab.
- Type in the User Name for the account that was set on the DUT.
- In the Level box select the appropriate level (generally Authentication/Privacy).
- Type in the password in the Authentication Password and Privacy Password boxes.
- Select an Authentication Protocol and Privacy Protocol.
- Click on the Save button.
- Select the Start button from the Get SNMP Variables to Test box.
- Once completed, click on the Close box.
- Select the appropriate SNMP version from the left hand side under Syntax Test Suites and click on the green start arrow located at the top of the screen.
- Once the test has completed, select View and HyperText Markup (HTM) Language (HTML) Summary.
- Save the summary as an HTM document.

Procedure 2:

- Verify all products on the network with SNMPv3 capability are set with the same community strings as found in the NMS.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Continue to monitor the packet exchange to observe that SNMPv3 Authentication policies are negotiated properly.
- Access a network infrastructure device using the user interface of the NMS.
- Complete a Management Information Base (MIB) walk of the following Object Identifiers (OID):
  - 1.3.6.1.2.1.1.1 – sysDescr.
  - 1.3.6.1.2.1.1.2 – sysObjectID.
  - 1.3.6.1.2.1.1.3 – sysUpTime.
  - 1.3.6.1.2.1.1.4 – sysContact.
  - 1.3.6.1.2.1.1.5 – sysName.
  - 1.3.6.1.2.1.1.6 – sysLocation.
  - 1.3.6.1.2.1.1.7 – sysServices.
  - Attempt to change a non-locked OID. (Suggested 1.3.6.1.2.1.1.4 – sysContact).
- Complete a MIB walk of the Private branch of the MIB tree (1.3.6.1.4.1) utilizing OID that are specific to the device manufacturer.
- Record the results and archive all packet captures and screen shots.
- Save the summary as an HTM document.

Expected Results: The device will negotiate a SNMPv3 handshake, including authentication as well as compare community strings with the network infrastructure device. The MIB-2 and Private party OID will be available for perusal using the NMS. The NMS will be able to alter non-locked OID in the MIB-2 side of the tree.

C.3.10

RFC 3412: Message Processing and Dispatching for the SNMP

References: RFC 3412

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 3412.

Background: This RFC describes the Message Processing and Dispatching for SNMP messages within the SNMP architecture. It defines the procedures for dispatching potentially multiple versions of SNMP messages to the proper SNMP Message Processing Models and for dispatching Protocol Data Units to SNMP applications. This RFC also describes one Message Processing Model - the SNMPv3 Message Processing Model. See page C-1 for criteria and procedures.

Interoperability Test

The industry has been slow to implement IPv6 NMS, and as a result, there have been no IPv6 capable NMSs identified. The Use of SNMPv3 Conformance Test software performs many of the functions expected of an IPv6 NMS application. Because of this point, Procedure 1 in Test C.3.10 satisfies the interoperability test requirements of RFCs 3411, 3412, and 3413.

Purpose: To determine if the DUT can send and receive SNMP Messages.

References: RFC 3412

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer, SNMP SimpleTesterPro

Criteria: The DUT will be able to be managed using the SNMPv3 protocol by a NMS.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Continue to monitor the packet exchange to observe that SNMPv3 messages are being sent and received by authorized devices.
- Verify all devices on the network with SNMP capability are set with the same community strings as found in the NMS.
- Access a network infrastructure device that is configured to receive SNMPv3 messages from the DUT.
- Record the results and archive all packet captures and screen shots.

Expected Results: The DUT will be managed using the SNMP protocol via an NMS.

C.3.11

RFC 3413: SNMP Applications

References: RFC 3413

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 3413.

Background:

This RFC describes five types of SNMP applications which make use of an SNMP engine as described in Standard 62, RFC 3411. The types of application described are Command Generators, Command Responders, Notification Originators, Notification Receivers, and Proxy Forwarders.

This RFC also defines MIB modules for specifying targets of management operations, notification filtering, and proxy forwarding. See page C-1 for criteria and procedures.

Interoperability Test

The industry has been slow to implement IPv6 NMS, and as a result, there have been no IPv6 capable NMSs identified. The Use of SNMPv3 Conformance Test software performs many of the functions expected of an IPv6 NMS application. Because of this point, Procedure 1 in Test C.3.10 satisfies the interoperability test requirements of RFCs 3411, 3412, and 3413.

Purpose: To determine if the DUT can send and receive SNMP applications.

References: RFC 3413

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer, SNMP SimpleTesterPro

Criteria: The DUT will be able to be managed using the SNMPv3 protocol by a NMS.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Verify all devices on the network with SNMP capability are set with the same community strings as found in the NMS.
- Access a network infrastructure device using the user interface of the NMS.
- Record the results.

Expected Results: The DUT will be managed using the SNMP protocol via an NMS. All RFC MUSTs will receive a passing grade via test software.

C.3.12

RFC 3484: Default Address Selection for IPv6

References: RFC 3484

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 3484.

Background:

This RFC describes two algorithms, for source address selection and for destination address selection. The IPv6 addressing architecture [1] allows multiple unicast addresses to be assigned to interfaces. These addresses may have different reachability scopes (link-local, site-local, or global). The algorithms specify default behavior for all IPv6 implementations. They do not override choices made by applications or upper-layer protocols, nor do they preclude the development of more advanced mechanisms for address selection. The two algorithms share a common context, including an optional mechanism for allowing administrators to provide policy that can override the default behavior. In dual stack implementations, the destination address selection algorithm can consider both IPv4 and IPv6 addresses depending on the available source addresses, the algorithm might prefer IPv6 addresses over IPv4 addresses, or vice-versa.

All IPv6 nodes, including both hosts and routers, MUST implement default address selection as defined in this RFC. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT can select the proper source and destination address to communicate with a Host.

References: RFC 3484

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: The DUT will be able to make the correct determination of which address it needs to use (link-local, global unicast, multicast) to send its traffic to the correct destination network.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Configure a unique link-local, site-local, and global IPv6 unicast address for each interface on the network.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Continue to monitor the packet exchange to observe that the DUT will be able to make the correct determination as to which address it needs to use (link-local, global unicast, multicast) to send its traffic to the correct destination network.
- Pass traffic between the interfaces.
- If testing a router, create an Access Control List to ensure the router does not forward unique local IPv6 unicast addresses out to the Global Domain.
- Record the results and archive all packet captures and screen shots.

Expected Results: The captured traffic should demonstrate that end-point to end-point communications will be conducted in the appropriate IPv6 unicast address format. All devices will pass traffic without interference from other devices on the network.

C.3.13

RFC 3596: Domain Name Service (DNS) Extensions to Support IPv6

References: RFC 1034, 1035, 2136, 3226, and 3596

Resource Requirements:

Hardware: TGA
Software: There are no automated conformance test suites available at this time. These procedures are included for clarity and completeness. When a conformance test suite for this RFC becomes available, this section will be completed. A server-based DNS for IPv6 implementation.

Conformance Test

Purpose: To determine if the DUT conforms to RFC 3596.

Background: The RFC 3596 defines the changes that need to be made to the DNS to support hosts running IPv6. The changes include a resource record type to store an IPv6 address; a domain to support lookups based on an IPv6 address, and updated definitions of existing query types that return Internet addresses as part of additional section processing. The designed extensions are compatible with existing applications and DNS implementations. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if a DUT can interoperate utilizing DNS for fully qualified Domain Name resolution to IPv6 addresses.

References: RFC 1034, 1035, 2136, 3226, and 3596

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: The DUT MUST successfully operate using fully qualified domain names accessed via DNS.

Test Procedure: The tester will configure the network as shown in Figure E-2 and complete the following:

- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Continue to monitor the packet exchange to observe that a properly transacted IPv6 DNS (AAAA) record exchange is carried out.
- From the Client/Host 1, initiate a DNS IPv6 128 bit address record (AAAA) name resolution request from Server 1 running an implementation of DNS for IPv6.
- Examine the response from Server 1 for correct addressing information.
- Examine the packet captures of the network segments on either side of the target device for handshake transactions.
- From the Client/Host 1, initiate a DNS AAAA name resolution request that requires a DNS redirect to a different zone than the Root Server occupies.
- Examine the packet captures of the network segments on either side of the target device for handshake transactions.
- Record the results and archive all packet captures and screen shots.

Expected Results: Depending on the DUT, the expected result is for the device to interoperate properly within the test network. In the case of an End-user Device or a Network Server, the result will be the ability to successfully complete a DNS transaction. If the device is a router or other infrastructure device, the device will not impede the flow of control information between the client and server. During the redirect portion, the client will allow the redirect and the transaction will be completed.

C.3.14

RFC 3775: Mobility Support for IPv6

References: RFC 3775

Resource Requirements:

Hardware: TGA
Software: There are no automated conformance test suites available at this time. These procedures are included for clarity and completeness. When a conformance test suite for this RFC becomes available, this section will be completed. Telnet server and client software.

Conformance Test

Purpose: To determine if the DUT conforms to RFC 3775.

Background: The RFC 3775 specifies a protocol that allows nodes to remain reachable while moving around in the IPv6 Internet. Each Mobile Node (MN) is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a MN is also associated with a Care-of-Address (CoA), which provides information about the MN's current location. The IPv6 packets addressed to a MN's home address are transparently routed to its CoA. The protocol enables IPv6 nodes to cache the binding of a MN's home address with its CoA and then send any packets destined for the MN directly to it at this CoA. To support this operation, mobile IPv6 defines a new IPv6 protocol and a new destination option. All IPv6 nodes, whether mobile or stationary, can communicate with MNs. See page C-1 for criteria and procedures.

Interoperability Test - MN to Correspondent Node (CN) Communication

Purpose: Determine that a MN can move away from its Home Network (HN) among various subnets and maintain a Transmission Control Protocol (TCP) session with a stationary CN on the MN's HN or on a Foreign Network (FN).

References: RFC 3775

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Background:

Mobile IPv6 allows a MN to move from one link to another without changing the MN's IP address. A MN is always addressable by its "home address," an IP address assigned to the MN within its HN prefix on its home link. Packets may be routed to the MN using this address regardless of the MN's current point of attachment to the Internet, and the MN may continue to communicate with other nodes (stationary or mobile) after moving to a new link. The movement of a MN away from its home link is transparent to transport and higher-layer protocols and applications.

In general, when a MN sends a Binding Update to its Home Agent (HA) to register a new primary CoA, the MN will also send a Binding Update to each other node for which an entry exists in the MN's Binding Update List. Thus, other relevant nodes are generally kept updated about the MN's current CoA.

A MN, whether on its HN or on a FN, should be able to communicate with a CN located on the HN or on a FN.

Criteria: The MN will maintain connectivity with the CN without dropping the TCP session.

Test Procedure: The tester will connect the device as shown in Figure E-5 and complete the following:

- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Continue to monitor the packet exchange to observe that a MN to move from one link to another without changing the MN's IP address.
- Establish a Telnet session between MN1 and CN1 (either device may be the server or client, depending on the capabilities of each).
- Move MN1 to FN1.
- Determine that MN1 is able to reach CN1.
- Determine that CN1 and HA1 have created a binding cache entry for MN1.
- Move MN1 to FN2.
- Determine that MN1 is able to reach CN1.
- Determine that CN1 and HA1 have updated the binding cache entry for MN1.
- MN1 moves to HN1.
- Determine that MN1 is able to reach CN1 and that CN1 and HA1 have deleted the binding cache entry for MN1.
- Record the results and archive all packet captures and screen shots.

Note: The MN, referred to as MN1 is configured with HN1 as its HN, and HA1, as it is HA. The DR, DR1 is configured to act as default router for all of its attached networks. The DR1 does not provide HA services. The HA1 is configured to act as a HA for its

network, but not a default router. The HA1 and DR1 may be the same device, if necessary. Router parameters are displayed in table C-3-1.

Table C-3-1. Test Case C.3.14 Router Parameters

Designated Router 1	Home Agent 1
Router Lifetime: 30 minutes Minimum Advance Interval: 0.5 seconds Maximum Advance Interval: 1.5 seconds Each prefix Valid Lifetime: 30 minutes Preferred Lifetime: 20 minutes	Router Lifetime: 0 seconds Minimum Advance Interval: 0.5 seconds Maximum Advance Interval: 1.5 seconds Home Agent Lifetime: 30 minutes Each prefix R Bit: Set, full address included Valid Lifetime: 30 minutes Preferred Lifetime: 20 minutes

Expected Results: Once MN1 has detected movement to a different network and binding cache entries have been created, updated, or deleted (as appropriate), reachability between MN1 and CN1 should be re-established. With each movement of the MN, the Telnet session may be briefly interrupted but should remain connected through HA1. The MN1 should update the binding for HA1 and CN1 reflecting the change in CoA. The HA1 should tunnel packets to MN1 from CN1, when necessary. There may be some delay before the MN detects that it has moved to a FN.

C.3.15

RFC 3776: Using IP Security (IPSec) to Protect Mobile IPv6 Signaling Between MN and HA

References: RFC 3775 and 3776

Resource Requirements:

Hardware: TGA
Software: There are no automated conformance test suites available at this time. These procedures are included for clarity and completeness. When a conformance test suite for this RFC becomes available, this section will be completed.

Conformance Test

Purpose: To determine if the DUT conforms to RFC 3776.

Background:

Mobile IPv6 uses IPSec to protect signaling between the HA and the MN. Mobile IPv6 base document defines the main requirements these nodes must follow. The RFC 3776 discusses these requirements in more depth, illustrates the used packet formats, describes suitable configuration procedures, and shows how implementations can process the packets in the right order.

Mobile IPv6 allows a MN to move from one link to another without changing the MN's IP address. A MN is always addressable by its "home address," an IP address assigned to the MN within its HN prefix on its home link. Packets may be routed to the MN using this address regardless of the MN's current point of attachment to the Internet, and the MN may continue to communicate with other nodes (stationary or mobile) after moving to a new link. The movement of a MN away from its home link is transparent to transport and higher-layer protocols and applications.

The MNs will send a Binding Update to the respective HAs to register a new primary CoA; the MNs will also send a Binding Update to other nodes for which an entry exists in the MN's Binding Update List. Thus, other relevant nodes are generally kept updated about each MN's current CoA. See page C-1 for criteria and procedures.

Interoperability Test 1 - MN to MN Communication

Purpose: To determine that two MNs can move away from the HN to various FNs, and remain in contact with each other.

References: RFC 3775 and 3776

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: The MNs will maintain communication without dropping the TCP session.

Test Procedure: The tester will connect the device as shown in Figure E-6. During the test, the movement of the MN can be seen in Figure E-7.

- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Continue to monitor the packet exchange to observe that a MN to move from one link to another without changing the MN's IP address.
- Establish a Telnet session between MN1 and MN2 (either device may be the server or client, depending on the capabilities of each).
- Move MN1 to FN1.
- Determine that MN1 and MN2 are able to reach one another.
- Determine that MN1, MN2, and HA1 have created the appropriate binding cache entries.
- Move MN2 to FN2.
- Determine that MN1 and MN2 are able to reach one another.
- Determine that MN1, MN2, and HA1 have updated the appropriate binding cache entries.
- Move MN1 to FN2 and move MN2 to FN1.
- Determine that MN1 and MN2 are able to reach one another.
- Determine that MN1, MN2, and HA1 have updated the appropriate binding cache entries.
- Record the results and archive all packet captures and screen shots.

Note: The MN1 is configured with HN1 as its HN and HA1 as it is HA. The MN2 is configured with HN2 as its HN and HA2 as it is HA. The HA1 and HA2 are not default routers for the respective networks. The DR1 is configured to act as the default router for all of its attached networks. The DR1 does not provide HA services. The HA1, HA2, and DR1 may be the same device, if necessary. Router parameters are displayed in Table C-3-2.

Table C-3-2. Test Case C.3.15 Router Parameters Interoperability Test 1

Designated Router 1	Home Agent 1 And 2
Router Lifetime: 30 minutes Minimum Advance Interval: 0.5 seconds Maximum Advance Interval: 1.5 seconds Each prefix Valid Lifetime: 30 minutes Preferred Lifetime: 20 minutes	Router Lifetime: 0 seconds Minimum Advance Interval: 0.5 seconds Maximum Advance Interval: 1.5 seconds Home Agent Lifetime: 30 minutes Each prefix R Bit: Set, full address included Valid Lifetime: 30 minutes Preferred Lifetime: 20 minutes

Expected Results: Once MN1 and MN2 have detected movement to a different network and binding cache entries have been created, updated, or deleted (as appropriate), reachability between MN1 and MN2 should be re-established. When MN1 and MN2 make each move, the two should update the bindings for the appropriate HA (HA1 or HA2) and CN reflecting the change in CoA. The HA1 and HA2 should tunnel packets destined for MN1 and MN2, respectively, when necessary. There may be some delay before each MN detects that it has moved to a FN.

Interoperability Test 2 - HN Renumbering

Purpose: Determine that a MN can move away from its HN, and while away, have its HN renumbered.

References: RFC 3775 and 3776

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Background: Mobile IPv6 allows a MN to move from one link to another without changing the MN's IP address. A MN is always addressable by its "home address," an IP address assigned to the MN within its HN prefix on its home link. Packets may be routed to the MN using this address regardless of the MN's current point of attachment to the Internet, and the MN may continue to communicate with other nodes (stationary or mobile) after moving to a new link. The movement of a MN away from its home link is thus transparent to transport and higher-layer protocols and applications. While a MN is away from its HN, its HN may be renumbered. This may occur, for instance, if an Internet service provider is changed. In this case, a HA can send Mobile Prefix Advertisements to the MN to advertise the new prefix. This way, the MN can configure the advertised prefix and maintain connectivity with it is HA.

Criteria: When the HN is re-prefixed with a different address, the HA must remember the MN and be able to forward control information to it.

Test Procedure: The tester will connect the device as shown in Figure E-6 and complete the following:

- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Continue to monitor the packet exchange to observe that when the HN is re-prefixed the HA will remember the MN and continue to forward control information to it.
- Establish a Telnet session between MN1 and CN1 (either device may be the server or client, depending on the capabilities of each).
- Move MN1 to FN1.
- Determine that MN1 is able to reach CN1.
- Determine that CN1 and HA1 have created a binding cache entry for MN1.
- Allow time for HN1 and HA1 to be configured with a new prefix (the old prefix is configured to time out such that the old and new prefix lifetimes overlap).
- Allow enough time to elapse so the old prefix has timed out.
- Move MN1 to FN2.
- Allow time for MN1 to be configured with the new home prefix, duplicate address detection to be performed, and new binding updates to be sent.
- Re-establish the Telnet session between MN1 and CN1.
- Determine that MN1 is able to reach CN1.
- Determine that CN1 and HA1 have updated the binding cache entry for MN1.
- Record the results and archive all packet captures and screen shots.

Note: The MN1 is configured with HN1 as its HN and HA1 as it is HA. The MN2 is configured with HN2 as its HN and HA2 as it is HA. The DR1 is configured to act as the default router for all of its attached networks. The DR1 does not provide HA services. The HA1 is configured to act as a HA for network HN1, but not a default router. The HA1 and DR1 may be the same device, if necessary. Router parameters are displayed in Table C-3-3.

Table C-3-3. Test Case C.3.15 Router Parameters Interoperability Test 2

Designated Router 1	Home Agent 1
Router Lifetime: 30 minutes Minimum Advance Interval: 0.5 seconds Maximum Advance Interval: 1.5 seconds Each prefix Valid Lifetime: 30 minutes Preferred Lifetime: 20 minutes	Router Lifetime: 0 seconds Minimum Advance Interval: 0.5 seconds Maximum Advance Interval: 1.5 seconds Home Agent Lifetime: 30 minutes Each prefix R Bit: Set, full address included Valid Lifetime: 30 minutes Preferred Lifetime: 20 minutes

Expected Results: Once MN1 has detected movement to a different network and binding cache entries have been created, updated, or deleted (as appropriate), reachability between MN1 and CN1 should be re-established. The MN1 should update

the bindings for HA1 and CN1 reflecting the change in CoA. The HA1 should tunnel packets to MN1 from CN1 when necessary. There may be some delay before the MN detects that it has moved to a FN. The MN1 should learn and configure the new home prefix through Mobile Prefix Solicitations and Advertisements. Following the HN renumbering, MN1 should be able to communicate normally with both CN1 and HA1.

Interoperability Test 3 - DAD

Purpose: Determine that a MN can resolve its home address when a node on its HN has claimed the same address.

References: RFC 3775 and 3776

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Background: While the mobile node is away from home, it relies on the HA to participate in DAD to defend its home address against stateless auto-configuration performed by another node.

Criteria: The HA will respond and defend DAD requests for IP addresses already associated with MNs under its auspices.

Test Procedure: The tester will connect the device as shown in Figure E-5 and complete the following:

- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Continue to monitor the packet exchange to observe that a MN to move from one link to another without changing the MN's IP address.
- Move MN1 to FN1.
- Connect CN1 to HN1.
- Attempt to configure CN1 with the same link-local and global addresses as MN1 (allow time for DAD to take place).
- Record the results and archive all packet captures and screen shots.

Note: The MN1 is configured with HN1 as its HN and HA1 as it is HA. The MN2 is configured with HN2 as its HN and HA2 as it is HA. The DR1 is configured to act as default router for all of its attached networks. The DR1 does not provide HA services. The HA1 is configured to act as a HA for networks HN1 and FN1 but not a default router. The HA1 and DR1 may be the same device, if necessary. Router parameters are displayed in Table C-3-4.

Table C-3-4. Test Case C.3.15 Router Parameters Interoperability Test 3

Designated Router 1	Home Agent 1
Router Lifetime: 30 minutes Minimum Advance Interval: 0.5 seconds Maximum Advance Interval: 1.5 seconds Each prefix Valid Lifetime: 30 minutes Preferred Lifetime: 20 minutes	Router Lifetime: 0 seconds Minimum Advance Interval: 0.5 seconds Maximum Advance Interval: 1.5 seconds Home Agent Lifetime: 30 minutes Each prefix R Bit: Set, full address included Valid Lifetime: 30 minutes Preferred Lifetime: 20 minutes

Expected Results: The HA1 should successfully defend the global and link-local addresses of MN1.

C.3.16

RFC 3963: Network Mobility (NEMO) Basic Support Protocol

References: RFC 3963

Resource Requirements:

Hardware: TGA
Software: There are no automated conformance test suites available at this time. These procedures are included for clarity and completeness. When a conformance test suite for this RFC becomes available, this section will be completed. Telnet server and client software.

Conformance Test

Purpose: To determine if the DUT conforms to RFC 3963.

Background: The RFC 3963 describes the NEMO Basic Support Protocol that enables Mobile Networks to attach to different points in the Internet. The protocol is an extension of Mobile IPv6 and allows session continuity for every node in the Mobile Network as the network moves. It also allows every node in the Mobile Network to be reachable while moving around. The Mobile Router (MR), which connects the network to the Internet, runs the NEMO Basic Support protocol with it's HA. The protocol is designed so that network mobility is transparent to the nodes inside the Mobile Network. See page C-1 for criteria and procedures.

Interoperability Test 1

Purpose: Determine that a MR can perform the necessary procedures to change locations and maintain proper communication capabilities.

References: RFC 3963

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Background: While the mobile network is away from home, the nodes located on that network, without needing to be aware of mobility, are able to maintain communication with CN.

Criteria: The MR will be able to shift from HN and still maintain communications for products on its subnets.

Test Procedure: The tester will connect the device as shown in Figure E-7 and complete the following:

- Establish a Telnet session between Test Node (TN) TN1 and CN1.
- Move MR1 with HN0 to FN1.
- Determine reachability between TN1 and CN1.
- Move MR1 with HN0 back to HN1.
- Determine reachability between TN1 and CN1.
- Document the results.

Note: An MR, referred to as MR1, is configured with HN1 as its HN, and HA1, as it is HA. The Border Router (BR) is configured to act as such for MR1. The BR does not provide HA services. The HA1 is configured to act as a HA for networks HN1.

Expected Results: When HN0 moves from HN1 to FN1 and back, communication must still be possible between TN1 and CN1.

Interoperability Test 2 - NEMO with MN

Purpose: Determine that a MR with a MN attached can perform the necessary procedures to change locations and maintain proper communications.

References: RFC 3963

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Background: While the mobile network is away from home, the nodes located on that network, mobile or fixed, are able to maintain communication with CNs.

Criteria: The MN from a subnet gateway-ed by a MR will be able to maintain TCP sessions with CNs as the MR leaves the HN returns.

Test Procedure: The tester will connect the device as shown in Figure E-7 and complete the following:

- Move MR1 with HN0 to FN1.
- Establish a Telnet session between MN1 and CN1.
- Move MN1 to HN0.
- Determine reachability between MN1 and CN1.
- Move MR1 with HN0 to HN1.
- Determine reachability between MN1 and CN1.
- Document the results.

Note: An MR, referred to as MR1, is configured with HN1 as its HN, and an HA, HA1, as it is HA. The BR is configured to act as the BR for MR1. The BR does not provide HA services. The HA1 is configured to act as a HA for HN1.

Expected Results: When MN1 is connected to HN0, while the network is mobile and when it returns to HN1, it should be able to communicate with CN1.

C.3.17

RFC 3986: Uniform Resource Identifier (URI): Generic Syntax

References: RFC 3986

Resource Requirements:

Hardware: TGA
Software: Ixia IxANVL Test Suite IPv6 Core, Spirent AX4000 Conformance Test Suite #404687, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 3986.

Background:

A URI provides a simple and extensible means for identifying a resource. This RFC of URI syntax and semantics is derived from concepts introduced by the World Wide Web global information initiative, whose use of these identifiers dates from 1990.

A URI is a compact sequence of characters that identifies an abstract or physical resource. This specification defines the generic URI syntax and a process for resolving URI references that might be in relative form, along with guidelines and security considerations for the use of URIs on the Internet. The URI syntax defines a grammar that is a superset of all valid URIs, allowing an implementation to parse the common components of a URI reference without knowing the scheme-specific requirements of every possible identifier. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT URIs have correct syntax.

References: RFC 3986

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: The device will interoperate with the test bed and be able to access or support all of the protocols described in Table C-3-5.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

Utilizing the Uniform Resource Locator (URL) schema as depicted Table C-3-5. Perform a URL mapping to:

- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Setup an FTP server on the server depicted in Figure E-2.
- Setup an Hypertext Transfer Protocol (HTTP) server on the server depicted in Figure E-2.
- Setup Simple Mail Transfer Protocol (SMTP) server on the server depicted in Figure E-2.
- Allow Web Based Telnet services on the server depicted in Figure E-2.
- Continue to monitor the packet exchange to observe whether device will interoperate with the test bed and be able to access or support all of the protocols described in Table C-3-5.
- From Host 1 the client will use FileZilla software to access the FTP server.
- From Host 1 the client will use Mozilla Firefox Browser to access an Internet Information server.
- From Host 1 the client will use Mozilla Thunderbird to access the mail server.
- From Host 1 the client will use Telnet sessions to access the device.
- Record the results and archive all packet captures and screen shots.

Table C-3-5. IPv6 Mappings

Protocol	Port
FTP	21
HTTP	80
SMTP	25
Telnet	23

LEGEND:

IPv6	Internet Protocol Version 6
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
SMTP	Simple Mail Transfer Protocol

Expected Results: All tested protocols will successfully establish connections across the network using URLs with fully qualified names.

C.3.18

RFC 4213: Transition Mechanisms for IPv6 Host and Routers

References: RFC 4213

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404679, Agilent N2X Test Suite #N5701A-002, Ixia IxANVL Test Suite IPv6 Advanced, or equivalent. IPv6 Test Bed

Conformance Test

Purpose: To determine if the DUT conforms to RFC 4213.

Background: The RFC 4213 specifies IPv4 compatibility mechanisms that can be implemented by IPv6 hosts and routers. These mechanisms include providing complete implementations of both versions of the IP (IPv4 and IPv6), and tunneling IPv6 packets over IPv4 routing infrastructures. It is designed to allow IPv6 nodes to maintain complete compatibility with IPv4, which should greatly simplify the deployment of IPv6 on the Internet, and facilitate the eventual transition of the entire Internet to IPv6. See page C-1 for criteria and procedures.

Interoperability Test 1

Purpose: To determine if the DUT interoperates utilizing dual stack techniques.

References: RFC 4213

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Criteria: The device will initialize on a network and be able to independently process IPv4 and IPv6 datagrams.

Test Procedure: The tester will configure the network as shown in Figure E-2 and complete the following:

- Configure the test bed with each segment's products utilizing both IPv4 and IPv6 TCP/IP stacks (commonly known as dual stack architecture).

- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Transmit data packets (using HTTP, FTP, SMTP, and Real-Time Streaming Protocol (RTSP) formatted packets over both IPv4 and IPv6) by manual means or from the TGA 2 through the network to the TGA 1.
- The HTTP should attempt to access eight web pages (four-IPv4 and four-IPv6). Two of the four IPv6 web pages should be accessed using Literal IPv6 addresses in brackets. The FTP should attempt six file transfers (three-IPv4 and three-IPv6). The SMTP should attempt six e-mail exchanges (three-IPv4 and three-IPv6). The RTSP should transmit six streaming video transfers (three-IPv4 and three-IPv6). Observe with the TGA the results of the protocol transfers.
- Monitor the packet exchange to observe that the data transfers were successful.
- Record the results and archive all packet captures and screen shots.

Expected Results: All four major traffic types will transit the network on both IPv4 and IPv6 with a 100 percent success rate.

Interoperability Test 2

Purpose: To determine if the DUT interoperates utilizing configured tunneling techniques.

References: RFCs 2473 and 4213

Resource Requirements:

Hardware: IPv6 Test Bed
Software: The network operating systems necessary to operate the IPv6 Test Bed

Background: Configured tunnels are used to encapsulate IPv6 datagrams for transmission across an IPv4 network or IPv4 datagrams for transmission across an IPv6 network.

Criteria: The device will have the capability for the operator to manually configure tunnels and successfully pass end-to-end traffic.

Test Procedure: The tester will configure the network as shown in Figure E-2 and complete the following:

- Configure the test bed with each LAN segment utilizing pure IPv6 traffic.
- Configure the WAN link between the two routers to be an IPv4 segment.

- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Manually configure an IPv6-in-IPv4 tunnel across the IPv4 segment.
- Transmit data packets (using HTTP, FTP, SMTP, and RTSP formatted packets over both IPv4 and IPv6) by manual means or from the TGA 2 through the network to the TGA 1.
- The HTTP should attempt to access eight web pages (four-IPv4 and four-IPv6). Two of the four IPv6 web pages should be accessed using Literal IPv6 addresses in brackets. The FTP should attempt six file transfers (three-IPv4 and three-IPv6). The SMTP should attempt six e-mail exchanges (three-IPv4 and three-IPv6). The RTSP should transmit six streaming video transfers (three-IPv4 and three-IPv6). Observe with the TGA the results of the protocol transfers.
- Observe with the TGA the results of the protocol transfers.
- Monitor the packet exchange to observe that the data transfers were successful.
- Record the results and archive all packet captures and screen shots.

Expected Results: All four major traffic types will transit the network over the tunnels.

C.3.19

RFC 4271: A Border Gateway Protocol 4 (BGP-4)

References: RFCs 1772, 2464, 2545, and 4271

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 4271.

Background:

This RFC discusses the BGP, which is an inter-AS routing protocol. The BGP-4 provides a set of mechanisms for supporting Classless Inter-Domain Routing (CIDR). These mechanisms include support for advertising a set of destinations as an IP prefix, and eliminating the concept of network "class" within BGP. The BGP-4 also introduces mechanisms that allow aggregation of routes, including aggregation of AS paths.

The primary function of a BGP speaking system is to exchange network reachability information with other BGP systems. This network reachability information includes information on the list of ASs that reachability information traverses. This information is sufficient for constructing a graph of AS connectivity for this reachability from which routing loops may be pruned, and, at the AS level, some policy decisions may be enforced. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT can support both internal and external BGP4+ sessions with various router types. This will be determined by whether the DUT can process advertised BGP4+ routes and correctly determine the most desirable path for incoming packets from various equipment manufacturers.

References: RFCs 1772, 2464, 2545, and 4271

Resource Requirements:

Hardware: TGA and a Switch capable of port mirroring
or
Software: IPv6 Capable Packet Analyzer

Background: The BGP4+ is the primary routing protocol used to exchange routing information between ASs. When two routers are sharing routing information and are in different ASs, the routers are referred to as external peers. Various router types will be used in both internal and external peer configurations.

Criteria: The device will pass advertised routes back to port A on the TGA based upon the preference of routes obtained from the TGA off ports B and C. The device must have equivalent performance independent of connected vendor platforms.

Test Procedure: The tester will establish a network topology as shown in Figure E-4 with the temporary routing loop cable disconnected and complete the following:

Part A: eBGP Peer Establishment

- Configure all three routers to advertise a unique set of routes.
- Configure all three routers to be eBGP peers.
- Capture the routing table and BGP4+ neighbor database on each of these routers.
- Install the temporary routing loop from Figure E-4 and wait 3 minutes.
- Capture the routing table and BGP4+ neighbor database on each of these routers along with routing loop information.
- Establish a network topology as shown in Figure E-4 with the temporary routing loop cable disconnected.

Part B: iBGP Peer Establishment

- Configure all routers to advertise unique sets of routes.
- Configure routers A and B to be iBGP peers.
- Configure routers B and C to be eBGP peers.
- Capture the routing table and BGP4+ neighbor database on each of these three routers.

Part C: iBGP Peer Establishment with Redistribution

- Configure all three routers to advertise unique sets of routes.
- Configure routers A and B to be iBGP peers.
- Configure routers A and B to be running OSPF with redistribution from BGP.
- Configure routers B and C to be eBGP peers.
- Capture the routing table and BGP4+ neighbor database on each of these three routers.
- Install the temporary routing loop from Figure E-4 and wait 3 minutes.
- Capture the routing table and BGP4+ neighbor database on each of these routers along with routing loop information.

Expected Results: The routing tables should reflect both the eBGP and the iBGP peering relationships configured on each device. By following the route tables, discern which routes were chosen due to a more favorable metric count and correctly determine the most desirable path was taken.

C.3.20

RFC 2858/4760: Multi-protocol Extensions for BGP Version 4 (BGP-4)

References: RFCs 2858 and 4760

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 4760.

Background:

Currently, BGP-4 is capable of carrying routing information only for IPv4. This RFC defines extensions to BGP-4 to enable it to carry routing information for multiple NLPs (e.g., IPv6 or Internetwork Packet Exchange (IPX)). The extensions are backward compatible - a router that supports the extensions can interoperate with a router that does not support the extensions.

The only three pieces of information carried by BGP-4 that are IPv4 specific are (a) the NEXT_HOP attribute (expressed as an IPv4 address), (b) AGGREGATOR (contains an IPv4 address), and (c) Network Layer Reachability Information (NLRI) (expressed as IPv4 address prefixes). This RFC assumes that any BGP speaker (including the one that supports multiprotocol capabilities defined in this RFC) has to have an IPv4 address (which will be used, among other things, in the AGGREGATOR attribute). Therefore, to enable BGP-4 to support routing for multiple Network Layer protocols the only two things that have to be added to BGP-4 are (a) the ability to associate a particular NLPs with the next hop information, and (b) the ability to associate a particular NLP with NLRI. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT can support both IPv4 and IPv6 networks and will advertise the IPv6 networks to the DUT's BGP neighbor routers.

References: RFC 4760

Resource Requirements:

Hardware: TGA
Software: Spirent TeraRouterTester, or equivalent

Criteria: The device will pass all advertised routes regardless of Layer-3 protocol back to its configured BGP neighbors. The device must have equivalent performance independent of connected vendor platforms.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

BGP Peer Establishment:

- Configure a point-to-point link between router A and router B using IPv4.
- Configure IPv6 networks behind the routers.
- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).
- Continue to monitor the packet exchange to observe the transmitted traffic on all links.
- Configure BGP+ on both routers creating neighbor statements pointing to the opposite router.
- Advertise the IPv6 networks.
- Capture the routing table and BGP4+ neighbor database on each of these routers.
- Transmit stateful application traffic from Host 1 to Host 3.
- Record the results and archive all packet captures and screen shots.

Expected Results: Each routing table should show the advertised networks of the opposite router regardless of Layer-3 protocol used.

Note: Other protocols may be tested if the vendor so chooses. Examples include IPX, Appletalk, and Novell.

C.3.21

Network Management: Management Information Base (MIB)

References:

RFC 3595	Textual Conventions for IPv6 Flow Label (Contains NO MUST requirements in RFC)
RFC 4022	Management Information Base for the Transmission Control Protocol (Contains MUST requirements in RFC)
RFC 4113	Management Information Base for the User Datagram Protocol (Contains MUST requirements in RFC)
RFC 4087	IP Tunnel MIB (Contains NO MUST requirements in RFC)
RFC 4293	Management Information Base (MIB) for IP (Contains MUST requirements in RFC)
RFC 4295	Mobile IP Management MIB (Contains NO MUST requirements in RFC)
RFC 4807	IPSec Security Policy Database Configuration (Contains MUST requirements in RFC)
RFC 4292	IP Forwarding Table MIB (Contains MUST requirements in RFC)

Resource Requirements:

Hardware: TGA
Software: IPv6 Capable Packet Analyzer or SNMP SimpleTesterPro

Background: The Network Management portion of IPv6 continues to lag behind other more developed areas of IPv6. This is further illustrated by the lack of vendor developed MIBs to correspond with the MIB related RFCs.

SNMP Manager: An SNMP manager, also known as an SNMP management system or a management console, is any computer that sends queries for IP-related information to a managed computer, known as an SNMP agent. In some cases, the SNMP manager can send a request to an SNMP agent to change a configuration value.

SNMP MIB Definition: Each system in a network (workstation, server, router, bridge, and so forth) maintains a MIB that reflects the status of the managed resources on that system, such as the version of the software running on the device, the IP address assigned to a port or interface, the amount of free hard drive space, or the number of open files. The MIB does not contain static data, but is instead an object-oriented, dynamic database that provides a logical collection of managed object definitions. The MIB defines the data type of each managed object and describes the object.

SNMP Agent Definition: A software process that responds to queries using the SNMP to provide status and statistics about a network (node).

Procedures:

Perform either procedure A or B:

Test Procedure (A):

- Contact the OEM of the test equipment and ask them for the MIB developed against the RFC under test.
- Once that is in hand, compile that MIB to be utilized by your SNMP management system.
- Open the MIB Browser and walk the tree until arriving at the specific objects to be viewed.
- Now change each value and verify that the MIB OBJECT reacts the same way as required in the RFC.
- Record the results and compare them to the requirements within the RFC.

Test Procedure (B):

- Obtain a SNMP test agent such as Simple Soft SimpleTesterPro.
- Verify that the software selected covers the MIB RFCs.
- Execute the test against the DUT, collect the results, and analyze the data for compliance to the MUST requirements in the RFC.

Note: At this time, current industry support could only be found for RFCs 4022, 4113, and 4293.

(This page intentionally left blank.)

APPENDIX C, ANNEX 4

OPTIONAL CONNECTION TECHNOLOGIES

The current version of the Department of Defense Internet Protocol Version 6 (IPv6) Standard Profiles for IPv6 Capable Products document mandates that the vendor must support one of the listed Connection Technologies. Additional Connection technologies will be tested upon request of the vendor.

C.4.1

Request for Comments (RFC) 2491: IPv6 Over Non-Broadcast Multiple Access (NBMA) Networks

References: RFC 2491

Resource Requirements:

Hardware: Traffic Generator/Analyzer (TGA)
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IP Security (IPSec) Internet Key Exchange (IKE), or equivalent

Conformance Test

Purpose: To determine if the device under test (DUT) conforms to RFC 2491.

Background:

This RFC describes a general architecture for IPv6 over NBMA networks. It forms the basis for subsidiary companion documents that describe details for various specific NBMA technologies (such as Asynchronous Transfer Mode (ATM) or Frame Relay). The IPv6 over NBMA architecture allows conventional Host-side operation of the IPv6 Neighbor Discovery protocol, while also supporting the establishment of 'shortcut' NBMA forwarding paths when dynamically signaled NBMA links are available. Operations over administratively configured Point-to-Point NBMA links are also described.

Dynamic NBMA shortcuts are achieved through the use of IPv6 Neighbor Discovery protocol operation within Logical Links, and inter-router Next Hop Resolution Protocol for the discovery of off-Link NBMA destinations. Both flow-triggered and explicitly source-triggered shortcuts are supported. See page C-1 for criteria and procedures.

Interoperability Test

This RFC is optional and currently no test case has been written.

C.4.2

RFC 2492: IPv6 over ATM Networks January 1999

References: RFC 2492

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 2492.

Background: This RFC provides specific details on how to apply the IPv6 over NBMA architecture to ATM networks. This architecture allows conventional Host-side operation of the IPv6 Neighbor Discovery protocol, while also supporting the establishment of 'shortcut' ATM forwarding paths (when using Switched Virtual Circuits). Operation over administratively configured Point-to-Point Private Virtual Circuits is also supported. See page C-1 for criteria and procedures.

Interoperability Test

Purpose: To determine if the DUT can send properly formatted IPv6 packets over a Layer-2 ATM protocol link.

References: RFC 2492

Resource Requirements:

Hardware: TGA

Criteria: The DUT will send properly formatted IPv6 packets over a Layer-2 ATM topology network to a remote Host. The remote Host must be able to receive and process these packets for the test to be a success.

Test Procedure: The tester will establish a network topology as shown in Figure E-2 and complete the following:

- Using a switch capable of port mirroring (creating a network tap), monitor the packet exchange using an IPv6 capable packet capturing software (such as Wireshark).

- Ensure the network topology is an ATM network. This can be determined by capturing some packets with Wireshark and examining them to check the Layer-2 protocol.
- Monitor the packet exchange and examine them to check the Layer-2 protocol.
- Configure a unique IPv6 unicast address on the DUT and the remote Host.
- Launch Wireshark.
- Send traffic across the ATM segment from the DUT to the remote Host.
- Capture traffic to show that IPv6 traffic is running across the Layer-2 ATM protocol.
- Record the results and archive all packet captures and screen shots.

Expected Results: The devices should be able to communicate with the remote Host, using IPv6 formatted packets running across an ATM segment.

C.4.3

RFC 2497: Transmission of IPv6 Packets over ARCnet Networks

References: RFC 2497

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 2497.

Background: This RFC specifies a frame format for transmission of IPv6 packets and the method of forming IPv6 link-local and statelessly auto-configured addresses on ARCnet networks. It also specifies the content of the Source/Target Link-layer Address option used by the Router Solicitation, Router Advertisement, Neighbor Solicitation, Neighbor Advertisement and Redirect messages when those messages are transmitted on an ARCnet. See page C-1 for criteria and procedures.

Interoperability Test

This RFC is optional and currently no test case has been written.

C.4.4

RFC 2590: Transmission of IPv6 Packets over Frame Relay Networks Specification

References: RFC 2890

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 2590.

Background: This RFC specifies the frame format for transmission of IPv6 packets over Frame Relay networks, the method of forming IPv6 link-local addresses on Frame Relay links, and the mapping of the IPv6 addresses to Frame Relay addresses. It also specifies the content of the Source/Target link-layer address option used in Neighbor Discovery and Inverse Neighbor Discovery messages when those messages are transmitted over a Frame Relay link. It is part of a set of specifications that define such IPv6 mechanisms for NBMA media (NBMA and ATM), and a larger set that defines such mechanisms for specific link layers (Ethernet, Fiber Optic Digital Data Interface, Point-to-Point Protocol (PPP), and ATM). See page C-1 for criteria and procedures.

Interoperability Test

This RFC is optional and currently no test case has been written.

C.4.5

RFC 3146: Transmission of IPv6 over Institute of Electrical and Electronic Engineers, Inc., (IEEE) 1394 Networks

References: RFC 3146

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 3146.

Background: This RFC describes the frame format for transmission of IPv6 packets and the method of forming IPv6 link-local addresses and statelessly auto-configured addresses on IEEE 1394 networks. It also describes the content of the Source/Target Link-layer Address option used in Neighbor Discovery when the messages are transmitted on an IEEE 1394 network. See page C-1 for criteria and procedures.

Interoperability Test

This RFC is optional and currently no test case has been written.

C.4.6

RFC 4338: Transmission of IPv6, IP Version 4, and Address Resolution Protocol (ARP) Packets over Fiber Channel

References: RFC 4338

Resource Requirements:

Hardware: TGA
Software: Spirent AX4000 Conformance Test Suite #404718, Ixia IxANVL Test Suite IPSec IKE, or equivalent

Conformance Test

Purpose: To determine if the DUT conforms to RFC 4338.

Background: This RFC specifies the way of encapsulating IPv6, IPv4, and ARP packets over Fiber Channel. This RFC also specifies the method of forming IPv6 link-local addresses and statelessly auto-configured IPv6 addresses on Fiber Channel networks, and a mechanism to perform IPv4 address resolution over Fiber Channel networks. See page C-1 for criteria and procedures.

Interoperability Test

This RFC is optional and currently no test case has been written.

APPENDIX C, ANNEX 5

NATIONAL SECURITY AGENCY (NSA) IPv6 INFORMATION ASSURANCE TEST PLAN (IATP) PROCEDURES

The current version of the Department of Defense Internet Protocol (IP) Version 6 (IPv6) Standard Profiles for IPv6 Capable Products document mandates that firewalls and Intrusion Protection System/Intrusion Detection Systems (IPS/IDS) be tested in accordance with the NSA IPv6 IATP.

C.5.1

NSA IPv6 Information Assurance Test Plan (IATP), Annex 1, Firewalls

References: NSA IPv6 IATP, Version 1

Resource Requirements:

Hardware: Traffic Generator/Analyzer (TGA) or packet capture device
Software: Wireshark, IP Packet Capture Software, or equivalent

Information Assurance and Functionality Test Procedures

Test Cases: The following list of test cases correspond to the NSA IATP, Version 1, Annex 1, Sections 2 and 3.

Test 2.1.01: Role Separation
Test 2.1.02: Role Revocation
Test 2.1.03: Pre-Authentication Advisory Notice
Test 2.1.04: Post-Authentication Advisory Notice
Test 2.1.05: User Session Access
Test 2.1.06: Authentication Policy
Test 2.1.07: Local and Remote Administration
Test 2.2.01: Basic: Ports, Protocols, and Services
Test 2.2.02: Basic: Inactivity Guard
Test 2.2.03: Basic: Traffic Integrity Test
Test 2.2.04: Basic: TCP Traffic Enforcement
Test 2.2.05: Basic: Access Control
Test 2.2.06: Basic: Stateful Inspection
Test 2.3.01: Advanced: Trusted Computing Base
Test 2.3.02: Advanced: Environmental Variables
Test 2.3.03: Advanced: Trusted Path
Test 2.3.04: Advanced: Controlled Interface
Test 2.3.05: Advanced: Classification Review
Test 2.3.06: Advanced: Classification Protection
Test 2.3.07: Advanced: Classification Transmission
Test 2.3.08: Advanced: Configuration Surety
Test 2.4.01: Audit Inspection
Test 2.4.03: Discretionary Access Control
Test 2.4.04: Mandatory Access Control
Test 2.4.05: Configuration of Alert Mechanisms
Test 2.5.01: ICMPv6 Control Traffic
Test 2.5.02: Hop-by-Hop Header
Test 2.5.03: Default Router
Test 2.5.04: IPSec Forwarding
Test 2.5.05: IPSec Verification

Test 2.5.06: Address Auto-configuration
Test 2.5.07: Transition Mechanism Blocking
Test 2.6.01: Attacks: Denial of Service
Test 2.6.02: Attacks: Man-in-the-Middle (Replay)
Test 2.6.03: Attacks: Common Vulnerabilities and Exploits
Test 2.6.04: Attacks: Penetration Test
Test 2.6.05: Attacks: Startup/Shutdown Vulnerabilities
Test 2.6.06: Attacks: Tiny Fragments for IPv4 and IPv6
Test 2.7.01: Documentation: Firewall Developer
Test 2.7.02: Documentation: Developer Pre-Coverage
Test 2.7.03: Documentation: Strength of Firewall
Test 2.7.04: Documentation: Development Processes
Test 2.7.05: Documentation: Configuration Management
Test 2.7.06: Documentation: Delivery Processes
Test 2.7.07: Documentation: Administrator/User Guidance
Test 2.7.08: Documentation: Vulnerability Analysis
Test 2.7.09: Documentation: Software Design
Test 2.7.10: Documentation: Cryptography
Test 2.7.11: Documentation: Software Design Test
Test 3.1.01: Performance Test

C.5.2

NSA IPv6 Information Assurance Test Plan (IATP), Annex 3, IPS/IDS

References: NSA IPv6 IATP, Version 1

Resource Requirements:

Hardware: TGA or packet capture device
Software: Wireshark, IP Packet Capture Software, or equivalent

Information Assurance and Functionality Test Procedures

Test Cases: The following list of test cases corresponds to the NSA IATP, Version 1, Annex 3, Sections 2 and 3.

Test 2.1.01: Role Separation
Test 2.1.02: Role Revocation
Test 2.1.03: Pre-Authentication Advisory Notice
Test 2.1.04: Post-Authentication Advisory Notice
Test 2.1.05: User Session Access
Test 2.1.06: Authentication Policy
Test 2.1.07: Local and Remote Administration
Test 2.2.02: Basic: Inactivity Guard
Test 2.2.04: Basic: TCP Traffic Enforcement
Test 2.2.06: Basic: Stateful Inspection
Test 2.3.01: Advanced: Trusted Computing Base
Test 2.3.02: Advanced: Environmental Variables
Test 2.3.08: Advanced: Configuration Surety
Test 2.4.01: Audit Inspection
Test 2.4.02: Data Collection
Test 2.4.03: Discretionary Access Control
Test 2.4.04: Mandatory Access Control
Test 2.5.01: ICMPv6 Control Traffic
Test 2.5.05: IPSec Verification
Test 2.5.06: Address Auto-configuration
Test 2.5.07: Transition Mechanism Blocking
Test 2.6.01: Attacks: Denial of Service
Test 2.6.02: Attacks: Man-in-the-Middle (Replay)
Test 2.6.03: Attacks: Common Vulnerabilities and Exploits
Test 2.6.04: Attacks: Penetration Test
Test 2.6.05: Attacks: Startup/Shutdown Vulnerabilities
Test 2.6.06: Attacks: Tiny Fragments for IPv4 and IPv6
Test 2.7.01: Documentation: IPS Developer
Test 2.7.02: Documentation: Developer Pre-Coverage
Test 2.7.03: Documentation: Strength of IPS

Test 2.7.04: Documentation: Development Processes
Test 2.7.05: Documentation: Configuration Management
Test 2.7.06: Documentation: Delivery Processes
Test 2.7.07: Documentation: Administrator/User Guidance
Test 2.7.08: Documentation: Vulnerability Analysis
Test 2.7.09: Documentation: Software Design
Test 2.7.10: Documentation: Cryptography
Test 2.7.11: Documentation: Software Design Test
Test 3.1.01: Performance Test

(This page intentionally left blank.)

APPENDIX D

PERFORMANCE MEASUREMENT PROCEDURES

This appendix is included as a guide to performance testing. There is little requirement for performance testing before the question of a device's Internet Protocol (IP) Version 6 (IPv6) capability is answered.

Once IPv6 capability has been established, the performance of the device is of particular interest. The following methodology will give an introduction to measuring performance by way of automated equipment.

Performance: analysis of a device while under "load/stress" conditions, while producing a measurable set of metrics. These metrics may be used later for comparisons to other products and protocols.

Automated performance testing will take the form of three categories, Bit Level, Protocol Level, Routed simulation. Testing will be conducted on device under test (DUT) and network under test conditions. Refer to Figures D-1 for the DUT and D-2 for the network under test architecture.

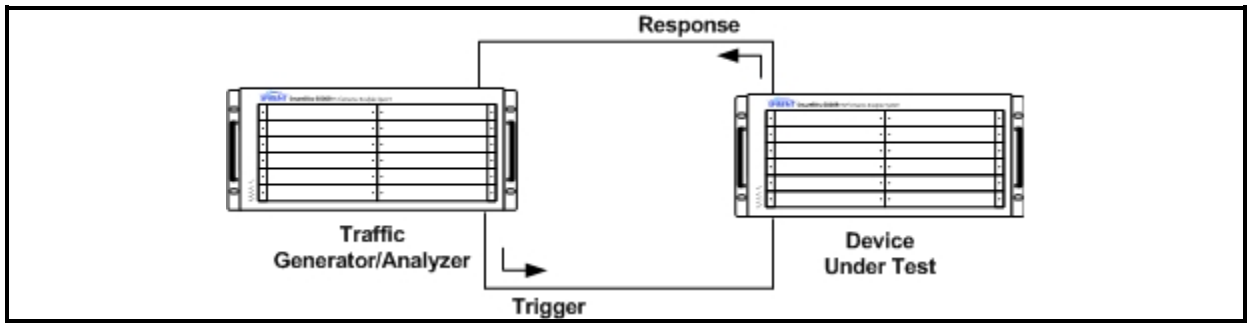
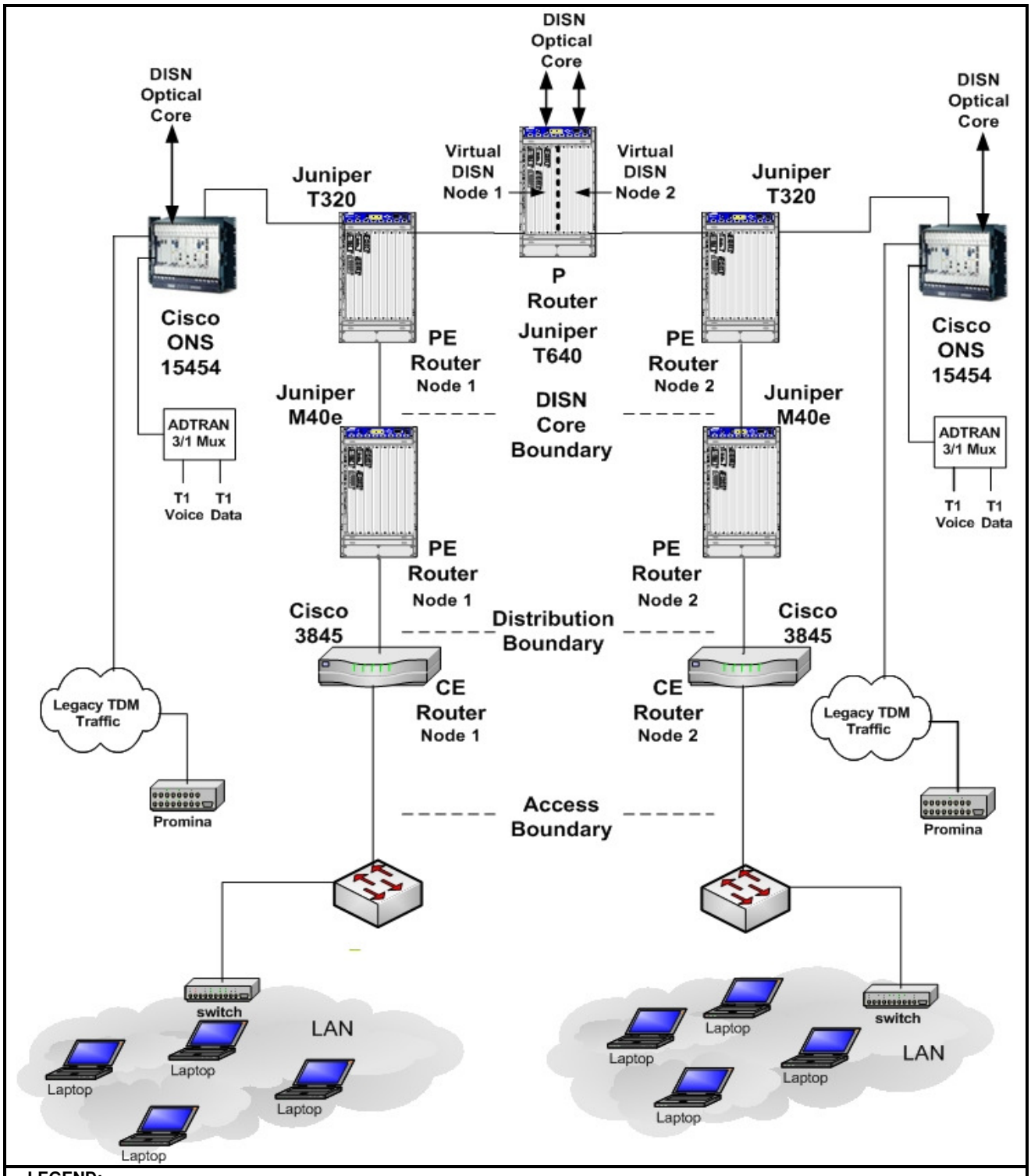


Figure D-1. Device Under Test



LEGEND:

CE	Customer Edge	ONS	Optical Network System
DISN	Defense Information Systems Network	P	Provider
IP	Internet Protocol	PE	Provider Edge
LAN	Local Area Network	TDM	Time Division Multiplexer
MUX	Multiplexer		

Figure D-2. Simulated DISN IP Core Test Network

Performance Test Summary

Bit Level Performance Test (Network Under Test)

These tests will be run using the Spirent Smartflow software on the SMB-6000 SmartBits Chassis or equivalent. The objective is to test the performance of a network under test from a bit loading/transfer point of view. The following parameters will be put in place, and the maximum loading effect of 1000 Megabits of bit traffic will be used to protect the integrity of the network under test. The frame sizes tested will be 64, 96, 128, 256, 512, 1024, 1280, and 1518 Bytes.

Protocol Level Performance Test

A 16-protocol IP Version 4 (IPv4) or IPv6 test was created using the Spirent SmartBits 6000, with Terametric 3325XD blades running Avalanche/Reflector Version 7.02 software. The client side (Avalanche) action script specifies that each user request for data (session) will result in a request for one of each of the following files: Hypertext Transfer Protocol (HTTP) 1.1, HTTP Secure 1.1, File Transfer Protocol (FTP), Telnet, Domain Name Server (DNS) A, DNS AAAA, Real-Time Streaming Protocol (RTSP), Real Networks streaming audio and video, Quick Time RTSP, Post Office Protocol Version 3 (PoP3), Simple Mail Transfer Protocol (SMTP), Microsoft Management system, Session Initiation Protocol, Simple Network Management Protocol (SNMP), IP Security (IPSec), and Multicast. The client load generator will be set to a value of 60 seconds to reach a beginning level of 50 simultaneous sessions. Then, every 16 seconds for 10 steps, the generator will add another 10 users until 220 seconds into the test; the generator will be carrying 150 simultaneous users. This load level will be held for 400 seconds and then allowed to decrease over a period of 160 seconds while Transmission Control Protocol connections are permitted to close. A representation of this routine is in Figure D-3.

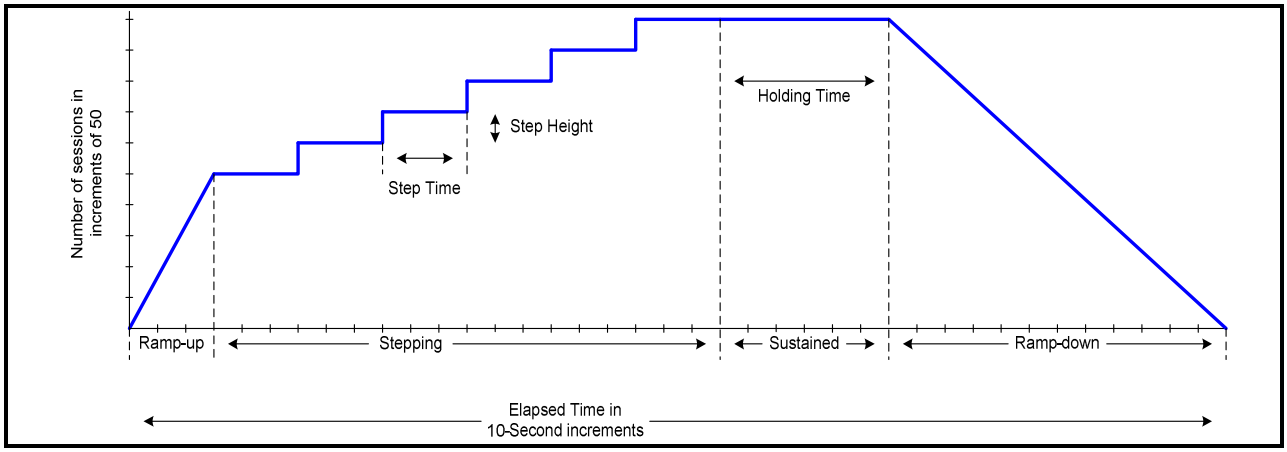


Figure D-3. Protocol Performance Test - Client Loading Routine

Routing Protocols Performance Test

Two ports are used on the tester and the DUT; the Quality of Service (QoS) test requires three ports to validate packet forwarding and processing in oversubscribed conditions. When modular DUTs are tested, these ports should be on separate cards.

The tests described in the subsequent pages will use Gigabit Ethernet ports (fiber or copper). However, all of these methodologies are equally applicable for other types of interfaces.

Tests will be conducted using IPv4 (to establish baselines), IPv6 and combined IPv4/IPv6 data and control plane traffic. The primary metrics will focus on data plane throughput, packet loss, latency, and packet ordering. Refer to Appendix G for templates to facilitate quick data analysis.

Equipment Requirements:

Each test will require a SmartBits 600 or 6000, with two 4-port TeraMetrics XD modules. Dual media modules (fiber and copper) are recommended to accommodate either type of interface on the DUT. A copy of Smartflow, Avalanche Reflector, and TeraRoutingTester (TRT) software running on a high-performance Personal Computer (at least 1 Gigahertz Central Possessing Unit with at least 1 gigabyte of Random Access Memory) will also be necessary.

Test Methodology - IP Throughput and Latency for IPv4 and IPv6, and mixed IPv4 and IPv6

References: 1242 - Benchmarking Terminology for Network Interconnect Devices
2544 - Benchmarking Methodology for Network Interconnect Devices

Objective:

This test is designed to provide throughput and latency information for a single switch, router, DUT, or a network under test.

The throughput of a device or system is the maximum packet-forwarding rate for which the device or system will not drop any of the offered packets. Any packet loss can induce significant delays in the execution of upper layer applications; thus, knowing the maximum data rate a device or system can support without any packet loss is of crucial importance when judging the performance of a switch, router, or system of interconnected devices.

This test also determines the latency of a device or system (the time it takes a packet to travel through the device or system), calculated at the maximum forwarding rate for which no packet loss is experienced (throughput rate).

Overview:

To determine the throughput and latency of a DUT or network under test, a minimum of two test ports will be required. All ports will be connected to the DUT/network under test.

One or more test ports will act as data sources and will offer traffic to the DUT/network under test. The other port(s) will receive traffic from the DUT/network under test. The DUT/network under test must be configured so traffic offered by the data source will be forwarded to the receiver(s). A routing protocol is the simplest way to accomplish this, but other manual methods are also acceptable.

From the data source test ports, a predetermined number of packets will be offered to the DUT/network under test. The packets will be forwarded by the DUT/network under test to the receiver ports. The number of packets received will be compared with the quantity transmitted. If packet loss occurs, then the offered load rate is decreased and the test is repeated. If packet loss is not observed, then the test is repeated with an increased packet rate. By implementing a simple binary search pattern, the maximum rate for which no packet loss occurs can be recorded. This rate corresponds to the DUT/network under test's throughput or the first measurement of this test.

To calculate latency, a predefined test stream is delivered to the DUT/network under test from the source test ports at the calculated throughput rate. The transmitting timestamp, corresponding to when the test packet was emitted is subtracted from the receiving timestamp, and the resulting difference indicates the latency experienced by this packet. Multiple packets should be used to collect a valid statistical sample of latency measurements.

Both of these test methodologies will be repeated several times, modifying the input variables.

Baseline Test Steps:

- Configure the DUT/network under test so it will forward traffic from the source port to the receiver's port. A routing protocol (such as Border Gateway Protocol Multi-protocol Extensions (BGP4+)) is recommended for this purpose so that the tester can advertise the appropriate routes for each iteration of the test. However, static routes are also acceptable.
- Configure the test parameters:
  - Initial packet rate - 50 percent of the line rate.
  - Packet size - 64 bytes.
  - Packet quantity (for fixed duration tests only) - suggested starting point is 100,000.
  - IP version - start with IPv4 to establish a benchmark.

    - Test duration time - this can be a fixed duration or the test can be run interactively so that modifications can be made in real-time.
- Transmit packets from the source port. Measure the packet loss. If no loss occurs, increase the data rate incrementally (a binary search is recommended) until a loss is experienced or the maximum rate (line rate) is reached. If packet loss does occur during the first iteration, decrease the packet rate incrementally until no loss occurs. Record the maximum data rate at which no packet loss is experienced.
- Transmit an IPv4 packet stream at the maximum rate and measure the latency and jitter (deviation from the average latency).
- After the benchmarks for IPv4 are identified, repeat the test using IPv6 routes and packets.
- Transmit an IPv6 packet stream at the maximum rate and measure the latency and jitter (deviation from the average latency).
- After a benchmark for IPv6 is established, repeat the test using two data streams - one running IPv4 and one running IPv6. Transmit the streams at equal rates and determine the maximum throughput for dual stack operations.
    - Note that the results for this test iteration should be identified in two separate streams - one for each version of IP.
- Repeat the IPv6 benchmark test using packets with different prefix lengths (this probably will impact latency). Suggested prefix lengths are: 16, 32, 48, 64, 80, 96, 112, and 128 bits.
    - Repeat this test using multiple simultaneous streams with all of the different prefix values. Measure each stream's latency individually. Also see if this impacts the maximum throughput rate.
- Repeat the dual stack benchmark test using the different prefix values indicated.

Test Methodology - Packet Loss and Latency for IPv4 and IPv6, and mixed IPv4 and IPv6

References: 1242 - Benchmarking Terminology for Network Interconnect Devices
2544 - Benchmarking Methodology for Network Interconnect Devices

Objective:

This test determines the packet loss rate and latency for a single switch or router (DUT) or for a system of interconnected switches or routers (network under test) for various input data rates and packet sizes.

The packet loss rate of a device or system is the percentage of Layer-3 frames that were offered at the input of the device or system, but were not successfully forwarded by the device or system due to hardware or software limitations. Calculating the packet loss rate of a system under different load conditions (input data rate, packet size, and packet type) serves to evaluate how the system will perform under similar operational conditions in a production network.

This test also determines the latency of the device or system (the time it takes a packet to travel through the device or system) calculated from the various input data rates, for which packet loss may or may not be experienced.

Overview:

To determine the packet loss rate and latency of a DUT or network under test, a minimum of two test ports will be required. All ports will be connected to the DUT/network under test.

One or more test ports will act as data sources and will offer traffic to the DUT/network under test. The other port(s) will receive traffic from the DUT/network under test. The DUT/network under test must be configured so traffic offered by the data source will be forwarded to the receiver(s). A routing protocol is the simplest way to accomplish this, but other manual methods are also acceptable.

From the data sources, a predetermined number of packets will be offered to the DUT/network under test for a given amount of time. The packets will be forwarded by the DUT/network under test to the receiver ports. The number of packets received (RxPacketCount) will be compared to the number of packets transmitted from the source ports (TxPacketCount).

The packet loss rate is calculated using the following formula:

[TxPacketCount - RxPacketCount)*100]/TxPacketCount

The packet loss is calculated for input data rates starting with 100 percent of the maximum rate that can be offered from the source test ports. The input data is decremented and the test is repeated until there are two successive trials with no packet loss. The test may be stopped when the input data rate reaches a user-selected threshold beyond which no measurements are required. The amount by which the input rate is decremented should be at most 10 percent of the maximum input data rate, and it can be as low as 1 percent.

System latency is measured at every trial; thus, every input data rate is included.

To calculate latency, a predefined test stream is delivered to the DUT/network under test from the source test ports at the calculated throughput rate. The transmitting timestamp, corresponding to when the test packet was emitted is subtracted from the receiving timestamp, and the resulting difference indicates the latency experienced by this packet. Multiple packets should be used in order to collect a valid statistical sample of latency measurements.

Test Steps:

- Configure the DUT/network under test so that it will forward traffic from the source port to the receiver's port. A routing protocol (such as BGP4+) is recommended for this purpose so that the tester can advertise the appropriate routes for each iteration of the test. However, static routes are also acceptable.
- Configure the test parameters:
  - Initial packet rate - 100 percent of the line rate.
  - Initial packet size - 64 bytes.
  - Initial packet quantity (if a fixed duration test is going to be used).
  - IP version - start with IPv4 to establish a benchmark.
  - Test duration time for each iteration - this can be a fixed duration or the test can be run interactively so that modifications can be made in real-time (the latter alternative is highly recommended).
- Send IPv4 packets from the source port(s). It is recommended to start with the maximum packet rate supported by the test port(s). Measure the number of packets transmitted at the source port(s) and the number of packets that arrive at the receiver port(s).
- If no packet loss occurs, stop the test. Conduct a second iteration of the test at the same rate to verify that no packet loss occurs.
- If packet loss occurs, calculate the loss rate and latency. Then decrement the input data rate and repeat.
- Other iterations can also be conducted using different packet sizes.
- After a benchmark is established for the IPv4 traffic, repeat the test using IPv6. Calculate the loss rates and latency for each iteration.
- Repeat the test using two data streams. Both streams should be transmitted at equal data rates. One stream will generate IPv4 traffic and the other will generate IPv6 traffic.
- Repeat the IPv6 benchmark test using packets with different prefix lengths (this probably will impact latency). Suggested prefix lengths are: 16, 32, 48, 64, 80, 96, 112, and 128 bits.
  - Repeat this test using multiple simultaneous streams with all of the different prefix values. Measure each stream's latency individually. Also see if this impacts the maximum throughput rate.
- Repeat the dual stack benchmark test using the different prefix values indicated.

Test Methodology - Back-to-Back (Burst Size) Test for IPv4 and IPv6

References: 1242 - Benchmarking Terminology for Network Interconnect Devices
2544 - Benchmarking Methodology for Network Interconnect Devices

Objective:

This test determines the maximum number of packets a switch or router (DUT) or a system of interconnected switches or routers (network under test) can forward back-to-back without packet loss. The number of packets in the longest burst that does not cause packet loss is the back-to-back value.

In a back-to-back test, packets are delivered at full line rate with no pause between successive packets, except the required "legal" separation for a given technology or physical medium - such as the Ethernet inter-frame gap.

Overview:

To determine the back-to-back value of a DUT or network under test, a minimum of two test ports will be required. All ports will be connected to the DUT/network under test.

One or more test ports will act as data sources and will offer traffic to the DUT/network under test. The other port(s) will receive traffic from the DUT/network under test. The DUT/network under test must be configured so traffic offered by the data source will be forwarded to the receiver(s). A routing protocol is the simplest way to accomplish this, but other manual methods are also acceptable.

From the data source test port(s), a burst of back-to-back packets will be offered to the DUT/network under test. The packets will be forwarded by the DUT/network under test to the receiver ports. The quantity of packets received will be compared to the quantity transmitted. If packet loss occurs, then the burst size is decreased (the number of back-to-back packets is decreased) and the test is repeated. If no packet loss is observed, then the burst size is increased and the test is repeated. By implementing a binary search, the back-to-back value can be determined.

Test Steps:

- Configure the DUT/network under test so that it will forward traffic from the source port to the receiver's port. A routing protocol (such as BGP4+) is recommended for this purpose so that the tester can advertise the appropriate routes for each iteration of the test. However, static routes are also acceptable.
- Configure the test parameters:
  - Initial packet rate - 100 percent of the line rate.
  - Packet size - 64 bytes.
  - IP version - start with IPv4 to establish a benchmark.
  - Burst size - recommended starting point is 100,000 packets.
  - Burst increment/decrement resolution (for a binary search).

- Send a burst of packets from the source port(s) for an extended duration (ten minutes is suggested). Measure the number of packets transmitted by the source port(s) and the quantity received at the destination port(s).
- If no packet loss occurs, the DUT/network under test can handle back-to-back packets at full line rate; thus, there is no burst size limitation. Stop the test.
- If packet loss occurs, generate another burst of packets at the initial burst size. If packet loss occurs again, decrease the burst size and repeat.
- Continue the binary search algorithm until the maximum burst size with no packet loss is determined.
- Repeat steps 2 - 6 using IPv6.
- Repeat steps 2 - 6 using two streams of packets – one stream will offer IPv4 packets at 50 percent of the line rate and the other will offer IPv6 packets at 50 percent of the line rate.
- Repeat steps 2 - 6 using IPv6 streams with different prefix lengths. The following prefix lengths are recommended: 16, 32, 48, 64, 80, 96, 112 and 128 bits.
- Repeat the dual stack measurements using various IPv6 prefix lengths.

Test Methodology - QoS for IPv4 and IPv6 and mixed IPv4 and IPv6

Objective:

This test will validate the DUT or network under test's ability to correctly process IPv4 and IPv6 packets with varying QoS requirements. The Type of Service (ToS) and Differentiated Services Code Points (DSCPs) parameters in the IPv6 "Traffic Class" field will be modified for separate data streams. These streams will be tracked individually and measured for data throughput, loss and latency. The DUT will be tested in under-subscribed, full bandwidth and over-subscribed conditions. The IPv4 traffic will then be mixed with the IPv6 data to validate the impact on QoS in dual traffic environments.

Overview:

To determine the ability of a DUT or network under test to correctly process IPv4 and IPv6 QoS parameters, a minimum of three test ports will be necessary. All ports will be directly connected to the DUT/network under test. Additional ports can also be used to further increase the level of stress on the DUT/network under test.

This is a complex test. The QoS parameters and processes generally need to be set manually, meaning that the proper procedure for each different ToS or DSCP value must be preset. Furthermore, some DUTs may offer several alternatives for queuing algorithms, so the user will need to select the appropriate methods for their test, or possibly conduct multiple iterations of this test to validate several different policing and queuing algorithms.

Two test ports will act as data sources and will offer several traffic streams with various QoS (ToS or DSCP) levels to the DUT/network under test. The other port will

receive traffic from the DUT/network under test. The DUT/network under test must be configured so traffic offered by the data sources will be forwarded to the receiver(s). A routing protocol is the simplest way to accomplish this, but other manual methods are also acceptable.

From the data source test ports, several continuous streams of packets will be offered to the DUT/network under test. These packets will have various QoS markings, and should be treated differently by the DUT/network under test. The packets will be forwarded by the DUT/network under test to the receiver port. The received streams will be individually analyzed based upon the configured QoS values. All traffic should be successfully delivered in an undersubscribed or line-rate situation. However, when the input traffic is increased to oversubscribe the output port, packets must be dropped. The policing algorithms of the DUT will determine how and when this occurs.

The configuration for this test is presented in Figure D-4. In a baseline test, three test ports are used. The test ports shown on the left-hand side of the diagram are the data sources while the port on the right-hand side is the receiver. For more complex (and thorough) tests, multiple transmitting and receiving ports can be used.

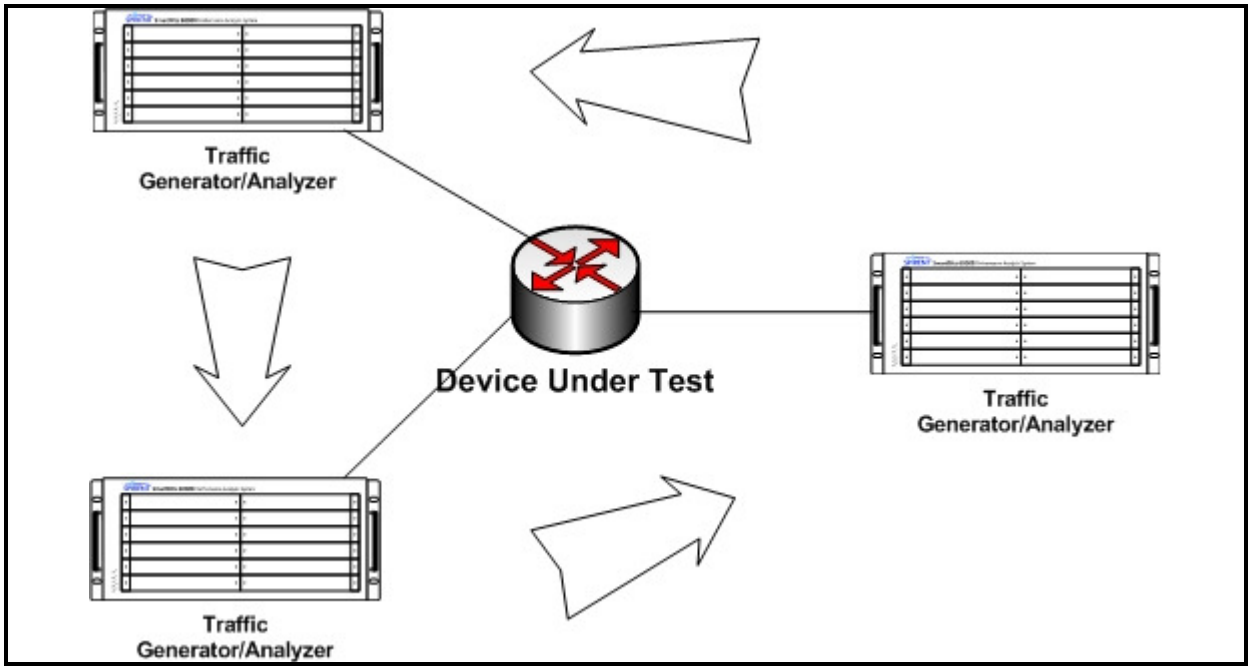


Figure D-4. Quality of Service Testing Concept

Test Steps:

- Configure the DUT so that it will forward traffic from the source ports to the receiver's port. A routing protocol (such as BGP4+) is recommended for this purpose so that the tester can advertise the appropriate routes for each iteration of the test. However, static routes are also acceptable.

- Configure the ToS and/or DSCP values for the DUT in accordance with prescribed policy. Identify the quantity of settings that will be tested and the correct treatment for each setting. These can be hierarchical levels of priority and strict queuing (which could ultimately lead to queue starvation for the low priority traffic) or specific weights can be assigned to each queue (perhaps reserving 5 percent of the bandwidth for the lowest priority traffic).
- Configure the following test parameters:
  - Packet size - 64 bytes.
  - Stream quantity - use at least three; more are preferable.
  - Initial packet rate - the aggregate rate for all of the input streams should begin at 50 percent of the line rate of the receiver port. Note that the transmit rates do not need to be the same for each individual stream or QoS value.
  - IP DSCP or ToS parameters for each stream.
  - IP version - start with IPv4 to establish a benchmark.
  - Test duration time - this can be a fixed duration or the test can be run interactively so that modifications can be made in real-time (this is the preferable mode).
  - Ensure that the results will be graphed and logged on a *per-stream* basis so that the tester will have a good view of each QoS level.
  - Transmit packets from the source ports. Measure the throughput, loss and latency associated with each stream. It is recommended that the streams be tracked based upon the QoS settings.
- Increase the input packet rate to equal 100 percent of the receiver port's capacity. At this point, all traffic should still arrive at the output port. If not, validate the policing functions for 100 percent loading.
- Increase the input rate to equal 150 percent of the receiver port's capacity. Now policing will be necessary. Some manual calculations (based upon the DUT's particular bandwidth and queue management algorithms) may be required to predict the policing behavior. Validate the policing functions. Also check to see if the policing activities have impacted the packet latency of the DUT.
- After benchmarks for IPv4 are established, repeat the test using similar IPv6 parameters. Many DUTs cannot forward IPv6 traffic at line-rate, so some policing is likely to be observed during the iteration using 100 percent of the output bandwidth.
  - If any latency discrepancies are observed, repeat the test using different IPv6 prefix lengths, and see if these changes affect the results.
  - Repeat the test using more input streams (up to eight ToS settings or 12 DSCP options are possible).
  - Repeat the test using combined IPv4 and IPv6 settings. Compare the loss and latency for each version of IP.
  - If multiple different queuing algorithms are used by the DUT, repeat these tests for each option.

APPENDIX E

TEST CONFIGURATION DIAGRAMS

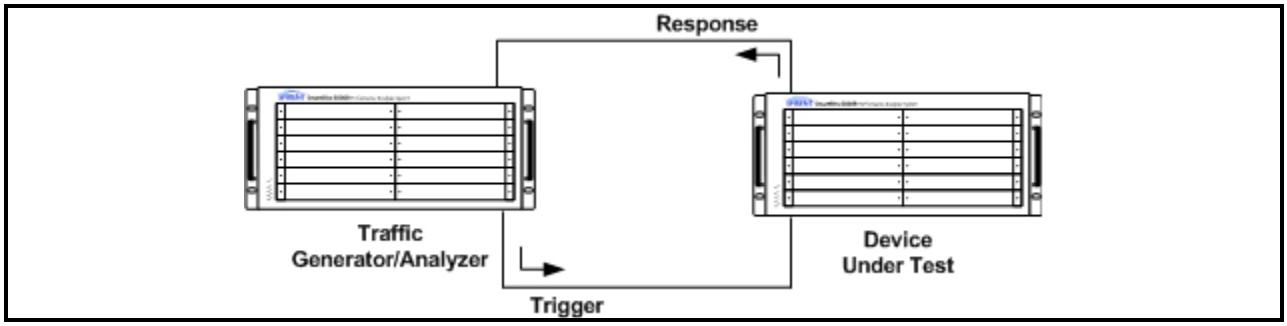


Figure E-1. Traffic Generator/Analyzer

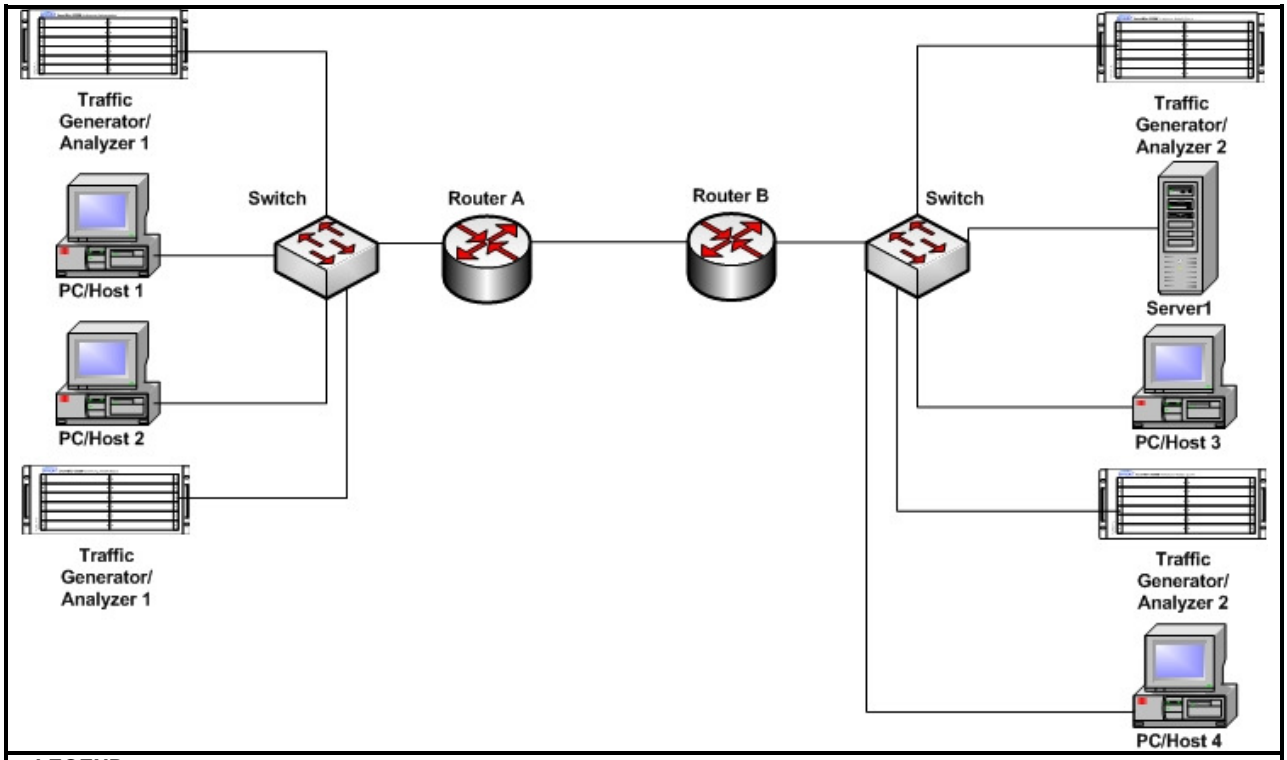
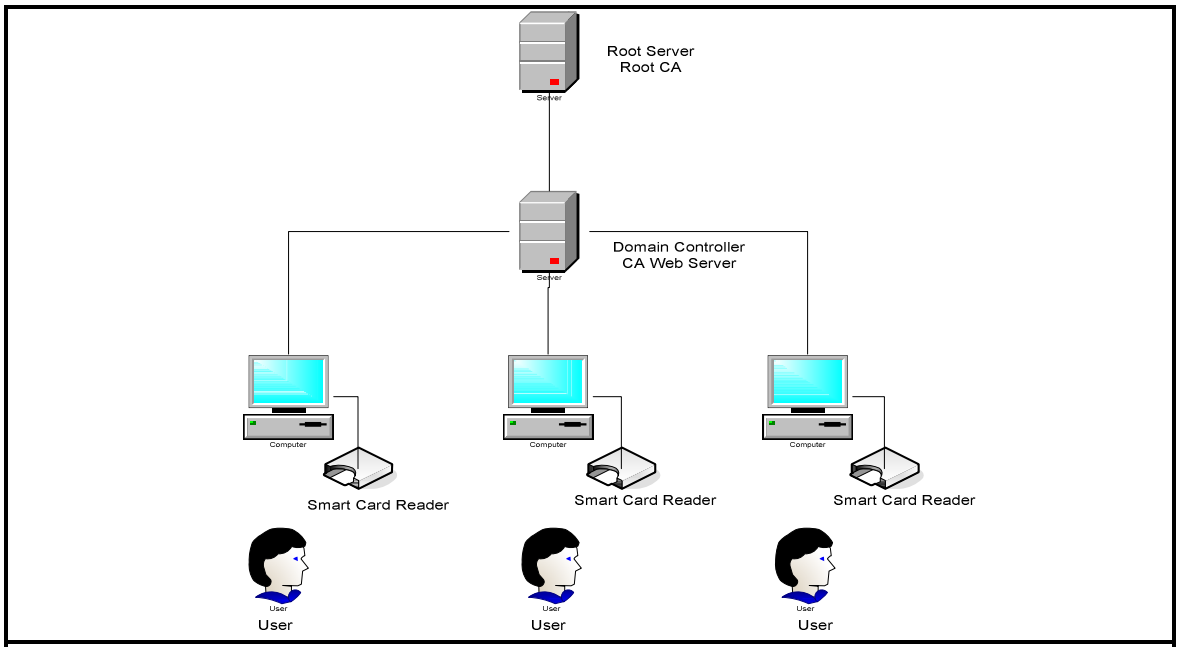


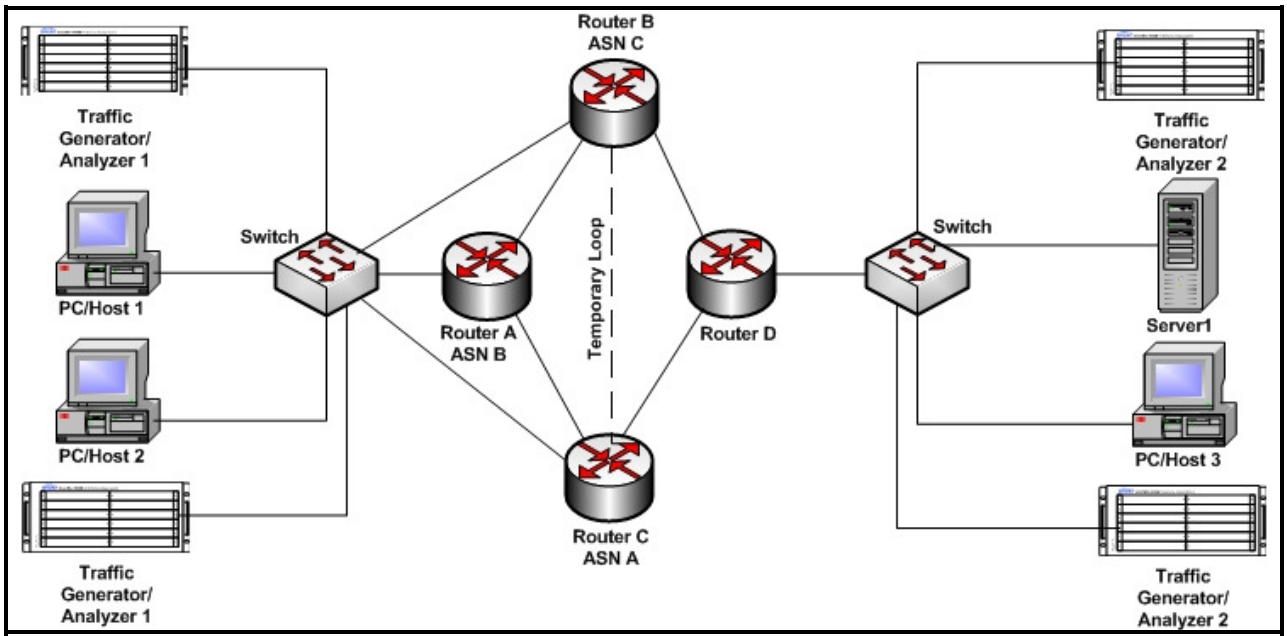
Figure E-2. Conceptual Test Drawing



LEGEND:

CA	Certificate Authority	PKI	Public Key Infrastructure
IPSec	Internet Protocol Security		

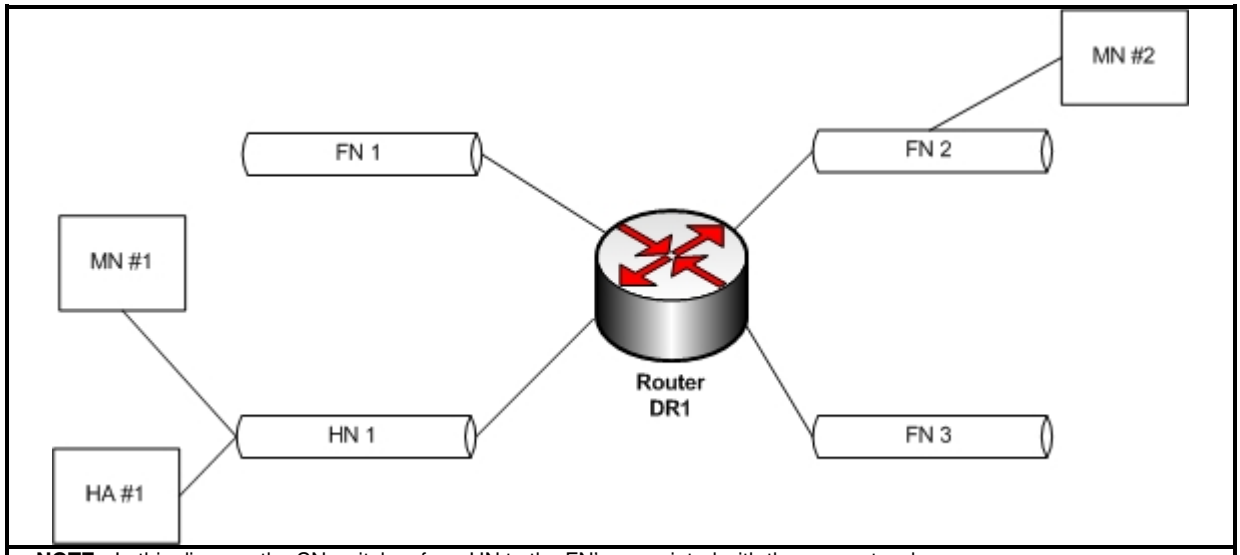
Figure E-3. PKI and IPSec Test Network Topology



LEGEND:

ASN	Autonomous System Number	PC	Personal Computer

Figure E-4. Routing Protocol Diagram

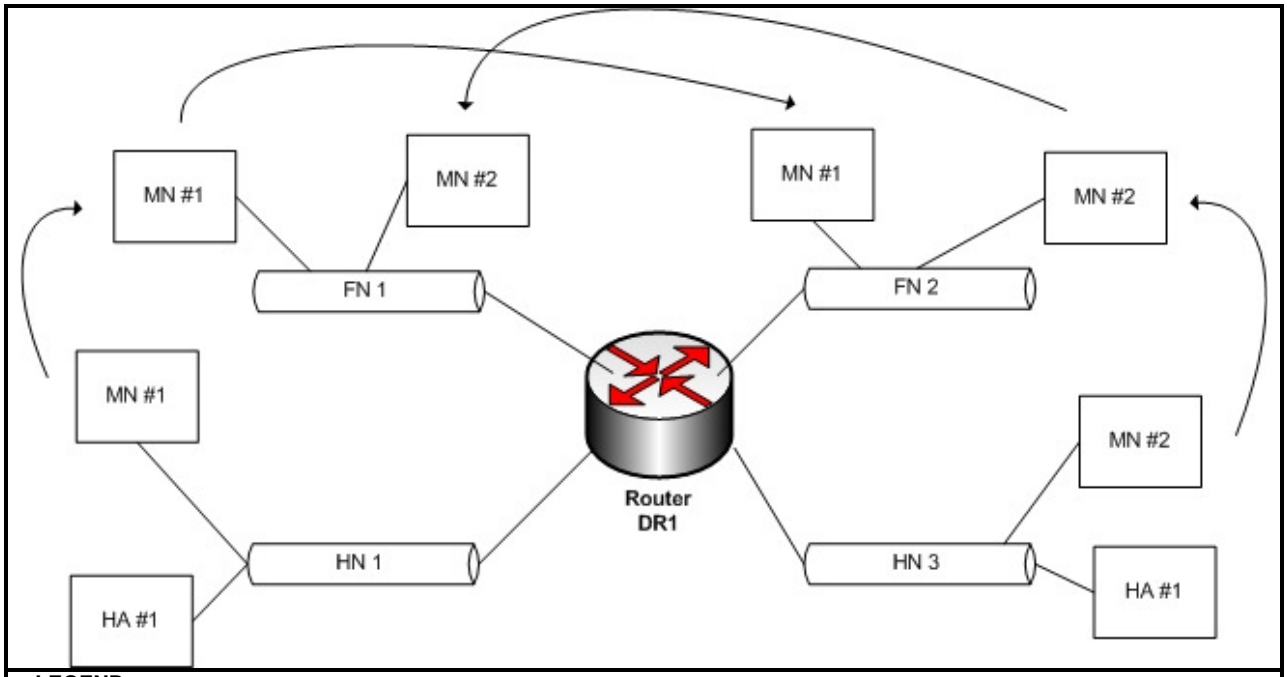


NOTE: In this diagram the CN switches from HN to the FN's associated with the new network.

LEGEND:

CN	Correspondent Node	HA	Home Agent
DR	Designated Router	HN	Home Network
FN	Foreign Network	MN	Mobile Node

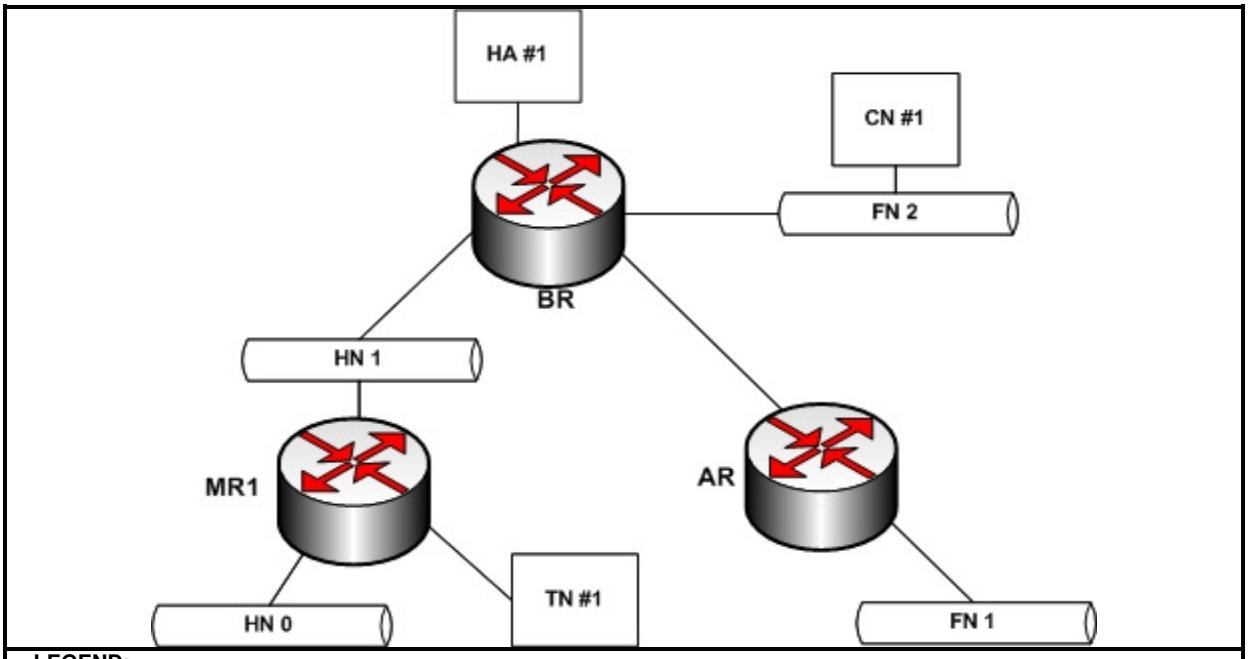
Figure E-5. MN to CN Communication



LEGEND:

DR	Designated Router	HN	Home Network
FN	Foreign Network	MN	Mobile Node
HA	Home Agent		

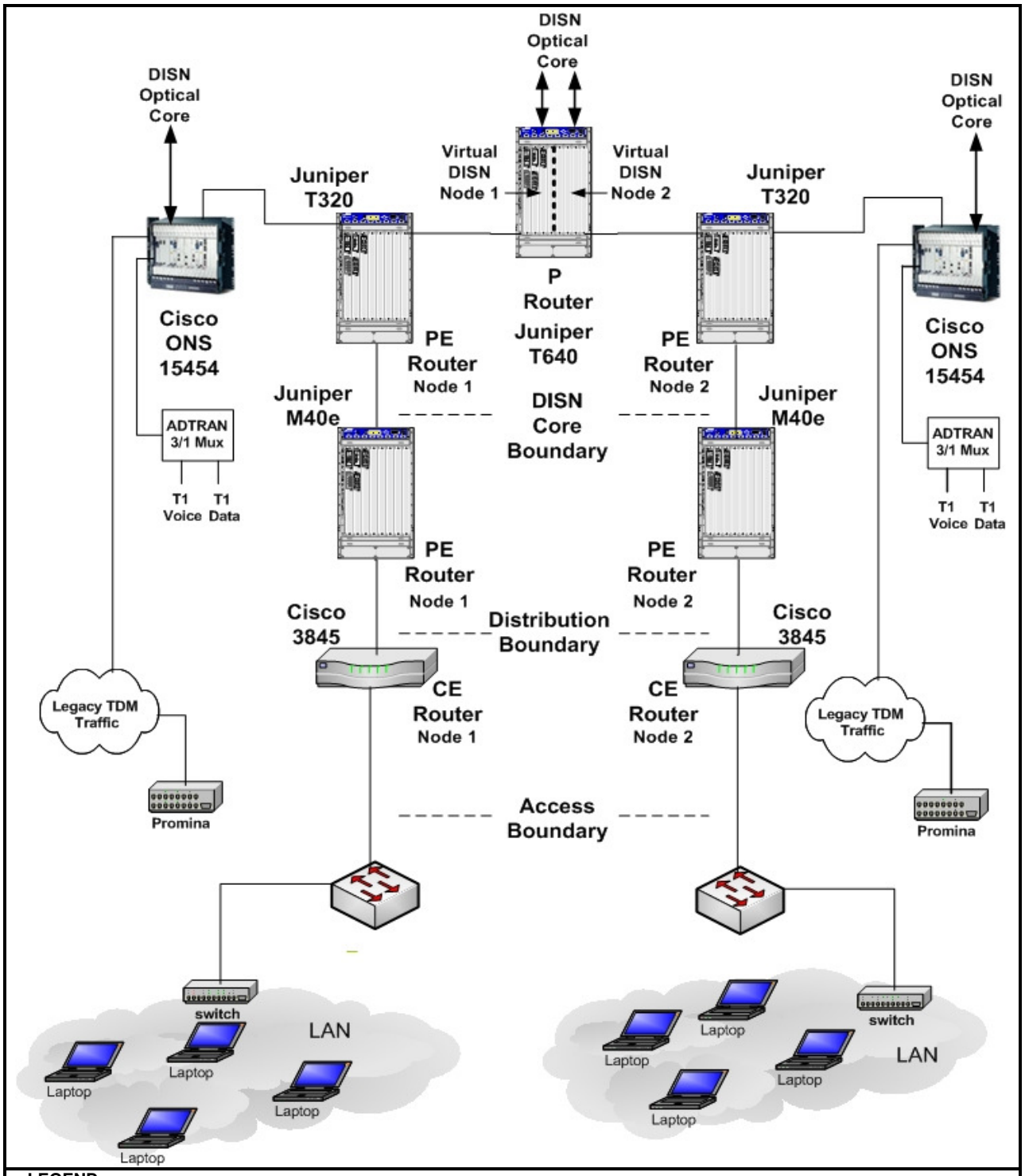
Figure E-6. MN to MN Communication



LEGEND:

AR	Area Router	HA	Home Agent
BR	Border Router	HN	Home Network
CN	Correspondent Node	MR	Mobile Router
FN	Foreign Network	TN	Test Node

Figure E-7. Network Mobility



LEGEND:

CE	Customer Edge	ONS	Optical Network System
DISN	Defense Information Systems Network	P	Provider
IP	Internet Protocol	PE	Provider Edge
LAN	Local Area Network	TDM	Time Division Multiplexer
MUX	Multiplexer		

Figure E-8. Simulated DISN IP Core Test Network

(This page intentionally left blank.)

APPENDIX F

LETTER OF CONFORMANCE CHECKLIST

This checklist is provided to allow vendors to pretest all devices for Internet Protocol (IP) Version 6 (IPv6) conformance to various Request for Comments (RFC) prior to interoperability and performance testing. These checklists are the minimum required RFCs needed to verify each device type before formal interoperability and performance testing.

- Host and Workstation Checklist
- Network Appliance Checklist
- Simple Server Appliance Checklist
- Advanced Server Appliance Checklist
- Router Checklist
- Layer-3 Switch Checklist
- Information Assurance: Firewall Checklist
- Information Assurance: IPS/IDS Checklist

The following is a description of all the Department of Defense (DoD) Information Technology Standards Registry (DISR) requirements terms as referenced in the DoD IPv6 Standards Profiles for IPv6 Capable Products, Version 3.0.

INFORMATIONAL: Useful information that is not generally required but permitted for use.

EMERGING: A new or evolving standard that is likely to eventually be MANDATED.

MANDATED: A mature standard that can be cited as a requirement in acquisition; typically several vendor implementations already exist.

MUST: This term indicates an imperative; the requirement is essential to IPv6 capability and interoperability. This level of requirement is indicated in the DISR by MANDATED. Synonyms used elsewhere include SHALL or REQUIRED.

MUST NOT: This term indicates an absolute prohibition of a behavior. A synonym is SHALL NOT.

SHOULD: This term indicates a desirable or expected course of action or policy that is to be followed unless inappropriate or cost-prohibitive for a particular circumstance. This corresponds to the EMERGING level in the DISR.

SHOULD NOT: This term is used to indicate a desirable or expected that the particular behavior is discouraged though not prohibited. There may be valid reasons in particular

circumstances when the behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing.

MAY: This term denotes the permissive or an item is truly optional. An implementation which does not include a particular option MUST interoperate with another implementation which does include the option. In the same vein, an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (in both cases without the feature the option provides). Normally standards that a product MAY follow would be listed in the DISR as INFORMATIONAL.

SHOULD+: This term indicates a near-term goal for technology insertion that is strongly expected to be elevated to a MUST or MANDATED in the near future. SHOULD+ means a strongly recommended and expected course of action or policy that is to be followed unless inappropriate for a particular circumstance. This term is normally associated with an EMERGING specification in the DISR.

Host/Workstation Requirements

IPv6 Base

- RFC 1981 Path MTU Discovery for IPv6
- RFC 2460 Internet Protocol v6 (IPv6) Specification
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- RFC 4861 Neighbor Discovery for IPv6
  - RFC 2461 Neighbor Discovery for IPv6 is acceptable until July 2009
- RFC 4862 IPv6 Stateless Address Auto-configuration
  - RFC 2462 IPv6 Stateless Address Auto-configuration is acceptable until July 2009
  - Only link-local addresses and Duplicate Address Detection
  - Section 5.5 Disable auto-configuration
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4443 Internet Control Message Protocol (ICMPv6)
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
- Listener mode
- RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6
- Listener mode

(Required support for at least one of the below)

- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 2467 Transmission of IPv6 Packets over FDDI Networks
- RFC 5072 IP Version 6 over PPP
- RFC 2472 IP Version 6 over PPP is acceptable until July 2009
- RFC 3572 IPv6 over MAPOS (Multiple Access Protocol over SONET/SDH) (JITC Recommended)

Optional additional connection technologies)

- RFC 2491 IPv6 Over Non-Broadcast Multiple Access (NBMA) Networks
- RFC 2492 IPv6 over ATM Networks January 1999
- RFC 2497 Transmission of IPv6 Packets over ARCnet Networks
- RFC 2590 Transmission of IPv6 Packets over Frame Relay Networks Specification
- RFC 3146 Transmission of IPv6 over IEEE 1394 Networks
- RFC 4338 Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel

IPv6 Address Autoconfiguration: Can be one of the below options

- RFC 4862/2462 IPv6 Stateless Address Auto-configuration
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

IPSec

- RFC 4301 Security Architecture for the Internet Protocol
- (Optional) RFC 4302 IP Authentication Header (AH)
- RFC 4303 IP Encapsulating Security Payload (ESP)

- RFC 4835 (ESP and AH) Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4305 (ESP and AH) Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) is acceptable until July 2009
- RFC 4308 Cryptographic Suites for IPsec (July 2009 In-Effect Date)
- RFC 4869 Suite B Cryptographic Suites for IPsec (July 2009 In-Effect Date)

IPSec Fallback: If product cannot comply with 43XX Series of IPSec, then 24XX Series is acceptable

- RFC 2401 Security Architecture for the Internet Protocol
- (Optional) RFC 2402 IP Authentication Header (AH)
- RFC 2406 IP Encapsulating Security Payload (ESP)

IKEv1

- RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 4109 Algorithms for Internet Key Exchange Version 1 (IKEv1)

IKEv2: If product supports IKEv2, it must also support IKEv1 for backwards compatibility. In effect date for IKEv2 support is July 2010

- RFC 4306 Internet Key Exchange (IKEv2) Protocol
- RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)

Transition Mechanisms

- RFC 4213 Transition Mechanisms for IPv6 Host and Routers

Common Network Applications

- RFC 3986 Uniform Resource Identifier (URI): Generic Syntax
- RFC 3484 Default Address Selection for IPv6
- RFC 3596 DNS Extensions to Support IPv6 (Hosts must be capable of using IPv6 DNS)
- (Optional) RFC 3041 Privacy Extensions for Stateless Address Auto-configuration in IPv6

Please refer to the DoD IPv6 Standard Profiles for IPv6 Capable Products Version 3.0, for SHOULD+ and SHOULD device requirements.

Network Appliance Requirements

IPv6 Base

- RFC 2460 Internet Protocol v6 (IPv6) Specification
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- RFC 4861 Neighbor Discovery for IPv6
  - RFC 2461 Neighbor Discovery for IPv6 is acceptable until July 2009
- RFC 4862 IPv6 Stateless Address Auto-configuration
  - RFC 2462 IPv6 Stateless Address Auto-configuration is acceptable until July 2009
  - Only link-local addresses and Duplicate Address Detection
  - Section 5.5 Disable auto-configuration
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4443 Internet Control Message Protocol (ICMPv6)
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
  - Listener mode

(Required support for at least one of the below)

- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 2467 Transmission of IPv6 Packets over FDDI Networks
- RFC 5072 IP Version 6 over PPP
  - RFC 2472 IP Version 6 over PPP is acceptable until July 2009
- RFC 3572 IPv6 over MAPOS (Multiple Access Protocol over SONET/SDH) (JITC Recommended)

Optional additional connection technologies)

- RFC 2491 IPv6 Over Non-Broadcast Multiple Access (NBMA) Networks
- RFC 2492 IPv6 over ATM Networks January 1999
- RFC 2497 Transmission of IPv6 Packets over ARCnet Networks
- RFC 2590 Transmission of IPv6 Packets over Frame Relay Networks Specification
- RFC 3146 Transmission of IPv6 over IEEE 1394 Networks
- RFC 4338 Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel

IPv6 Address Auto-configuration: Can be one of the below options

- RFC 4862/2462 IPv6 Stateless Address Auto-configuration
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

Please refer to the DoD IPv6 Standard Profiles for IPv6 Capable Products Version 3.0, for SHOULD+ and SHOULD device requirements.

Simple Server Requirements (Network Appliance plus a network service)

IPv6 Base

- RFC 2460 Internet Protocol v6 (IPv6) Specification
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- RFC 4861 Neighbor Discovery for IPv6
  - RFC 2461 Neighbor Discovery for IPv6 is acceptable until July 2009
- RFC 4862 IPv6 Stateless Address Auto-configuration
  - RFC 2462 IPv6 Stateless Address Auto-configuration is acceptable until July 2009
  - Only link-local addresses and Duplicate Address Detection
  - Section 5.5 Disable auto-configuration
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4443 Internet Control Message Protocol (ICMPv6)
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
  - Listener mode

(Required support for at least one of the below)

- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 2467 Transmission of IPv6 Packets over FDDI Networks
- RFC 5072 IP Version 6 over PPP
  - RFC 2472 IP Version 6 over PPP is acceptable until July 2009
- RFC 3572 IPv6 over MAPOS (Multiple Access Protocol over SONET/SDH) (JITC Recommended)

Optional additional connection technologies)

- RFC 2491 IPv6 Over Non-Broadcast Multiple Access (NBMA) Networks
- RFC 2492 IPv6 over ATM Networks January 1999
- RFC 2497 Transmission of IPv6 Packets over ARCnet Networks
- RFC 2590 Transmission of IPv6 Packets over Frame Relay Networks Specification
- RFC 3146 Transmission of IPv6 over IEEE 1394 Networks
- RFC 4338 Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel

IPv6 Address Auto-configuration: Can be one of the below options

- RFC 4862/2462 IPv6 Stateless Address Auto-configuration
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

IPv6 Service: Device must run an embedded network service in order to be classified as a Simple Server. Below are some examples of some.

- RFC 4330, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OS
- RFC 3596, DNS Extensions to Support IPv6
- RFC 3226, DNS Security and IPv6 Aware Server/Resolver Message Size Requirements
- RFC 3261, Session Initiation Protocol (SIP)

- Section 2.9.3 Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Server
- Section 2.9.4 DHCPv6 Relay Agent
- RFC 3053, IPv6 Tunnel Broker
- RFC 3162, RADIUS (Remote Authentication Dial In User Service) and IPv6
- RFC 2911, Internet Printing Protocol (IPP)
- RFC 2821, Simple Mail Transfer Protocol (SMTP)
- RFC 2428, FTP Extensions for IPv6 and NATs; Server must be capable of transferring files with IPv6 and support Extended Data Port (EPRT) and Extended Passive (EPSV) commands
- Standard 9/RFC 959, File Transfer Protocol (FTP)

Please refer to the DoD IPv6 Standard Profiles for IPv6 Capable Products Version 3.0 for SHOULD+ and SHOULD device requirements.

Advanced Server Requirements

IPv6 Base

- RFC 1981 Path MTU Discovery for IPv6
- RFC 2460 Internet Protocol v6 (IPv6) Specification
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- RFC 4861 Neighbor Discovery for IPv6
  - RFC 2461 Neighbor Discovery for IPv6 is acceptable until July 2009
- RFC 4862 IPv6 Stateless Address Auto-configuration
  - RFC 2462 IPv6 Stateless Address Auto-configuration is acceptable until July 2009
  - Only link-local addresses and Duplicate Address Detection
  - Section 5.5 Disable auto-configuration
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4443 Internet Control Message Protocol (ICMPv6)
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
  - Listener mode
- RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6
  - Listener mode

(Required support for at least one of the below)

- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 2467 Transmission of IPv6 Packets over FDDI Networks
- RFC 5072 IP Version 6 over PPP
  - RFC 2472 IP Version 6 over PPP is acceptable until July 2009
- RFC 3572 IPv6 over MAPOS (Multiple Access Protocol over SONET/SDH) (JITC Recommended)

Optional additional connection technologies)

- RFC 2491 IPv6 Over Non-Broadcast Multiple Access (NBMA) Networks
- RFC 2492 IPv6 over ATM Networks January 1999
- RFC 2497 Transmission of IPv6 Packets over ARCnet Networks
- RFC 2590 Transmission of IPv6 Packets over Frame Relay Networks Specification
- RFC 3146 Transmission of IPv6 over IEEE 1394 Networks
- RFC 4338 Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel

IPv6 Address Auto-configuration: Can be one of the below options

- RFC 4862/2462 IPv6 Stateless Address Auto-configuration
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

IPSec

- RFC 4301 Security Architecture for the Internet Protocol
- (Optional) RFC 4302 IP Authentication Header (AH)
- RFC 4303 IP Encapsulating Security Payload (ESP)

- RFC 4835 (ESP and AH) Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
  - RFC 4305 (ESP and AH) Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) is acceptable until July 2009
- RFC 4308 Cryptographic Suites for IPsec (July 2009 In-Effect Date)
- RFC 4869 Suite B Cryptographic Suites for IPsec (July 2009 In-Effect Date)

IPSec Fallback: If product cannot comply with 43XX Series of IPSec, then 24XX Series is acceptable

- RFC 2401 Security Architecture for the Internet Protocol
- (Optional) RFC 2402 IP Authentication Header (AH)
- RFC 2406 IP Encapsulating Security Payload (ESP)

IKEv1

- RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 4109 Algorithms for Internet Key Exchange Version 1 (IKEv1)

IKEv2: If product supports IKEv2, it must also support IKEv1 for backwards compatibility. In effect date for IKEv2 support is July 2010

- RFC 4306 Internet Key Exchange (IKEv2) Protocol
- RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)

Transition Mechanisms

- RFC 4213 Transition Mechanisms for IPv6 Host and Routers

Common Network Applications

- RFC 3986 Uniform Resource Identifier (URI): Generic Syntax
- RFC 3484 Default Address Selection for IPv6
- RFC 3596 DNS Extensions to Support IPv6 (Hosts must be capable of using IPv6 DNS)
- (Optional) RFC 3041 Privacy Extensions for Stateless Address Auto-configuration in IPv6

IPv6 Service: Device must run multiple "services" in order to be classified as an Advanced Server. Below are some examples of some.

- RFC 4330, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OS
- RFC 3596, DNS Extensions to Support IPv6
- RFC 3226, DNS Security and IPv6 Aware Server/Resolver Message Size Requirements

- RFC 3261, Session Initiation Protocol (SIP)
- Section 2.9.3 Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Server
- Section 2.9.4 DHCPv6 Relay Agent
- RFC 3053, IPv6 Tunnel Broker
- RFC 3162, RADIUS (Remote Authentication Dial In User Service) and IPv6
- RFC 2911, Internet Printing Protocol (IPP)
- RFC 2821, Simple Mail Transfer Protocol (SMTP)
- RFC 2428, FTP Extensions for IPv6 and NATs; Server must be capable of transferring files with IPv6 and support Extended Data Port (EPRT) and Extended Passive (EPSV) commands
- Standard 9/RFC 959, File Transfer Protocol (FTP)

Please refer to the DoD IPv6 Standard Profiles for IPv6 Capable Products Version 3.0 for SHOULD+ and SHOULD device requirements.

Router Requirements (Intermediate Node)

IPv6 Base

- RFC 1981 Path MTU Discovery for IPv6
  - Function to issue "packet too big" message
- RFC 2460 Internet Protocol v6 (IPv6) Specification
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- RFC 4861 Neighbor Discovery for IPv6
  - RFC 2461 Neighbor Discovery for IPv6 is acceptable until July 2009
- RFC 4862 IPv6 Stateless Address Auto-configuration
  - RFC 2462 IPv6 Stateless Address Auto-configuration is acceptable until July 2009
  - Only link-local addresses and Duplicate Address Detection
  - Section 5.5 Disable auto-configuration
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4443 Internet Control Message Protocol (ICMPv6)
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
  - Router and/or Listener mode
- RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6
  - Router and/or Listener mode

(Required support for at least one of the below)

- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 2467 Transmission of IPv6 Packets over FDDI Networks
- RFC 5072 IP Version 6 over PPP
  - RFC 2472 IP Version 6 over PPP is acceptable until July 2009
- RFC 3572 IPv6 over MAPOS (Multiple Access Protocol over SONET/SDH) (JITC Recommended)

Optional additional connection technologies)

- RFC 2491 IPv6 Over Non-Broadcast Multiple Access (NBMA) Networks
- RFC 2492 IPv6 over ATM Networks January 1999
- RFC 2497 Transmission of IPv6 Packets over ARCnet Networks
- RFC 2590 Transmission of IPv6 Packets over Frame Relay Networks Specification
- RFC 3146 Transmission of IPv6 over IEEE 1394 Networks
- RFC 4338 Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel

IPv6 Address Auto-configuration: Can be one of the below options

- RFC 4862/2462 IPv6 Stateless Address Auto-configuration
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
  - Server mode
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
  - Relay mode

IPSec

- RFC 4301 Security Architecture for the Internet Protocol
- (Optional) RFC 4302 IP Authentication Header (AH)
- RFC 4303 IP Encapsulating Security Payload (ESP)
- RFC 4835 (ESP and AH) Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
  - RFC 4305 (ESP and AH) Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) is acceptable until July 2009
- RFC 4308 Cryptographic Suites for IPsec (July 2009 In-Effect Date)
- RFC 4869 Suite B Cryptographic Suites for IPsec (July 2009 In-Effect Date)

IPSec Fallback: If product cannot comply with 43XX Series of IPSec, then 24XX Series is acceptable

- RFC 2401 Security Architecture for the Internet Protocol
- (Optional) RFC 2402 IP Authentication Header (AH)
- RFC 2406 IP Encapsulating Security Payload (ESP)

IKEv1

- RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 4109 Algorithms for Internet Key Exchange Version 1 (IKEv1)

IKEv2: If product supports IKEv2, it must also support IKEv1 for backwards compatibility. In effect date for IKEv2 support is July 2010

- RFC 4306 Internet Key Exchange (IKEv2) Protocol
- RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)

Transition Mechanisms

- RFC 4213 Transition Mechanisms for IPv6 Host and Routers
  - Dual-Stack function required
  - Configured function required
- (Conditional) RFC 2473 Generic Packet Tunneling in IPv6 Specification
- (Conditional) RFC 2784 Generic Router Encapsulation (GRE):

Quality of Service

- RFC 2474 Definition of the DiffServ Field in the IPv4 and IPv6 Headers

Mobility *(Only if router functions as a Home Agent)*

- RFC 3775 Mobility Support in IPv6
- RFC 3776 Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents

- RFC 3963 Network Mobility (NEMO) Basic Support Protocol
- RFC 4295 Mobile IP Management MIB

Net Management

- RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
- SNMPv3 operation over IPv6 (July 2010 In-Effect Date)
- RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413 SNMP Applications

Management Information Base (MIBs)

- RFC 3595 Textual Conventions for IPv6 Flow Label
- RFC 4022 Management Information Base for the Transmission Control Protocol
- RFC 4113 Management Information Base for the User Datagram Protocol
- RFC 4293 Management Information Base (MIB) for IP
- RFC 4292 IP Forwarding Table MIB

Interior Routers

- RFC 2740 OSPF for IPv6
- (Conditional) RFC 4552 Authentication/Confidentiality for OSPFv3

Exterior Router

- RFC 4271 A Border Gateway Protocol 4 (BGP-4)
- RFC 1772 Application of the Border Gateway Protocol in the Internet
- RFC 2545 Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
- RFC 4760 Multiprotocol Extensions for BGP-4

Please refer to the DoD IPv6 Standard Profiles for IPv6 Capable Products Version 3.0, for SHOULD+ and SHOULD device requirements.

Layer-3 (L3) Switch Requirements (Intermediate Node): Interior and Exterior System Nodes

IPv6 Base

- RFC 1981 Path MTU Discovery for IPv6
  - Function to issue "packet too big" message
- RFC 2460 Internet Protocol v6 (IPv6) Specification
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- RFC 4861 Neighbor Discovery for IPv6
  - RFC 2461 Neighbor Discovery for IPv6 is acceptable until July 2009
- RFC 4862 IPv6 Stateless Address Auto-configuration
  - RFC 2462 IPv6 Stateless Address Auto-configuration is acceptable until July 2009
  - Only link-local addresses and Duplicate Address Detection
  - Section 5.5 Disable auto-configuration
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4443 Internet Control Message Protocol (ICMPv6)
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
  - Router and/or Listener mode

(Required support for at least one of the below)

- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 2467 Transmission of IPv6 Packets over FDDI Networks
- RFC 5072 IP Version 6 over PPP
  - RFC 2472 IP Version 6 over PPP is acceptable until July 2009
- RFC 3572 IPv6 over MAPOS (Multiple Access Protocol over SONET/SDH) (JITC Recommended)

Optional additional connection technologies)

- RFC 2491 IPv6 Over Non-Broadcast Multiple Access (NBMA) Networks
- RFC 2492 IPv6 over ATM Networks January 1999
- RFC 2497 Transmission of IPv6 Packets over ARCnet Networks
- RFC 2590 Transmission of IPv6 Packets over Frame Relay Networks Specification
- RFC 3146 Transmission of IPv6 over IEEE 1394 Networks
- RFC 4338 Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel

IPv6 Address Auto-configuration: Can be one of the below options

- RFC 4862/2462 IPv6 Stateless Address Auto-configuration
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
  - Server mode

- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
  - Relay mode

Transition Mechanisms

- RFC 4213 Transition Mechanisms for IPv6 Host and Routers
  - Dual-Stack function conditional
  - Configured function conditional
- (Conditional) RFC 2473 Generic Packet Tunneling in IPv6 Specification
- (Conditional) RFC 2784 Generic Router Encapsulation (GRE):

Net Management (Conditional for managed Layer-3 Switches)

- RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
  - SNMPv3 operation over IPv6 (July 2010 In-Effect Date)
- RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413 SNMP Applications

Management Information Base (MIBs) (Conditional for managed Layer-3 Switches)

- RFC 3595 Textual Conventions for IPv6 Flow Label
- RFC 4022 Management Information Base for the Transmission Control Protocol
- RFC 4113 Management Information Base for the User Datagram Protocol
- RFC 4293 Management Information Base (MIB) for IP
- RFC 4292 IP Forwarding Table MIB

Interior System Node

- RFC 2740 OSPF for IPv6
- (Conditional) RFC 4552 Authentication/Confidentiality for OSPFv3

Exterior System Node

- RFC 4271 A Border Gateway Protocol 4 (BGP-4)
- RFC 1772 Application of the Border Gateway Protocol in the Internet
- RFC 2545 Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
- RFC 4760 Multiprotocol Extensions for BGP-4

Please refer to the DoD IPv6 Standard Profiles for IPv6 Capable Products Version 3.0 for SHOULD+ and SHOULD device requirements.

Information Assurance (IA) Device: Firewall Requirements

IPv6 Base

- RFC 1981 Path MTU Discovery for IPv6
- RFC 2460 Internet Protocol v6 (IPv6) Specification
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- RFC 4861 Neighbor Discovery for IPv6
  - RFC 2461 Neighbor Discovery for IPv6 is acceptable until July 2009
- RFC 4862 IPv6 Stateless Address Auto-configuration
  - RFC 2462 IPv6 Stateless Address Auto-configuration is acceptable until July 2009
  - Only link-local addresses and Duplicate Address Detection
  - Section 5.5 Disable auto-configuration
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4443 Internet Control Message Protocol (ICMPv6)
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
  - Listener mode

(Required support for at least one of the below)

- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 2467 Transmission of IPv6 Packets over FDDI Networks
- RFC 5072 IP Version 6 over PPP
  - RFC 2472 IP Version 6 over PPP is acceptable until July 2009
- RFC 3572 IPv6 over MAPOS (Multiple Access Protocol over SONET/SDH) (JITC Recommended)

Optional additional connection technologies)

- RFC 2491 IPv6 Over Non-Broadcast Multiple Access (NBMA) Networks
- RFC 2492 IPv6 over ATM Networks January 1999
- RFC 2497 Transmission of IPv6 Packets over ARCnet Networks
- RFC 2590 Transmission of IPv6 Packets over Frame Relay Networks Specification
- RFC 3146 Transmission of IPv6 over IEEE 1394 Networks
- RFC 4338 Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel

IPv6 Address Auto-configuration: Can be one of the below options

- RFC 4862/2462 IPv6 Stateless Address Auto-configuration
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

IPSec: Conditional for IA Devices if IPSec is a managed service

- RFC 4301 Security Architecture for the Internet Protocol
- (Optional) RFC 4302 IP Authentication Header (AH)
- RFC 4303 IP Encapsulating Security Payload (ESP)
- RFC 4835 (ESP and AH) Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)

- RFC 4305 (ESP and AH) Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) is acceptable until July 2009

- RFC 4308 Cryptographic Suites for IPsec (July 2009 In-Effect Date)
- RFC 4869 Suite B Cryptographic Suites for IPsec (July 2009 In-Effect Date)

IPSec Fallback: If product cannot comply with 43XX Series of IPSec, then 24XX Series is acceptable

- RFC 2401 Security Architecture for the Internet Protocol
- (Optional) RFC 2402 IP Authentication Header (AH)
- RFC 2406 IP Encapsulating Security Payload (ESP)

IKEv1

- RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 4109 Algorithms for Internet Key Exchange Version 1 (IKEv1)

IKEv2: If product supports IKEv2, it must also support IKEv1 for backwards compatibility. In effect date for IKEv2 support is July 2010

- RFC 4306 Internet Key Exchange (IKEv2) Protocol
- RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)

NSA IPv6 Firewall Requirements

- Test 2.1.01: Role Separation
- Test 2.1.02: Role Revocation
- Test 2.1.03: Pre-Authentication Advisory Notice
- Test 2.1.04: Post-Authentication Advisory Notice
- Test 2.1.05: User Session Access
- Test 2.1.06: Authentication Policy
- Test 2.1.07: Local and Remote Administration
- Test 2.2.01: Basic: Ports, Protocols, and Services
- Test 2.2.02: Basic: Inactivity Guard
- Test 2.2.03: Basic: Traffic Integrity Test
- Test 2.2.04: Basic: TCP Traffic Enforcement
- Test 2.2.05: Basic: Access Control
- Test 2.2.06: Basic: Stateful Inspection
- Test 2.3.01: Advanced: Trusted Computing Base
- Test 2.3.02: Advanced: Environmental Variables
- Test 2.3.03: Advanced: Trusted Path
- Test 2.3.04: Advanced: Controlled Interface
- Test 2.3.05: Advanced: Classification Review
- Test 2.3.06: Advanced: Classification Protection
- Test 2.3.07: Advanced: Classification Transmission

- Test 2.3.08: Advanced: Configuration Surety
- Test 2.4.01: Audit Inspection
- Test 2.4.03: Discretionary Access Control
- Test 2.4.04: Mandatory Access Control
- Test 2.4.05: Configuration of Alert Mechanisms
- Test 2.5.01: ICMPv6 Control Traffic
- Test 2.5.02: Hop-by-Hop Header
- Test 2.5.03: Default Router
- Test 2.5.04: IPSec Forwarding
- Test 2.5.05: IPSec Verification
- Test 2.5.06: Address Autoconfiguration
- Test 2.5.07: Transition Mechanism Blocking
- Test 2.6.01: Attacks: Denial of Service
- Test 2.6.02: Attacks: Man-in-the-Middle (Replay)
- Test 2.6.03: Attacks: Common Vulnerabilities and Exploits
- Test 2.6.04: Attacks: Penetration Test
- Test 2.6.05: Attacks: Startup/Shutdown Vulnerabilities
- Test 2.6.06: Attacks: Tiny Fragments for IPv4 and IPv6
- Test 2.7.01: Documentation: Firewall Developer
- Test 2.7.02: Documentation: Developer Pre-Coverage
- Test 2.7.03: Documentation: Strength of Firewall
- Test 2.7.04: Documentation: Development Processes
- Test 2.7.05: Documentation: Configuration Management
- Test 2.7.06: Documentation: Delivery Processes
- Test 2.7.07: Documentation: Administrator/User Guidance
- Test 2.7.08: Documentation: Vulnerability Analysis
- Test 2.7.09: Documentation: Software Design
- Test 2.7.10: Documentation: Cryptography
- Test 2.7.11: Documentation: Software Design Test
- Test 3.1.01: Performance Test

Please refer to the DoD IPv6 Standard Profiles for IPv6 Capable Products Version 3.0 for SHOULD+ and SHOULD device requirements.

Information Assurance (IA) Device: IPS and IDS Requirements

IPv6 Base

- RFC 1981 Path MTU Discovery for IPv6
- RFC 2460 Internet Protocol v6 (IPv6) Specification
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- RFC 4861 Neighbor Discovery for IPv6
  - RFC 2461 Neighbor Discovery for IPv6 is acceptable until July 2009
- RFC 4862 IPv6 Stateless Address Auto-configuration
  - RFC 2462 IPv6 Stateless Address Auto-configuration is acceptable until July 2009
  - Only link-local addresses and Duplicate Address Detection
  - Section 5.5 Disable auto-configuration
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4443 Internet Control Message Protocol (ICMPv6)
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
  - Listener mode

(Required support for at least one of the below)

- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 2467 Transmission of IPv6 Packets over FDDI Networks
- RFC 5072 IP Version 6 over PPP
  - RFC 2472 IP Version 6 over PPP is acceptable until July 2009
- RFC 3572 IPv6 over MAPOS (Multiple Access Protocol over SONET/SDH) (JITC Recommended)

Optional additional connection technologies)

- RFC 2491 IPv6 Over Non-Broadcast Multiple Access (NBMA) Networks
- RFC 2492 IPv6 over ATM Networks January 1999
- RFC 2497 Transmission of IPv6 Packets over ARCnet Networks
- RFC 2590 Transmission of IPv6 Packets over Frame Relay Networks Specification
- RFC 3146 Transmission of IPv6 over IEEE 1394 Networks
- RFC 4338 Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel

IPv6 Address Auto-configuration: Can be one of the below options

- RFC 4862/2462 IPv6 Stateless Address Auto-configuration
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

IPSec: Conditional for IA Devices if IPSec is a managed service

- RFC 4301 Security Architecture for the Internet Protocol
- (Optional) RFC 4302 IP Authentication Header (AH)
- RFC 4303 IP Encapsulating Security Payload (ESP)
- RFC 4835 (ESP and AH) Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)

- RFC 4305 (ESP and AH) Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) is acceptable until July 2009

- RFC 4308 Cryptographic Suites for IPsec (July 2009 In-Effect Date)
- RFC 4869 Suite B Cryptographic Suites for IPsec (July 2009 In-Effect Date)

IPSec Fallback: If product cannot comply with 43XX Series of IPSec, then 24XX Series is acceptable

- RFC 2401 Security Architecture for the Internet Protocol
- (Optional) RFC 2402 IP Authentication Header (AH)
- RFC 2406 IP Encapsulating Security Payload (ESP)

IKEv1

- RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 4109 Algorithms for Internet Key Exchange Version 1 (IKEv1)

IKEv2: If product supports IKEv2, it must also support IKEv1 for backwards compatibility. In effect date for IKEv2 support is July 2010

- RFC 4306 Internet Key Exchange (IKEv2) Protocol
- RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)

NSA IPv6 IPS/IDS Requirements

1. Test 2.1.01: Role Separation
2. Test 2.1.02: Role Revocation
3. Test 2.1.03: Pre-Authentication Advisory Notice
4. Test 2.1.04: Post-Authentication Advisory Notice
5. Test 2.1.05: User Session Access
6. Test 2.1.06: Authentication Policy
7. Test 2.1.07: Local and Remote Administration
8. Test 2.2.02: Basic: Inactivity Guard
9. Test 2.2.04: Basic: TCP Traffic Enforcement
10. Test 2.2.06: Basic: Stateful Inspection
11. Test 2.3.01: Advanced: Trusted Computing Base
12. Test 2.3.02: Advanced: Environmental Variables
13. Test 2.3.08: Advanced: Configuration Surety
14. Test 2.4.01: Audit Inspection
15. Test 2.4.02: Data Collection
16. Test 2.4.03: Discretionary Access Control
17. Test 2.4.04: Mandatory Access Control
18. Test 2.5.01: ICMPv6 Control Traffic
19. Test 2.5.05: IPSec Verification
20. Test 2.5.06: Address Auto-configuration

21. Test 2.5.07: Transition Mechanism Blocking
22. Test 2.6.01: Attacks: Denial of Service
23. Test 2.6.02: Attacks: Man-in-the-Middle (Replay)
24. Test 2.6.03: Attacks: Common Vulnerabilities and Exploits
25. Test 2.6.04: Attacks: Penetration Test
26. Test 2.6.05: Attacks: Startup/Shutdown Vulnerabilities
27. Test 2.6.06: Attacks: Tiny Fragments for IPv4 and IPv6
28. Test 2.7.01: Documentation: IPS Developer
29. Test 2.7.02: Documentation: Developer Pre-Coverage
30. Test 2.7.03: Documentation: Strength of IPS
31. Test 2.7.04: Documentation: Development Processes
32. Test 2.7.05: Documentation: Configuration Management
33. Test 2.7.06: Documentation: Delivery Processes
34. Test 2.7.07: Documentation: Administrator/User Guidance
35. Test 2.7.08: Documentation: Vulnerability Analysis
36. Test 2.7.09: Documentation: Software Design
37. Test 2.7.10: Documentation: Cryptography
38. Test 2.7.11: Documentation: Software Design Test
39. Test 3.1.01: Performance Test

Information Assurance (IA) Device: Generic Security Device Requirements

IPv6 Base

- RFC 1981 Path MTU Discovery for IPv6
- RFC 2460 Internet Protocol v6 (IPv6) Specification
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- RFC 4861 Neighbor Discovery for IPv6
  - RFC 2461 Neighbor Discovery for IPv6 is acceptable until July 2009
- RFC 4862 IPv6 Stateless Address Auto-configuration
  - RFC 2462 IPv6 Stateless Address Auto-configuration is acceptable until July 2009
  - Only link-local addresses and Duplicate Address Detection
  - Section 5.5 Disable auto-configuration
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4443 Internet Control Message Protocol (ICMPv6)
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
  - Listener mode

(Required support for at least one of the below)

- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 2467 Transmission of IPv6 Packets over FDDI Networks
- RFC 5072 IP Version 6 over PPP
  - RFC 2472 IP Version 6 over PPP is acceptable until July 2009
- RFC 3572 IPv6 over MAPOS (Multiple Access Protocol over SONET/SDH) (JITC Recommended)

Optional additional connection technologies)

- RFC 2491 IPv6 Over Non-Broadcast Multiple Access (NBMA) Networks
- RFC 2492 IPv6 over ATM Networks January 1999
- RFC 2497 Transmission of IPv6 Packets over ARCnet Networks
- RFC 2590 Transmission of IPv6 Packets over Frame Relay Networks Specification
- RFC 3146 Transmission of IPv6 over IEEE 1394 Networks
- RFC 4338 Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel

IPv6 Address Autoconfiguration: Can be one of the below options

- RFC 4862/2462 IPv6 Stateless Address Autoconfiguration
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

IPSec: Conditional for IA Devices if IPSec is a managed service

- RFC 4301 Security Architecture for the Internet Protocol
- (Optional) RFC 4302 IP Authentication Header (AH)
- RFC 4303 IP Encapsulating Security Payload (ESP)
- RFC 4835 (ESP and AH) Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)

- RFC 4305 (ESP and AH) Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) is acceptable until July 2009

- RFC 4308 Cryptographic Suites for IPsec (July 2009 In-Effect Date)
- RFC 4869 Suite B Cryptographic Suites for IPsec (July 2009 In-Effect Date)

IPSec Fallback: If product cannot comply with 43XX Series of IPSec, then 24XX Series is acceptable

- RFC 2401 Security Architecture for the Internet Protocol
- (Optional) RFC 2402 IP Authentication Header (AH)
- RFC 2406 IP Encapsulating Security Payload (ESP)

IKEv1

- RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 4109 Algorithms for Internet Key Exchange Version 1 (IKEv1)

IKEv2: If product supports IKEv2, it must also support IKEv1 for backwards compatibility. In effect date for IKEv2 support is July 2010

- RFC 4306 Internet Key Exchange (IKEv2) Protocol
- RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)

(This page intentionally left blank.)

APPENDIX G

INTERNET PROTOCOL VERSION 6 DATA COLLECTION FORMS

It is requested that any data collected for any test event be sent to Joint Interoperability Test Command using the example Tables G-1 and G-2 for auto-generated data and G-3 for functional category verification. This will greatly enhance the efficiency by which the data may be analyzed and will act as a template for data comparison.

Table G-1. Device Under Test Performance - Frame Transfer

Hardware Version					
Software Version/Firmware					
Name	**Frame Size (Bytes)**	**Load (Megabits)**	**Tx Frames**	**Rx Frames**	**Lost Frames**
LEGEND: Rx Receive Tx Transmit					

Table G-2. Device Under Test Performance - Frame Standard Deviation

Hardware Version								
Software Version/Firmware								
Name	Frame Size (Bytes)	Load (Mb)	Standard Deviation	Latency (µs)			In Sequence	Out of Sequence
				Min	Ave	Max		

LEGEND:

Ave	Average	Min	Minimum
Max	Maximum	µs	Microseconds
Mb	Megabits		

Table G-3. Interoperability Test Summary

DUT			
Functional Category	Critical	Verified	Remarks
IPv6 Base			
IPSec			
Transition Mechanisms			
Quality of Service			
Mobility			
Network Management			
Internal Router			
External Router			

LEGEND:

DUT	Device Under Test	IPSec	Internet Protocol Security
IPv6	Internet Protocol Version 6		

APPENDIX H

REFERENCES

DEPARTMENT OF DEFENSE (DoD) DOCUMENTS

DoD Directive 8500.1, “Information Assurance,” 24 October 2002

“DoD Information Technology (IT) Standards Registry 05-1.0,” June 2005

DoD Instruction 5200.40 “DoD IT Security Certification and Accreditation Process,” 30 December 1997

“DoD Internet Protocol Version 6 (IPv6) Standard Profiles for IPv6 Capable Products Version 3.0,” July 2008

“DoD IPv6 Master Test Plan Version 2,” September 2006

National Security Agency, “NSA IPv6 Information Assurance Test Plan, Version 1,” June 2008

OTHER DOCUMENTS

Table H-1. RFC References

RFC	RFC Title
959	File Transfer Protocol
1772	Application of the Border Gateway Protocol in the Internet
1981	Path Maximum Transmission Unit Discovery for IPv6
2205	Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification
2207	RSVP Extensions for IPSEC Data Flows
2210	The Use of RSVP with IETF Integrated Services
2401	Security Architecture for Internet Protocol
2402	IP Authentication Header
2404	The Use of Hash Message Authentication Code Federal Information Processing Standard 180-1 within Encapsulating Security Payload and Authentication Header
2406	IP Encapsulating Security Payload (ESP)
2407	The Internet IP Security Domain of Interpretation for ISAKMP
2408	Internet Security Association and Key Management Protocol (ISAKMP)
2409	The Internet Key Exchange (IKE)
2428	FTP Extensions for IPv6 and NAT
2460	Internet Protocol Version 6 (IPv6) Specification
2461/4861	Neighbor Discovery for IP Version 6 (IPv6)
2462/4862	IPv6 Stateless Address Auto-configuration
2464	Transmission of IPv6 Packets over Ethernet Networks
2467	Transmission of IPv6 Packets over FDDI Networks
2472/5072	IP Version 6 over PPP
2473	Generic Packet Tunneling in IPv6 Specification
2474	Definition of the DiffServ Field in the IPv4 and IPv6 Headers
2491	IPv6 over Non-Broadcast Multiple Access (NBMA) networks
2492	IPv6 over ATM Networks
2497	Transmission of IPv6 Packets over ARCnet Networks
2507	IP Header Compression

Table H-1. RFC References (continued)

RFC	RFC Title
2508	Compressing IP/UDP/RTP Headers for Low-Speed Serial Links
2544	Benchmarking Methodology for Network Interconnect Devices
2545	Border Gateway Protocol Extensions for IPv6 Inter-domain Routing
2590	Transmission of IPv6 Packets over Frame Relay Networks Specification
2710	Multicast Listener Discovery (MLD) for IPv6
2740	Open Shortest Path First for IPv6
2746	RSVP Operation Over IP Tunnels
2747	RSVP Cryptographic Authentication
2750	RSVP Extensions for Policy Control
2766	Network Address Translation- Protocol Translation (NAT-PT)
2784	Generic Routing Encapsulation (GRE)
2821	Simple Mail Transfer Protocol (SMTP)
2858/4760	Multiprotocol Extensions for BGP-4
2872	Application and Sub Application Identity Policy Element for Use with RSVP
2911	Internet Printing Protocol
2961	RSVP Refresh Overhead Reduction Extension
2996	Format of the RSVP DCLASS Object
2998	A Framework for Integrated Services Operation over DiffServ Networks
3041/4941	Privacy Extensions for Stateless Address Auto-configuration in IPv6
3053	IPv6 Tunnel Broker
3095	Robust Header Compression (RoHC)
3146	Transmission of IPv6 Packets over IEEE 1394 Networks
3162	RADIUS (Remote Authentication Dial-In User Service) and IPv6
3168	The Addition of Explicit Congestion Notification (ECN) to IP
3173	IP Payload Compression
3175	Aggregation of RSVP for IPv4 and IPv6 Reservations
3181	Signaled Preemption Priority Policy Object
3182	Identity Representation for RSVP
3226	DNS Security and IPv6 A6 Aware Server/Resolver Message Size Requirements
3241	RoHC over PPP
3261	Session Initiation Protocol (SIP)
3315	Dynamic Host Configuration Protocol for IPv6
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
3413	Simple Network Management Protocol (SNMP) Applications
3484	Default Address Selection for Internet Protocol version 6 (IPv6)
3572	Internet Protocol Version 6 over MAPOS (Multiple Access Protocol Over SONET/SDH)
3585	IPsec Configuration Policy Information Model
3586	IP Security Policy Requirements
3595	Textual Conventions for IPv6 Flow Label
3596	DNS Extensions to Support IP Version 6
3633	IPv6 Prefix Options for DHCPv6
3769	IPv6 Prefix Delegation
3775	Mobility Support in IPv6
3776	Using IPSec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6
3843	RoHC: A Compression Profile for IP
3963	Network Mobility (NEMO) Basic Support Protocol
3971	Secure Neighbor Discovery
3972	Cryptographically Generated Addresses
3973	Protocol Independent Multicast – Dense Mode
3986	Uniform Resource Identifier (URI): Generic Syntax
4007	IPv6 Scoped Address Architecture
4022	Management Information Base for the Transmission Control Protocol
4087	IP Tunnel MIB
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)
4113	Management Information Base for the User Datagram Protocol
4193	Unique Local IPv6 Unicast Addresses
4213	Transition Mechanisms for IPv6 Host and Routers

Table H-1. RFC References (continued)

RFC	RFC Title
4271	A Border Gateway Protocol 4 (BGP-4)
4282	The Network Access Identifier
4283	Mobile Node Identifier for Option for IPv6
4291	IP Version 6 Addressing Architecture
4292	IP Forwarding Table MIB
4293	Management Information Base (MIB) for IP
4295	Mobile IP Management MIB
4301	Security Architecture for Internet Protocol
4302	IP Authentication Header
4303	IP Encapsulating Security Payload (ESP)
4304	Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)
4305/4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
4306	Internet Key Exchange (IKEv2) Protocol
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
4308	Cryptographic Suites for IPsec
4330	Simple Network Time Protocol (SNTP)
4338	Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel
4362	RoHC: A Link-Layer Assisted Profile for IP/UDP/RTP
4443	Internet Control Message Protocol for the IPv6 Specification
4495	A Resource Reservation Protocol (RSVP) Extension for the Reduction of Bandwidth of a Reservation Flow
4541	Considerations for IGMP and MLD Snooping Switches
4552	Authentication/Confidentiality for OSPFv3
4601	Protocol Independent Multicast – Sparse Mode (PIM-SM)
4798	Connecting IPv6 Islands over IPv4 MPLS using IPV6 Provider Edge (6PE) routers
4807	IPsec Security Policy Database Configuration
4815	Corrections and Clarification to RFC 3095
4877	Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture
4869	Suite B Cryptographic Suites for IPsec
4944	Transmission of IPv6 Packets Over IEEE 802.15.4 Networks
4995	RoHC Framework
4996	RoHC: A profile for TCP/IP
5095	Deprecation of Type 0 Routing Headers in IPv6
5175	Extensions to Router Advertisement Flags

LEGEND:

A6	IPv6 Address Record	IPv6	Internet Protocol Version 6
ATM	Asynchronous Transfer Mode	ISAKMP	Internet Security Association and Key Management Protocol
ARCnet	Attached Resource Computer Network		
BGP-4	Border Gateway Protocol Version 4	MAPOS	Multiple Access Protocol Over SONET/SDH
DHCPv6	Dynamic Host Configuration Protocol for IPv6	MPLS	Multi-protocol Label Switching
DiffServ	Differentiated Services	NAT	Network Address Translation
DNS	Domain Name Service	OSPFv3	Opened Shortest Path First for IPv6
FDDI	Fiberoptic Digital Data Interface	PPP	Point-to-Point Protocol
FTP	File Transfer Protocol	RADIUS	Remote Authentication Dial-In User Service
IEEE	Institute of Electrical and Electronic Engineers, Inc.	RFC	Request for Comments
IETF	Internet Engineering Task Force	RTP	Real Time Transport Protocol
IGMP	Internet Group Multicast Protocol	SDH	Synchronous Digital Hierarchy
IKEv2	Internet Key Exchange Version 2	SONET	Synchronous Optical Network
IP	Internet Protocol	TCP	Transmission Control Protocol
IPSec	Internet Protocol Security	UDP	User Datagram Protocol
IPv4	Internet Protocol Version 4		

(This page intentionally left blank.)

APPENDIX I

POINTS OF CONTACT

Beckman, Todd	ATTN: JTE3/Beckman P.O. Box 12798 Fort Huachuca, AZ 85670-2798 E-mail: todd.beckman@disa.mil	(520) 538-5174 DSN 879-5174 Fax (DSN) 879-4347
Hann, Donald	ATTN: JTE3/Hann P.O. Box 12798 Fort Huachuca, AZ 85670-2798 E-mail: donald.hann@disa.mil	(520) 538-5130 DSN 879-5130 Fax (DSN) 879-4347
Thomas, Kent	ATTN: INTEROP/Thomas P.O. Box 12798 Fort Huachuca, AZ 85670-2798 E-mail: kent.thomas.ctr@disa.mil	(520) 538-5189 DSN 879-5189