DEFENSE INFORMATION SYSTEMS AGENCY

JOINT INTEROPERABILITY TEST COMMAND
FORT HUACHUCA, ARIZONA

MOONV6 PHASE II INTERNET PROTOCOL VERSION 6 INTEROPERABILITY ASSESSMENT PLAN

JANUARY 2004

MOONV6 PHASE II
INTERNET PROTOCOL
VERSION 6
INTEROPERABILITY
ASSESSMENT PLAN

JANUARY 2004

Submitted by:

ALVIN M. SLARVE
Chief
Global Information Grid
Tactical Networks Branch

Approved by:

_____

LESLIE F. CLAUDIO
Chief
Networks, Transmission and
Intelligence Division

Prepared Under the Direction of:

MAJOR ROSWELL DIXON, USMC
Joint Interoperability Test Command
Fort Huachuca, Arizona 85613-7051

(This page intentionally left blank.)

EXECUTIVE SUMMARY

The Department of Defense (DOD) runs the largest enterprise Internet Protocol (IP) network in the world. IP version 4 (IPv4) is the computing and communications protocol used by virtually all computers to facilitate communications between other computers across various network types, including local area networks and wide area networks. IPv4 is implemented on a wide array of computing platforms from simple desktop workstations to sensor interfaces for various systems like access control and gasoline pumps to complex high-end computing platforms. It is also implemented on the routers and other communications equipment that interconnect multiple disparate networks.

IPv4 has been in use for almost 30 years and cannot support emerging requirements for address space, mobility, and security in peer-to-peer networking. IP version 6 (IPv6) is an improved version of IP that will coexist with IPv4 and eventually replace it in most networks. IPv6 is equipped with significant enhancements that will provide better internetworking capabilities than those currently available within IPv4.

The Joint Interoperability Test Command (JITC) is assessing IPv6 for the DOD. IPv6 can support most of the software utilities and applications previously used with IPv4, providing those utilities and applications have been properly modified, or ported, for interaction with IPv6. IPv6 interoperability assessment testing is necessary to help evaluate a variety of key interoperability and portability issues associated with the transition to IPv6 and to begin development of methodologies needed to support the lengthy coexistence of IPv4 and IPv6.

The requirements profile developed for Moonv6 Phase II identified two levels of requirements that will be used in this interoperability assessment. Primary requirements for Moonv6 Phase II are Request for Comments (RFCs) associated with IPv6 and designated as emerging by Joint Technical Architecture (JTA) List of Mandated and Emerging Standards Version 5.1 (Draft) dated 21 July 2003. Secondary requirements are those needed to effectively assess applications and Global Information Grid Bandwidth Expansion routing mechanisms. Summaries of the requirements that will be referenced during Moonv6 assessment execution are provided in appendix B.

The assessment environment consists of network communications interfaces, network hardware, operating system software, and application software configured to provide network-based assessment capabilities including native IPv6 assessment capabilities, IPv4 over IPv6 tunneled assessment capabilities, and dual stack IPv4/IPv6 assessment capabilities.

Results of the Moonv6 assessment will be presented in JITC Assessment Report format at the conclusion of assessment and data analysis activities.

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

APPENDICES (continued)

LIST OF FIGURES

TABLE OF CONTENTS (continued)

Page

LIST OF FIGURES (continued)

LIST OF TABLES

TABLE OF CONTENTS (continued)

Page

LIST OF TABLES (continued)

(This page intentionally left blank.)

SYSTEM FUNCTIONAL DESCRIPTION

The Department of Defense (DOD) runs the largest enterprise Internet Protocol (IP) network in the world. IP version 4 is the computing and communications protocol used by virtually all computers to facilitate communications between other computers across various network types, including local area networks and wide area networks. IPv4 is implemented on a wide array of computing platforms from simple desktop workstations to sensor interfaces for various systems like access control and gasoline pumps to complex high-end computing platforms. It is also implemented on the routers and other communications equipment that interconnect multiple disparate networks. Implementation details for both IPv4 and IP version 6 (IPv6) are standardized in documents titled Request for Comments (RFCs) that are produced under the direction of the Internet Engineering Task Force.

ASSESSMENT BACKGROUND

IPv4 has been in use for almost 30 years and cannot support emerging requirements for address space, mobility, and security in peer-to-peer networking. IPv6 is an improved version of IP that will coexist with IPv4 and eventually replace it in most networks. IPv6 is equipped with significant enhancements that will provide better internetworking capabilities than those currently available within IPv4. For example, IPv6 extends the IP address space from 32 bits to 128 bits, provides extended routing capabilities, adds capabilities for mobile applications, provides improved security via authentication and privacy features, allows auto configuration, and provides increased quality of service capabilities.

The Joint Interoperability Test Command (JITC) is assessing IPv6 for DOD. IPv6 can support most of the software utilities and applications previously used with IPv4, providing those utilities and applications are modified, or ported, for proper interaction. IPv6 interoperability assessment testing is necessary to help evaluate a variety of key interoperability and portability issues associated with the transition to IPv6 and to begin development of methodologies needed to support the lengthy coexistence of IPv4 and IPv6.

ASSESSMENT PURPOSE

To determine to what extent current vendor implementations of IP routing mechanisms and applications, including routing mechanisms used by Global Information Grid Bandwidth Expansion (GIG-BE) and DOD-centric applications, can interoperate in a dual IPv4/IPv6 environment.

REQUIREMENTS

The requirements profile developed for Moonv6 Phase II identified two levels of requirements that will be used in this interoperability assessment. Primary requirements for Moonv6 Phase II are Request for Comments (RFCs) associated with IPv6 and designated as emerging by Joint Technical Architecture (JTA) List of Mandated and Emerging Standards Version 5.1 (Draft) dated 21 July 2003. Secondary requirements

are those needed to effectively assess critical GIG-BE applications and routing mechanisms. Summaries of the requirements that will be referenced during Moonv6 are provided in appendix B.

SCOPE

Environment and Configuration

The assessment environment consists of network communications interfaces, network hardware, operating system software, and application software configured to provide assessment capabilities including native IPv6 assessment capabilities, IPv4 over IPv6 tunneled assessment capabilities, and dual stack IPv4/IPv6 assessment capabilities.

The assessment will be conducted by passing traffic between multiple sites distributed over North America and Europe. This backbone network will resemble a realistic IPv4/IPv6 network, including multiple host and router interfaces interconnected by Defense Research and Engineering Network circuits, Defense Information Systems Network Leading Edge Services circuits, and T1 circuits. Figure 1 depicts the network that will be used for application and performance testing during Moonv6 Phase II. This network will be stable prior to beginning testing; any intrusive testing will be deferred until application testing is complete to limit test delays due to network reconfiguration efforts. Additional network-related testing will be accomplished using local networks constructed at JITC Ft. Huachuca.

Multiple applications will be tested over the core network, including electronic mail (e-mail), Hypertext Transfer Protocol (HTTP), Joint Logistics Warfighter Initiative (JLWI), Public Key Infrastructure (PKI), VideoTeleconference (VTC), Defense Collaboration Tool Suite (DCTS) IPv6 Mobility, IPv6 Security (IP Sec), and certain Domain Name System (DNS) features.

The network-related tests that will be conducted over the local network(s) are IPv6 performance, response to link failures, Intermediate System-Intermediate System (IS-IS) routing conformance, and Multi-Protocol Label Switching (MPLS) conformance tests.

The addition of Moonv6 participants or test activities after submission of this test plan may expand the scope of this assessment. Additions to the test plan may take the form of procedures to support other test sites, or may be additional equipment vendors, telecommunications carriers, military sites, and/or civilian sites. These additions may create an opportunity for testing that goes beyond what is currently specified. If this occurs, the test requirements will be documented in Test Plan Annexes and results from the additional testing will be included in the Moonv6 Phase II Assessment Report.

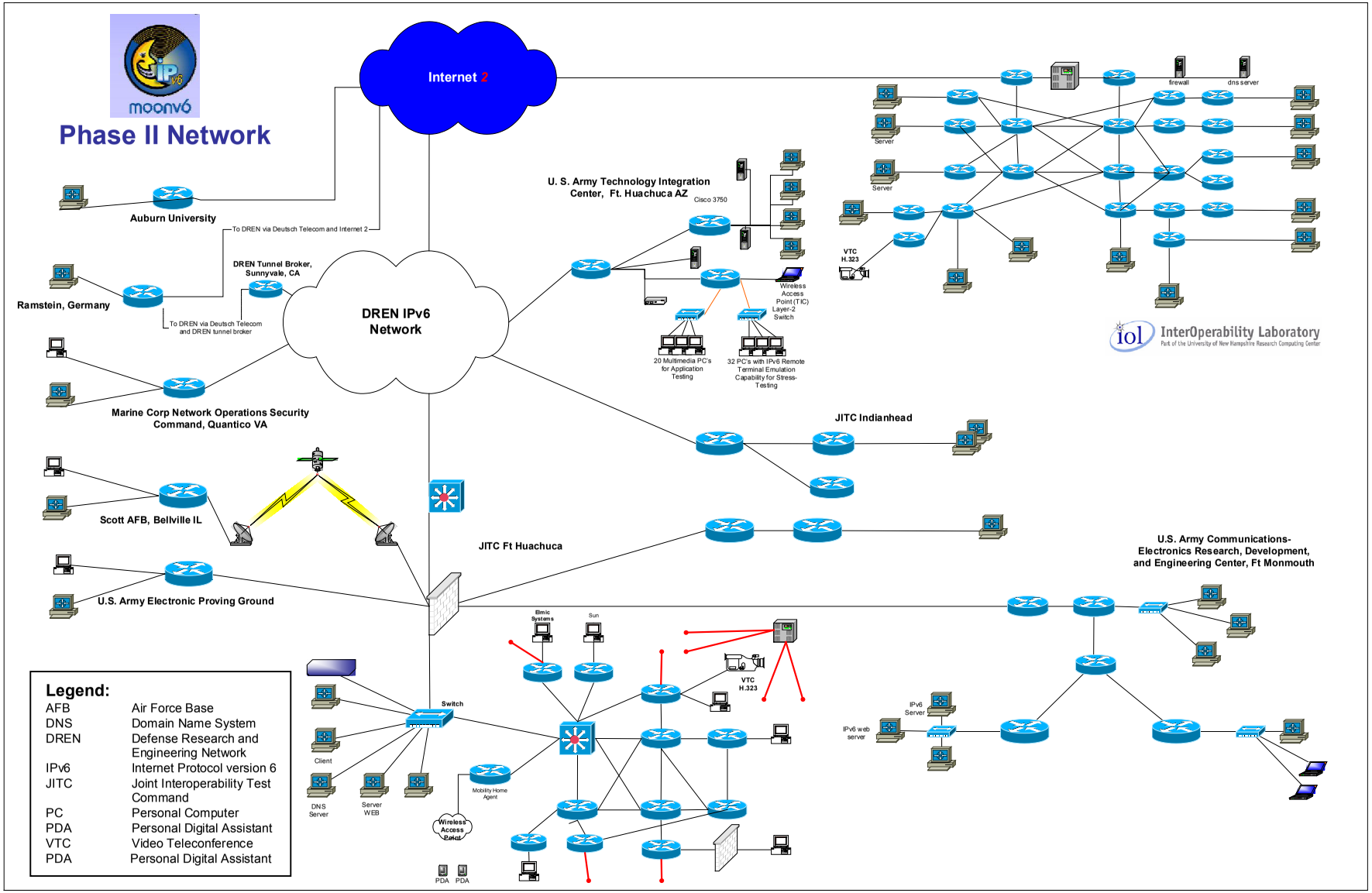


Figure 1. Moonv6 Phase II Network Configuration

Table 1. Moonv6 Phase II Hardware and Software

INTERFACES	ROUTER HARDWARE VENDORS	HOST HARDWARE VENDORS	OPERATING SYSTEM SOFTWARE VENDORS	APPLICATION SOFTWARE
100 BaseT Ethernet	Cisco	Agilent	Elmic Systems	DCTS
1000 BaseLX Ethernet	Extreme	Compaq	HP	DNS
1000 BaseSX Ethernet	Foundry	Elmic Systems	Microsoft	E-mail
1000 BaseT Ethernet	Fujitsu	HP	Red Hat	Internet Explorer
ATM OC-3	Hitachi	IBM	Sun Microsystems	IPv6 Mobility
T1	IP Infusion	Ixia		IPv6 Security
	Ixia	Spirent		JLWI
	Juniper	Sun		Netscape
	NEC			PKI
	Nokia			VTC

Notes:
Each column is a list of the interfaces, vendors, or software associated with a specific category, e.g. Router Hardware Vendors and should be read down, not across. The columns are mutually exclusive.

Legend:

ATM	Asynchronous Transfer Mode	IP	Internet Protocol
DCTS	Defense Collaboration Tool Suite	IPv6	Internet Protocol version 6
DMS	Defense Message System	JLWI	Joint Logistics Warfighter Initiative
DNS	Domain Name System	OC	Optical Carrier
E-mail	Electronic Mail	PKI	Public Key Infrastructure
HP	Hewlett Packard	VTC	VideoTeleconference
IBM	International Business Machines	WWW	World Wide Web

Moonv6 Phase II will be conducted from the 2nd February through the 6th of April 2004. Participants include Joint Interoperability Test Command (JITC), Ft. Huachuca, JITC, Indian Head, the University of New Hampshire Interoperability Laboratory (UNH-IOL), the Marine Corp Network Operation Security Command (MCNOSC), Air Force Communications Agency (AFCA), the U.S. Army Communications-Electronics Research, Development, and Engineering Center (CERDEC), the U.S Army Electronic Proving Ground (EPG), Auburn University, and the U.S. Air Force in Europe Integration and Evaluation Facility.

Limitations

Since some operating systems and applications have not been ported to IPv6, limitations include the unavailability of these operating systems and applications software packages. Further, many vendors lack complete IPv6 protocol implementations, particularly complete implementations for IPv6 Security and IPv6 Mobility.

The evolution of existing RFCs and the creation of new ones means vendor implementations will be dynamic, creating the need for follow on evaluations that keep pace with vendor implementations.

Additional limitations stem from the broad scope and large number of test participants. Due to this broad scope, testing will be limited to representative test cases for each of the 12 test activities. For example, during e-mail testing, instead of attempting exhaustive testing on every file type, file size, and client e-mail package, testing will be limited to those file types, file sizes, and client packages in common use within DOD and currently available at each participating DOD site.

OBJECTIVES, CRITERIA, AND METHODOLOGY

Objectives

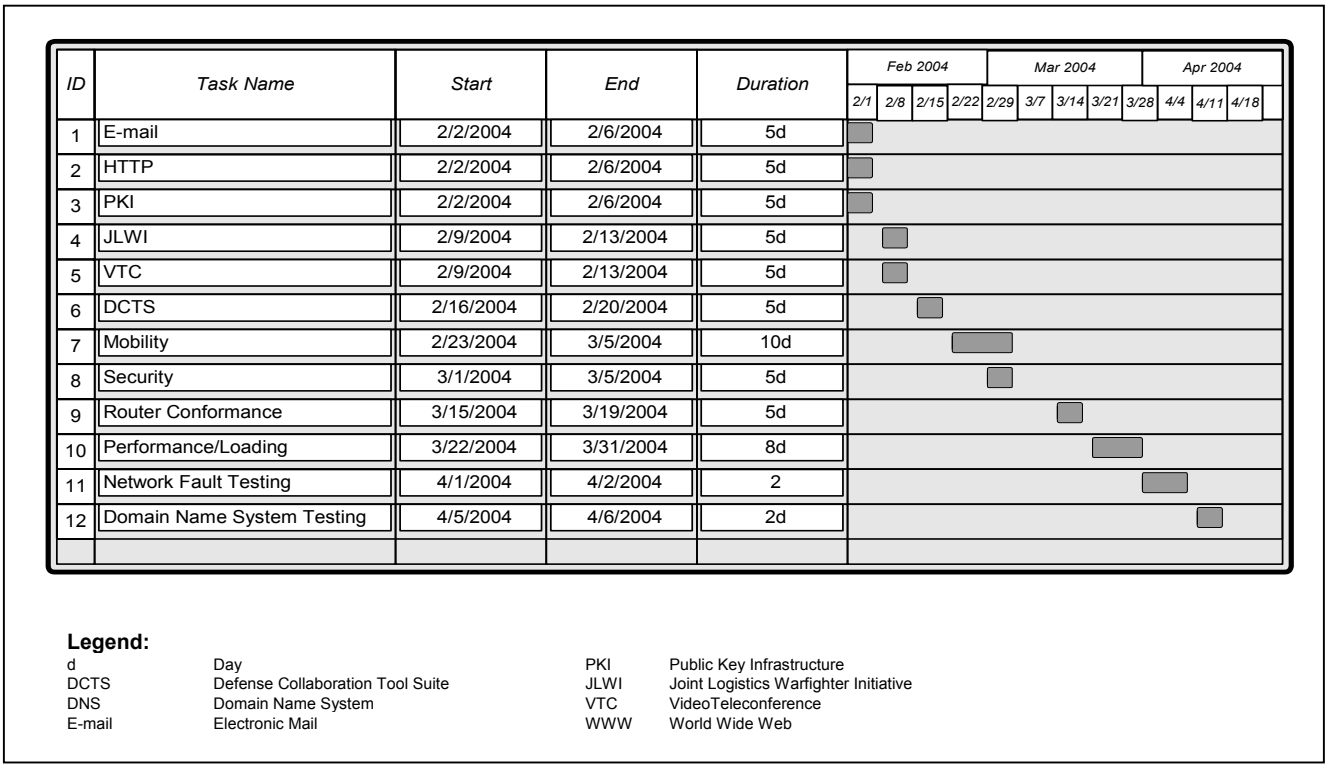
The Moonv6 assessment will be divided into two test categories: Application tests and Network tests. Satisfaction of assessment criteria as listed in the Criteria section of this document constitutes the major assessment objectives. See table 2 for a listing of the assessment efforts in each category. See figure 2 for the Moonv6 Phase II schedule

Table 2. Test Categories and Test Activities

Application Tests	Network Tests
DCTS: Manual testing distributed over all sites	IPv6 Performance/Load Test: Automated testing distributed over six sites and local testing at JITC Ft. Huachuca
E-mail: Manual and automated testing distributed over all sites	DNS Primary server failure: Manual testing distributed over all sites
Hypertext Transfer Protocol: Manual and automated testing distributed over all sites	Ethernet and ATM Link Failures: Testing done manually on the Moonv6 Phase II local area networks (LAN) at JITC Ft. Huachuca.
Joint Logistics Warfighter Initiative: Manual testing distributed over two sites.	MPLS and IS-IS interoperability: Testing done manually on the Moonv6 Phase II Network at JITC Ft. Huachuca.
IPv6 Mobility: Manual testing distributed between four sites	
IPv6 Security: Manual testing distributed between two sites	
PKI: Manual testing distributed between two sites	
VTC: Manual testing distributed between four sites	

Legend:

ATM	Asynchronous Transfer Mode	IPv6	Internet Protocol version 6	MPLS	Multi-Protocol Label Switching
DCTS	Defense Collaboration Tool Suite	IS-IS	Intermediate System-Intermediate System	PKI	Public Key Infrastructure
DNS	Domain Name System	JITC	Joint Interoperability Test Command	UNH	University of New Hampshire
E-mail	Electronic Mail	LAN	Local Area Network	VTC	VideoTeleconference



ID	Task Name	Start	End	Duration
1	E-mail	2/2/2004	2/6/2004	5d
2	HTTP	2/2/2004	2/6/2004	5d
3	PKI	2/2/2004	2/6/2004	5d
4	JLWI	2/9/2004	2/13/2004	5d
5	VTC	2/9/2004	2/13/2004	5d
6	DCTS	2/16/2004	2/20/2004	5d
7	Mobility	2/23/2004	3/5/2004	10d
8	Security	3/1/2004	3/5/2004	5d
9	Router Conformance	3/15/2004	3/19/2004	5d
10	Performance/Loading	3/22/2004	3/31/2004	8d
11	Network Fault Testing	4/1/2004	4/2/2004	2
12	Domain Name System Testing	4/5/2004	4/6/2004	2d

Legend:

d	Day	PKI	Public Key Infrastructure
DCTS	Defense Collaboration Tool Suite	JLWI	Joint Logistics Warfighter Initiative
DNS	Domain Name System	VTC	VideoTeleconference
E-mail	Electronic Mail	WWW	World Wide Web

Figure 2. Moonv6 Phase II Schedule

Criteria

Electronic Mail

The IPv6 application and protocol implementation shall exchange e-mail, including multiple file attachments, multiple file attachment types, and varying sized files with a 90% probability of success.

HTTP

The IPv6 application and protocol implementations shall support HTTP sessions, including file transfer, with a 90% probability of success.

Public Key Infrastructure

The IPv6 application and protocol implementation shall support PKI sessions that obtain digital certificates from the JITC PKI server, exchange secure e-mail, access public key enabled websites, use validation services and access directory services with a 90% probability of success.

Joint Logistics Warfighter Initiative

The JLWI Relay Agent, located at Ft. Huachuca, shall properly access the JLWI servers located at JITC Indian Head.

Video Teleconference

The IPv6 application and protocol implementation shall support H.323 Video Teleconferences with a 90% probability of success.

Defense Collaboration Tool Suite

DCTS shall support voice and video conferencing, document sharing, application sharing, instant messaging and whiteboard functionality with no significant protocol induced errors or failures.

Mobility

The IPv6 protocol implementation shall support IPv6 mobility mechanisms that provide host mobility and router mobility with no significant protocol induced errors or failures.

Security

The IPv6 protocol implementation shall support IPv6 Security mechanisms that provide end-to-end security with no significant protocol induced errors or failures.

Router Conformance

Routing devices that support the IS-IS and/or MPLS protocols shall conform to selected automated test suites provided by Spirent, Ixia, and Agilent.

Network Performance and Loading

The network routing and switching devices shall continue to operate correctly when loaded at 80% of the interface bit rate for the interface under test. (Note: Performance limitations due to service provider traffic-related issues on links between sites may preclude testing at 80% of the interface bit rate. If the inter-site links cannot support performance testing due to carrier issues, performance testing will be done on links constructed between network devices located on Ft. Huachuca and/or UNH.) For Ethernet interfaces the maximum transmission unit shall be no smaller than 1518 bytes.

Network Fault Testing

Upon link failure, the network routing and switching devices shall properly re-route traffic, process alarms (if applicable), and provide network management visibility to the failure.

Domain Name System Primary Server Failure

DNS testing will test the response of a dual-stack DNS server when the IPv6 interface fails. Upon network device interface failure (or circuit failure) the DNS server under test will support DNS name resolutions using its IPv4 interface.

Methodology

Figure 1 depicts the stable network that will be used to assess most application and network-related criteria. Test activities will be executed based on the Gantt chart shown in figure 2. The assessment activities documented in table 2 are designed to exercise specific protocol interfaces. As a given software interface or function is exercised its performance will be compared to the desired performance as documented in the associated requirement. Data collection tools include packet capture utilities, and packet analysis utilities found on Spirent, Agilent, and Ixia diagnostic equipment. Methodology for each test activity is presented on a per-category basis in the following paragraphs.

E-mail Testing

E-mail will be tested by passing messages between clients and servers. E-mail servers will be located at JITC Ft. Huachuca, MCNOSC, AFCA, and UNH. Each site will provide at least one e-mail client. E-mail messages will include various attachments, including Microsoft Word, Microsoft Excel, Microsoft PowerPoint, picture files in Joint Photographic Experts Group format, and text. Each mail recipient will use a binary file comparison tool to verify the integrity of the attachment. Additional e-mail testing will be performed to determine if the network can support a high volume of email traffic. Using an automated test system, 250,000 e-mail messages will traverse the network over a 48 period. During all e-mail testing, the network will be monitored for protocol-induced failures. Figure 3 depicts the network that will be used to test e-mail. Refer to appendix C, annex 1 for the detailed procedures associated with e-mail testing.

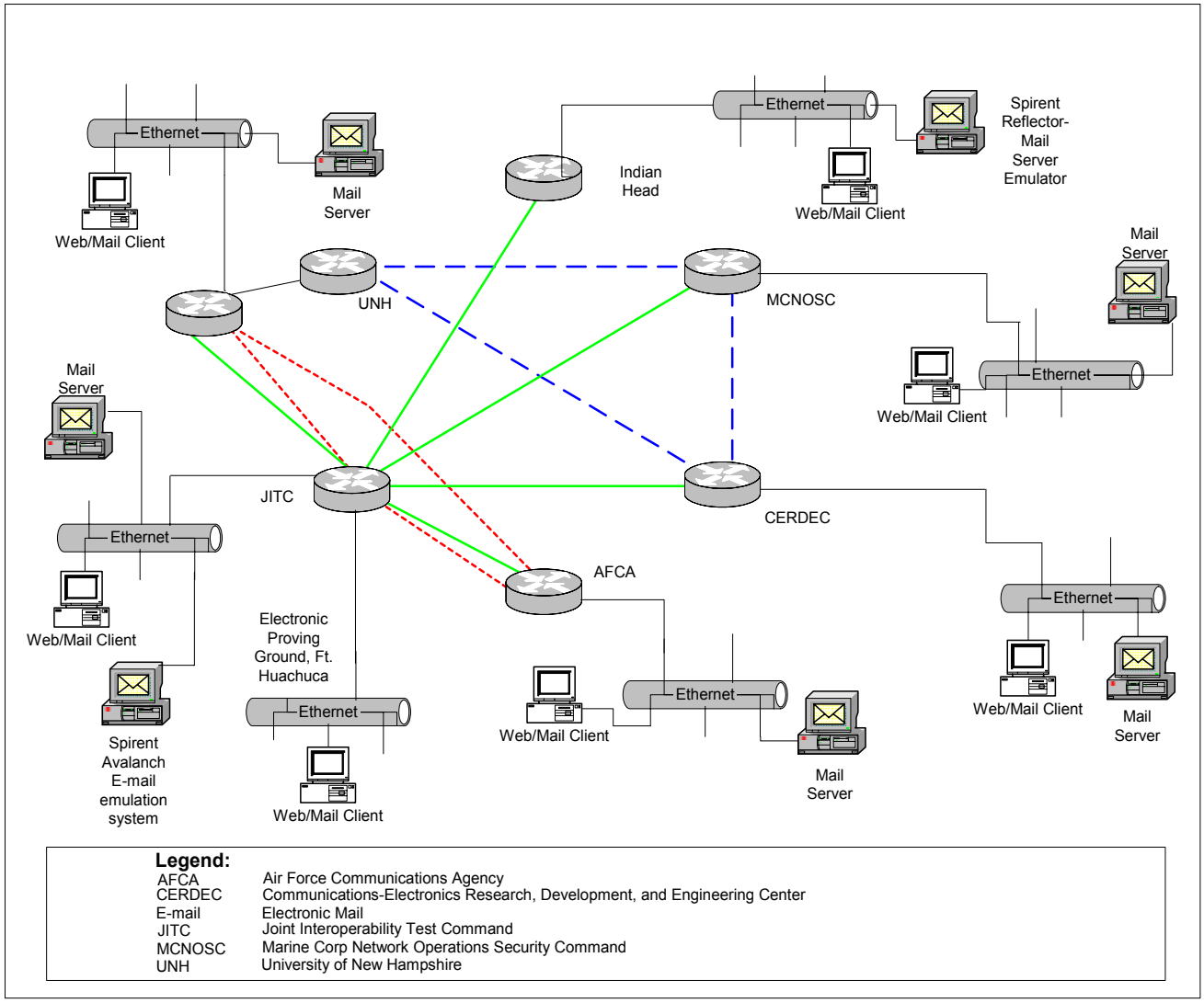


Figure 3. E-mail Test Network

Hypertext Transfer Protocol Testing

This test verifies that a device can properly perform as an IPv6 HTTP client. A client at each site will request a web page from servers located at all other sites except Indian Head and the U.S. Army EPG. Each client will use a combination of domain names and literal IPv6 addresses when requesting a web page. Each client will also successfully navigate to and update a form located on each server. Additionally, the automated test system will load-test the network by initiating 500,000 web sessions over a 48 hour period. Figure 4 depicts the network that will be used for HTTP testing. Refer to appendix C; annex two for the detailed procedures associated with HTTP testing.

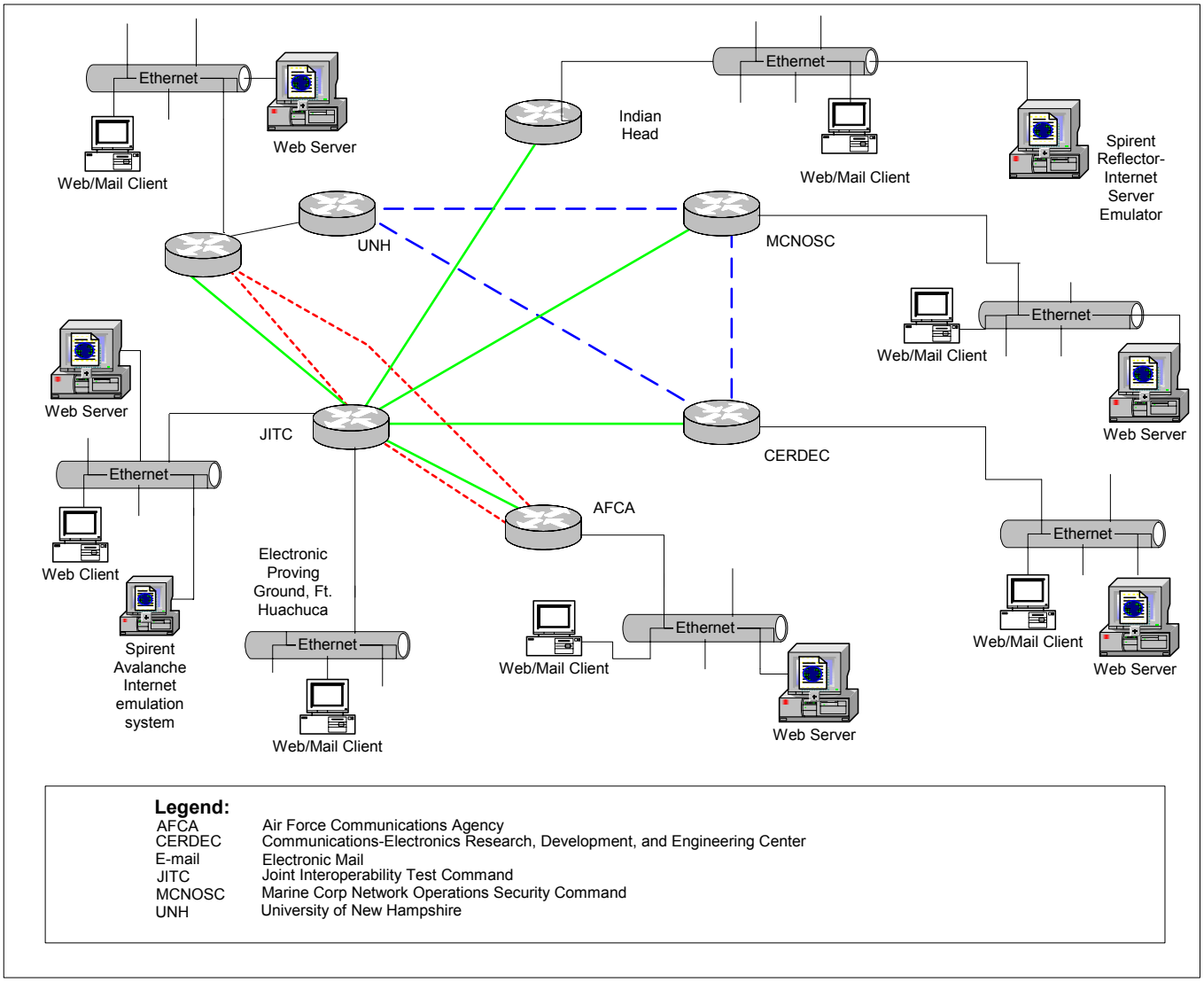


Figure 4. HTTP Test Network

Public Key Infrastructure Testing

A PKI server will be set up at JITC Ft. Huachuca. Using this server, test participants on client systems at MCNOSC will obtain certificates, exchange secure emails, access PKI-enabled websites, use validation services, and use directory services. The network that will be used for PKI testing is shown in figure 5. The detailed procedures associated with PKI testing can be found in appendix C, annex three.

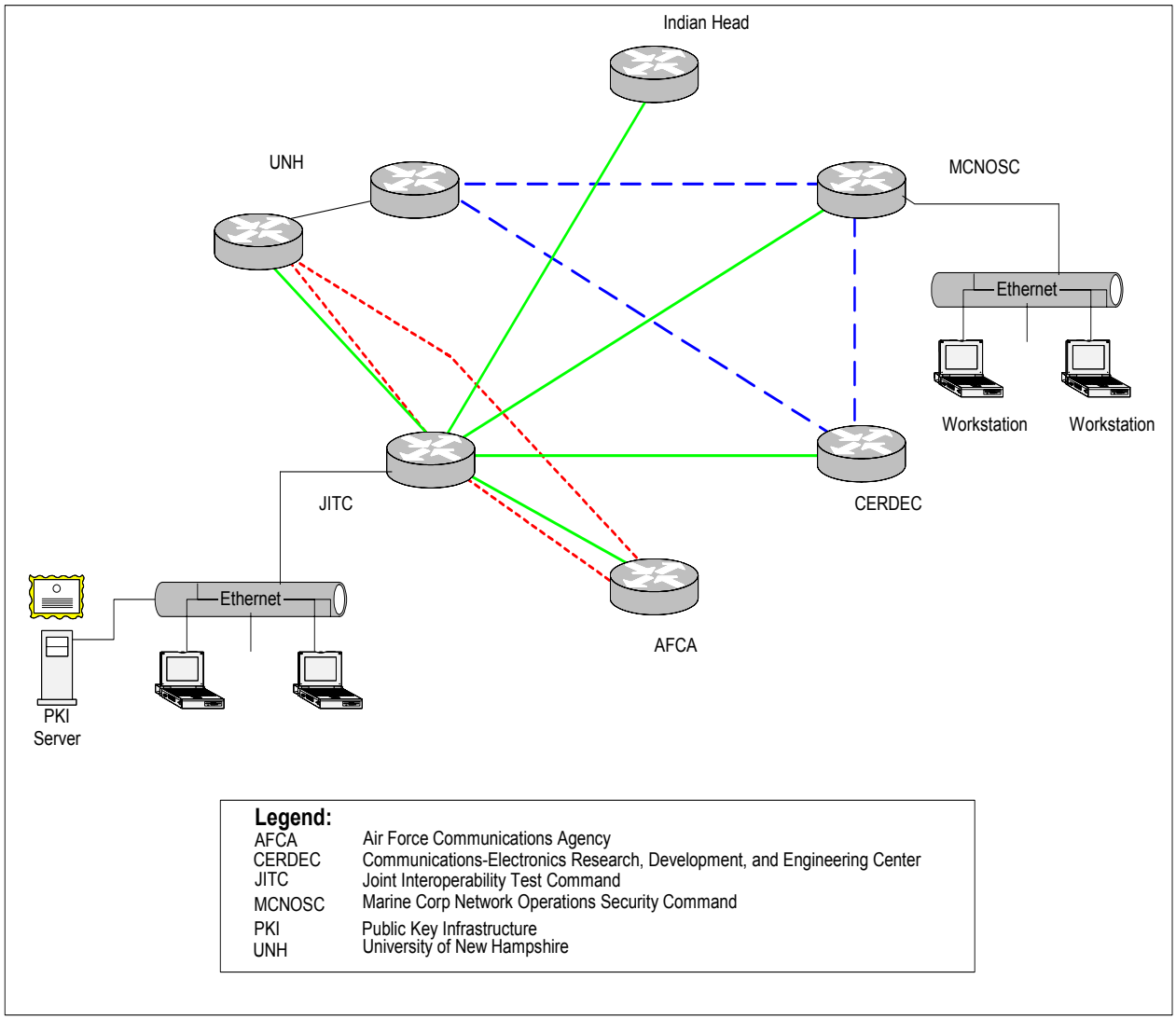


Figure 5. PKI Test Network

Joint Logistics Warfighter Initiative Testing

JLWI will be tested by installing a JLWI Relay Agent at JITC Ft. Huachuca and executing various JLWI tasks on a web and application server located at JITC Indian Head. Refer to figure 6 for the network that will be used to assess JLWI. Detailed procedures for JLWI testing can be found in appendix C, annex 4.

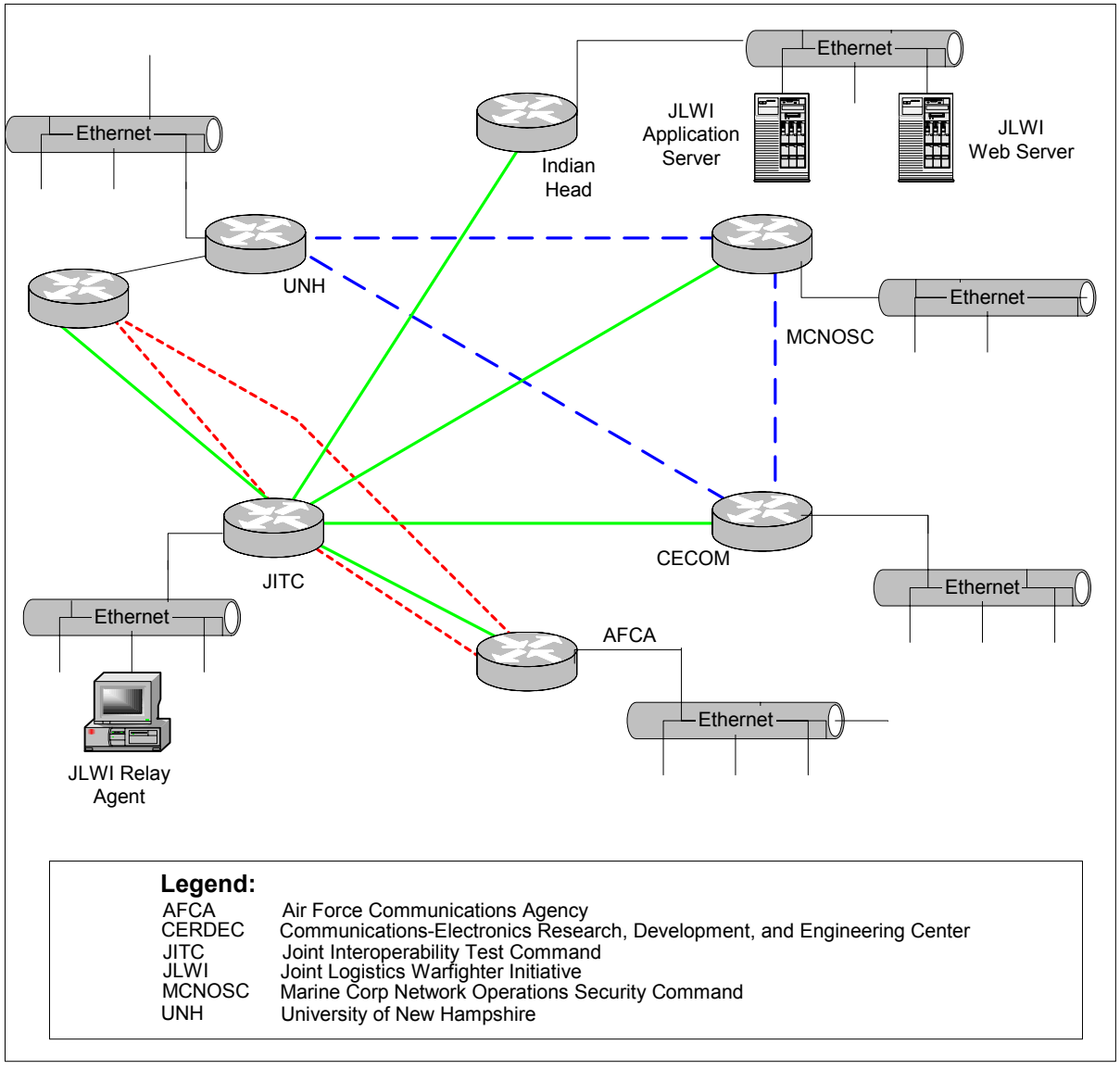


Figure 6. JLWI Test Network

VideoTeleconferencing Testing

VideoTeleconferencing testing will involve establishing and monitoring VTC sessions between four sites. VTC equipment will include the PolyCom Viewstation 128 and/or the PolyCom Viewstation v.35 running in dual (IPv4/IPv6) protocol stack (if available by the beginning of VTC testing). Refer to figure 7 for the network that will be used to assess VTC. Detailed procedures for VTC testing can be found in appendix C, annex 5.

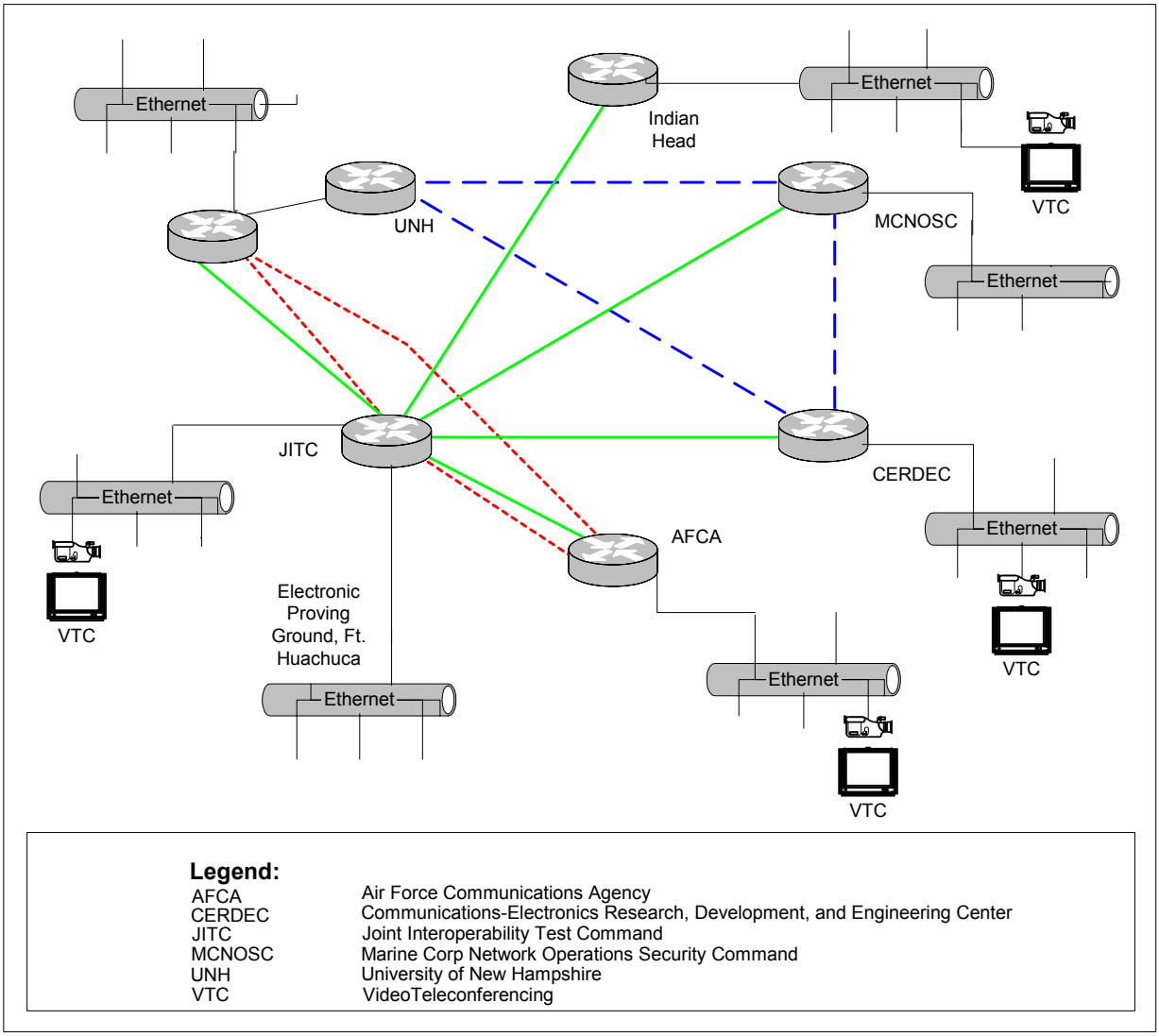


Figure 7. VTC Test Network

DCTS Testing

DCTS testing will occur between six sites, each equipped with DCTS-capable personal computers and DCTS software. The DCTS server, located at JITC Indian Head, will be configured to support the Moonv6 DCTS user community as shown in figure 8. At least one client at each site will initiate and host multiple DCTS sessions. Each session will include audio, video, white boarding, document sharing, and instant messaging. Refer to appendix C; annex 6 for the detailed procedures that will be used to test DCTS.

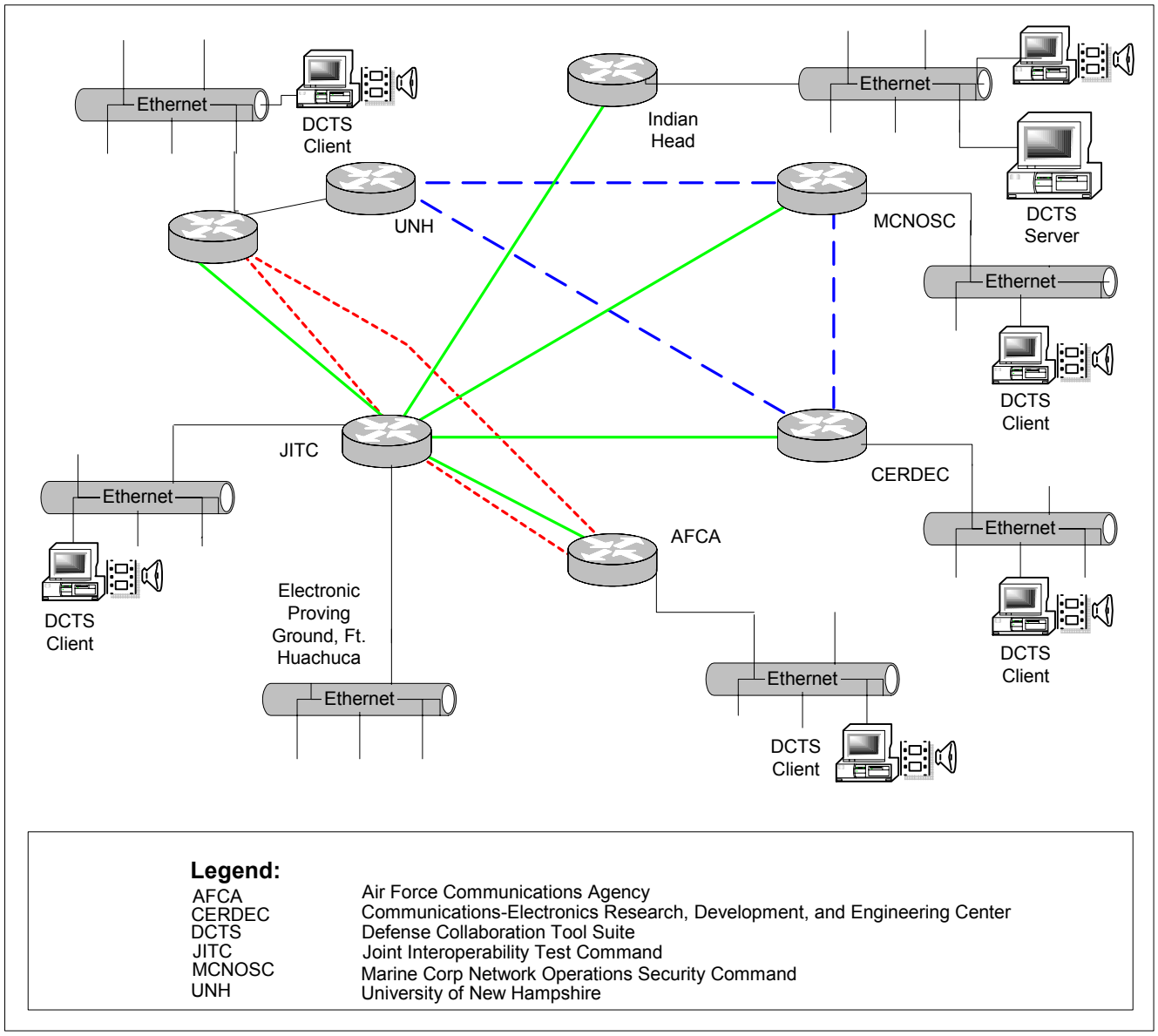


Figure 8. DCTS Test Network

Mobility Testing

IPv6 Mobility testing will be conducted between five sites. Wireless mobile nodes will be used at JITC Indian Head, AFCA, and JITC Ft. Huachuca. Home agents will be installed and configured at JITC Ft. Huachuca and MCNOSC. Correspondent nodes will be located at each participating site. The wireless mobile nodes will traverse multiple wireless access points located on different sub networks, creating the need for binding updates to be processed by the home Agent and the correspondent node(s). Testing will determine if each Mobility implementation properly supports binding updates, mobile node functionality, correspondent node functionality, and home agent functionality. Figure 9 depicts the network configuration that will be used for Mobility testing. Refer to appendix C; annex 7 for detailed Mobility test procedures.

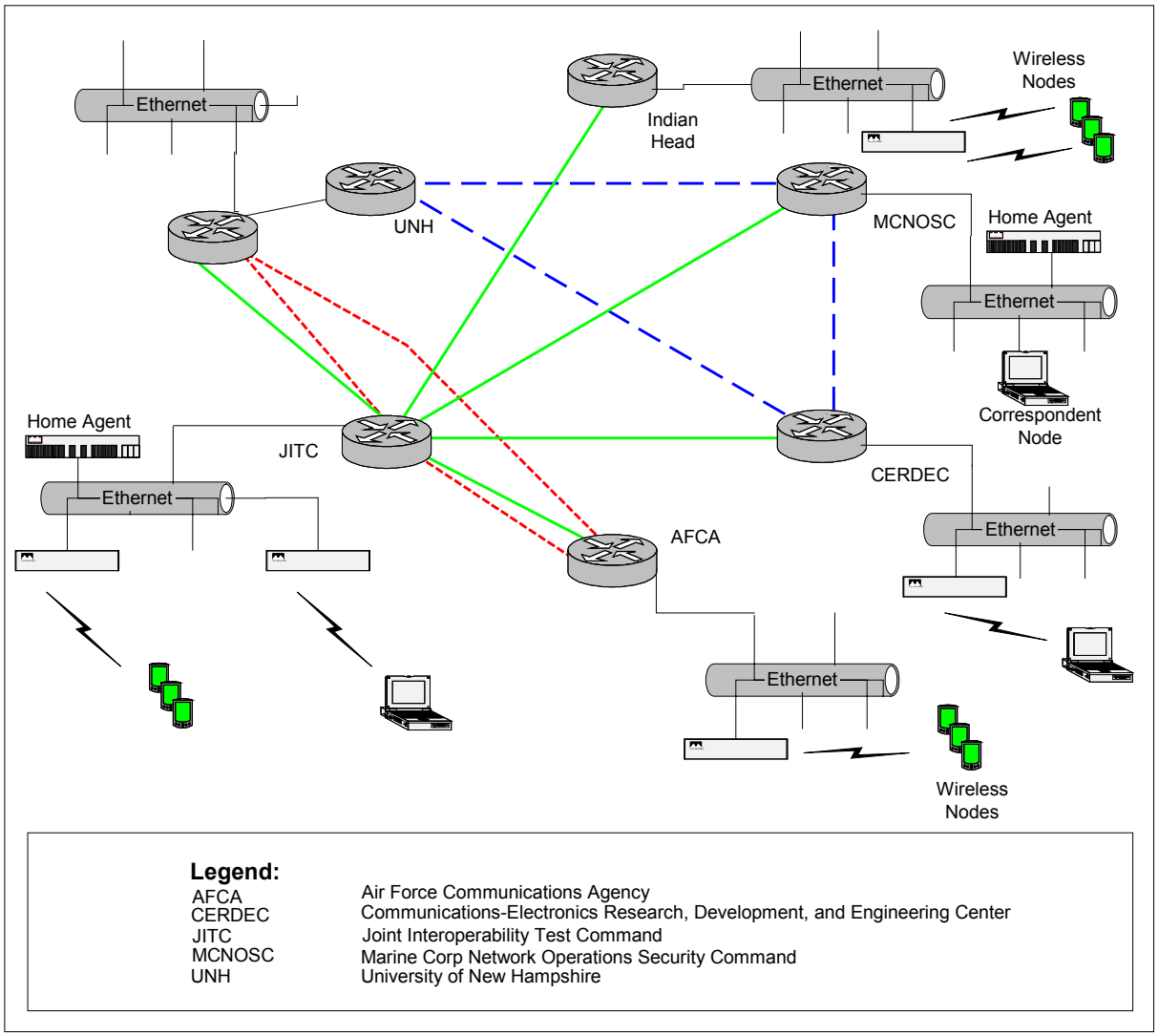


Figure 9. Mobility Test Network

Security Testing

Security testing will take place between JITC Ft. Huachuca and MCNOSC. IPv6 Security (IP Sec)-capable workstations will be installed and configured at both sites. Certificates will be obtained from the PKI server located at Ft. Huachuca and these shared certificates will be used to establish secure connections between the workstations. Testing will determine if Authentication Header and Encapsulating Security Payload interoperate properly across the end-to-end network. Telnet, Trivial File Transfer Protocol and ICMP (Internet Control Message Protocol) will be used to verify proper operation of the security mechanism. Figure 10 shows the network configuration that will be used for IP Sec testing. Refer to appendix C; annex 8 for the detailed procedures associated with IP Sec testing.

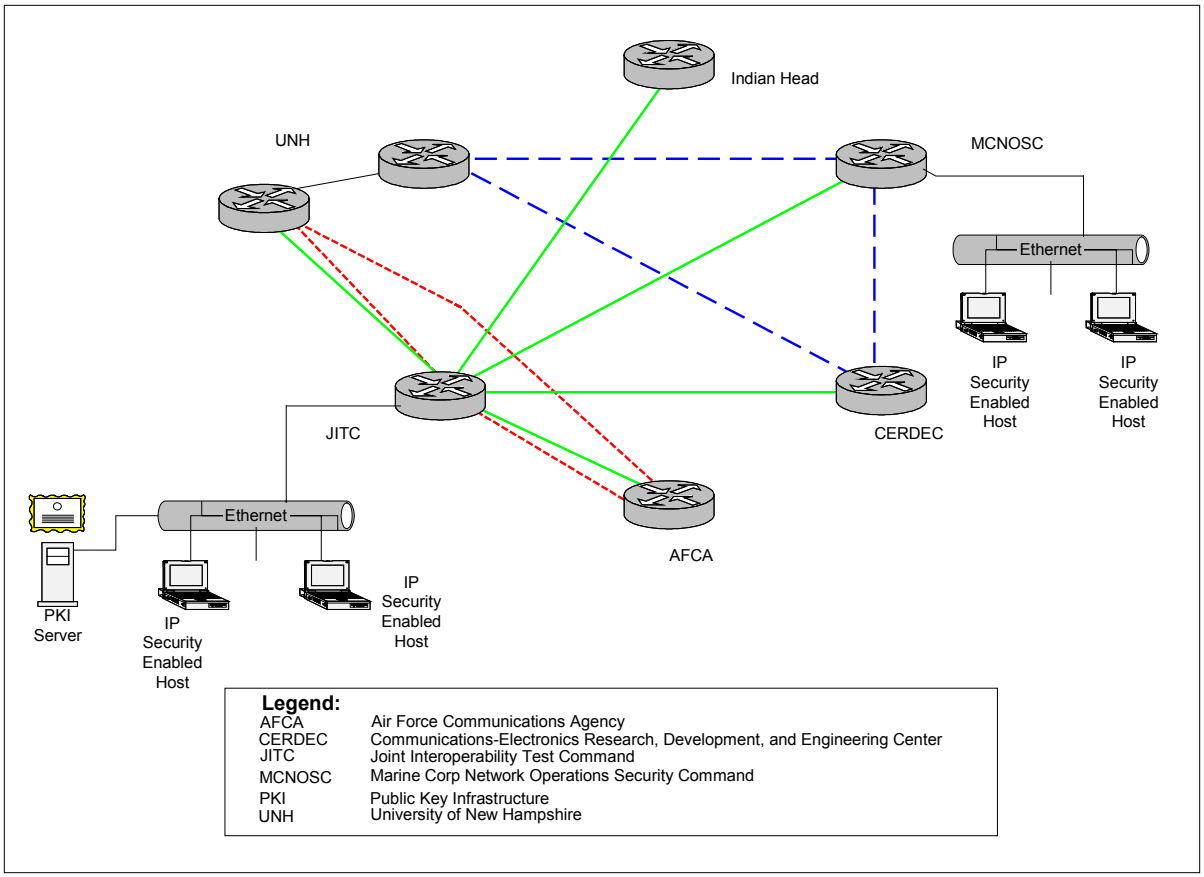


Figure 10. IP Security Test Network

Router Conformance Testing

Figure 11 depicts the network and test equipment string that will be used to perform router conformance testing. Using automated test suites from Spirent, Ixia, and Agilent, various IPv6 and IPv4-specific router conformance tests will be executed. Each network device will be connected to the test equipment and, if necessary, a second network device. Connectivity between the network device(s) and the test equipment will be verified after which the test script will be started. For the duration of a specific test, the test equipment and network device(s) will be monitored for anomalies. See

appendix C, annex 9 for the detailed test procedures that will be used to perform router conformance testing.

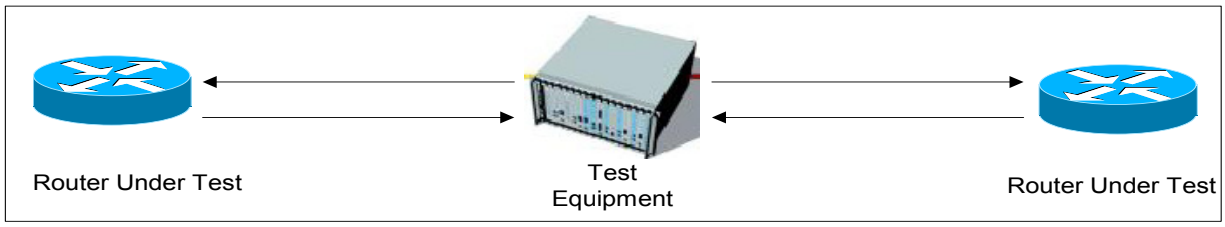


Figure 11. Device-Centric Testing

Network Performance and Loading

Performance testing will occur over the end-to-end network (network-centric testing) and between devices (device-centric testing). Equipment and network configurations for both topologies are shown in figures 11 and 12. Tests will include throughput, forwarding rate and latency of automatic tunnels, configured tunnels, and 6-to-4 tunnels. A 48-hour network stability test will be run. During stability testing, each site will be loaded with varying levels of IPv4 and IPv6 datagram's at approximately 80% of the available bandwidth.

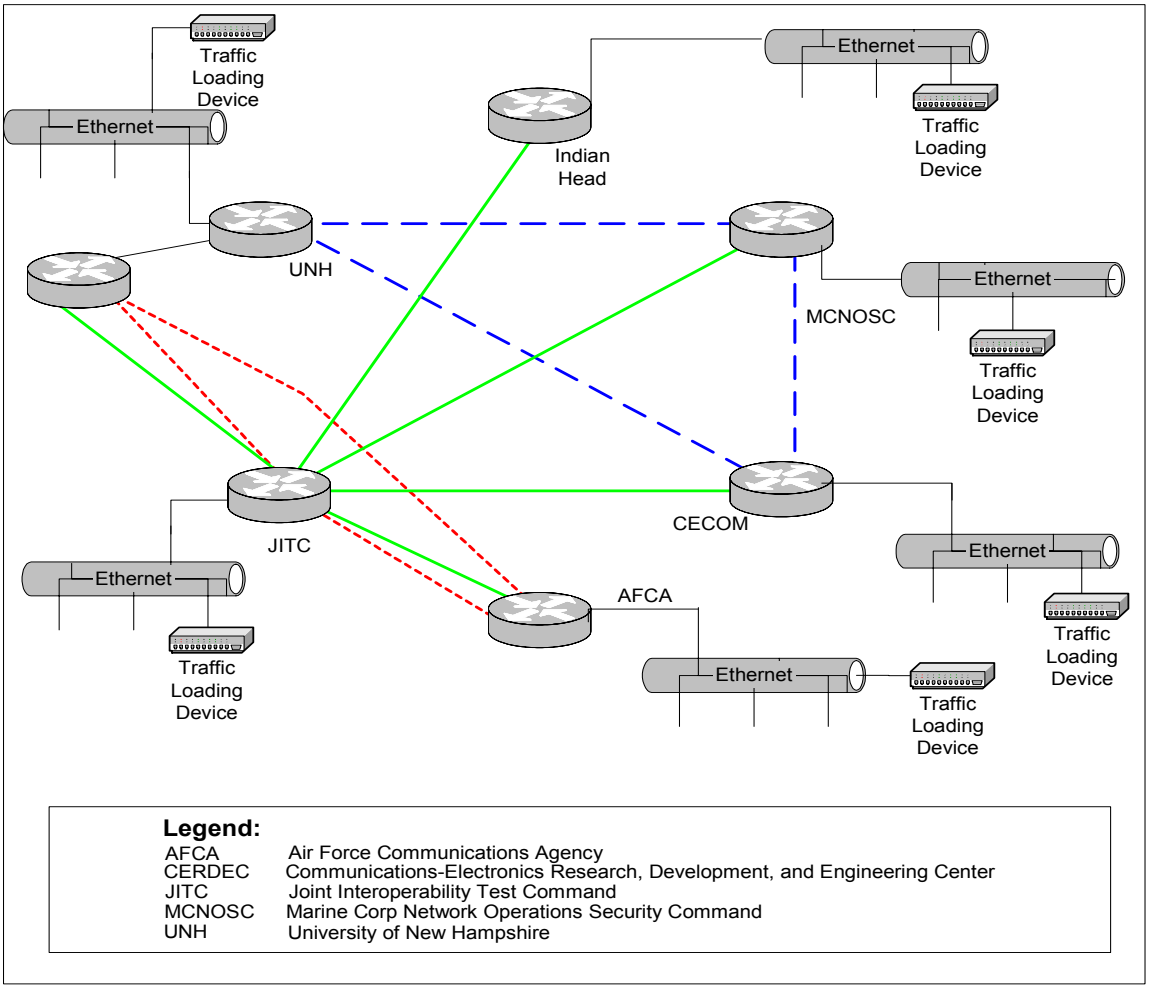


Figure 12. Network-Centric Testing

Network Fault Testing

Figure 13 shows the network configuration that will be used for network fault testing. Circuits under test will include Gigabit Ethernet, Asynchronous Transfer Mode, and Fast Ethernet. Circuit failures will be inserted at each red X as shown in figure 12 and the network monitored to determine if each network device responds appropriately by rerouting traffic, processing alarms, providing network management failure notification, and recalculating routes.

Domain Name System Primary Server Failure Testing

This test will determine if an IPv4 DNS server will properly resolve domain names when the primary IPv6 DNS server has failed. Servers will support both IPv4 and IPv6 addresses and resolve A and quad A records as needed. Refer to appendix C annex 12 for the detailed procedures associated with DNS testing.

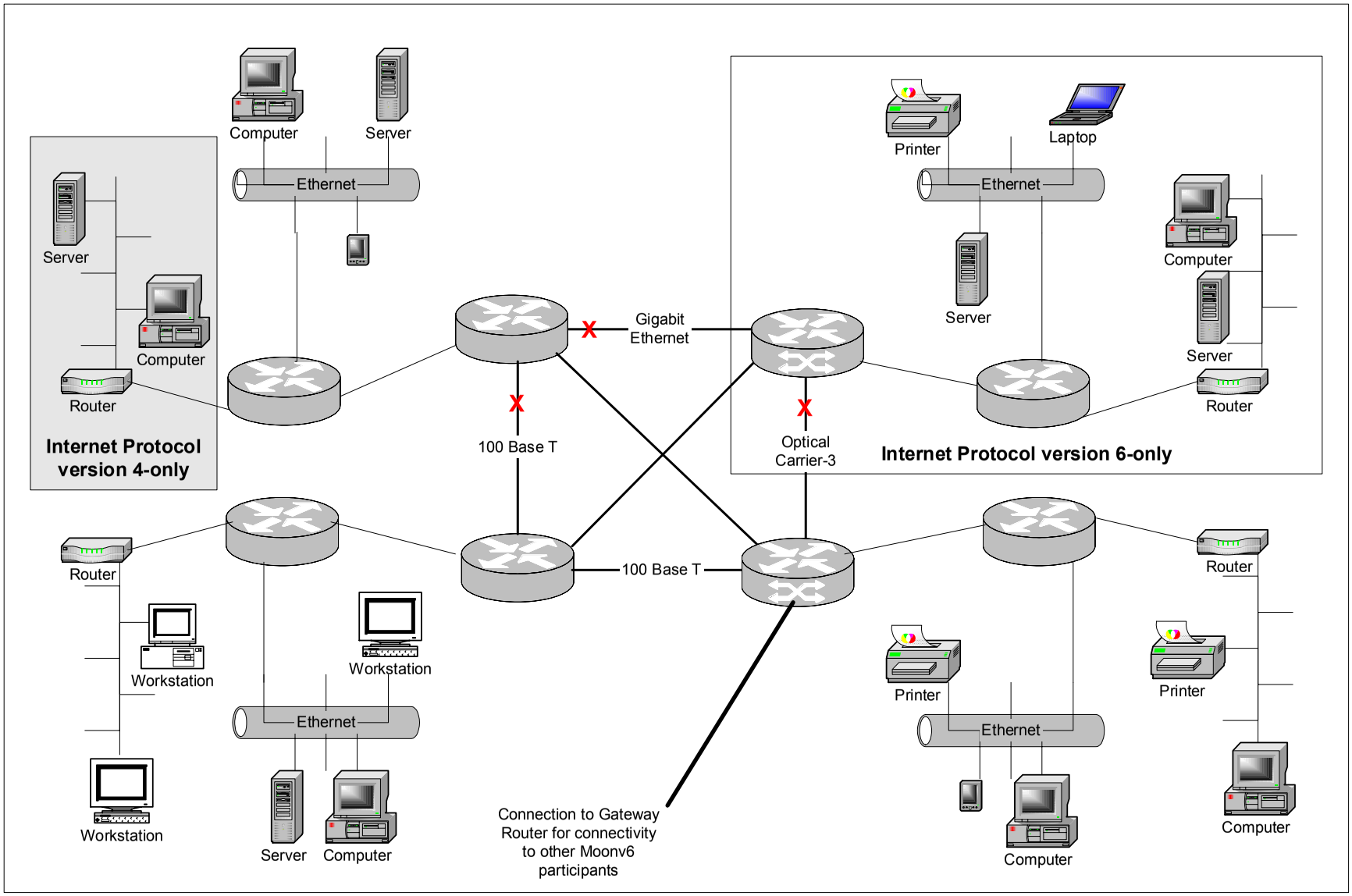


Figure 13. Network Fault Testing

PRESENTATION OF RESULTS AND ANALYSIS PROCEDURES

Assessment results will be summarized using text, tables, and figures. Tables 3 through 5 represent example results for e-mail, PKI, and HTTP. Results for other tests will be presented in a similar format. Results will be summarized using descriptive statistics. The estimated impact on DOD networks or network implementations of any failures or anomalies discovered during testing will also be presented.

Table 3. Example E-mail Results

CLIENT SENDS	EMAIL WITH PPT FILE ATTACHED	EMAIL WITH XLS FILE ATTACHED	EMAIL WITH TXT FILE ATTACHED	EMAIL WITH DOC FILE ATTACHED	EMAIL WITH JPG FILE ATTACHED	LARGE FILE (5.0 M)
From: MCNOSC						
To:						
CERDEC	Message exchanged with no errors					
Indian Head	Message exchanged with no errors					
AFCA	Message exchanged with no errors					
JITC	Message exchanged with no errors					
UNH	Message exchanged with no errors					

Legend:

AFCA	Air Force Communications Agency	MCNOSC	Marine Corp Network Operations Security Command
CERDEC	Communications-Electronics Research, Development, and Engineering Center	ppt	Microsoft PowerPoint file format
doc	Microsoft Word file format	txt	Text file format
JITC	Joint Interoperability Test Command	unh	University of New Hampshire
jpg		xls	Microsoft Excel file format
M	Megabytes		

Table 4. Example PKI Results

CLIENT ACTION	OBTAIN CERTIFICATE	EXCHANGE SECURE E-MAIL	ACCESS PKI ENABLED WEBSITES	USE VALIDATION SERVICES	USE DIRECTORY SERVICES
From: MCNOSC					
To: JITC	Certificate obtained	Message exchanged with no errors	Website accessed properly	Validation functioned properly	Directory Services functioned properly

Legend:

AFCA	Air Force Communications Agency	MCNOSC	Marine Corp Network Operations Security Command
CERDEC	Communications-Electronics Research, Development, and Engineering Center	ppt	Microsoft PowerPoint file format
doc	Microsoft Word file format	txt	Text file format
JITC	Joint Interoperability Test Command	unh	University of New Hampshire
jpg		xls	Microsoft Excel file format
M	Megabytes		

Table 5. Example HTTP Results

CLIENT ACCESS	SERVER USING IPv6 ADDRESS	SERVER USING DNS	FILE TRANSFER	FORM COMPLETION USING IPv6 ADDRESS OR DNS
Web Client Location: MCNOSC				
Server Location:				
CERDEC	Access successful	Access successful	File transfer successful	Form completed successfully
Indian Head				
AFCA				
JITC				
UNH				

Legend:

AFCA	Air Force Communications Agency	MCNOSC	Marine Corp Network Operations Security Command
CERDEC	Communications-Electronics Research, Development, and Engineering Center	ppt	Microsoft PowerPoint file format
doc	Microsoft Word file format	txt	Text file format
JITC	Joint Interoperability Test Command	unh	University of New Hampshire
jpg		xls	Microsoft Excel file format
M	Megabytes		

(This page intentionally left blank.)

APPENDIX A

ACRONYMS

AFCA	Air Force Communications Agency
CERDEC	Communications-Electronics Research, Development, and Engineering Center
DCTS	Defense Collaborative Tool Suite
DNS	Domain Name System
DOD	Department of Defense
E-mail	Electronic Mail
EPG	Electronic Proving Ground
GIG-BE	Global Information Grid-Bandwidth Expansion
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPSEC	Internet Protocol IPv6 Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IS-IS	Intermediate System-Intermediate System
JITC	Joint Interoperability Test Command
JLWI	Joint Logistics Warfighter Initiative
JTA	Joint Technical Architecture
LMES	List of Mandated and Emerging Standards
MCNOSC	Marine Corp Network Operations Security Command
MPLS	Multi-Protocol Label Switching
PKI	Public Key Infrastructure
RFC	Request for Comments
TIC	Technology Integration Center
UNH-IOL	University of New Hampshire-Interoperability Lab
VTC	VideoTeleconference

(This page intentionally left blank.)

APPENDIX B

REQUIREMENTS

Table B-1. RFCs Associated with Common Network Applications

RFC NUMBER	JTA STATUS	RFC TITLE
RFC 768	Mandated	User Datagram Protocol
RFC 793	Mandated for IPv6	Transmission Control Protocol
RFC 854	Mandated for IPv6	TELNET Protocol Specification
RFC 855	Mandated for IPv6	Telnet Option Specification
RFC 959	Mandated for IPv6	File Transfer Protocol
RFC 1034	Mandated for IPv6	Domain Names – Concepts and Facilities
RFC 1035	Mandated for IPv6	Domain Names – Implementation and Specification
RFC 1886	Mandated for IPv6	DNS Extensions to Support IPv6
RFC 2136	Mandated for IPv6	Dynamic Updates in the Domain Name System
RFC 3152	Mandated for IPv6	Delegation of IPv6 Advanced Research Projects Agency
RFC 3226	Not Specified	DNS Security and IPv6 Aware Server/Resolver message size requirements
RFC 2874	Not Specified	DNS Extensions to Support IPv6 Address Aggregation and Renumbering
RFC 1350	Mandated for IPv4	The Trivial File Transfer Protocol (Revision 2)
RFC 1570	Mandated for IPv6	Point-to-Point Link Control Protocol Extensions
RFC 1618	Mandated for IPv6	Point-to-Point Protocol over Integrated Services Digital Network
RFC 1661	Mandated for IPv6	The Point to Point Protocol
RFC 1662	Mandated for IPv6	Point-to-Point Protocol in High Level Data Link Control like framing
RFC 1738	Mandated for IPv6	Uniform Resource Locators
RFC 1777	Mandated for IPv6	Lightweight Directory Access Protocol
RFC 1870	Mandated for IPv6	Simple Mail Transfer Protocol Extension for Message Size Declaration
RFC 1989	Mandated for IPv6	Point-to-Point Protocol Link Quality Monitoring
RFC 1994	Mandated for IPv6	Point-to-Point Protocol Challenge Handshake Authentication Protocol
RFC 2045	Mandated for IPv6	Multipurpose Internet Mail Extensions Part One: Format of Internet Message Bodies
RFC 2046	Mandated for IPv6	Multipurpose Internet Mail Extensions Part Two: Media Types
RFC 2047	Mandated for IPv6	Multipurpose Internet Mail Extensions Part Three: Message Header Extensions for Non-American Standard Code for Information Interchange
RFC 2048	Mandated for IPv6	Multipurpose Internet Mail Extensions Part Four: Registration Procedures
RFC 2049	Mandated for IPv6	Multipurpose Internet Mail Extensions Part Five: Conformance Criteria and Examples
RFC 2133	Not Specified	Basic Socket Extensions for IPv6
RFC 2256	Not Specified	A Summary of the X.500 (96) Schema for use with Lightweight Directory Access Protocol version 3
RFC 2251	Emerging	Lightweight Directory Access Protocol Version 3

Table B-1. RFCs Associated with Common Network Applications (continued)

RFC NUMBER	MANDATED BY JTA	RFC TITLE
RFC 2396	Mandated for IPv6	Uniform Resource Identifiers Generic Syntax
RFC 2428	Mandated for IPv6	File Transfer Protocol Extensions for IPv6 and Network Address Translations
RFC 2461	Mandated for IPv6	Neighbor Discovery Protocol
RFC 2616	Mandated for IPv6	Hypertext Transfer Protocol version 1.1
RFC 2821	Mandated for IPv6	Simple Mail Transfer Protocol
RFC 2822	Mandated for IPv6	Internet Message Format
RFC 3315	Emerging	Dynamic Host Configuration Protocol for IPv6

Legend:

DNS	Domain Name System	JTA	Joint Technical Architecture
IPv4	Internet Protocol version 4	RFC	Request For Comment
IPv6	Internet Protocol version 6		

Table B-2. RFCs Associated with Transition Mechanisms

RFC NUMBER	MANDATED BY JTA	RFC TITLE
RFC 1933	Not Specified	Transition Mechanisms for IPv6 Hosts and Routers
RFC 2185	Not Specified	Routing Aspects of IPv6 Transition
RFC 2893	Not Specified	Transition Mechanisms for IPv6 Hosts and Routers

Legend:

IPv6	Internet Protocol version 6	RFC	Request For Comment
JTA	Joint Technical Architecture		

Table B-3. RFCs Associated with Base IPv6 Specifications

RFC NUMBER	MANDATED BY JTA	RFC TITLE
RFC 2374	Emerging	IPv6 Aggregatable Global Unicast Address Format
RFC 2460	Mandated for IPv6	IPv6 Specification
RFC 2464	Emerging	Transmission of IPv6 Packets over Ethernet Networks
RFC 3513	Emerging	IPv6 Addressing Architecture
RFC 1981	Emerging	Path Maximum Transmission Unit Discovery for IPv6

Legend:

IPv4	Internet Protocol version 4	JTA	Joint Technical Architecture
IPv6	Internet Protocol version 6	RFC	Request For Comment

Table B-4. RFCs Associated with Routing Protocols

RFC NUMBER	MANDATED BY JTA	RFC TITLE
RFC 1771	Mandated for IPv6	Border Gateway Protocol version 4
RFC 1772	Mandated for IPv6	Application of the Border Gateway Protocol in the Internet
RFC 2462	Mandated for IPv6	IPv6 Stateless Address Autoconfiguration
RFC 2463	Mandated for IPv6	Internet Control Message Protocol for the IPv6 Specification
RFC 2507	Emerging	Internet Protocol Header Compression
RFC 2545	Mandated for IPv6	Border Gateway Protocol Extensions for IPv6 Interdomain Routing
RFC 2581	Mandated for IPv6	Transmission Control Protocol Congestion Control
RFC 2740	Mandated for IPv6	Open Shortest Path First for IPv6
RFC 2858	Mandated for IPv6	Border Gateway Protocol Extensions
RFC 3168	Emerging	The Addition of Explicit Congestion Notification to Internet Protocol

Legend:

IPv6	Internet Protocol version 6	RFC	Request For Comment
JTA	Joint Technical Architecture		

Table B-5. RFCs Associated with Mobility

RFC NUMBER	MANDATED BY JTA	RFC TITLE
RFC 3220	Not Specified	Internet Protocol Mobility Support for IPv4
RFC 2710	Emerging	Multicast Listener Discovery for IPv6

Legend:

IPv4	Internet Protocol version 4	JTA	Joint Technical Architecture
IPv6	Internet Protocol version 6	RFC	Request For Comment

Table B-6. RFCs Associated with Security

RFC NUMBER	MANDATED BY JTA	RFC TITLE
RFC 1510	Mandated for IPv6	The Kerberos Network Authentication Service version 5
RFC 2401	Mandated for IPv6	Security Architecture for the Internet Protocol
RFC 2402	Mandated for IPv6	Internet Protocol Authentication Header
RFC 2404	Mandated for IPv6	The Use of Hash Message Authentication Code Federal Information Processing Standard 180-1 within Encapsulating Security Payload and Authentication Header
RFC 2406	Mandated for IPv6	Encapsulating Security Payload
RFC 2407	Mandated for IPv6	The Internet IP Security Domain of Interpretation for Internet Security Association and Key Management Protocol
RFC 2408	Mandated for IPv6	Internet Security Association and Key Management Protocol
RFC 2409	Mandated for IPv6	The Internet Key Exchange
RFC 2412	Mandated for IPv6	The Oakley Key Determination Protocol
RFC 2630	Mandated for IPv6	Cryptographic Message Syntax
RFC 2632	Mandated for IPv6	Secure/Multipurpose Internet Mail Extensions version 3 Certificate Handling
RFC 2633	Mandated for IPv6	Secure/Multipurpose Internet Mail Extensions version 3 Message Specification
RFC 2634	Mandated for IPv6	Enhanced Security Services for Secure/Multipurpose Internet Mail Extensions

Legend:

DNS	Domain Name System	IPv6	Internet Protocol version 6
IP	Internet Protocol	JTA	Joint Technical Architecture
IPv4	Internet Protocol version 4	RFC	Request For Comment

APPENDIX C

DETAILED ASSESSMENT PROCEDURES

This appendix is divided into 11 annexes, shown below, that correspond to the 11 major assessment objectives. Detailed procedures for each major assessment objective are found in the associated Annex.

- Electronic Mail (E-mail) — Annex 1
- Hypertext Transfer Protocol (HTTP — Annex 2
- Public Key Infrastructure (PKI) — Annex 3
- Joint Logistics Warfighter Initiative (JLWI) — Annex 4
- Video Teleconferencing (VTC) — Annex 5
- Defense Collaborative Tool Suite (DCTS) — Annex 6
- Mobility — Annex 7
- Security — Annex 8
- Router Conformance: Multi-Protocol Label Switching (MPLS) and Intermediate System-Intermediate System (IS-IS) conformance — Annex 9
- Network Performance and Loading — Annex 10
- Network Failure Testing — Annex 11
- Domain Name System — Annex 12

(This page intentionally left blank.)

APPENDIX C, ANNEX ONE

ELECTRONIC MAIL

Test 1.1. Electronic Mail (E-mail) Test

Purpose: To verify that a Simple Mail Transfer Protocol (SMTP) session between two nodes can occur over an IPv6 link.

References: RFC-2821 – Sections 3 and 4

Resource Requirements: Packet capture tools, binary file comparison tools.

Discussion: This test verifies that an electronic mail transfer session can be held over an IPv6 link between properly configured nodes.

Test Setup: Establish a network of email clients and servers as shown in figure C-1-1. Ensure network connectivity exists between all attached devices.

Procedures:

- Part A: Sending E-mail
- A Client at each site sends an e-mail destined to every other client on the network as shown in tables C-1-1 through C-1-6.
- Part B: Receiving E-mail
- Each Client should receive the email.

Measurable Results:

- In Part A, each client should successfully send the email.

- In part B, each client should successfully receive the email and run a binary file comparison on each file attachment to confirm that they are unchanged.

Test 1.2. E-mail Load Test

Procedures: At the conclusion of manual e-mail testing, begin an e-mail load test lasting 48 hours using one of the automated e-mail test systems. Send and receive at least 250,000 emails. During the test, monitor the network for protocol-induced failures or anomalies.

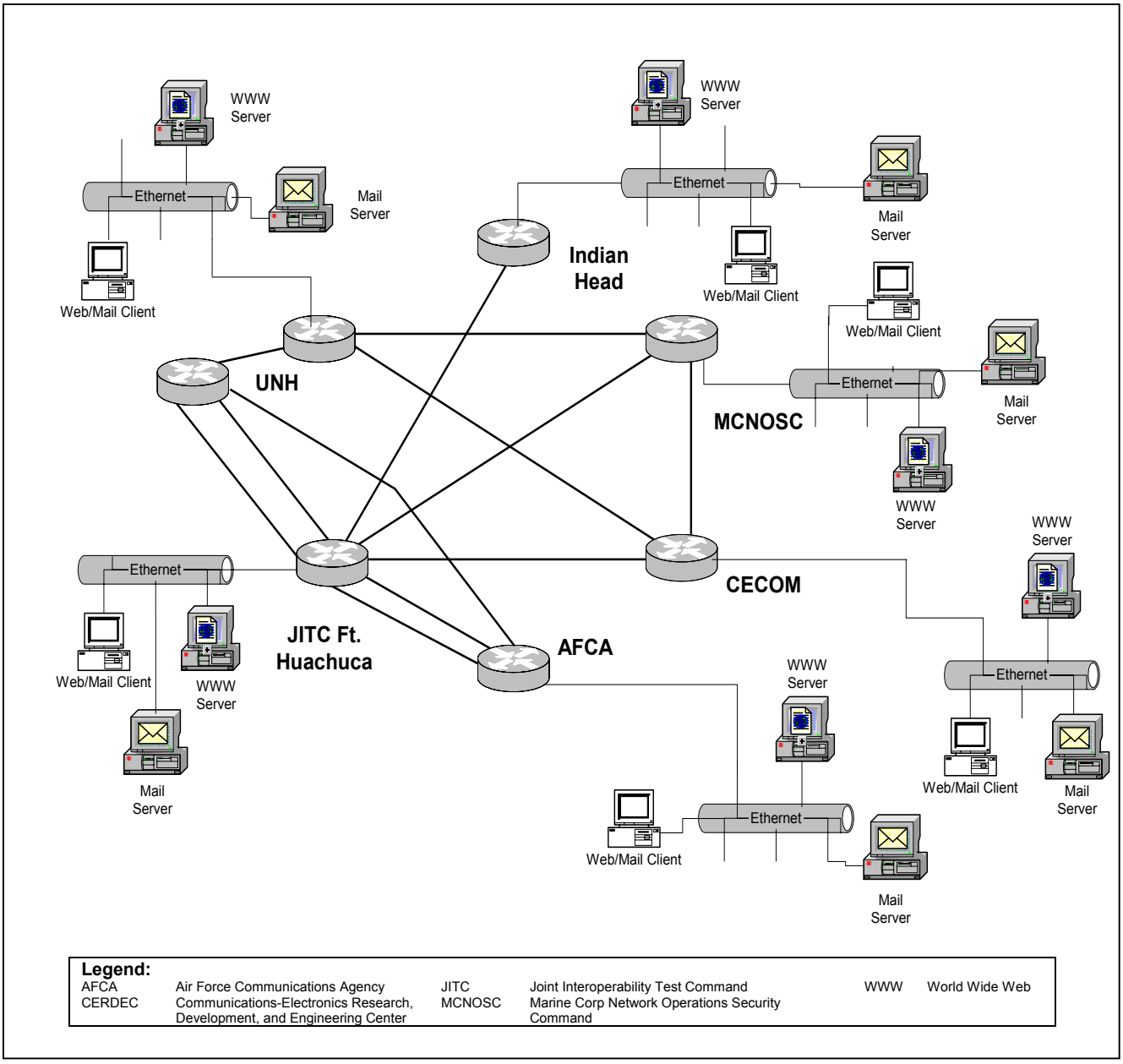


Figure C-1-1. E-mail Test Network

Table C-1-1. MCNOSC Originating Client

Client Sends	Email with ppt attachment	Email with xls attachment	Email with txt attachment	Email with doc attachment	Email with jpg attachment	Large File Attachment (5.0 M)
From: MCNOSC						
To: CERDEC						
Indian Head						
AFCA						
JITC						
UNH						

Legend:

AFCA	Air Force Communications Agency	MCNOSC	Marine Corp Network Operations Security Command
CERDEC	Communications-Electronics Research, Development, and Engineering Center	ppt	Microsoft PowerPoint file format
doc	Microsoft Word file format	txt	Text file format
JITC	Joint Interoperability Test Command	unh	University of New Hampshire
jpg		xls	Microsoft Excel file format
M	Megabytes		

Table C-1-2. CERDEC Originating Client

Client Sends	Email with ppt attachment	Email with xls attachment	Email with txt attachment	Email with doc attachment	Email with jpg attachment	Large File Attachment (5.0 M)
From: CERDEC						
To: MCNOSC						
Indian Head						
AFCA						
JITC						
UNH						

Legend:

AFCA	Air Force Communications Agency	MCNOSC	Marine Corp Network Operations Security Command
CERDEC	Communications-Electronics Research, Development, and Engineering Center	ppt	Microsoft PowerPoint file format
doc	Microsoft Word file format	txt	Text file format
JITC	Joint Interoperability Test Command	unh	University of New Hampshire
jpg		xls	Microsoft Excel file format
M	Megabytes		

Table C-1-3. Indian Head Originating Client

Client Sends	Email with ppt attachment	Email with xls attachment	Email with txt attachment	Email with doc attachment	Email with jpg attachment	Large File Attachment (5.0 M)
From: Indian Head						
To:						
CERDEC						
MCNOSC						
AFCA						
JITC						
UNH						

Legend:

AFCA	Air Force Communications Agency	MCNOSC	Marine Corp Network Operations Security Command
CERDEC	Communications-Electronics Research, Development, and Engineering Center	ppt	Microsoft PowerPoint file format
doc	Microsoft Word file format	txt	Text file format
JITC	Joint Interoperability Test Command	unh	University of New Hampshire
jpg		xls	Microsoft Excel file format
M	Megabytes		

Table C-1-4. AFCA Originating Client

Client Sends	Email with ppt attachment	Email with xls attachment	Email with txt attachment	Email with doc attachment	Email with jpg attachment	Large File Attachment (5.0 M)
From: AFCA						
To:						
CERDEC						
Indian Head						
MCNOSC						
JITC						
UNH						

Legend:

AFCA	Air Force Communications Agency	MCNOSC	Marine Corp Network Operations Security Command
CERDEC	Communications-Electronics Research, Development, and Engineering Center	ppt	Microsoft PowerPoint file format
doc	Microsoft Word file format	txt	Text file format
JITC	Joint Interoperability Test Command	unh	University of New Hampshire
jpg		xls	Microsoft Excel file format
M	Megabytes		

Table C-1-5. UNH Originating Client

Client Sends	Email with ppt attachment	Email with xls attachment	Email with txt attachment	Email with doc attachment	Email with jpg attachment	Large File Attachment (5.0 M)
From: UNH						
To:						
CERDEC						
Indian Head						
AFCA						
MCNOSC						
JITC						

Legend:

AFCA	Air Force Communications Agency	MCNOSC	Marine Corp Network Operations Security Command
CERDEC	Communications-Electronics Research, Development, and Engineering Center	ppt	Microsoft PowerPoint file format
doc	Microsoft Word file format	txt	Text file format
JITC	Joint Interoperability Test Command	unh	University of New Hampshire
jpg		xls	Microsoft Excel file format
M	Megabytes		

Table C-1-6. JITC Ft. Huachuca Originating Client

Client Sends	Email with ppt attachment	Email with xls attachment	Email with txt attachment	Email with doc attachment	Email with jpg attachment	Large File Attachment (5.0 M)
From: JITC						
To:						
CERDEC						
Indian Head						
AFCA						
MCNOSC						
UNH						

Legend:

AFCA	Air Force Communications Agency	MCNOSC	Marine Corp Network Operations Security Command
CERDEC	Communications-Electronics Research, Development, and Engineering Center	ppt	Microsoft PowerPoint file format
doc	Microsoft Word file format	txt	Text file format
JITC	Joint Interoperability Test Command	unh	University of New Hampshire
jpg		xls	Microsoft Excel file format
M	Megabytes		

(This page intentionally left blank.)

APPENDIX C, ANNEX TWO

HYPERTEXT TRANSFER PROTOCOL

Test 2.1. Hyptertext Transfer Protocol

Purpose: To verify that Hypertext Transfer Protocol (HTTP) communications can be accomplished over an IPv6 link.

References: RFC-2616 – Sections 4, 5 and 6

Resource Requirements: Packet capture tools.

Discussion: This test verifies that a device can properly perform as an IPv6 HTTP client.

Test Setup: Establish a network of web clients and web servers as shown in figure C-2-1. Ensure network connectivity exists between all attached devices.

Procedures:

- Part A: Requesting information using literal IPv6 addresses
    - Each site should access the Moonv6 Phase II web page at every other site using literal IPv6 addresses.
    - Each site should access the Moonv6 Phase II web page at every other site using domain names.

- Part B: Posting information using literal IPv6 addresses or domain names
    - Each site should access the Moonv6 Phase II web page at every other site using domain names or literal IPv6 addresses.
    - Each site should then navigate to the Form link, access the form and input the data as requested by the fields on the form.

- **Observable Results:**
- In Part A, each clients web browser should receive the web pages requested.

- In Part B, each client must be able to properly update the form.

Test 2.2. HTTP Load Test

Procedures: At the conclusion of manual HTTP testing, begin an HTTP load test lasting 48 hours using one of the automated e-mail test systems. Initiate at least 500,000 HTTP sessions. During the test, monitor the network for protocol-induced failures or anomalies.

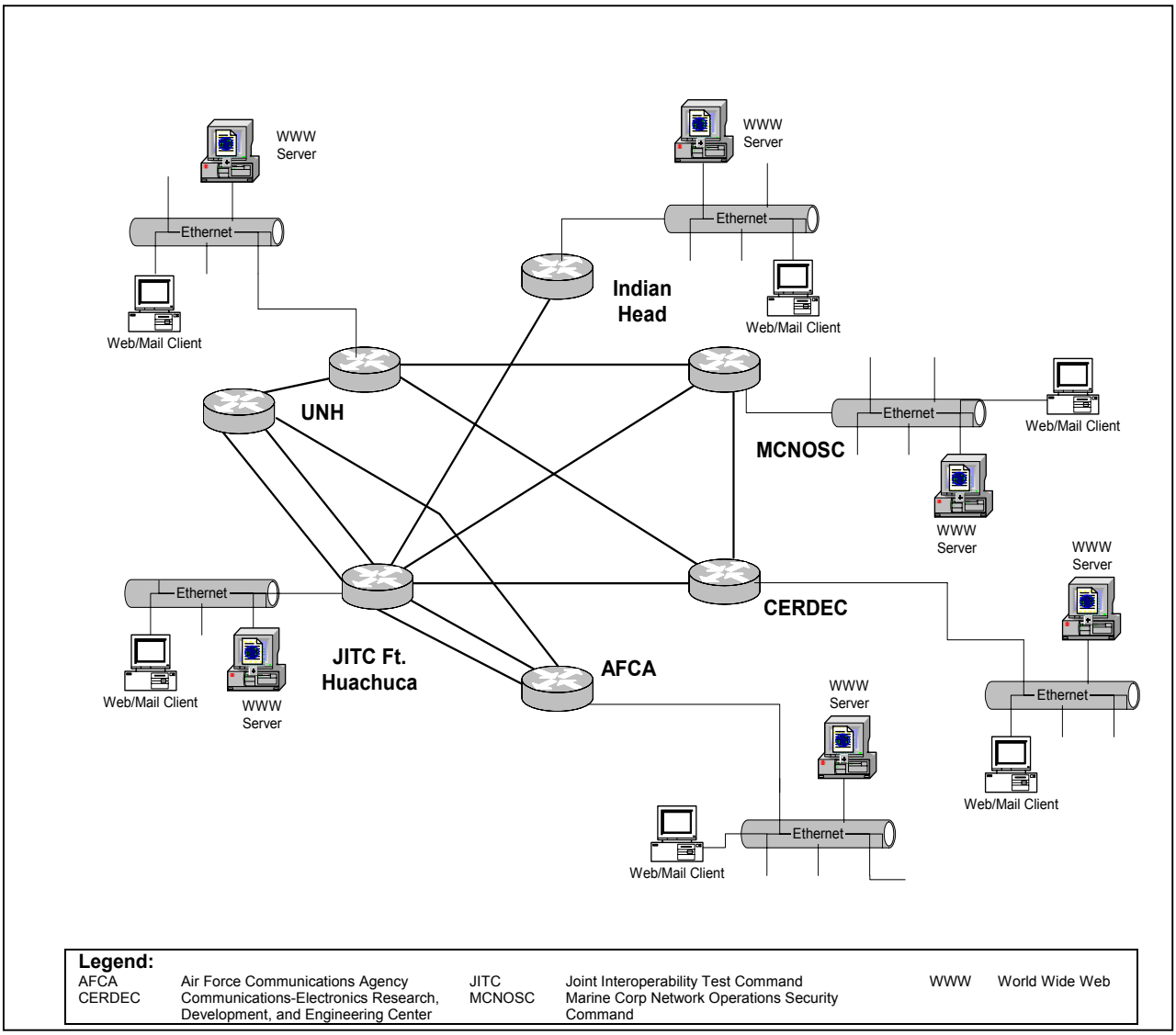


Figure C-2-1. Internet Application Test Network

Table C-2-1. Internet Tests-Client at MCNOSC

CLIENT ACCESS	CONNECT TO SERVER USING IPv6 ADDRESS	CONNECT TO SERVER USING DOMAIN NAMES	FILE TRANSFER	FORM COMPLETION USING IPv6 ADDRESS OR DNS
Web Client Location: MCNOSC				
Server Location:				
CERDEC				
Indian Head				
AFCA				
JITC				
UNH				

Legend:

AFCA	Air Force Communications Agency	MCNOSC	Marine Corp Network Operations Security Command
CERDEC	Communications-Electronics Research, Development, and Engineering Center	ppt	Microsoft PowerPoint file format
doc	Microsoft Word file format	txt	Text file format
JITC	Joint Interoperability Test Command	unh	University of New Hampshire
Jpg		xls	Microsoft Excel file format
M	Megabytes		

Table C-2-2. Internet Tests-Client at CERDEC

CLIENT ACCESS	CONNECT TO SERVER USING IPv6 ADDRESS	CONNECT TO SERVER USING DOMAIN NAMES	FILE TRANSFER	FORM COMPLETION USING IPv6 ADDRESS OR DNS
Web Client Location: CERDEC				
Server Locations:				
MCNOSC				
Indian Head				
AFCA				
JITC				
UNH				

Legend:

AFCA	Air Force Communications Agency	MCNOSC	Marine Corp Network Operations Security Command
CERDEC	Communications-Electronics Research, Development, and Engineering Center	ppt	Microsoft PowerPoint file format
doc	Microsoft Word file format	txt	Text file format
JITC	Joint Interoperability Test Command	unh	University of New Hampshire
Jpg		xls	Microsoft Excel file format
M	Megabytes		

Table C-2-3. Internet Tests-Client at Indian Head

CLIENT ACCESS	CONNECT TO SERVER USING IPv6 ADDRESS	CONNECT TO SERVER USING DOMAIN NAMES	FILE TRANSFER	FORM COMPLETION USING IPv6 ADDRESS OR DNS
Web Client Location: Indian Head				
Server Locations:				
MCNOSC				
CERDEC				
AFCA				
JITC				
UNH				

Legend:

AFCA	Air Force Communications Agency	MCNOSC	Marine Corp Network Operations Security Command
CERDEC	Communications-Electronics Research, Development, and Engineering Center	ppt	Microsoft PowerPoint file format
doc	Microsoft Word file format	txt	Text file format
JITC	Joint Interoperability Test Command	unh	University of New Hampshire
Jpg		xls	Microsoft Excel file format
M	Megabytes		

Table C-2-4. Internet Tests-Client at AFCA

CLIENT ACCESS	CONNECT TO SERVER USING IPv6 ADDRESS	CONNECT TO SERVER USING DOMAIN NAMES	FILE TRANSFER	FORM COMPLETION USING IPv6 ADDRESS OR DNS
Web Client Location: AFCA				
Server Locations:				
MCNOSC				
Indian Head				
CERDEC				
JITC				
UNH				

Legend:

AFCA	Air Force Communications Agency	MCNOSC	Marine Corp Network Operations Security Command
CERDEC	Communications-Electronics Research, Development, and Engineering Center	ppt	Microsoft PowerPoint file format
doc	Microsoft Word file format	txt	Text file format
JITC	Joint Interoperability Test Command	unh	University of New Hampshire
Jpg		xls	Microsoft Excel file format
M	Megabytes		

Table C-2-5. Internet Tests-Client at UNH

CLIENT ACCESS	CONNECT TO SERVER USING IPv6 ADDRESS	CONNECT TO SERVER USING DOMAIN NAMES	FILE TRANSFER	FORM COMPLETION USING IPv6 ADDRESS OR DNS
Web Client Location: UNH				
Server Locations:				
MCNOSC				
Indian Head				
AFCA				
JITC				
CERDEC				

Legend:

AFCA	Air Force Communications Agency	MCNOSC	Marine Corp Network Operations Security Command
CERDEC	Communications-Electronics Research, Development, and Engineering Center	ppt	Microsoft PowerPoint file format
doc	Microsoft Word file format	txt	Text file format
JITC	Joint Interoperability Test Command	unh	University of New Hampshire
Jpg		xls	Microsoft Excel file format
M	Megabytes		

Table C-2-6. Internet Tests-Client at JITC Ft. Huachuca

CLIENT ACCESS	CONNECT TO SERVER USING IPv6 ADDRESS	CONNECT TO SERVER USING DOMAIN NAMES	FILE TRANSFER	FORM COMPLETION USING IPv6 ADDRESS OR DNS
Web Client Location: JITC				
Server Locations:				
MCNOSC				
Indian Head				
AFCA				
UNH				
CERDEC				

Legend:

AFCA	Air Force Communications Agency	MCNOSC	Marine Corp Network Operations Security Command
CERDEC	Communications-Electronics Research, Development, and Engineering Center	ppt	Microsoft PowerPoint file format
doc	Microsoft Word file format	txt	Text file format
JITC	Joint Interoperability Test Command	unh	University of New Hampshire
Jpg		xls	Microsoft Excel file format
M	Megabytes		

(This page intentionally left blank.)

APPENDIX C, ANNEX THREE

PUBLIC KEY INFRASTRUCTURE

Test 3.1. PKI Operation

Purpose: To verify that Public Key Infrastructure (PKI) utilities can be used in an IPv6/IPv4 network.

References:

- Defense Information Systems Agency (DISA) and National Security Agency (NSA) "Department of Defense (DOD) Class 3 Public Key Infrastructure (PKI) Public-Key-Enabled Application Requirements," version 1.0, 13 2000.
- DISA and NSA "Department of Defense Class 3 Public Key Infrastructure Interface Specification", Version 1.2, 10 August 2000.

Resource Requirements: One PKI-capable server at JITC Ft. Huachuca and at least one PKI-capable client at MCNOSC.

Background: The Department of Defense (DOD) Public Key Infrastructure (PKI) provides information assurance (IA) support services for command, control, communications, computers and intelligence (C4I). DOD PKI refers to the framework and services that provide for the generation, production, distribution, control, revocation, recovery and tracking of Public Key (PK) certificates and their corresponding private keys. Operating in concert with directories and tokens such as the Common Access Card (CAC), it supports registration of subscribers, dissemination of certificates and a full range of certificate management services. It was developed in accordance with the DOD Defense-In-Depth, layered IA strategy and data integrity requirements.

The integrated DOD PKI provides critically needed support to individuals, a broad range of government and commercially based security-enabled applications and network devices. Services include application-layer encryption for e-mail and authentication of network transactions (e.g., client authentication using secure socket layer (SSL) sessions) as well as data integrity and non-repudiation. The DOD PKI also provides for secure interoperability within DOD and with its federal, allied and commercial partners through PKI bridges.

The DOD PKI has been designed to support the entire DOD community, particularly the military, DOD civilians, reservists, retirees and dependents. Currently, issuance of the DOD PKI certificates for the combatant commands, services and agencies is handled through their respective registration authorities (RA), local registration authorities (LRA) and Real-Time Automated Personnel Identifying System (RAPIDS) workstations.

Test Setup: Establish a PKI server at Ft. Huachuca and at least one PKI client at MCNOSC. Execute the test activities as shown in table C-4-1.

Procedures:

- From the client at MCNOSC, obtain a certificate from the PKI server.
- Using the certificate just obtained:
  - Exchange secure email with another site.
  - Access a PKI-enabled website

Table C-3-1. PKI Tests

CLIENT ACTION	OBTAIN CERTIFICATE	EXCHANGE SECURE E-MAIL	ACCESS PKI ENABLED WEBSITES	USE VALIDATION SERVICES	USE DIRECTORY SERVICES
MCNOSC					
To: JITC	Certificate obtained	Message exchanged with no errors	Website accessed properly	Validation functioned properly	Directory Services functioned properly

Legend:

AFCA	Air Force Communications Agency	MCNOSC	Marine Corp Network Operations Security Command
CERDEC	Communications-Electronics Research, Development, and Engineering Center	ppt	Microsoft PowerPoint file format
doc	Microsoft Word file format	txt	Text file format
JITC	Joint Interoperability Test Command	unh	University of New Hampshire
jpg		xls	Microsoft Excel file format
M	Megabytes		

APPENDIX C, ANNEX FOUR

JOINT LOGISTICS WARFIGHTER INITIATIVE

Test 4.1. JLWI Operation

Purpose: To determine if the Joint Logistics Warfighter Initiative (JLWI) properly functions in a mixed IPv4/IPv6 environment.

References: JLWI Quick Reference Guide. Anteon JLWI Test Plan, 8 Jan. 2004.

Resource Requirements: JLWI Relay Agent, JLWI Web Server, JLWI Application Server.

Test Setup: Install a JLWI Relay Agent at JITC Ft. Huachuca. The Relay Agent consists of one personal computer running Windows 2000 Professional pre-loaded with JLWI application software and JLWI data. Install a server suite at JITC Indian Head. The server suite consists of two Dell servers running Windows 2000 Server, J2EE Java version JRun 4.5, and Oracle 9i.

Procedures: Execute the test procedures as shown in table C-4-1, below.

Table C-4-1. JLWI Procedures

TEST CASE IDENTIFICATION							
Test Case Class: Inventory Search **Test Case Number:** J109			**Test Case Name:** Inventory Search Using a NSN/NIIN List and My Stock				
Test Case Objective: This test involves the functionality of conducting an inventory search using a NSN/NIIN list and My Stock.							
Test Case Procedures				**Pass/Fail**			
Steps	**Action**	**Expected Results**	**Actual Results**	**1**	**2**	**3**	**4**
1.	Select **Inventory** from the main menu.	The Inventory drop-down list appears.					
2.	Select **Search,** Select **Reset**. Observe "My Stock" is checked as the default, in Step 2 Where. Select the drop-down arrow on the NSN/NIIN list field and highlight a list. Select **Add.**	Note the selected NSN/NIIN list appears in the Item Window (left side) and the user's default (My Stock) DODAACs are shown in the Location Window (right side).					
3.	Select **Search**.	The Inventory Results Summary page displayed is reflecting the Item requested.					
4.	Drill into a stock number (link).	The reporting DODACCS displayed are reflecting the locations shown in the location window on the main inventory page and consistent with material in each location**.**					

Legend:

DODAAC	Department of Defense Activity Addressing Code
NIIN	National Item Identification Number
NSN	National Stock Number

APPENDIX C, ANNEX FIVE

VIDEO TELECONFERENCING

Test 5.1. VTC Operation

Purpose: To verify that Video Teleconferences can be accomplished over an IPv6 link using an IPv6-capable Video Terminal.

References: Federal Telecommunications Recommendation (FTR) 1080B-2002, dated 8 April 2002.

Resource Requirements: Packet capture tools.

Test Setup: Establish a network of VTC terminals as shown in figure C-1. Each site will execute a minimum of three sessions and a maximum of 10 sessions in each direction. The first call will be held for at least thirty minutes before termination. Each call thereafter will be held for a minimum of ten minutes. During each call, the audio and video quality will be rated using the audio and video quality-rating table. Any rating lower than 4 (Good-Quality is usable) is considered a failure. The ratings depicted in table C-1 were derived from the International Telecommunications Union-Telecommunications (ITU-T) P.80 (03/93) and experienced JITC personnel.

Table C-5-1. Audio and Video Quality Ratings

RATING	REFERENCE	DEFINITION
1	Unusable	Quality is unusable. Voice and video may be heard and seen but is unrecognizable.
2	Poor	Quality is unusable. Words and phrases are not fully understandable or video cannot be properly identified
3	Fair	Quality is seriously affected by distortion. Repeating words and phrases are required to convey speech or video is seriously impacted and barely recognizable
4	Good	Quality is usable. Audio or video is not impaired but some distortion is noticeable
5	Excellent	Quality is unaffected. No discernable problems with either audio or video.
NOTE: These ratings were used to complete the Data Collection Forms. A rating of lower than 4 on this reference scale is considered a failure.		

Procedures:

The test combinations presented in table C-2 will be used to conduct point-to-point conferences using the Moonv6 Phase II network. Systems will include the PolyCom Viewstation 128 and/or the PolyCom Viewstation v.35. Each VTU will be loaded with the most current version of software and configured through software and hardware setups using the appropriate user manual.

Table C-5-2. VTC Test Combinations

TEST PARTNER 1	TEST PARTNER 2	TERMINALS	CIRCUIT
Indian Head	AFCA	IPv4	Encapsulated IPv4 to configured tunnel
MCNOSC	CERDEC	IPv4	Encapsulated IPv4 to automatic tunnel
FHU	UNH	IPv6	Native IPv6

Legend:

AFCA	Air Force Communications Agency	IPv4	Internet Protocol version 4
CERDEC	Communications-Electronics Research, Development, and Engineering Center	IPv6	Internet Protocol version 6
FHU	Ft. Huachuca	MCNOSC	Marine Corp Network Operations Security Command
UNH	University of New Hampshire		

Table C-5-3. VTC Data Collection Form

Date:	**Time:**	**Tester Name:**

Test Partner #1:	**Recommendation**	**Test Partner #2:**	**Recommendation**
____ PictureTel Live 100 ____ PolyCom ViewStation 128 ____ PolyCom ViewStationV.35 ____ ____ ____ ____ ____ _____ Other	___ H.320 ___ H.323 **Location** ____ JITC ____ AFCA ____ UNH ___CERDEC ____ IH ____ MCNOSC	____ PictureTel Live 100 ____ PolyCom ViewStation 128 ____ PolyCom ViewStation V.35 ____ ____ ____ ____ ____ _____ Other	___ H.320 ___ H.323 **Location** ____ JITC ____ AFCA ____ UNH ___CERDEC ____ IH ____ MCNOSC

Network Under Test: ____IPv4/IPv6 ____IPv4 ____IPv6

IPv6 address:	**IPv6 Address:**
IPv4 address:	**IPv4 Address:**

Data Rate 784 Kbps

Call		Call Connect Pass/Fail	Exchange Completed Pass/Fail	Sync Established Pass/Fail	Voice Quality (1 - 5)	Video Quality (1 - 5)	Call Terminate Pass/Fail	Anomaly Number
VTU1 to VTU2	1							
	2							
	3							
	4							
	5							
VTU2 to VTU1	1							
	2							
	3							
	4							
	5							

APPENDIX C, ANNEX SIX

DEFENSE COLLABORATION TOOL SUITE

Test 6.1. DCTS Operation

Purpose: To verify that the Defense Collaboration Tool Suite (DCTS) can be used an IPv6/IPv4 network.

References: ITU-H.323, ITU-T.120, ITU-T.128, ITU-T.126, ITU-G.711, ITU-H.261, ITU-T.127

Resource Requirements: DCTS-capable clients at each site and one DCTS-capable server at Indian Head. Packet capture tools at each site (if needed).

Background: DCTS is a flexible, integrated set of applications providing interoperable, synchronous and asynchronous collaboration capability to the Department of Defense's (DOD) agencies, Combatant Commands and military services. The DCTS program identifies fields and sustains a dynamic set of evolving standard collaboration tools that bridge between DOD and the Intelligence Community. These tools enhance simultaneous, ad hoc crisis and deliberate continuous operational action planning (vertically and horizontally) across operational theaters and other domains that provide operational units and defense organizations simultaneous access to real-time operational, tactical and administrative information.

DCTS offers voice and video conferencing, document and application sharing, instant messaging and whiteboard functionality to support defense planning. It enables two or more distributed operational users to simultaneously participate in the mission planning process without the need to be co-located. With DCTS, military forces enjoy the capability to link various command, control, communications, computers and intelligence (C4I) and mission planning systems together on a common network to share data, conduct collaborative planning and collaboratively consult on information and data at various locations around the world.

Test Setup: Establish a network of DCTS terminals as shown in figure C-6-1. Each site will participate in a minimum of three sessions and a maximum of 10 sessions. The first session will be held for at least thirty minutes before termination. Each session thereafter will be held for a minimum of ten minutes.

Table C-6-1. Audio and Video Quality Ratings

RATING	REFERENCE	DEFINITION
1	Unusable	Quality is unusable. Voice and video may be heard and seen but is unrecognizable.
2	Poor	Quality is unusable. Words and phrases are not fully understandable or video cannot be properly identified
3	Fair	Quality is seriously affected by distortion. Repeating words and phrases are required to convey speech or video is seriously impacted and barely recognizable
4	Good	Quality is usable. Audio or video is not impaired but some distortion is noticeable
5	Excellent	Quality is unaffected. No discernable problems with either audio or video.

NOTE: These ratings were used to complete the Data Collection Forms. A rating of lower than 4 on this reference scale is considered a failure.

Procedures: Each site will participate in DCTS sessions simultaneously with all other sites. The DCTS client at each site will act as session coordinator for at least one session. While acting as session coordinator, the DCTS client shall successfully use and/or demonstrate audio utilities, video utilities, application sharing, whiteboarding, and file transfer. During each session, the audio and video quality will be rated using the audio and video quality-rating table. Any voice or video rating lower than 4 (good-quality is usable) is considered not met. The ratings depicted in table C-6-1 were derived from the International Telecommunications Union-Telecommunications (ITU-T) P.80 (03/93) and experienced JITC personnel. Application sharing, whiteboarding and file transfer will be rated using either a met or not met reference. (If the utility operates successfully for a given site, the rating should be documented as met. If the utility is unsuccessful for a given site the rating is not met.)

Table C-6-2. DCTS Test Combinations-AFCA as Coordinator

DCTS SESSION PARTICIPANTS	DCTS TEST ACTIVITIES				
SESSION COORDINATOR: AFCA	**AUDIO RESULTS** (USE TABLE C-6-1)	**VIDEO RESULTS** (USE TABLE C-6-1)	**APPLICATION SHARING RESULTS** (MET/NOT MET)	**WHITBOARDING RESULTS** (MET/NOT MET)	**FILE TRANSFER RESULTS** (MET/NOT MET)
SESSION PARTICIPANTS:					
CERDEC					
JITC FHU					
INDIAN HEAD					
MCNOSC					
UNH					

Legend:

AFCA	Air Force Communications Agency	JITC FHU	Joint Interoperability Test Command Fort Huachuca
CERDEC	Communications-Electronics Research, Development, and Engineering Center	MCNOSC	Marine Corp Network Operations Center
		UNH	University of New Hampshire

Table C-6-3. DCTS Test Combinations CERDEC as Coordinator

DCTS SESSION PARTICIPANTS	DCTS TEST ACTIVITIES				
SESSION COORDINATOR: CERDEC	**AUDIO RESULTS** (USE TABLE C-6-1)	**VIDEO RESULTS** (USE TABLE C-6-1)	**APPLICATION SHARING RESULTS** (MET/NOT MET)	**WHITBOARDING RESULTS** (MET/NOT MET)	**FILE TRANSFER RESULTS** (MET/NOT MET)
SESSION PARTICIPANTS:					
AFCA					
JITC FHU					
INDIAN HEAD					
MCNOSC					
UNH					

Legend:

AFCA	Air Force Communications Agency	JITC FHU	Joint Interoperability Test Command Fort Huachuca
CERDEC	Communications-Electronics Research, Development, and Engineering Center	MCNOSC	Marine Corp Network Operations Center
		UNH	University of New Hampshire

Table C-6-4. DCTS Test Combinations JITC FHU as Coordinator

DCTS SESSION PARTICIPANTS	DCTS TEST ACTIVITIES				
SESSION COORDINATOR: JITC FHU	**AUDIO RESULTS** (USE TABLE C-6-1)	**VIDEO RESULTS** (USE TABLE C-6-1)	**APPLICATION SHARING RESULTS** (MET/NOT MET)	**WHITBOARDING RESULTS** (MET/NOT MET)	**FILE TRANSFER RESULTS** (MET/NOT MET)
SESSION PARTICIPANTS:					
CERDEC					
AFCA					
INDIAN HEAD					
MCNOSC					
UNH					

Legend:

AFCA	Air Force Communications Agency	JITC FHU	Joint Interoperability Test Command Fort Huachuca
CERDEC	Communications-Electronics Research, Development, and Engineering Center	MCNOSC	Marine Corp Network Operations Center
		UNH	University of New Hampshire

Table C-6-5. DCTS Test Combinations Indian Head as Coordinator

DCTS SESSION PARTICIPANTS	DCTS TEST ACTIVITIES				
SESSION COORDINATOR: INDIAN HEAD	**AUDIO RESULTS** (USE TABLE C-6-1)	**VIDEO RESULTS** (USE TABLE C-6-1)	**APPLICATION SHARING RESULTS** (MET/NOT MET)	**WHITBOARDING RESULTS** (MET/NOT MET)	**FILE TRANSFER RESULTS** (MET/NOT MET)
SESSION PARTICIPANTS:					
CERDEC					
JITC FHU					
AFCA					
MCNOSC					
UNH					

Legend:

AFCA	Air Force Communications Agency	JITC FHU	Joint Interoperability Test Command Fort Huachuca
CERDEC	Communications-Electronics Research, Development, and Engineering Center	MCNOSC	Marine Corp Network Operations Center
		UNH	University of New Hampshire

Table C-6-6. DCTS Test Combinations MCNOSC as Coordinator

DCTS SESSION PARTICIPANTS	DCTS TEST ACTIVITIES				
SESSION COORDINATOR: MCNOSC	**AUDIO RESULTS** (USE TABLE C-6-1)	**VIDEO RESULTS** (USE TABLE C-6-1)	**APPLICATION SHARING RESULTS** (MET/NOT MET)	**WHITBOARDING RESULTS** (MET/NOT MET)	**FILE TRANSFER RESULTS** (MET/NOT MET)
SESSION PARTICIPANTS:					
CERDEC					
JITC FHU					
INDIAN HEAD					
AFCA					
UNH					

Legend:

AFCA	Air Force Communications Agency	JITC FHU	Joint Interoperability Test Command Fort Huachuca
CERDEC	Communications-Electronics Research, Development, and Engineering Center	MCNOSC	Marine Corp Network Operations Center
		UNH	University of New Hampshire

Table C-6-7. DCTS Test Combinations UNH as Coordinator

DCTS SESSION PARTICIPANTS	DCTS TEST ACTIVITIES				
SESSION COORDINATOR: UNH	**AUDIO RESULTS** (USE TABLE C-6-1)	**VIDEO RESULTS** (USE TABLE C-6-1)	**APPLICATION SHARING RESULTS** (MET/NOT MET)	**WHITBOARDING RESULTS** (MET/NOT MET)	**FILE TRANSFER RESULTS** (MET/NOT MET)
SESSION PARTICIPANTS:					
CERDEC					
JITC FHU					
INDIAN HEAD					
MCNOSC					
AFCA					

Legend:

AFCA	Air Force Communications Agency	JITC FHU	Joint Interoperability Test Command Fort Huachuca
CERDEC	Communications-Electronics Research, Development, and Engineering Center	MCNOSC	Marine Corp Network Operations Center
		UNH	University of New Hampshire

(This page intentionally left blank.)

APPENDIX C, ANNEX SEVEN
MOBILITY

SECTION 1: Interoperability background, test definitions, and test overview.

Scope

Tests in this section verify the ability of a Home Agent (HA), Mobile Node (MN), or Correspondent Node (CN) to correctly interoperate in a Mobile IPv6 environment.

Test Applicability

The specific program of tests performed on a device is determined by the device type, which may be a CN, MN, or HA.

CN

Test MIP6.4.1.1: Once for each pair of MN and HA test partners. If the CN and test partners are capable of multiple methods of authentication, this test is performed again for each additional method.

HA

All Tests: Once for each pair of MN and CN test partners. Test MIP6.4.1.2 should be run once against each group of two MNs and one HA. If the HA and test partners are capable of multiple methods of authentication, perform the test again for each additional method.

MN

All Tests: Once for each pair of HA and CN test partners. Test MIP6.4.1.2 should be run once against each group of two HAs and one MN. If the MN and test partners are capable of multiple methods of authentication, perform the test again for each additional method.

Overview

The following tests verify basic operations such as movement detection on the part of the MN, propagation of binding updates, primary care-of address registration, and tunneling of packets by the HA. In addition, these tests also verify the ability of a MN to maintain communication with a Correspondent or MN while moving amongst various foreign networks.

Test MIP1.1.1.1: MN to CN Communication

Purpose: Verify that a MN can move away from its home subnet among various subnets, and maintain a Transmission Control Protocol (TCP) session with a stationary CN on the MN's home network or on a foreign network.

References: Mobility Support in IPv6 (draft 24) – Section 4

Resource Requirements: Packet capture tools, Telnet 6 daemon and client software.

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 home subnet 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.

In general, when a MN sends a Binding Update to its HA to register a new primary care-of address, 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 care-of address.

A MN, whether on its home network or on a foreign network, should be able to communicate with a CN located on the home network or on a foreign network.

Test Setup:

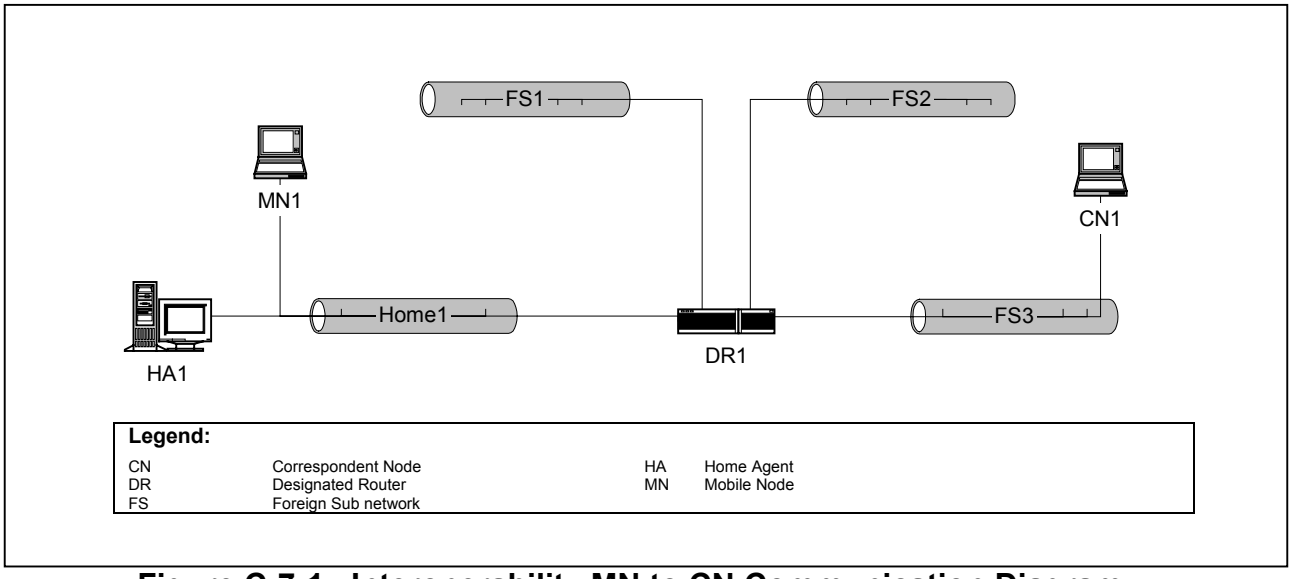


Figure C-7-1. Interoperability MN to CN Communication Diagram

A Mobile Node, MN1, is configured with Home1 as its home subnet, and a HA implementation from another vendor, HA1, as its Home Agent as pictured above. DR1 is configured to act as default router for all of its attached networks. DR1 does not provide HA services. HA1 is configured to act as a HA for its network, but not a default router. HA1 and DR1 may be the same device, if necessary.

Table C-7-1. Router Parameters

DR1	HA1
Router Lifetime: 30 minutes Minimum Advance Interval: 0.5 seconds Maximum Advance Interval: 1.5 seconds	Router Lifetime: 0 seconds Minimum Advance Interval: 0.5 seconds Maximum Advance Interval: 1.5 seconds Home Agent Lifetime: 30 minutes
Each prefix Valid Lifetime: 30 minutes Preferred Lifetime: 20 minutes	**Each prefix** R Bit: Set, full address included Valid Lifetime: 30 minutes Preferred Lifetime: 20 minutes

Procedures:

- Establish a Telnet session between MN1 and CN1. Either device may be the server or client, depending on the capabilities of each.
- MN1 moves to Foreign Subnet (FS) 1.
- Verify that MN1 is able to reach CN1. Also verify that CN1 and HA1 have created a binding cache entry for MN1.
- MN1 moves to FS2.
- Verify that MN1 is able to reach CN1. Also verify that CN1 and HA1 have updated the binding cache entry for MN1.
- MN1 moves to Home1.
- Verify that MN1 is able to reach CN1. Also verify that CN1 and HA1 have deleted the binding cache entry for MN1.

Observable Results: Once MN1 has detected that it has moved 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. MN1 should update the binding for HA1 and CN1 reflecting the change in care-of address. 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 foreign network.

Possible Problems:

- If MN1 and CN1 do not support Telnet, other protocols that run over TCP may be used. If no other protocol that runs over TCP is available, ICMP echo requests and Replies may be used.

- For wired devices, movement may be simulated by physically disconnecting the node, and reconnecting it to the new subnet.

Test MIP1.1.1.2: MN to MN Communication

Purpose: Verify that two MNs can move away from their home subnets among various foreign subnets, and communicate with each other.

References: [Mobility Support in IPv6 (draft 24)] – Section 4.

Resource Requirements: Packet capture tools, Telnet 6 daemon and client software.

Discussion: 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 home subnet 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.

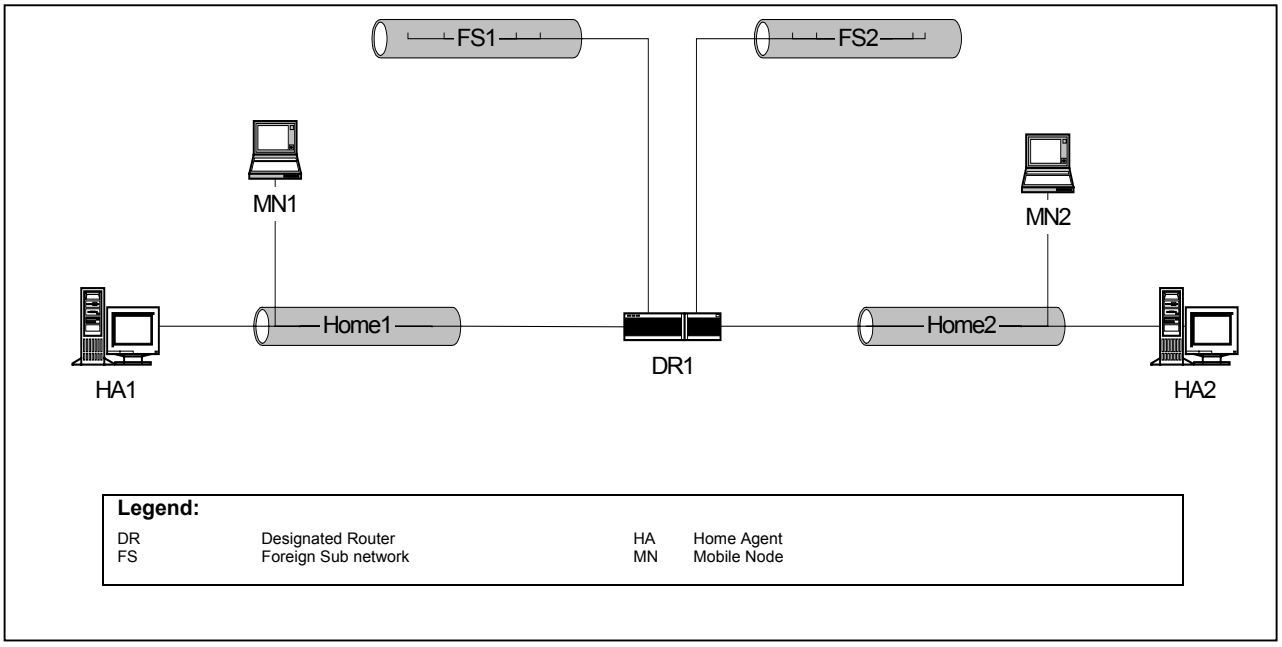


Figure C-7-2. Interoperability MN to MN Communication Diagram Part A

Test Setup:

MN1 is configured with Home1 as its home subnet, and HA1 as its HA. MN2 is configured with Home2 as its home subnet, and HA2 as its HA. HA1 and HA2 are not default routers for their respective networks. Default Router (DR) 1 is configured to act as default router for all of its attached networks. DR1 does not provide HA services. HA1, HA2, and DR1 may be the same device, if necessary.

Table C-7-2. Router Parameters

DR1	HA1 and HA2
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

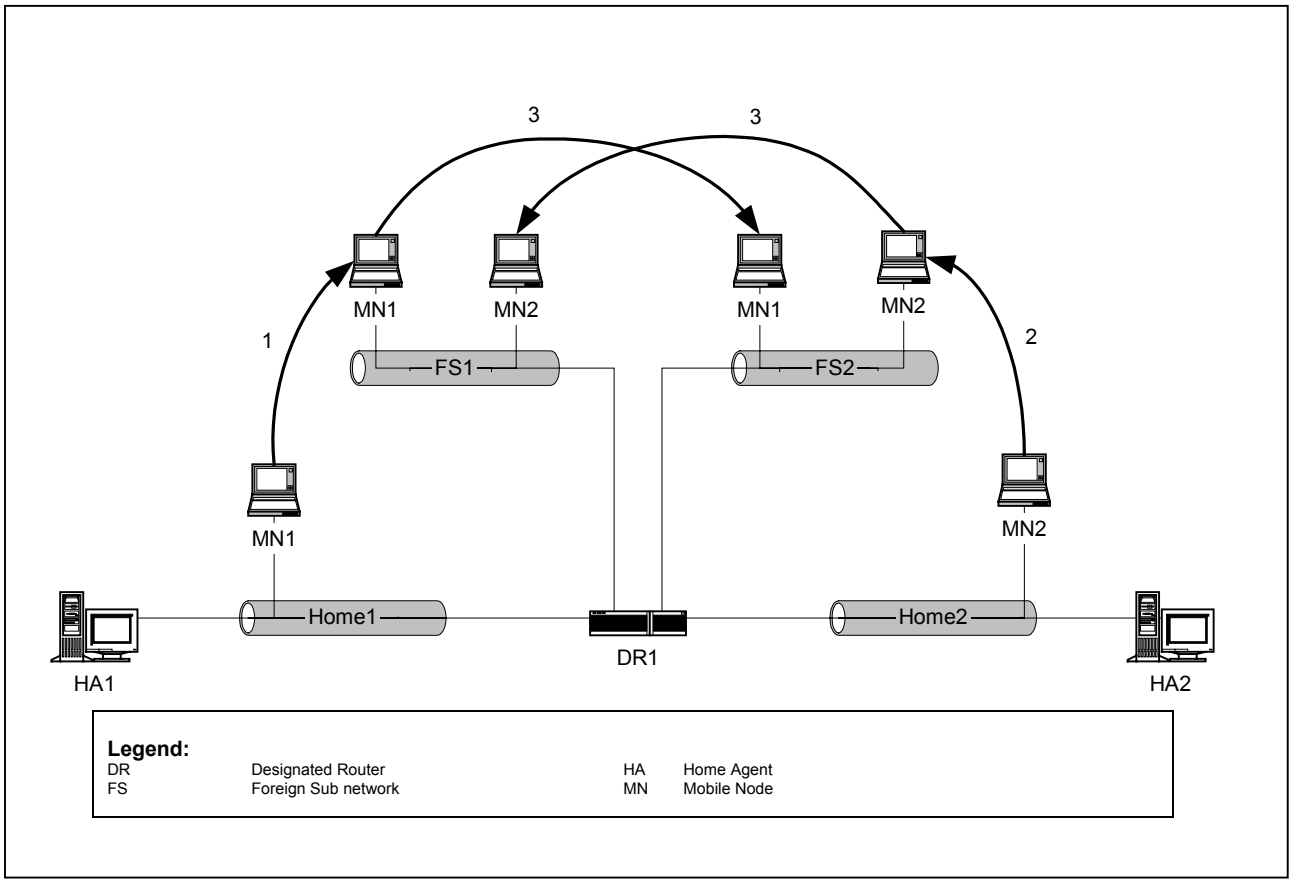


Figure C-7-3. Interoperability MN to MN Communication Diagram Part B

Procedures:

- Establish a Telnet session between MN1 and MN2. Either device may be the server or client, depending on the capabilities of each.

- MN1 moves to FS1.

- Verify that MN1 and MN2 are able to reach one another. Also verify that MN1, MN2, and HA1 have created the appropriate binding cache entries.

- MN2 moves to FS2.

- Verify that MN1 and MN2 are able to reach one another. Also verify that MN1, MN2, and HA1 have updated the appropriate binding cache entries.

- MN1 moves to FS2; MN2 moves to FS1.

- Verify that MN1 and MN2 are able to reach one another. Also verify that MN1, MN2, and HA1 have updated the appropriate binding cache entries.

Observable Results: Once MN1 and MN2 have detected that they have moved 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, they should update their bindings for their appropriate HA (HA1 or HA2) and CN reflecting the change in care-of address. 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 foreign network.

Possible Problems:

- If both MN1 and MN2 do not support Telnet, other protocols that run over TCP may be used. If no other protocol that runs over TCP is available, ICMP echo requests and replies may be used.

- For wired devices, movement may be simulated by physically disconnecting the node, and reconnecting it to the new subnet.

SECTION 2: INTEROPERABILITY

Scope

Tests in this group verify the ability of a MN, HA, and CN to correctly interoperate in a Mobile IPv6 environment.

Overview

Tests in this group include test cases where a MN and HA can correctly participate in dynamic home agent address discovery, network re-numbering, and duplicate address detection.

Test MIP1.2.2.1: Home Network Renumbering

Purpose: Verify that a MN can move away from its home subnet, and while away, have its home network renumbered.

References: Mobility Support in IPv6 (draft 24) – Section 4, 10.6, 11.4

Resource Requirements: Packet capture tools, Telnet 6 daemon and client software.

Discussion: 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 home subnet 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 home network, its home network 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 its HA.

Test Setup:

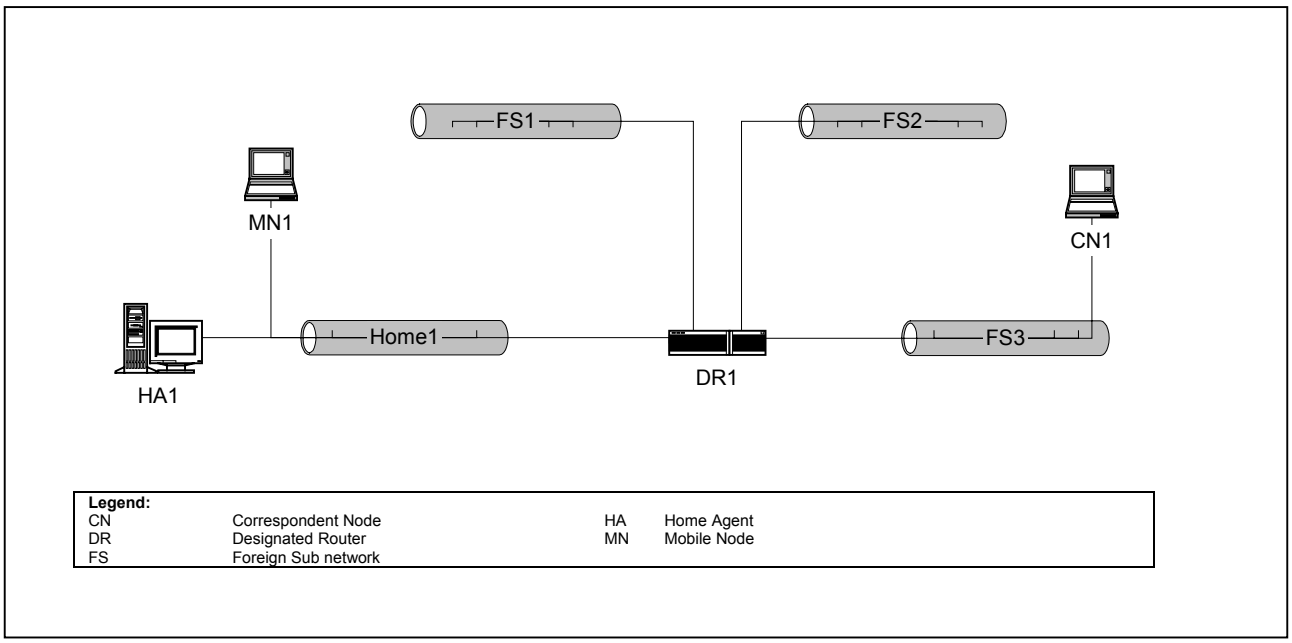


Figure C-7-4. Interoperability Home Network Renumbering Diagram

A MN, MN1, is configured with Home1 as its home subnet, and a HA implementation from another vendor, HA1, as its HA as pictured above. Designated Router (DR) 1 is configured to act as default router for all of its attached networks. DR1 does not provide HA services. HA1 is configured to act as a HA for network Home1, but not a default router. HA1 and DR1 may be the same device, if necessary.

Table C-7-3. Router Parameters

DR1	HA1
Router Lifetime: 30 minutes Minimum Advance Interval: 0.5 seconds Maximum Advance Interval: 1.5 seconds	Router Lifetime: 0 seconds Minimum Advance Interval: 0.5 seconds Maximum Advance Interval: 1.5 seconds HA Lifetime: 30 minutes
Each prefix Valid Lifetime: 30 minutes Preferred Lifetime: 20 minutes	**Each prefix** R Bit: Set, full address included Valid Lifetime: 30 minutes Preferred Lifetime: 20 minutes

Procedures:

- Establish a Telnet session between MN1 and CN1. Either device may be the server or client, depending on the capabilities of each.
- MN1 moves to FS1.
- Verify that MN1 is able to reach CN1. Also verify that CN1 and HA1 have created a binding cache entry for MN1.
- Home1 and HA1 are 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.
- MN1 moves to FS2.
- 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.
- Verify that MN1 is able to reach CN1. Also verify that CN1 and HA1 have updated the binding cache entry for MN1.

Observable Results:

- Once MN1 has detected that it has moved 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. MN1 should update the bindings

for HA1 and CN1 reflecting the change in care-of address. 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 foreign network.

- In Steps 4 and 5, MN1 should learn and configure the new home prefix through Mobile Prefix Solicitations and Advertisements. Following the home network renumbering, MN1 should be able to communicate normally with both CN1 and HA1.

Possible Problems:

- If both MN1 and CN1 do not support Telnet, other protocols that run over TCP may be used. If no other protocol that runs over TCP is available, ICMP echo requests and Replies may be used.

- For wired devices, movement may be simulated by physically disconnecting the node, and reconnecting it to the new subnet.

Test MIP1.1.2.2: Dynamic HA Address Discovery

Purpose: Verify that a MN can move away from its home subnet, and when knowing of no HA on its home network, initiate Dynamic HA Address Discovery.

References: Mobility Support in IPv6 (draft 24) – Section 4, 10.5, 11.4

Resource Requirements: Packet capture tools, Telnet 6 daemon and client software.

Discussion: 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 home subnet 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.

When a MN does not have the address of a valid HA on its home network to which it can establish its Primary care-of address, it may perform Dynamic HA Address Discovery. This may occur when a HA has had its network address changed or has been replaced with a different router serving the role of HA on the home network.

Test Setup:

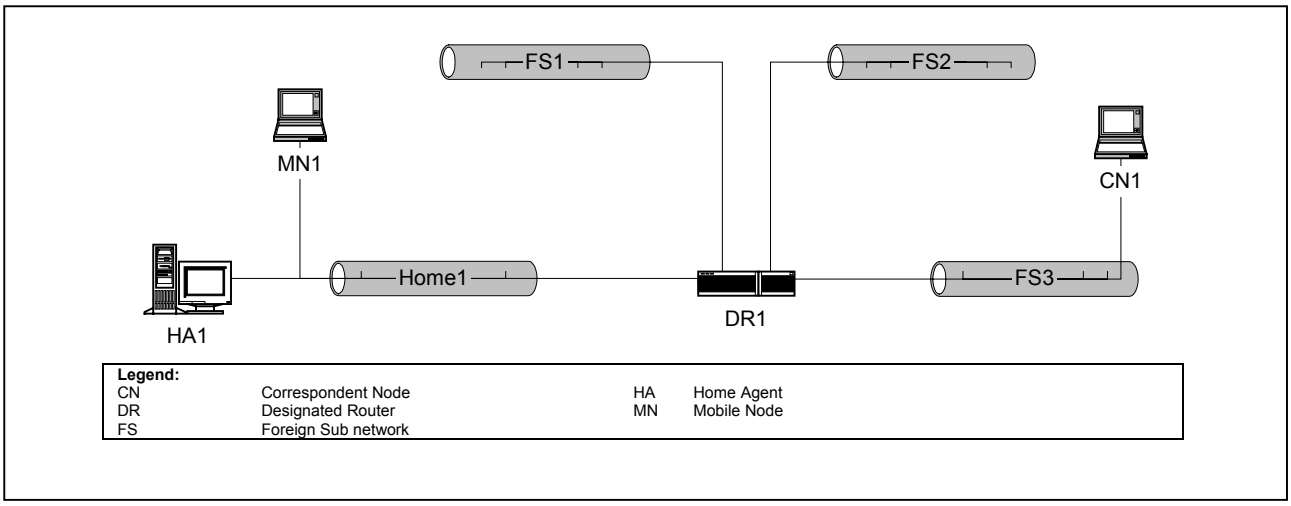


Figure C-7-5. Interoperability Dynamic HA Address Discovery Diagram

A MN, MN1, is configured with Home1 as its home subnet, and a HA implementation from another vendor, HA1, as its HA as pictured above. DR1 is configured to act as default router for all of its attached networks. DR1 does not provide HA services. HA1 is configured to act as a HA for network Home1, but not a default router. HA1 and DR1 may be the same device, if necessary.

Table C-7-4. Router Parameters

DR1	HA1
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 HA Lifetime: 30 minutes **Each prefix** R Bit: Set, full address included Valid Lifetime: 30 minutes Preferred Lifetime: 20 minutes

Procedures:

- Establish a Telnet session between MN1 and CN1. Either device may be the server or client, depending on the capabilities of each.

- MN1 moves to FS1.

- Verify that the MN1 is able to reach CN1. Also verify that CN1 and HA1 have created a binding cache entry for MN1.

- Change the token for HA1, leaving the prefix the same.

- MN1 moves to FS2. Allow time for MN1 to perform Dynamic HA Address Discovery.

- Verify that the MN1 is able to reach CN1. Also verify that CN1 and HA1 have updated the binding cache entry for MN1.

Observable Results:

- Once MN1 has detected that it has moved 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. MN1 should update the binding for HA1 and CN1 reflecting the change in care-of address. 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 foreign network.

- In Step 5, MN1 should perform Dynamic HA Address Discovery and re-establish connectivity with HA1. MN1 should register its primary care-of address with its "new" HA.

Possible Problems:

- If both MN1 and CN1 do not support Telnet, other protocols that run over TCP may be used. If no other protocol that runs over TCP is available, ICMP echo requests and Replies may be used.

- For wired devices, movement may be simulated by physically disconnecting the node, and reconnecting it to the new subnet.

- MNs are not required to implement Dynamic HA Address Discovery

Test MIP1.1.2.3: Duplicate Address Detection

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

References: Mobility Support in IPv6 (draft 24) – Section 10.3.1, 11.5.4, RFC 2462 – Section 5.4

Resource Requirements: Packet capture tools, Telnet 6 daemon and client software.

Discussion: While the mobile node is away from home, it relies on the home agent to participate in Duplicate Address Detection (DAD) to defend its home address against stateless autoconfiguration performed by another node.

Test Setup:

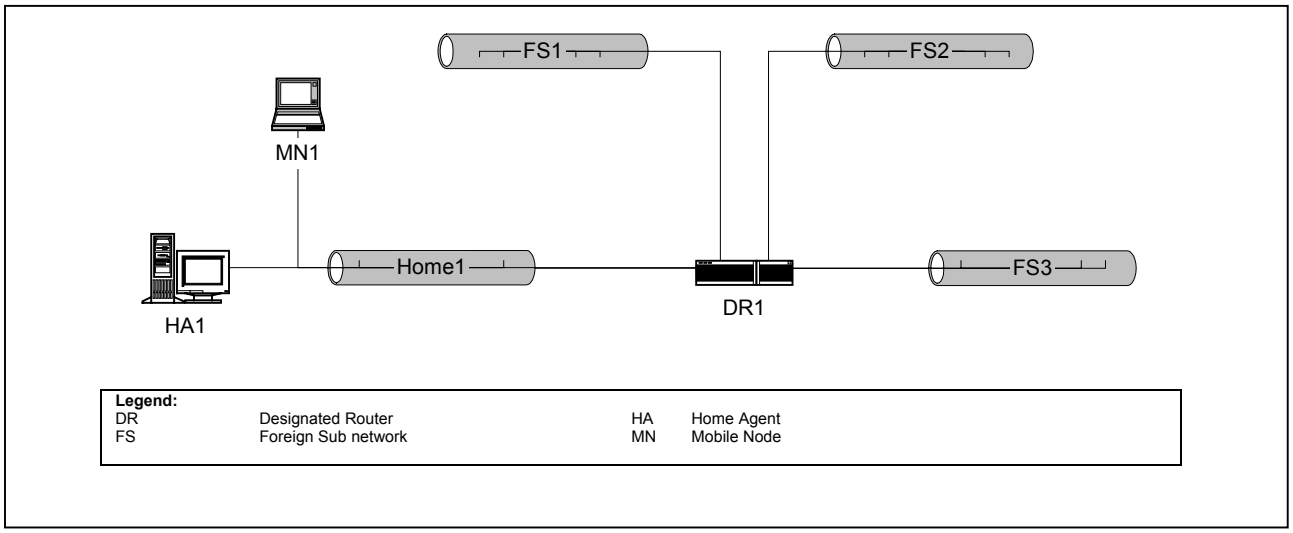


Figure C-7-6. Interoperability Duplicate Address Detection Diagram

A MN, MN1, is configured with Home1 as its home subnet, and a HA implementation from another vendor, HA1, as its HA as pictured above. DR1 is configured to act as default router for all of its attached networks. DR1 does not provide HA services. HA1 is configured to act as a HA for networks Home1 and FS1, but not a default router. HA1 and DR1 may be the same device, if necessary.

Table C-7-5. Router Parameters

DR1	HA1
Router Lifetime: 30 minutes Minimum Advance Interval: 0.5 seconds Maximum Advance Interval: 1.5 seconds	Router Lifetime: 0 seconds Minimum Advance Interval: 0.5 seconds Maximum Advance Interval: 1.5 seconds HA Lifetime: 30 minutes
Each prefix Valid Lifetime: 30 minutes Preferred Lifetime: 20 minutes	**Each prefix** R Bit: Set, full address included Valid Lifetime: 30 minutes Preferred Lifetime: 20 minutes

Procedures:

- MN1 moves to FS1.

- Connect CN1, a correspondent node, to network Home1. Attempt to configure CN1 with the same link-local and global addresses as MN1. Allow time for duplicate address detection to take place.

Observable Results:

- In Step 2, HA1 should successfully defend the global and link-local addresses of MN1.

Possible Problems:

- If both MN1 and CN1 do not support Telnet, other protocols that run over TCP may be used. If no other protocol that runs over TCP is available, ICMP echo requests and Replies may be used.

- For wired devices, movement may be simulated by physically disconnecting the node, and reconnecting it to the new subnet.

Test MIP1.1.2.4: Basic Mobile Network

Purpose: Verify that a mobile router (MR) can perform the necessary procedures in order to change locations and maintain proper communication capabilities.

References: Network Mobility Support (Sept 03)

Resource Requirements: Packet capture tools, Telnet 6 daemon and client software.

Discussion: 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 correspondent nodes.

Test Setup:

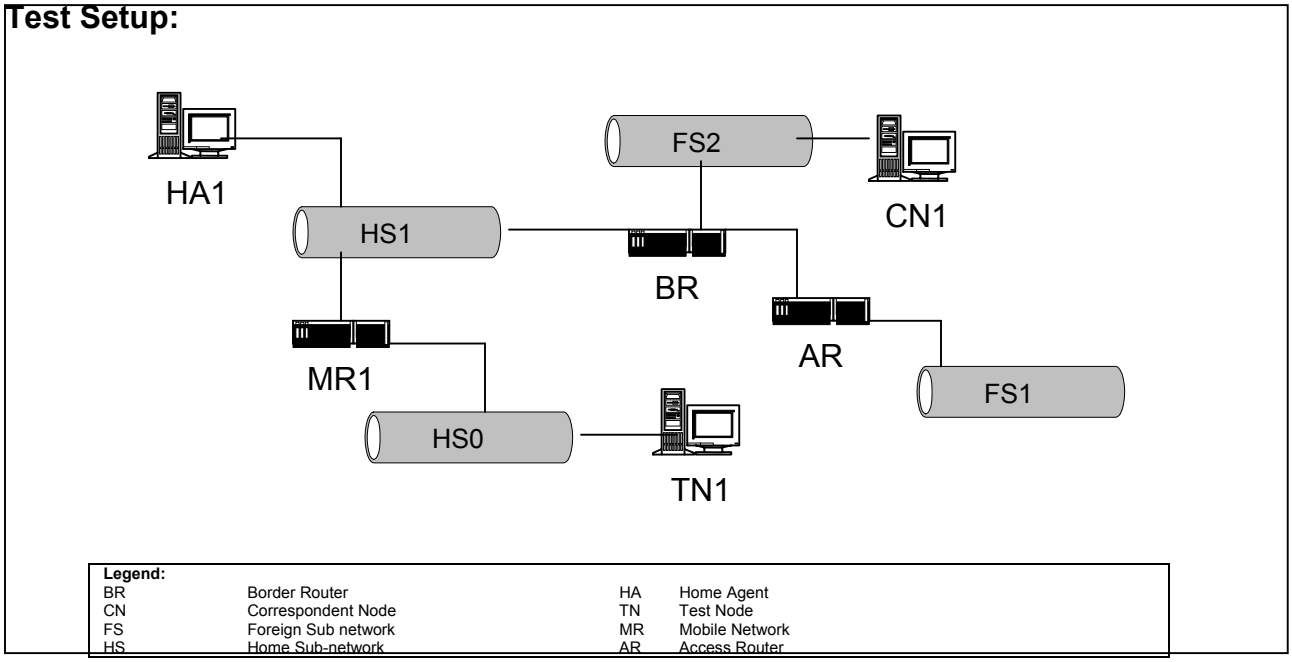


Figure C-7-7. Basic Mobile Network Diagram

A MR, MR1, is configured with Home Sub-network (HS) 1 as its home subnet, and a HA implementation from another vendor, HA1, as its HA as pictured above. Border Router (BR) is configured to act as such for MR1. BR does not provide HA services. HA1 is configured to act as a HA for networks HS1.

Procedures:

- Establish a Telnet session between TN1 and CN1.
- MR1 moves with HS0 to FS1.
- Verify reachability between TN1 and CN1.

- MR1 moves with HS0 back to HS1.

- Verify reachability between TN1 and CN1.

Observable Results:

- When HS0 moves from HS1 to FS1 and back, communication must still be possible between TN1 and CN1.

Possible Problems:

- If both TN1 and CN1 do not support Telnet, other protocols that run over TCP may be used. If no other protocol that runs over TCP is available, ICMP echo requests and Replies may be used.

- For wired devices, movement may be simulated by physically disconnecting the node, and reconnecting it to the new subnet.

Test MIP1.1.2.5: Mobile Network with Mobile Node

Purpose: Verify that a mobile network (MR) with a mobile node attached can perform the necessary procedures in order to change locations and maintain proper communication abilities.

References: Network Mobility Support (Sept 03)

Resource Requirements: Packet capture tools, Telnet 6 daemon and client software.

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

Test Setup:

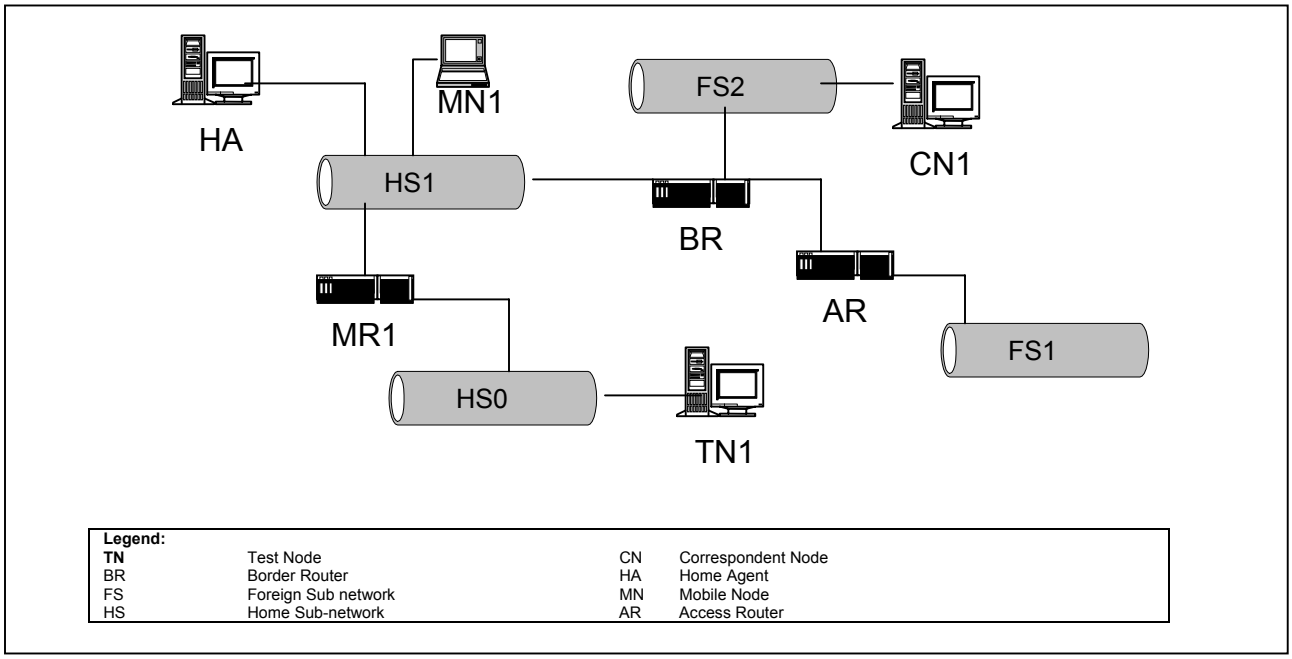


Figure C-7-8. Mobile Network with Mobile Node Diagram

A MR, MR1, is configured with HS1 as its home subnet, and a HA implementation from another vendor, HA1, as its HA as pictured above. BR is configured to act as the Border Router for MR1. BR does not provide HA services. HA1 is configured to act as a HA for networks HS1.

Procedures:

- MR1 moves with HS0 to FS1.
- Establish a Telnet session between MN1 and CN1.
- MN1 moves to HS0.
- Verify reachability between MN1 and CN1.
- MR1 moves with HS0 to HS1.
- Verify reachability between MN1 and CN1.

Observable Results:

- When MN1 is connected to HS0 while the network is mobile, as well as when it returns to HS1, it should be able to communicate with CN1.

Possible Problems:

- If both MN1 and CN1 do not support Telnet, other protocols that run over TCP may be used. If no other protocol that runs over TCP is available, ICMP echo requests and Replies may be used.
- For wired devices, movement may be simulated by physically disconnecting the node, and reconnecting it to the new subnet.

Test MIP1.1.2.6: Nested Mobile Networks

Purpose: Verify that a nested mobile network (MR) can perform the necessary procedures in order to change locations and maintain proper communication abilities.

References:

- Network Mobility Support (Sept 03)

Resource Requirements: Packet capture tools, Telnet 6 daemon and client software.

Discussion: 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 correspondent nodes.

Test Setup:

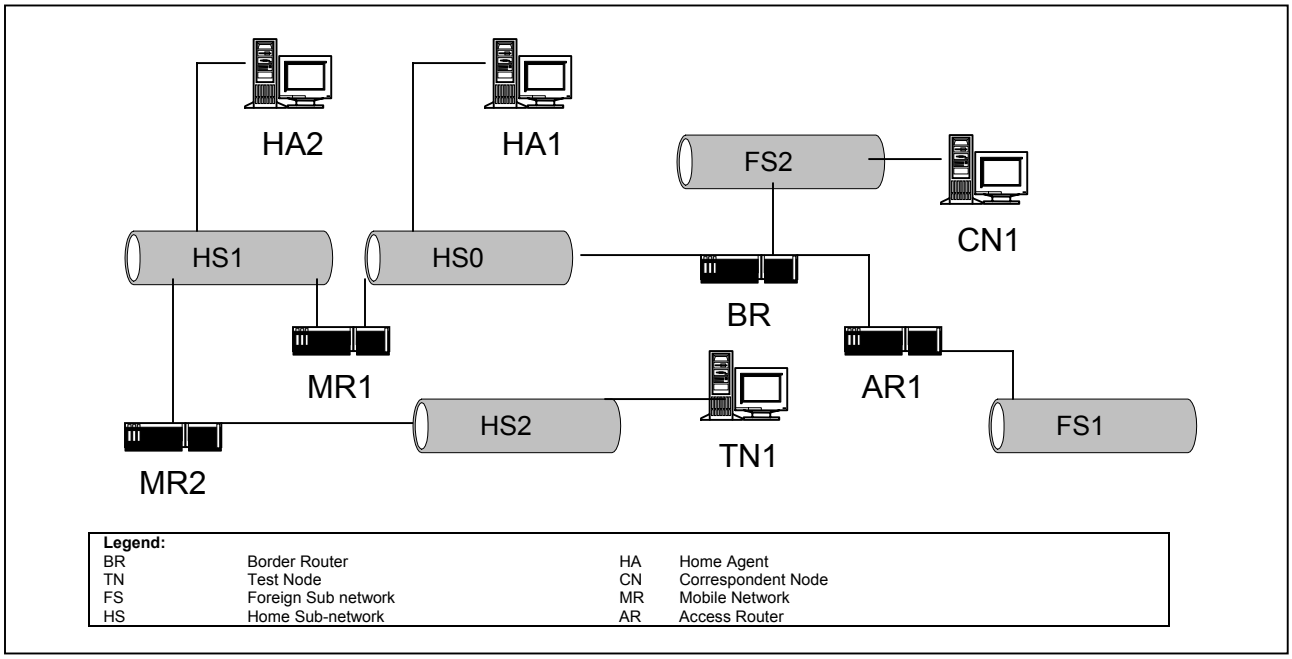


Figure C-7-9. Interoperability Nested Mobile Networks Diagram

A MR, MR1, is configured with HS0 as its home subnet, and a HA implementation from another vendor, HA1, as its HA as pictured above. A MR, MR2, is configured with HS1 as its home subnet, and a HA implementation from another vendor, HA2, as its HA as pictured above. BR is configured to act as the Border Router for MR1. BR does not provide HA services.

Procedures:

- Establish a Telnet session between TN1 and CN1.
- MR1 moves with HS0 to FS1.
- Verify reachability between TN1 and CN1.
- MR2 moves with HS2 to FS2.
- Verify reachability between TN1 and CN1.
- MR1 with HS1 moves back to HS0.
- MR2 with HS2 moves back to HS1.
- Verify reachability between TN1 and CN1.

Observable Results:

- When the mobile networks move to foreign subnets and back, communication must still be possible between TN1 and CN1.

Possible Problems:

- If both TN1 and CN1 do not support Telnet, other protocols that run over TCP may be used. If no other protocol that runs over TCP is available, ICMP echo requests and Replies may be used.
- For wired devices, movement may be simulated by physically disconnecting the node, and reconnecting it to the new subnet.

APPENDIX C, ANNEX EIGHT

SECURITY

Test IPsec INTEROP.1.1: Node to Node

Purpose: To verify that a pair of nodes can correctly communicate with each other when either Authentication Header (AH) or Encapsulating Security Payload (ESP) is used.

Resource Requirements:

- TCP application, such as Telnet.
- User Datagram Protocol (UDP) application, such as Trivial File Transfer Protocol.
- Internet Control Message Protocol (ICMP) application, such as ping.

Background: This test verifies that the nodes can successfully communicate with each other when Authentication Header or Encapsulating Security Payload is in use. Tunnel mode and transport mode are thoroughly tested with different upper layer protocols, such as TCP, UDP, and ICMP.

Test Setup:

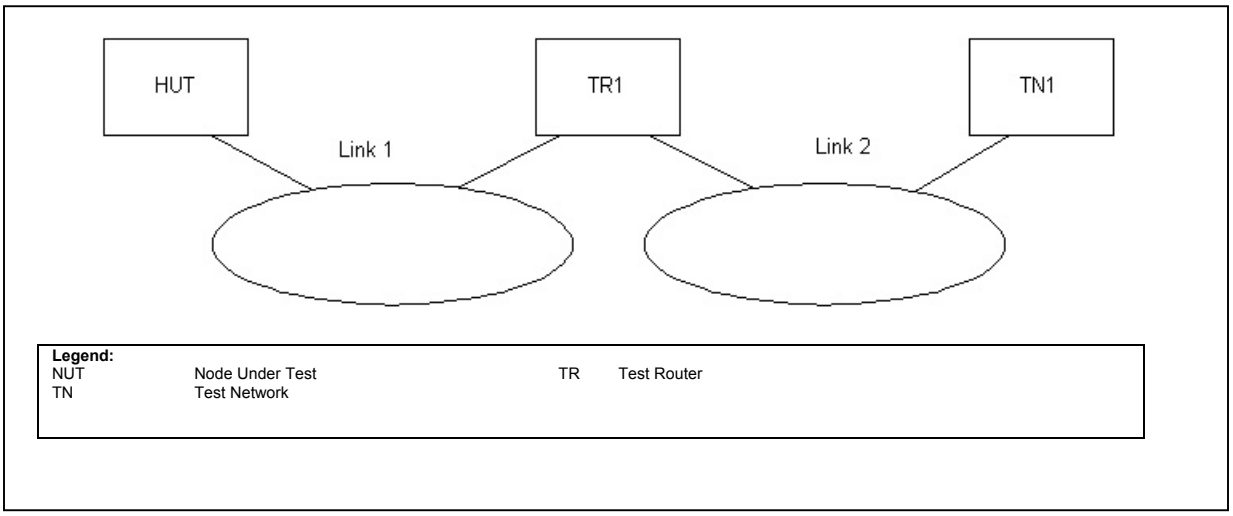


Figure C-8-1. Security Node-to-Node Diagram

Procedures:

- Part A: AH, transport mode
  - Configure the Node Under Test (NUT) and Test Network 1 (TN1) as a host pair to run AH in transport mode by specifying detailed information in their two-way Security Authentication (SA). Authentication algorithm could

be HMAC-MD5 or HMAC-SHA1. Specify ‘Any’ as the upper layer protocols in the SA configurations.
    - Verify the correctness in their communication by running a TCP application, a UDP application, and an ICMP application.

- Part B: AH, tunnel mode
    - Repeat Step 1 and Step 2, with AH running in tunnel mode instead.

- Part C: ESP, transport mode
    - Repeat Step 1 and Step 2, with ESP running in transport mode instead.

- Part D: ESP, tunnel mode
    - Repeat Step 1 and Step 2, with ESP running in tunnel mode instead.

Observable Results: In all parts, the NUT should be able to communicate correctly with TN1.

Possible Problems: None.

Test IPsec INTEROP.1.2: Multiple Security Associations with varying granularity

Purpose: To verify that a pair of nodes can correctly handle multiple security associations with varying granularity. This verifies the node's ability to correctly apply different levels of granularity as well as the ability to manage multiple security associations that share the same IP address and security protocol.

Resource Requirements:

- TCP application, such as Telnet.
- User Datagram Protocol (UDP) application, such as Trivial File Transfer Protocol.
- ICMP application, such as ping.

Discussion: This test verifies that a pair of nodes can correctly handle multiple security associations with varying granularity. This verifies the node's ability to correctly apply different levels of granularity as well as the ability to manage multiple security associations that share the same IP address and security protocol. Tunnel mode and transport mode are thoroughly tested with different upper layer protocols, such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

Test Setup:

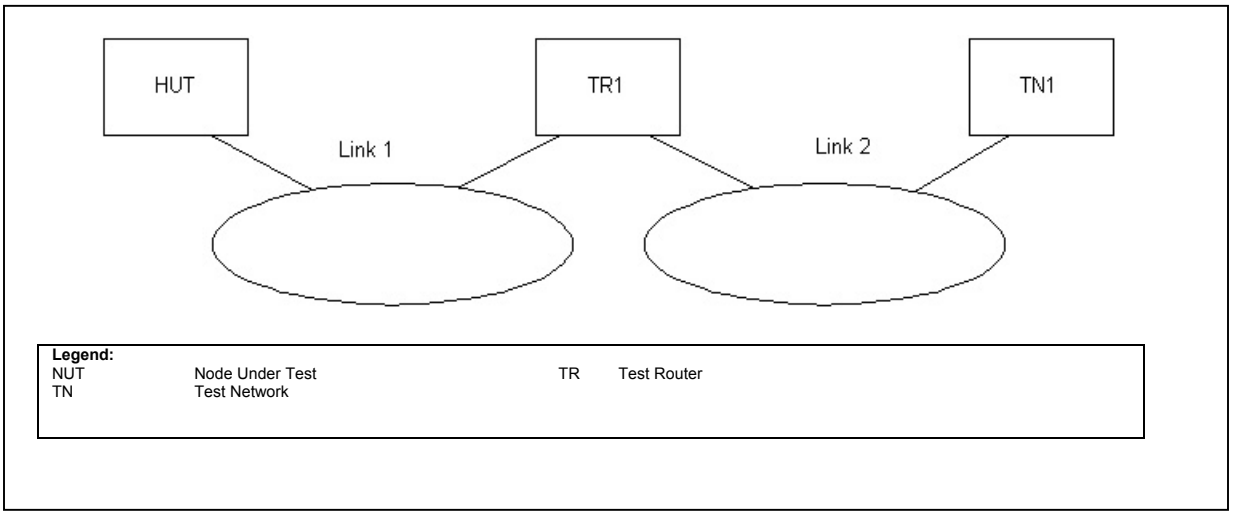


Figure C-8-2. Security Node-to-Node Diagram

Procedures:

- Part A: AH, transport mode
  - Configure the NUT and TN1 as a host pair to run AH in transport mode by specifying detailed information in their two-way Security Authentication (SA). Authentication algorithm could be HMAC-MD5 or HMAC-SHA1.

Specify different services for the three different upper layer protocols (TCP, UDP, and ICMP).
    - Verify the correctness in their communication by running a TCP application, a UDP application, and an ICMP application.

- Part B: AH, tunnel mode
    - Repeat Step 1 and Step 2, with AH running in tunnel mode instead.

- Part C: ESP, transport mode
    - Repeat Step 1 and Step 2, with ESP running in transport mode instead.

- Part D: ESP, tunnel mode
    - Repeat Step 1 and Step 2, with ESP running in tunnel mode instead.

Observable Results: In all parts, the NUT should be able to communicate correctly with TN1.

Possible Problems: None.

Test IPsec INTEROP.1.3: Security Association Bundles

Purpose: To verify that a pair of nodes can correctly communicate with each other when combining services over a single traffic flow.

Resource Requirements:

- TCP application, such as Telnet.
- UDP application, such as Trivial File Transfer Protocol.
- ICMP application, such as ping.

Discussion: This test verifies that a pair of nodes can correctly communicate with each other when combining services over a single traffic flow. Tunnel mode and transport mode are thoroughly tested with different upper layer protocols, such as TCP, UDP, and ICMP.

Test Setup:

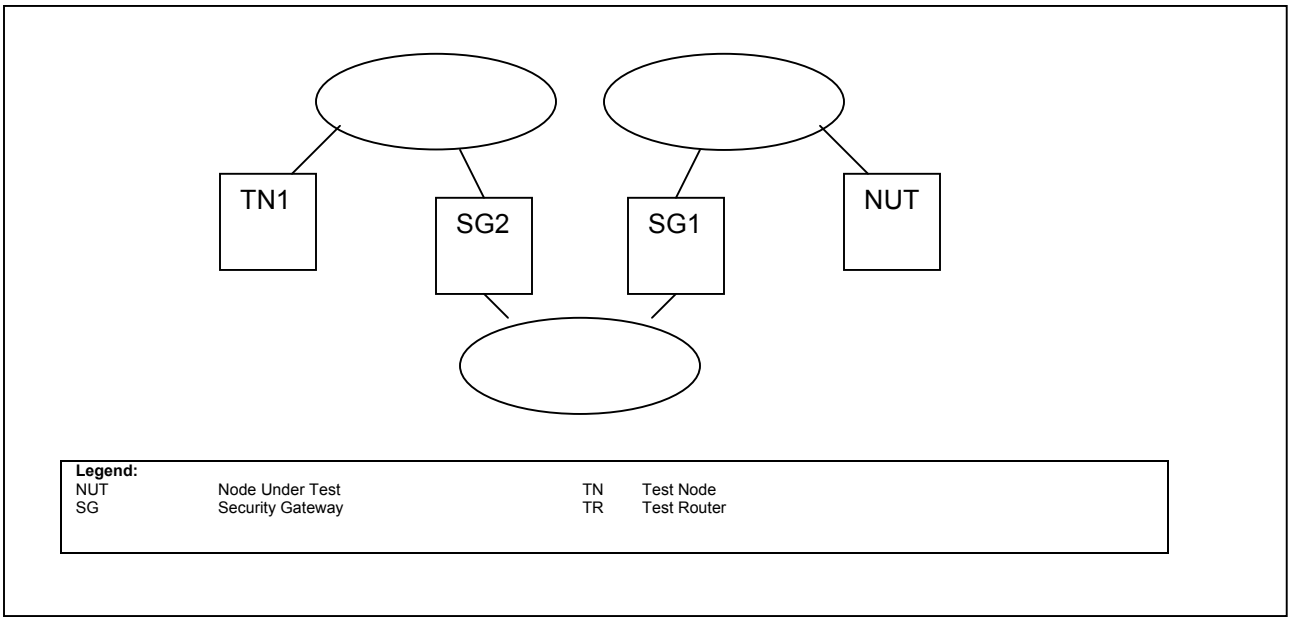


Figure C-8-3. Security Node to Node Diagram

Procedures:

- Part A: Transport Adjacency
  - Configure the NUT and TN1 as a host pair to run both AH and ESP in transport mode by specifying detailed information in their two-way Security Authentication (SA). Authentication algorithm could be HMAC-MD5 or

HMAC-SHA1. Specify ‘Any’ as the upper layer protocols in the SA configurations.
    - Verify the correctness in their communication by running a TCP application, a UDP application, and an ICMP application.

- Part B: Iterated Tunneling with one common endpoint (AH outside)
    - Configure the NUT and TN1 as a host pair to run AH in tunnel mode by specifying detailed information in their two-way Security Authentication (SA). Specify ‘Any’ as the upper layer protocols in the SA configurations.
    - Configure the NUT and SG2 as a pair to run ESP in tunnel mode by specifying detailed information in their two-way Security Authentication (SA). Specify ‘Any’ as the upper layer protocols in the SA configurations.
    - Verify the correctness in their communication by running a TCP application, a UDP application, and an ICMP application between the NUT and TN1.

- Part C: Iterated Tunneling with one common endpoint (ESP outside)
    - Repeat part B with ESP running between the NUT and TN1, and AH running between the NUT and Security Gateway 2 (SG2).
- Part D: Iterated Tunneling with no common endpoint (AH outside)
    - Configure the NUT and TN1 as a host pair to run AH in tunnel mode by specifying detailed information in their two-way Security Authentication (SA). Specify ‘Any’ as the upper layer protocols in the SA configurations.
    - Configure SG1 and SG2 as a pair to run ESP in tunnel mode by specifying detailed information in their two-way Security Authentication (SA). Specify ‘Any’ as the upper layer protocols in the SA configurations.
    - Verify the correctness in their communication by running a TCP application, a UDP application, and an ICMP application between the NUT and TN1.
- Part E: Iterated Tunneling with no common endpoint (ESP outside)
    - Repeat part D with ESP running between the NUT and TN1, and AH running between SG1 and SG2.

Observable Results: In all parts, the NUT should be able to communicate correctly with TN1.

Possible Problems: None.

Test IPsec INTEROP.1.4: Path Maximum Transmission Unit (PMTU)

Purpose: To verify that a pair of nodes can correctly calculate the effective PMTU for different security associations. This verifies the node's ability to accurately decide when to fragment packets that will traverse the same path (and therefore have the same PMTU), but use different security associations which causes the packets to have different overhead due to security information.

Resource Requirements:

- TCP application, such as Telnet.
- User Datagram Protocol (UDP) application, such as Trivial File Transfer Protocol.
- ICMP application, such as ping.

Discussion: This test verifies that a pair of nodes can correctly calculate and manage the effective PMTU for different security associations. This verifies the node's ability to accurately decide when to fragment packets that will traverse the same path (and therefore have the same PMTU), but use different security associations which causes the packets to have different overhead due to security information.

Test Setup:

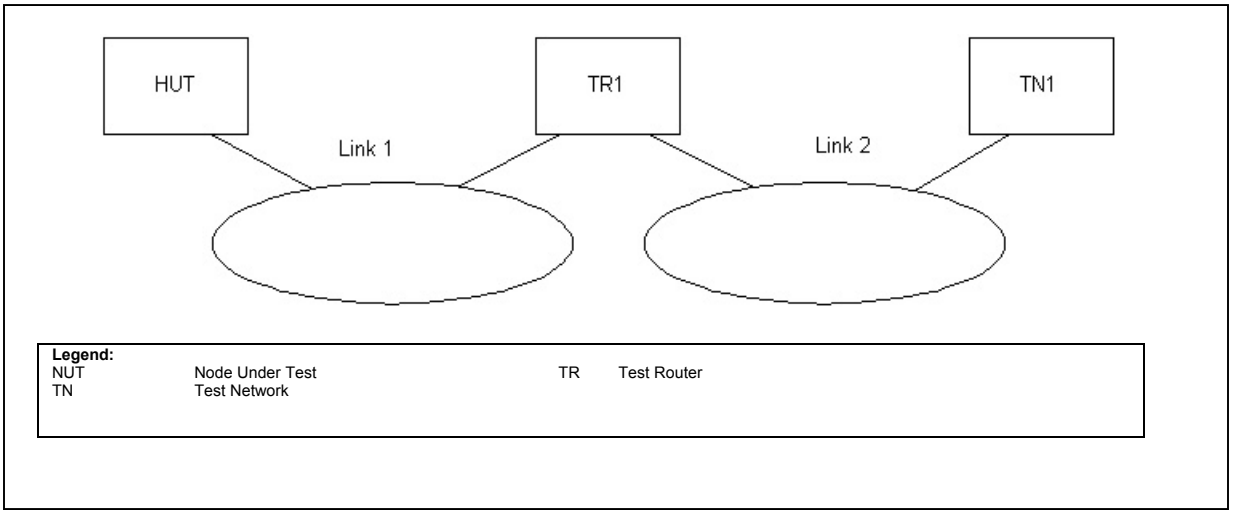


Figure C-8-4. Security Node-to-Node Diagram

Procedures:

- Part A: PMTU Calculation
  - Configure the NUT and TN1 as a host pair to run different IPSEC protocols/modes/services for the three different upper layer protocols (UDP, TCP, and ICMP) by specifying detailed information in their two-way Security Authentications (SAs).
  - Configure TR1 to decrease the advertised MTU on Link 1.

    - Verify the correctness in their communication by running a TCP application, a UDP application, and an ICMP application (with large packets).

- Part B: Minimum MTU
    - Repeat Step 1 and configure TR1 to advertise the IPv6 minimum MTU on Link 1.
    - Verify the correctness in their communication by running a TCP application, a UDP application, and an ICMP application (with large packets).

- Part C: En Route Fragmentation
    - Repeat Step 1. Increase the advertised MTU on Link 1 to its default, and decrease the advertised MTU on Link 2 to the IPv6 minimum MTU.
    - Verify the correctness in their communication by running a TCP application, a UDP application, and an ICMP application (with large packets).

Observable Results: In all parts, the NUT should be able to communicate correctly with TN1.

Test IPsec INTEROP.1.5: Security Gateway to Security Gateway

Purpose: To verify that a pair of security gateways can correctly provide IP security to their hosts when either AH or ESP is used.

Resource Requirements:

- TCP application, such as Telnet.
- UDP application, such as TFTP.
- ICMP application, such as ping.

Discussion: This test verifies that the security gateways can correctly provide IP security when Authentication Header or Encapsulating Security Payload is in use. Tunnel mode and transport mode are thoroughly tested with different upper layer protocols, such as TCP, UDP, and ICMP.

Test Setup: An interior routing protocol should be run among TR1, RUT and TR2. RUT should be advertising prefix A/64 over link 1 while TR2 should be advertising prefix B/64 over link 2, which enable hosts on each link auto-configure their addresses accordingly.

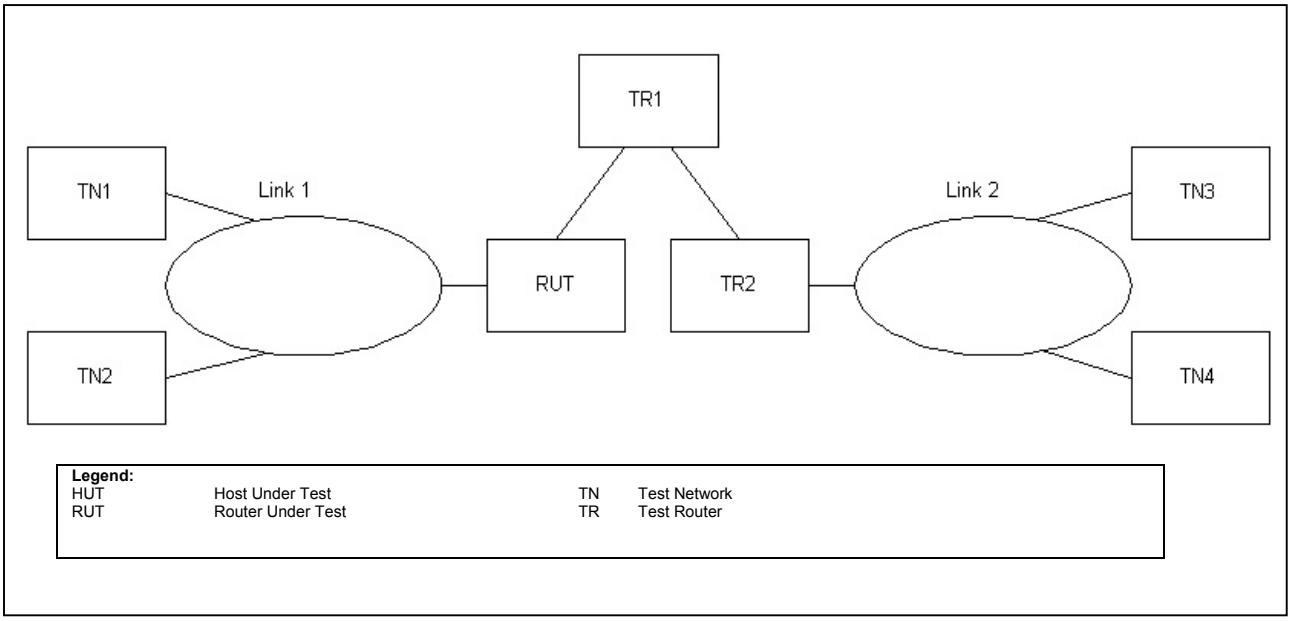


Figure C-8-5. Security Gateway to Gateway Diagram

Procedures:

- Part A: AH, Tunnel Mode, Host to Host
  - Configure the RUT and TR2 as a pair to run AH in tunnel mode by specifying detailed information in their two-way Security Associations

(SA). Authentication algorithm could be HMAC-MD5 or HMAC-SHA1 and the source destination pair on RUT should be TN1 and TN3 while the source destination pair on TR2 should be TN3 and TN1. Specify 'Any' as the upper protocol for the SAs.
    - Verify the correctness in their communications by running a TCP application, a UDP application, and an ICMP application on TN1 and TN3.

- Part B: AH, Tunnel Mode, Network to Network
    - Repeat Step 1 and Step 2, but use the network of prefix A/64 and the network of prefix B/64 as the source and destination pair instead in the SA configurations on the RUT and TR2.
    - Verify the correctness in their communications by running a TCP application, a UDP application, and an ICMP application on host pairs of TN1 and TN3, TN1 and TN4, TN2 and TN3, and TN2 and TN4.

- Part C: ESP, Tunnel Mode, Host to Host
    - Repeat Step 1 and Step 2, but configure the RUT and TR2 to use ESP instead of AH.
    - Verify the correctness in their communications by running a TCP application, a UDP application, and an ICMP application on TN1 and TN3.
- Part D: ESP, Tunnel Mode, Network to Network
    - Repeat Step 1 and Step 2, but configure the RUT and TR2 to use ESP, instead of AH, and use the network of prefix A/64 and the network of prefix B/64 as the source and destination pair instead in the SA configurations on the RUT and TR2.
    - Verify the correctness in their communications by running a TCP application, a UDP application, and an ICMP application on host pairs of TN1 and TN3, TN1 and TN4, TN2 and TN3, and TN2 and TN4.

Observable Results: In all parts, the specified host pairs should be able to communicate with each other correctly.

Test IPsec INTEROP.2.1: Multicast Group Functionality

Purpose: To verify that a group of nodes can correctly communicate in a secure centralized Multicast environment.

Resource Requirements:

- TCP application, such as Telnet.
- User Datagram Protocol (UDP) application, such as Trivial File Transfer Protocol.
- ICMP application, such as ping.

Discussion: This test verifies that a group of nodes can correctly communicate in a secure centralized Multicast environment.

Test Setup:

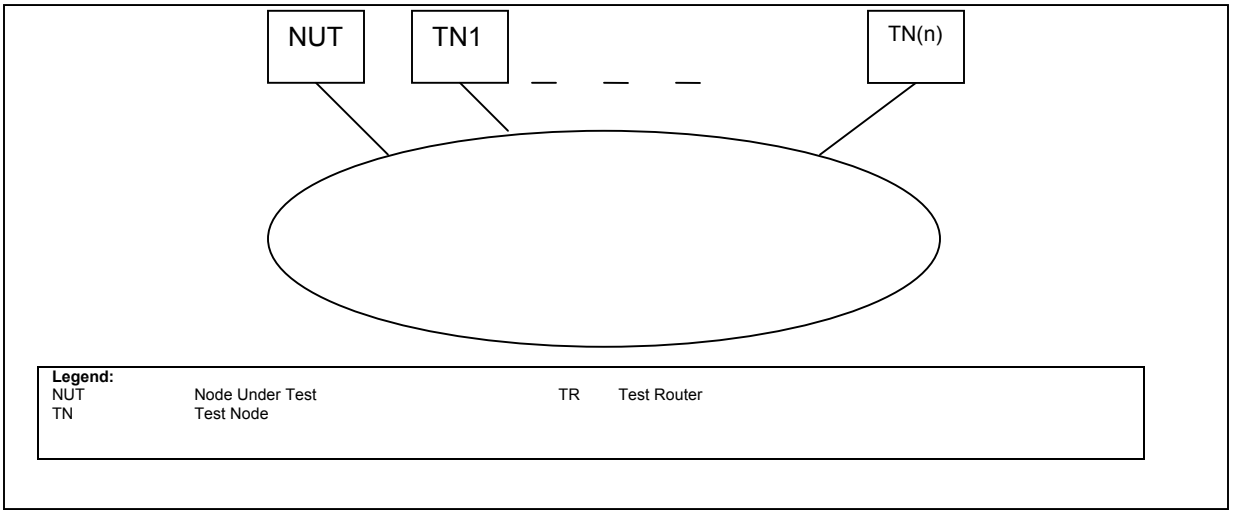


Figure C-8-6. Security Node-to-Node Diagram

Procedures:

- Part A: Multicast Encapsulating Security Payload (MESP)
  - Configure the nodes on the link as members of a secure Multicast group that is running MESP. Configure a policy server, and a Group Controller/Key Server on the link.
  - Verify the correctness in their communication by running a Multicast protocol or application.
- Part B: Multicast Source Authentication Transform Specification

- Repeat Step 1 but configure the secure Multicast group to be running MULTICAST SOURCE AUTHENTICATION TRANFORM SPECIFICATION.
- Repeat step 2.

Observable Results: In all parts, the nodes should be able to communicate correctly with the group.

Test IPsec INTEROP.2.2: Distributed Multicast Group Functionality

Purpose: To verify that a group of nodes can correctly communicate in a secure distributed Multicast environment.

Resource Requirements:

- TCP application, such as Telnet.
- User Datagram Protocol (UDP) application, such as Trivial File Transfer Protocol.
- ICMP application, such as ping.

Discussion: This test verifies that a group of nodes can correctly communicate in a secure distributed Multicast environment. This tests both the scenario when the sender and receiver are using the same Group Controller/Key Server (GCKS) entity as well as when the sender and receiver are using different GCKS entities. Additionally, this test verifies the ability of policy servers and GCKS entities to interact with their neighboring counterparts.

Test Setup:

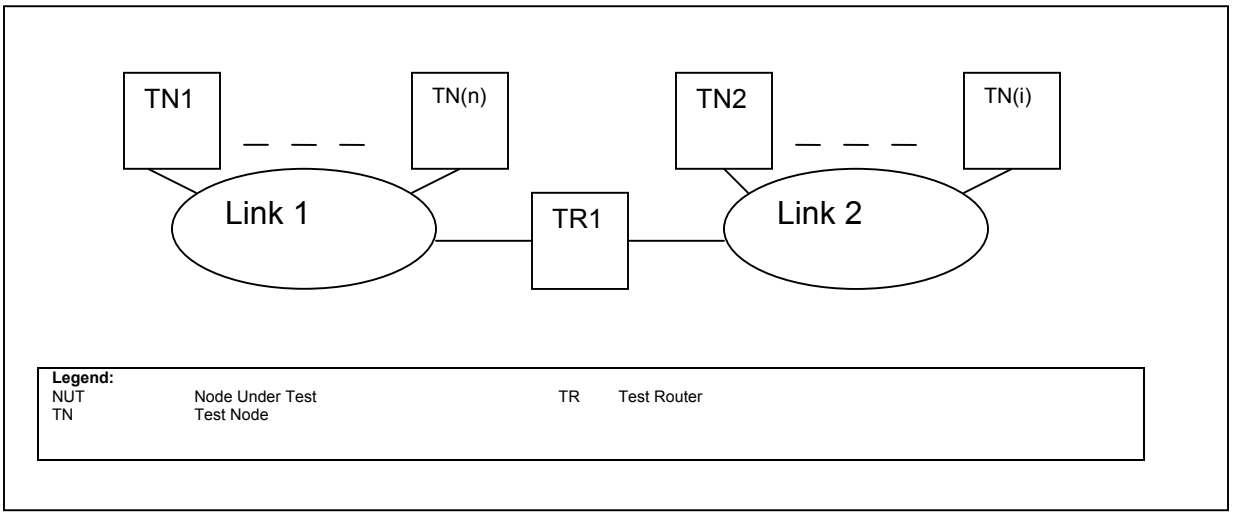


Figure C-8-7. Security Node-to-Node Diagram

Procedures:

- Part A: Multicast ESP
  - Configure the nodes on both link 1 and link 2 as members of the same secure Multicast group that is running MESP. Configure a policy server, and a Group Controller/Key Server on each link.
  - Verify the correctness in their communication by running a Multicast protocol or application.

- Part B: Multicast Source Authentication Transform Specification
    - Repeat Step 1 but configure the secure Multicast group to be running Multicast Source Authentication Transform Specification.
    - Repeat step 2.

Observable Results: In all parts, the nodes should be able to communicate correctly with the group on both links.

APPENDIX C ANNEX 9
ROUTER CONFORMANCE TESTS

Test 9.1. Intermediate System-Intermediate System (IS-IS) Tests

Purpose: To determine if the device under test conforms to common IS-IS conformance test produced my major test equipment manufacturers.

References: RFC-3056.

Resource requirements: Protocol tester.

Background: IS-IS is an International Standard produced to facilitate the interconnection of open systems. IS-IS is a network-layer protocol that functions at the network layer of the OSI 7 layer. This protocol permits routing systems within a routing domain to exchange configuration and routing information to traffic paths. The intra-domain IS-IS routing protocol is intended to support large routing domains consisting of combinations of many types of sub networks. This includes both point-to-point links and multipoint links. In order to support large routing domains, Intra-domain routing is organized hierarchically, so a large domain is administratively divided into multiple areas. Each system resides in exactly one area so routing within an area is referred to as level one and routing between areas is referred to as level two. Level one routers act on routes within their own area. Level two routers keep track of the paths to destination areas. For a packet destined to another area, a level 1 intermediate system sends the packet to the nearest level two intermediate system in its own area, regardless of what the destination area is. Then the packet travels via level two routing to the destination area, where it traverses level one routing to its destination.

Test Setup: Set up the device under test as shown in figure C-9-1.

Procedures: Run the IS-IS test using the procedures shown in tables C-9-1, C-9-2, and C-9-3

Table C-9-1. IPv6 Subnetwork Independent Functions

SUBNETWORK INDEPENDENT FUNCTIONS	
IPv6 Routing Information Exchanges	TC_1_5_1_1_i, TC_1_5_1_1_ii, TC_1_5_1_2_i_a, TC_1_5_1_2_i_b, TC_1_5_1_2_ii_a, TC_1_5_1_2_ii_b, TC_1_5_1_3, TC_1_5_1_4, TC_1_5_1_5, TC_1_5_1_6
IPv6 IP Reachability Info, Hierarchical Abbreviation	TC_1_5_2_1, TC_1_5_2_2, TC_1_5_2_3, TC_1_5_2_4, TC_1_5_2_6, TC_1_5_2_7
IPv6 External Links	TC_1_5_4_1, TC_1_5_4_2, TC_1_5_4_3
IPv6 IP Only Operation	TC_1_5_7_1
IPv6 Authentication	TC_1_5_9_1_i, TC_1_5_9_1_ii, TC_1_5_9_1_iii_a, TC_1_5_9_1_iii_b, TC_1_5_9_1_iv_a, TC_1_5_9_1_iv_b, TC_1_5_9_1_v_a, TC_1_5_9_1_v_b

Legend:

IP	Internet Protocol
IPV6	**INTERNET PROTOCOL VERSION 6**
TC	**TEST CASE**

Table C-9-2. IPv6 Subnetwork Dependent Functions

SUBNETWORK DEPENDENT FUNCTIONS	
IPv6 Multiple IP Addresses Per Interface	TC_2_4_1_1_i, TC_2_4_1_1_ii, TC_2_4_1_2_i, TC_2_4_1_2_ii, TC_2_4_1_3
IPv6 local area network Designated Router	TC_2_4_2_1, TC_2_4_2_2, TC_2_4_2_3
IPv6 Maintaining Router Adjacencies	TC_2_4_3_1_i, TC_2_4_3_1_ii, TC_2_4_3_2, TC_2_4_3_3, TC_2_4_3_4

Legend:

IP	Internet Protocol
IPv6	**Internet Protocol version 6**
TC	**Test Case**

Table C-9-3. IPv4 Subnetwork Dependent Functions

SUBNETWORK INDEPENDENT FUNCTIONS	
IPv6 Multiple IP Addresses Per Interface	TC_2_4_1_1_i, TC_2_4_1_1_ii, TC_2_4_1_2_i, TC_2_4_1_2_ii, TC_2_4_1_3
IPv6 local area network Designated Router	TC_2_4_2_1, TC_2_4_2_2, TC_2_4_2_3
IPv6 Maintaining Router Adjacencies	TC_2_4_3_1_i, TC_2_4_3_1_ii, TC_2_4_3_2, TC_2_4_3_3, TC_2_4_3_4

Legend:

IP	Internet Protocol	TC	Test Case
ipV4	**INTERNET PROTOCOL VERSION 4**		
IPv6	**INTERNET PROTOCOL VERSION 6**		

(This page intentionally left blank.)

APPENDIX C, ANNEX TEN

NETWORK PERFORMANCE AND LOADING TESTS

Test 10.1: Automatic Tunneling Latency

Purpose: To determine the throughput, forwarding rate, and latency of the Device under Test/System under Test when performing automatic tunneling

References: RFC-2893.

Resource requirements: Protocol tester.

Background: Automatic tunneling is one of the IPv6 transition mechanisms documented in RFC 2893. Automatic tunnels are used to tunnel IPv6 packets over an IPv4 network. Tunnels as set up using the IPv4 endpoint address as determined form the IPv4 address embedded in the IPv4-compatable destination address of the IPv6 packet being tunneled.

Test Setup: Set up the device under test as shown in figure C-10-1.

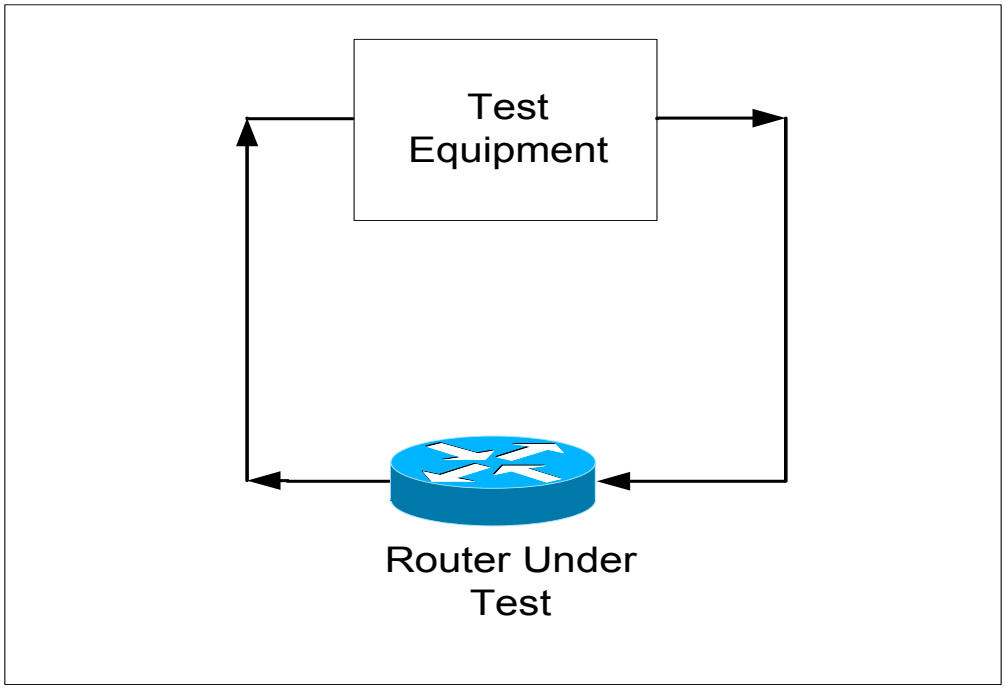


Figure C-10-1. Device-Centric Tests

Procedures: Run the automatic tunnel test on each device for 60 seconds with minimum and maximum frames sizes.

- Configure the test instrument to offer traffic at the MOL (Maximum Offered Load). The offered frames MUST contain an IPv4-compatable address as defined in RFC-2893.
- Begin offering frames (at the MOL) to the device under test for the specified test duration.
- If there is frames loss, a binary search algorithm will adjust the offered load to find the maximum rate at which none of the offered frames are lost.
- Perform a latency test at 50% and 100% of the measured throughput.
- Repeat steps 1 through 4 for all frame sizes if time allows (default to 1518 byte frame size).

Test 10.2: Configured Tunneling Latency

Purpose: To determine the throughput, forwarding rate, and latency of the device or system under test when using configured tunnels.

References: RFC-2893.

Resource requirements: Protocol tester.

Background: Configured tunnels are an IPv6 transition mechanism documented in RFC 2893. Configured tunnels are statically configured on the encapsulating node. The tunnels can be either unidirectional or bidirectional and act as virtual point-to-point links.

Test Setup: Set up the device under test as shown in figure C-9-1.

Procedures: Run the configured tunnel test on each device for 60 seconds with minimum and maximum frames sizes.

- Configure the tunnels in the device under test.
- Configure the test instrument to offer traffic at the MOL (Maximum Offered Load). The destination IP addresses of the offered frames must correspond to the tunnel mapping configured on the device under test/system under test.
- Offer frames at the MOL for the specified test duration.
- If there is frames loss, a binary search algorithm will adjust the offered load to find the maximum rate at which none of the offered frames are lost.
- Perform a latency test at 50% and 100% of the measured throughput.
- Repeat steps 1 through 4 for all frame sizes

Test 10.3: 6-to-4 Tunneling

Purpose: To determine the throughput, forwarding rate, and latency of the device or system under test when using 6-to-4 tunnels.

References: RFC-3056.

Resource requirements: Protocol tester.

Background: This transition mechanism is used to allow isolated IPv6 sites or hosts, attached to a wide area network which has no native IPv6 support, to communicate with other such IPv6 domains or hosts with minimal manual configuration.

Test Setup: Set up the device under test as shown in figure C-9-1.

Procedures: Run the configured tunnel test on each device for 60 seconds with minimum and maximum frames sizes.

- Configure the tunnels in the device under test.
- Configure the test instrument to offer traffic at the MOL (Maximum Offered Load). The destination IP addresses of the offered frames must correspond to the tunnel mapping configured on the device under test/system under test.
- Offered frames at the MOL for the specified test duration.
- If there is frames loss, a binary search algorithm will adjust the offered load to find the maximum rate at which none of the offered frames are lost.
- Perform a latency test at 50% and 100% of the measured throughput.
- Repeat steps 1 through 4 for all frame sizes. (Default to 1500 bytes.)

Test 10.4: Long-Term Network Stability (Under Load)

Purpose: To evaluate the capability of a realistically configured network to properly process relatively high levels of traffic over a 48-hour test window.

References: None.

Resource requirements: Protocol tester.

Background: IP networks in transition from IPv4 to IPv6 are required to pass a mixture of IPv4 and IPv6 packets. The capability of network devices to properly process this traffic at reasonably high rates (when compared to the theoretical maximum associated with a given link) is critical to proper network operation.

Test Setup: For end-to-end testing set up a network similar to the one shown in figure C-10-3. For localized testing, set up a network similar to the one shown in figure C-9-4.

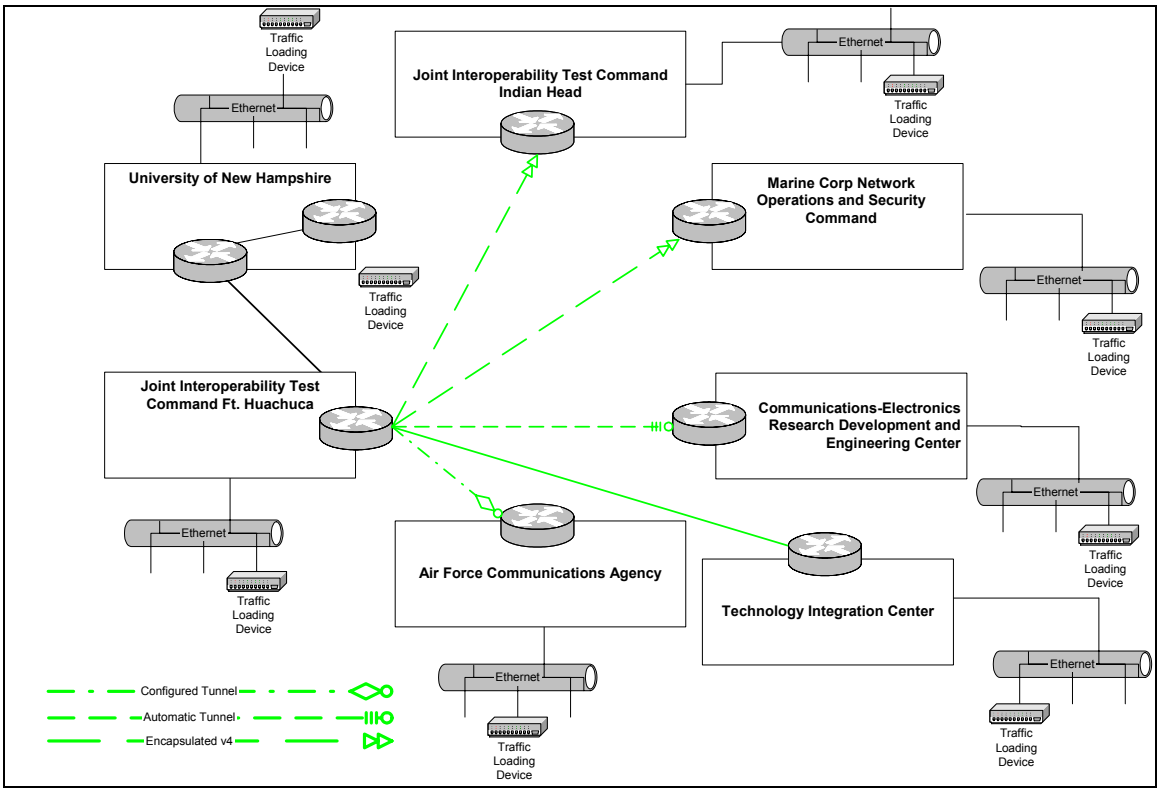


Figure C-10-2. End-to-End Network

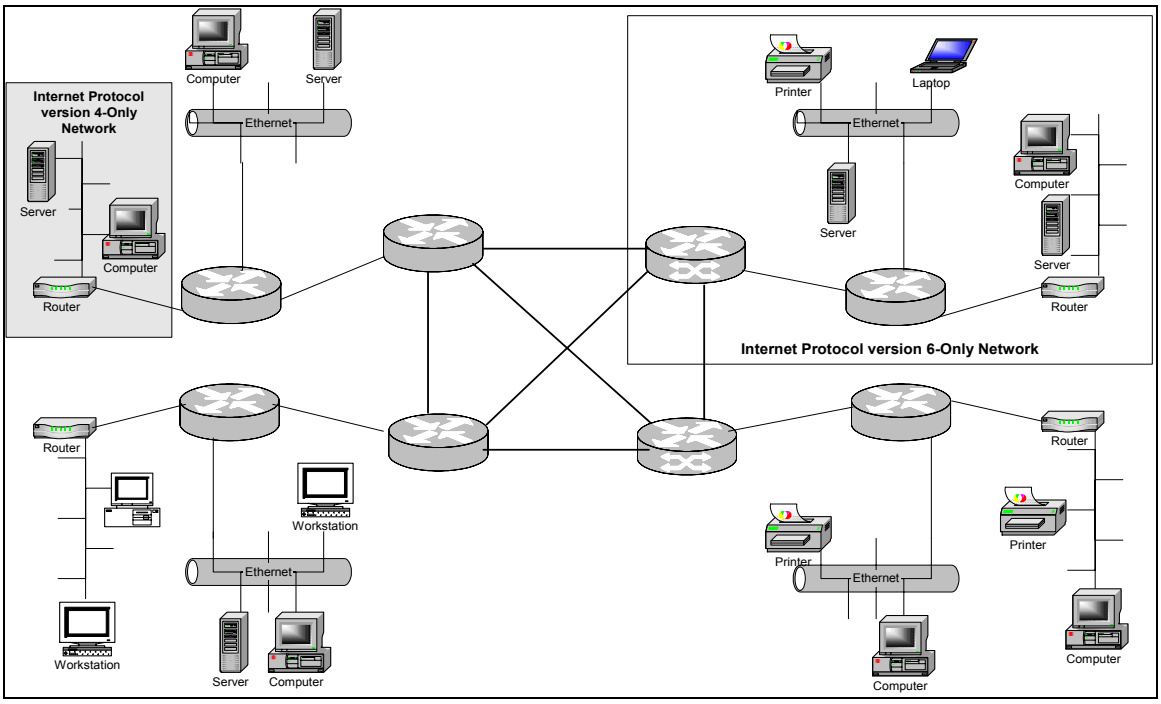


Figure C-10-3. Network-Centric Testing

Procedures: Configure the traffic loading devices to offer continuous IPv4 and IPv6 traffic using one of the two metrics shown below:

- For each backbone interface set the offered traffic at 80% of the theoretical maximum traffic forwarding rate using 1500 byte packets.
- If the local interface cannot offer traffic at the rate required to achieve 80% of the backbone interface rate, set the local interface rate to 100% of the local interface using 1500 byte packets.

(Note: Moonv6 Phase II traffic traverses networks over which the test team has no engineering or operational control. These networks may have traffic- restrictive requirements that require tuning offered traffic to levels below those described above. If this situation occurs, tune traffic to 80% of the highest level allowed by the traffic policies implemented on the interconnecting networks.)

- Monitor the received traffic on each backbone link for packet loss, receive rate, and latency.
- Write running log on local drive every 10 minutes.

Test 10.5: Switch Performance

The following tests measure the performance of a single device in a standalone environment. The goal of these tests is to determine if the use of IPv6 results in degraded network performance due to increased latency within switching and routing devices. Each IPv4 test establishes a performance baseline upon which the IPv6 performance results can be quantitatively compared. Each core switch is evaluated independently. Tests will be performed in the order listed.

10.5.1: IPv4 Routing/Forwarding

Purpose: Measure the routing and IP forwarding performance of the switch.

References: RFC 2544. Benchmarking Methodology for Network Interconnect Devices.

Resource Requirements: Protocol tester.

Background: Network design is based on non-blocking switches. This test records the actual throughput of the switch. The Device Under Test (DUT) is tested in full-mesh mode to stress both the backplane and the line cards. Run forwarding tests with one Media Access Control (MAC) address per port.

Test Setup: Figure C-10-4 shows the test configuration. Connect the packet generator/analyzer to the switch with the maximum number of 1000-Megabit per second (Mbps) streams using multimode fiber. Connect to the switch with the maximum number of 100-Mbps streams, across at least two blades, using category 5 cabling.

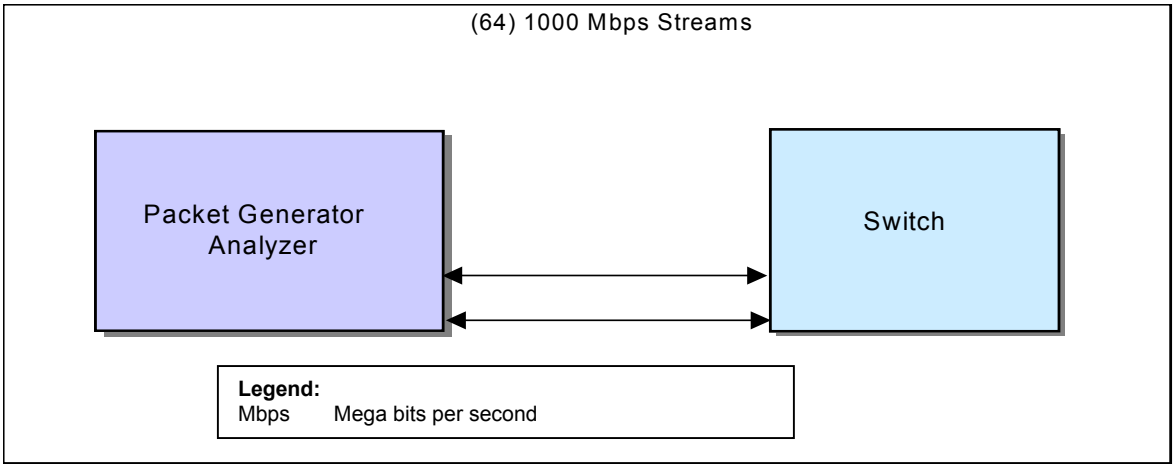


Figure C-10-4. Switch Performance Configuration

Procedures:

- Connect the packet generator/analyzer to the corresponding switch with an equal number of IPv4 streams per switch port. Use the packet analysis tool to perform

the Throughput and Jumbo tests in a full mesh mode. Configure the packet analysis tool to use the default Packet generator/analyzer MAC addresses.

- Configure the packet analysis tool to transmit traffic on a single subnet on each port. Measure performance for 64, 128, 256, 512, 1024, 1280, and 1518-byte frame sizes.
- Record the latency and throughput results.

10.5.2 IPv4 Multicast

Purpose: Measure switch Multicast performance using a mixture of Unicast and Multicast traffic.

References:

Resource Requirements: Protocol tester.

Background: Devices must be capable of supporting theater-wide IP Multicast traffic. Switches are typically capable of supporting Multicast protocols including Internet Group Multicast Protocol (IGMP), IGMP snooping (per port), and Distance Vector Multicast Routing Protocol (DVMRP) or Protocol Independent Multicast-Dense Mode (PIM-DM) and Sparse Mode (PIM-SM). The use of PIM (sparse mode) is preferred in lieu of PIM (dense mode) or DVMRP but not mandated. The device should not restrict Multicast traffic and send Multicast traffic to proper groups and subnets and not flood traffic onto Ethernet ports without express join requests by users attached to those ports. The installed devices must support simultaneous and concurrent transmission and operation of Multicast and IP data and protocols called out in this section.

Test Setup: Figure C-10-5 shows the Multicast Performance test configuration. The packet generator/analyzer is connected with the switch's maximum port count with 1,000-Mbps (or 100-Mpbs) transmit and receive streams.

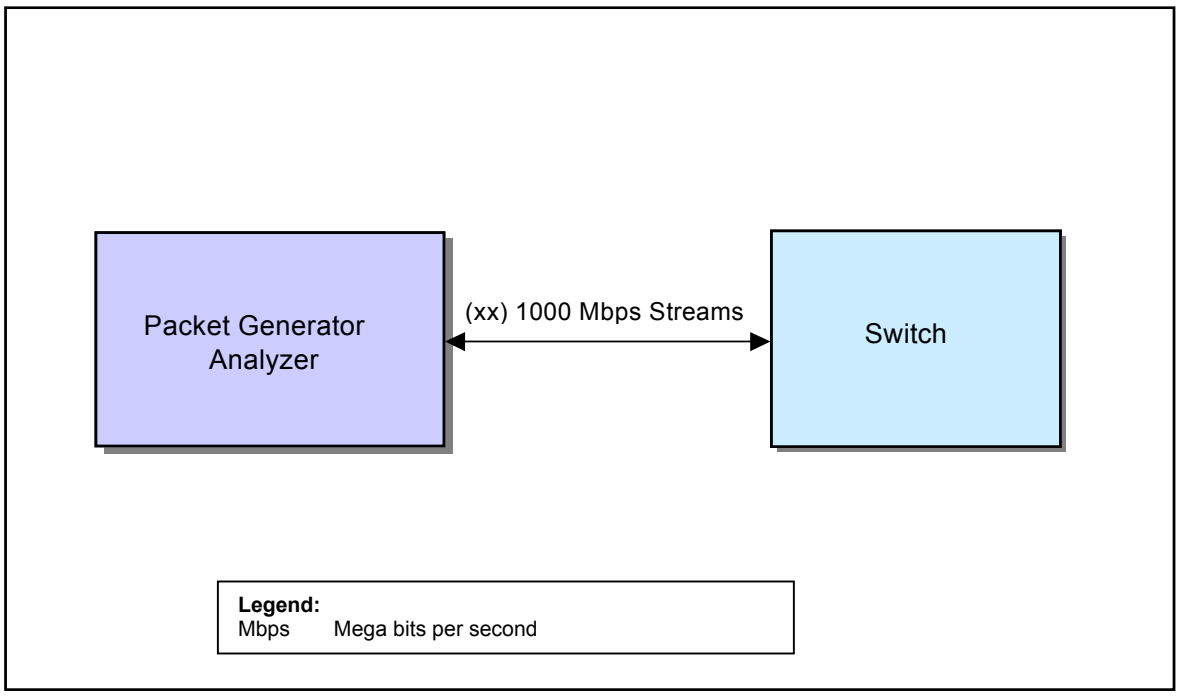


Figure C-10-5. Multicast Performance Configuration

Procedures:

- Enable IGMP snooping, OSPFv2 and Protocol Independent Multicast (PIM) routing protocols on the switch. Use Distance Vector Multicast Routing Protocol (DVMRP) if PIM is not supported.
- Configure the following the packet analysis tool general settings:

Duration	30 seconds
Number of trials	1
Transmit delay after joins	2 seconds
Delay after transmission	2 ms
Custom frame sizes	1024, 1408, and 1518 bytes

- Use the packet analysis tool to perform each of the three following subtests:
- Multicast Traffic. Configure the packet analysis tool for Multicast only traffic. Configure 16 concurrent traffic groups with one transmitter and at least two receivers per group. Configure one receiver on the same blade as the transmitter; configure the other receiver on a different blade than the transmitter. Configure each stream transmitted by the packet generator/analyzer in a separate subnet. Configure the packet analysis tool in step mode with the following settings:

Group count	1
Initial rate	40 percent
Maximum rate	100 percent
Step rate	20 percent

- Multicast Traffic. Configure the packet analysis tool for Multicast only traffic. Configure 32 concurrent traffic groups with one transmitter and at least two receivers per group. Configure one receiver on the same blade as the transmitter; configure the other receiver on a different blade than the transmitter. Configure each stream transmitted by Packet generator/analyzer in a separate subnet. Configure the packet analysis tool in step mode with the following settings:

Group count	1
Initial rate	40 percent
Maximum rate	100 percent
Step rate	20 percent

- Multicast and Unicast Traffic. Configure the packet analysis tool for Multicast and Unicast traffic. Use the same 16 groups during the Multicast traffic subtest, but gradually introduce Unicast traffic at the same rate as the Multicast traffic. Configure the packet analysis tool in step mode with the following settings:

Group count	1
Initial rate	10 percent
Maximum rate	50 percent
Step rate	10 percent

.

Test 10.6: IPv4 Traffic Prioritization

Purpose: Measure the switch's ability to classify and queue traffic using Differentiated Services.

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

Resource Requirements: Protocol tester.

Test Setup: Figure C-10-6 shows the Traffic Prioritization test configuration. The packet generator/analyzer connects to the switch with four transmit and two receive streams providing a 2:1 over-subscription.

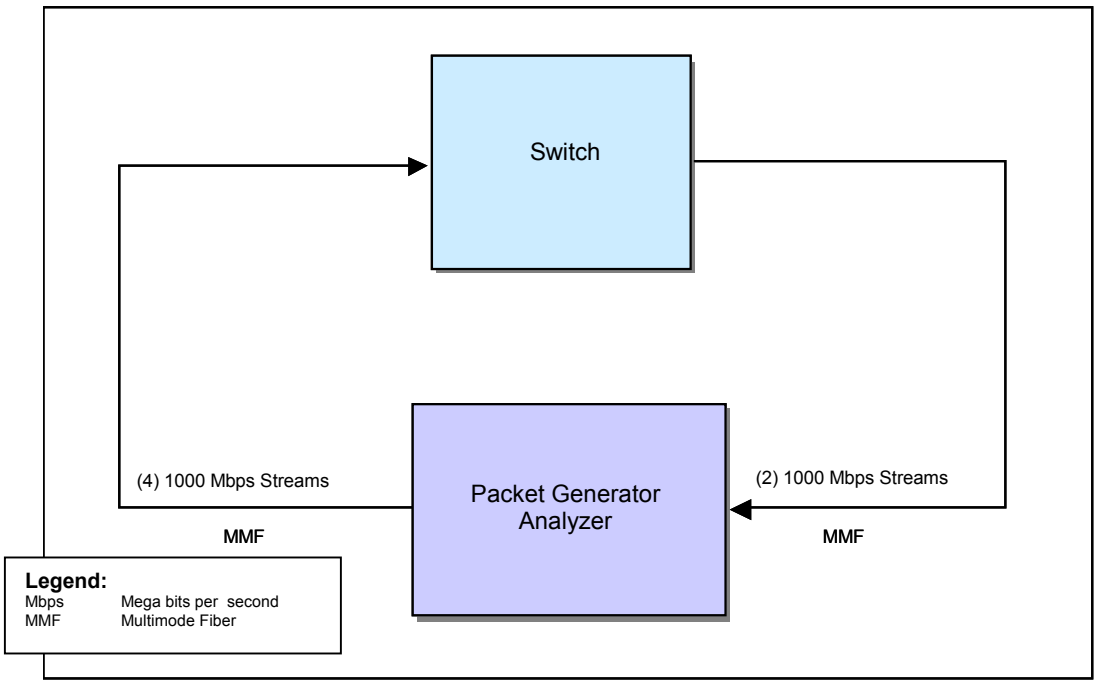


Figure C-10-6. Traffic Prioritization Configuration

Procedure:

- Connect Packet generator/analyzer to the core switch with four 1,000-Mbps transmit streams and two 1,000-Mbps receive streams.
- Use the packet analysis tool to perform the Jumbo tests using a 512-byte frame size. The following three Traffic Prioritization functional areas are tested.
- IP Address Prioritization. Use the packet analysis tool to configure four different traffic groups. Assign a different IP address to each group on each port. Configure the core switch to prioritize traffic based on IP address. Table C-10-1 shows the IP address priorities to use for the four groups:

Table C-10-1. IP Address Prioritization

GROUP	BANDWIDTH	DSCP
IP Group 1	40%	7
IP Group 2	20%	5
IP Group 3	10%	3
IP Group 4	5%	1

Legend:
DSCP Differentiated Services Point Code
IP Internet Protocol

- Application Flow Prioritization. Use the packet analysis tool to configure four different traffic groups. Assign each group to a different application. Configure the core switch to prioritize traffic based on application. Table C-10-2 shows the application flow priorities to use for the four groups:

Table C-10-2. Application Flow Prioritization

GROUP	BANDWIDTH	DSCP
SMTP	40%	7
TELNET	20%	5
FTP	10%	3
HTTP	5%	1

Legend:
DSCP Differentiated Services Point Code
FTP File Transfer Protocol
HTTP Hypertext Transfer Protocol
SMTP Simple Mail Transfer Protocol
TELNET Telecommunications Network

- Differentiated Services Code Point (DSCP) Prioritization. Use the packet analysis tool to configure eight different traffic groups. Assign each group a different prioritization as in Table C-10-3 below. Configure the core switch to prioritize traffic based on DSCP.

Table C-10-3. DSCP Prioritization

GROUP	BANDWIDTH	DSCP
VTC Setup (UDP port 1720)	15%	15
VTC Call Control (UDP port 1731)	13%	13
SIP (UDP port 5060)	11%	11
RTSP (TCP port 554)	9%	9
SMTP (TCP port 25)	7%	7
TELNET (TCP port 23)	5%	5
FTP (TCP port 21)	3%	3
HTTP (TCP port 80)	1%	1

Legend:
DSCP Differentiated Services Point Code
FTP File Transfer Protocol
HTTP Hypertext Transfer Protocol
RTSP Real Time Session Protocol
SIP Session Initiation Protocol
SMTP Simple Mail Transfer Protocol
TELNET Telecommunications Network
TCP Transmission Control Protocol
UDP User Datagram Protocol
VTC VideoTeleconference

Test 10.7. IPv6 Routing/Forwarding

Purpose: Measure the IPv6 routing performance of the switch.

References. RFC 2460, Internet Protocol, Version 6 (IPv6) Specification.

Resource Requirements: Protocol tester.

Test Setup: Figure 4 shows the IPv6 Routing test configuration. Configurations will have port densities identical to IPv4 configurations. IPv4 (current) and IPv6 address can be present on the device during the evaluation. Core Switch: Packet generator/analyzer is first connected to the switch with up to the maximum number of 1,000-Mbps streams available using multimode fiber.

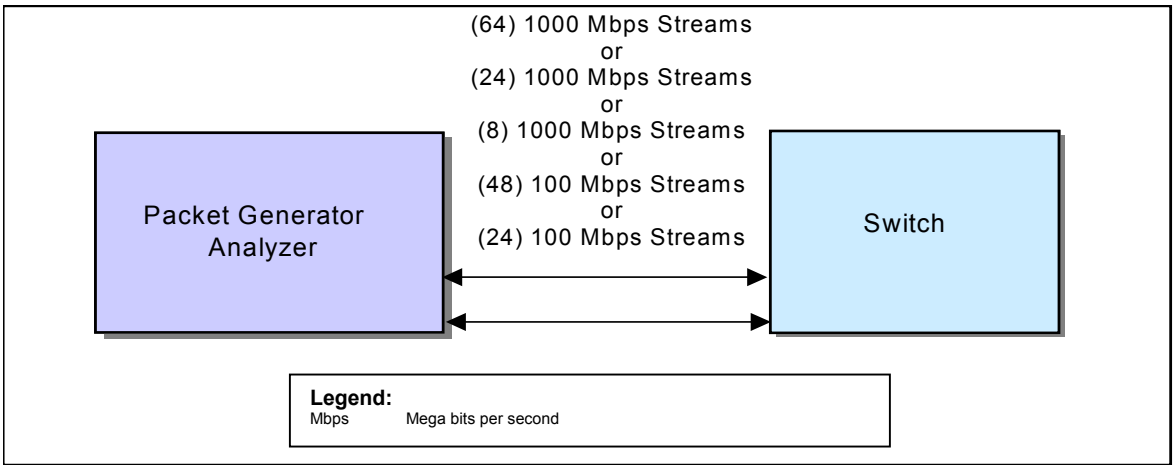


Figure C-10-7. IPv6 Routing/Forwarding Configuration

Procedures:

- Connect the packet generator/analyzer to the corresponding switch with an equal number of IPv6 streams per switch port. .
- Use the packet analysis tool to perform the Throughput and Jumbo tests in a full mesh mode. Configure the packet analysis tool to transmit cyclic traffic flows with a different subnet on each port. Verify the switch correctly routes IPv6 traffic between the subnets.
-

Test 10.8. IPv6 Traffic Prioritization

Purpose: Measure the switch's ability to classify and queue traffic using Differentiated Services.

References: RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.

Resource Requirements: Protocol tester.

Test Setup: Figure C-10-8 shows the Traffic Prioritization test configuration. Packet generator/analyzer connects to the switch with four transmit and two receive streams providing a 2:1 over-subscription.

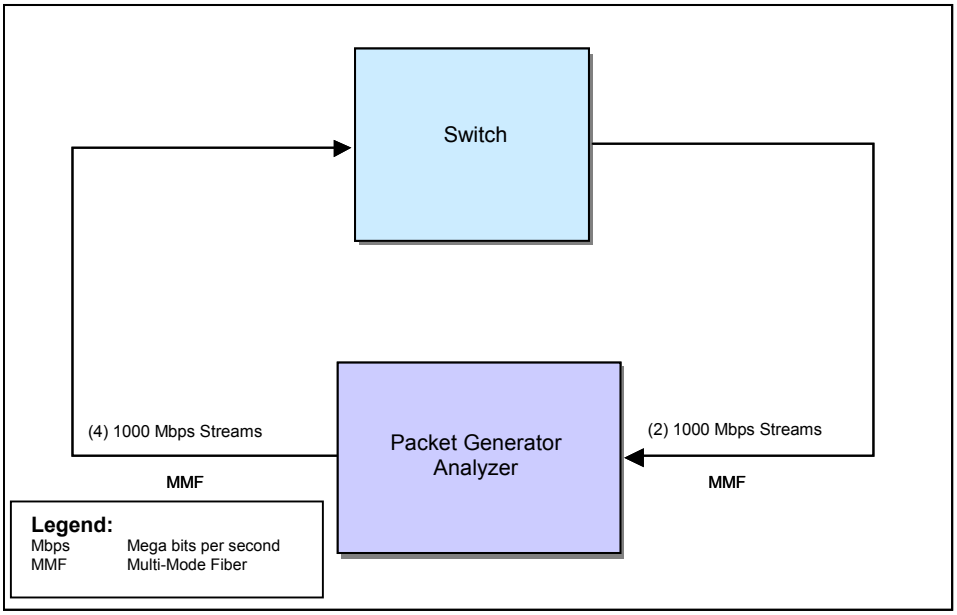


Figure C-10-8. Traffic Prioritization Configuration

Procedure.

- Connect Packet generator/analyzer to the core switch with four 1,000-Mbps transmit streams and two 1,000-Mbps receive streams.
- Use the packet analysis tool to perform the Jumbo tests using a 512-byte frame size. The following three Traffic Prioritization functional areas are tested.
- IP Address Prioritization. Use the packet analysis tool to configure four different traffic groups. Assign a different IP address to each group on each port. Configure the core switch to prioritize traffic based on IP address. Table C-10-4 shows the IP address priorities to use for the four groups:

Table C-10-4. IP Address Prioritization

GROUP	BANDWIDTH	DSCP
IP Group 1	40%	7
IP Group 2	20%	5
IP Group 3	10%	3
IP Group 4	5%	1

Legend:
DSCP Differentiated Services Point Code
IP Internet Protocol

- Application Flow Prioritization. Use the packet analysis tool to configure four different traffic groups. Assign each group to a different application. Configure the core switch to prioritize traffic based on application. Table C-10-5 shows the application flow priorities to use for the four groups:

Table C-10-5. Application Flow Prioritization

GROUP	BANDWIDTH	DSCP
SMTP	40%	7
TELNET	20%	5
FTP	10%	3
HTTP	5%	1

Legend:
DSCP Differentiated Services Point Code
FTP File Transfer Protocol
HTTP Hypertext Transfer Protocol
SMTP Simple Mail Transfer Protocol
TELNET Telecommunications Network

- Differentiated Services Code Point (DSCP) Prioritization. Use the packet analysis tool to configure eight different traffic groups. Assign each group a different prioritization as in Table C-10-6.. Configure the core switch to prioritize traffic based on DSCP.

Table C-10-6. DSCP Prioritization

GROUP	BANDWIDTH	DSCP
VTC Setup (UDP port 1720)	15%	15
VTC Call Control (UDP port 1731)	13%	13
SIP (UDP port 5060)	11%	11
RTSP (TCP port 554)	9%	9
SMTP (TCP port 25)	7%	7
TELNET (TCP port 23)	5%	5
FTP (TCP port 21)	3%	3
HTTP (TCP port 80)	1%	1

Legend:
DSCP Differentiated Services Point Code
FTP File Transfer Protocol
HTTP Hypertext Transfer Protocol
RTSP Real Time Session Protocol
SIP Session Initiation Protocol
SMTP Simple Mail Transfer Protocol
TELNET Telecommunications Network
TCP Transmission Control Protocol
UDP User Datagram Protocol
VTC VideoTeleconference

Test 10.9. IPv4/IPv6 Dual Stack Forwarding/Routing Performance

Purpose: Measure concurrent IPv4 and IPv6 (dual stack) routing/forwarding performance of the switch.

References: RFC 1242, RFC 2893, RFC 2544, DOD September 2003 IPv6 Interim Guidance.

Resource Requirements: Protocol tester.

Test Setup Figure C-10-9 shows the IPv4/IPv6 Routing/Forwarding configuration. Configurations will have port densities similar to IPv4 configurations.
Core Switch: Packet generator/analyzer is first connected to the switch with up to the maximum 1,000-Mbps streams available using multimode fiber.

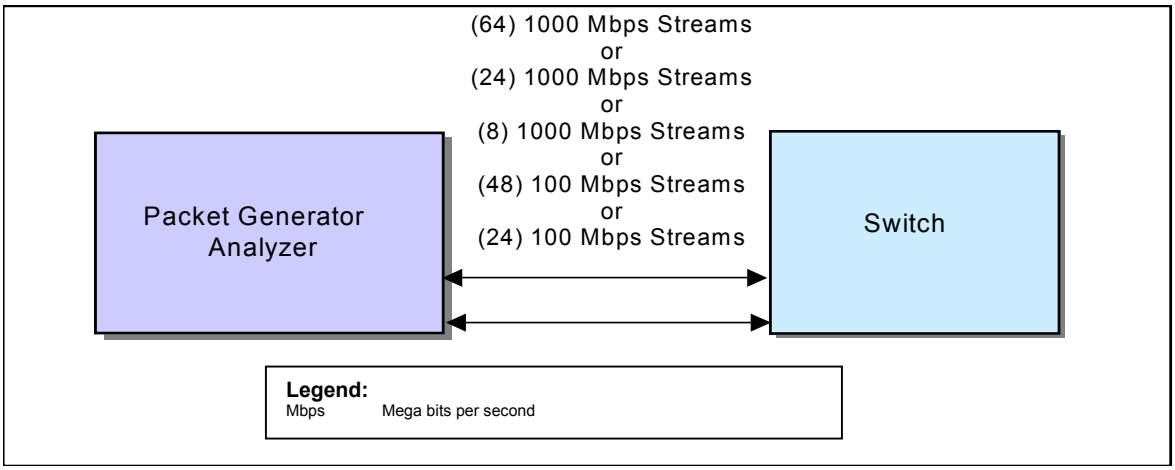


Figure C-10-9. IPv4/IPv6 Routing Configuration

Test Procedures:

- Connect the packet generator/analyzer to the corresponding switch with an equal number of IPv4 and IPv6 streams per switch port. Configure the switch with the IPv6 addresses specified in Appendix B. Use the packet analysis tool to perform the Throughput and Jumbo tests in two separate full mesh groups, one group for IPv4 traffic and a second for IPv6.
- Configure the packet analysis tool to transmit cyclic traffic flows with a different IPv4 and IPv6 subnet on each port. Verify the switch correctly routes IP traffic within its designated group, but not cross into the other group. Measure performance for partial mesh traffic pattern reflecting the Client/Server nature of DOD networks.

Test 10.10. Inter-Site Network Performance Test.

Purpose: To characterize the network performance between Moonv6 sites when using traffic representing IPv4 and IPv6 end-user applications.

References:

- IPv6 (RFC 2460)
- Neighbor Discovery Protocol (RFC 2461)
- Stateless Address Autoconfiguration (RFC 2462)
- ICMPv6 (RFC 2463)
- Transmission of IPv6 Packets over Ethernet Networks (RFC 2464)

Resource Requirements:

- Test Equipment with the capability to emulate stateless and stateless IPv4 and IPv6 TCP, UDP and RTP packets at the same time
- Test Script to automate procedures and expedite testing

Background: One of the biggest uncertainties with IPv6 is how it will work with an existing IPv4 network infrastructure. Although transition mechanisms have been tested extensively in the lab, network designers are still uneasy about how it will perform in an operational network with varying traffic loads. Consequently, designers are requiring that real-user behavior be emulated, such as generating TCP and UDP packets representative of real-world applications. In particular, TCP packets must be stateful traffic; this means end-to-end testing. To accomplish this, every edge device, service, and application must either be included in, or emulated in the test environment. By doing this, network performance can be characterized in a mixed-IP environment and the feasibility of migrating to a dual IPv4/IPv6 environment can be evaluated.

Test Setup: To allow for test scalability, a distributed test network is recommended. A minimum of four endpoints are to be strategically located across the Moonv6 network. The endpoints will be stationed at Ft. Huachuca, UNH, JITC Indian Head, and MCNOSC. The central console will be stationed at Ft. Huachuca. The central console will aggregate the performance data sent back from the four endpoints.

Procedures:

IPv4 network performance Test: This test is to measure the network performance when IPv4 stateful packets are being sent across moonv6 sites.

- Set up multiple IPv4 stateful traffic scripts; one for each protocol to be tested, i.e. TCP, UDP, RTP. Each script can have different properties.
- Make sure that no ACLs have been setup.

Observable Results:

- Run the test at different data rates. Initial data rates can be based on historical average rates for the respective networks.
- Measure key stateful traffic performance criteria such as throughput, response times, delay, or consecutive lost datagram's etc.

- Save test setup for dual IPv4/IPv6 network test.

IPv6 network performance test: This test is to measure the network performance when IPv6 stateful packets are being sent across moonv6 sites.

- Set up multiple IPv6 stateful traffic scripts; one for each protocol to be tested, i.e. TCP-IPv6, UDP-IPv6, RTP-IPv6. Each script can have different properties (e.g. HTTP text, RealAudio,).
- Enable IPv6 support on the DUT. Make sure that no ACLs have been setup.

Observable Results:

- Run the test at different data rates. Use data rates defined in procedure one.
- Measure key stateful traffic performance criteria such as throughput, response times, delay, consecutive lost datagrams etc…).
- Save test setup for dual IPv4/IPv6 network test.

Dual IPv4/IPv6 protocol performance test: This test is to measure the network performance when dual IPv4/IPv6 stateful packets are being sent across moonv6 sites.

- Combine scripts from the IPv4 and IPv6 stateful traffic scripts.

Observable Results:

- Run the test at different data rates. Use data rates defined in procedure one.
- Measure key stateful traffic performance criteria such as throughput, response times, delay, consecutive lost datagram's etc…).

Dual IPv4/IPv6 DUT load test: This test is recommended for DUT testing since the interfaces will be loaded up to capacity. The objective is to measure how a DUT will handle stateful traffic when it experiences congestion.

- Open saved "Dual IPv4/IPv6 protocol performance test script."
- Create dual IPv4/IPv6 stateless traffic at fixed lines rates set to be less than 100% combined to generate background traffic. Use streams with exactly defined (e.g. 74 bytes) frame size and/or random frame sizes.

Observable Results:

- Run combined test scripts for stateful and stateless IPv4/IPv6 traffic and measure key common stateful and stateless performance criteria such as throughput and delay.

IPv6 DUT overload and Quality of Service (QOS) test: This test is recommended for DUT testing since the interfaces will be overloaded. The objective is to measure how a DUT will handle stateful traffic tagged with different QOS priorities when the DUT is congested.

- Open saved integrated stateless and stateful IPv6 performance test.
- Increase combined line rate of stateless IPv4/IPv6 streams to more than 100%.
- Set QOS policies for some but not all stateful traffic generation scripts.

Observable Results:

- Run combined test scripts for stateful and stateless IPv4/IPv6 traffic and measure key common stateful and stateless performance criteria such as throughput and delay. Non-QOS traffic should have extremely low or no throughput.

Possible Problems:

- Traffic across the DREN and Internet 2 network is not exclusive to Moonv6 testing. Consequently, there might be a possibility that other network traffic might affect the network results. An initial assessment of the network traffic should be conducted.
    - If a dedicated circuit is being used for Moonv6 testing, then procedure 4 and 5 can be used across the network.
- The central console uses the IPv4 stack to collect statistics from the endpoint. Hence, there must be IPv4 reachability to the endpoints.
- For procedure 4 and 5, Make sure that the Operating Systems on the various test devices used to run the test endpoints support IPv6 and stateless stream generation at the same time.

Test 10.11: Multicast Listener Discovery (MLD) Join/Leave Latency.

Purpose: To determine the average join and leave latency of a DUT as multicast groups are added.

References: Multicast Listener Discovery version 1, RFC 2710, Multicast Listener Discovery version 2, IETF Draft-VIDA-MLD-V2-08.txt, Dynamic Host Configuration Protocol version 6, RFC 3315.

Resource Requirements: Test Equipment with the capability to emulate MLD functionality

Background: DOD offers a number of audio and video applications (VideoTeleconferencing and Defense Collaborative Tool Suite) for teleconferencing and group collaboration. Most of these applications offer only point-to-point support today. However, there is an increasing need to support point-to-multipoint capabilities, such as multiple simultaneous video signal transmissions to different sub networks, for future warfighter-centric applications like war gaming and training. Therefore it is prudent to begin testing router capabilities to support IPv6 subscriptions to multicast groups using Multicast Listener Discovery protocol.

Test Setup: Connect the device under test to the test equipment as shown in figure C-10-1.

Procedures: Join/Leave Test: This test will measure join and leave latency per port or Virtual Local Area Network (VLAN) when one or more hosts joins and leaves the same set of multicast groups.

- Set up multiple IPv6 multicast streams; one for each multicast group. Each stream can have different stream properties.
- Enable MLD support on the DUT. Make sure that IPv6 Multicast Routing is enabled.
- Each port will have one host unless VLANs are used which in that case it will be one host per VLAN.
- Each host will then join all the multicast groups by sending MLD joins. Measure the join latency per port or VLAN for all multicast groups. Also, measure the bit rate for all multicast groups per port or VLAN.
- Each host will then leave all the multicast groups by sending MLD Leaves. Measure the leave latency per port or VLAN for all multicast groups.

Rejoin Test: This test will measure the elapsed time from when a join and leave message is issued to the DUT to the time it takes to receive multicast traffic on the new set of groups.

- The test procedure is the same the Join/Leave test except for the last step. In this test, a leave and join MLD message should be sent at the same time.
- Add additional multicast groups to investigate scalability capability.

Overlap Test: This test will measure the time elapsed between the start of receiving multicast traffic on a new set of groups and the end of multicast traffic received on the old multicast groups.

- The test procedure is the same as the Rejoin test, however, the reporting is slightly different.
- Add additional multicast groups to investigate scalability capability.

Observable Results:

- Report join, leave, rejoin, and overlap latencies.
- Optionally graph results over time.

(This page intentionally left blank.)

APPENDIX C ANNEX 11
NETWORK FAULT TESTING

Test 11.1. Synchronous Optical Network (SONET) Failure Testing

Purpose: To determine if the devices under test will properly process and respond to SONET Loss of Signal conditions.

References: American National Standards Institute (ANSI) standard T1.231 and T1.105

Resource Requirements: Packet capture tools.

Background: A Loss of Signal (LOS) defect should be declared when no transitions are detected on the received signal. Specifically, the LOS defect should be detected if 2.3 to 100 microseconds of no transitions are experienced on the receive side of the SONET circuit. The LOS defect should be cleared after a 125 microsecond interval during which no LOS conditions are detected. The LOS *failure* is declared when the LOS defect persists for a period of 2.5 +/- 0.5 seconds, or if LOS is present when the criteria for LOF failure declaration have been met. The LOS failure is cleared when LOS is absent for a period of 10 +/- 0.5 seconds.

Test Setup: Set up a four-router network as shown in figure C-11-1

Procedures: Break link C-D.

- Determine if Routers C and D correctly respond to the SONET link outage by declaring LOS.
- Determine if an appropriate Simple Network Management Protocol (SNMP) trap is transmitted by Routers C and D.
- Determine if Router C correctly re-routes traffic to Router D via the least-cost path (Link C-A then Link C-D).
- Restore Link C-D.
- Determine if the SONET LOS is removed within 10 +/- 0.5 seconds.
- Determine if an appropriate Simple Network Management Protocol (SNMP) trap is transmitted by Routers C and D.
- Determine if traffic destined for Router D is restored to Link C-D

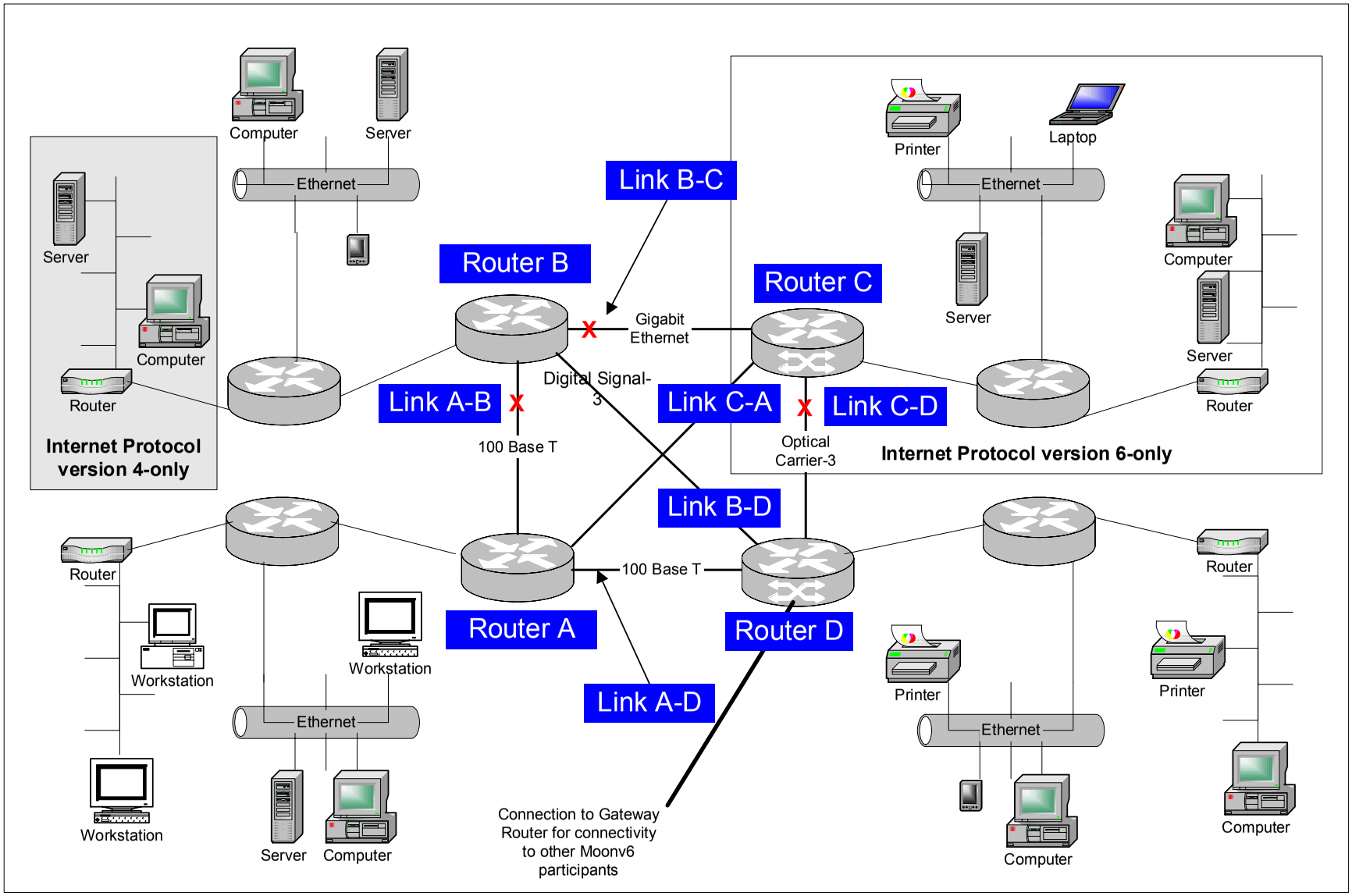


Figure C-11-1. Network Fault Testing

Test 11.2. DS-3 Failure Testing

Purpose: To determine if the devices under test will properly process and respond to Digital Signal-3 (DS-3) failures.

References: American National Standards Institute (ANSI) standard T1.107a.

Resource Requirements: Packet capture tools.

Background: The Remote Alarm Indication (RAI) failure is declared after detecting the Yellow Alarm Signal on the alarm channel. The Remote Alarm Indication failure, in C-bit Parity DS3 applications, is declared as soon as the presence of either one or two alarm signals are detected on the Far End Alarm Channel. The Remote Alarm Indication failure may also be declared after detecting the far-end yellow alarm. The Remote Alarm Indication failure is cleared as soon as the presence of the any of the above alarms are removed. Also, the incoming failure state is declared when a defect persists for at least 2-10 seconds. The defects are the following: Loss of Signal (LOS), an Out of Frame (OOF) or an incoming Alarm Indication Signal (AIS). The Failure State is cleared when the defect is absent for at least 20 seconds.

Test Setup: Set up a four-router network as shown in figure C-11-1**.** Clear any failures that may be present from the previous test.

Procedures: Break link B-D

- Determine if RAI is declared at Routers B and D.
- Determine if an appropriate Simple Network Management Protocol (SNMP) trap is transmitted by Routers B and D.
- Determine if Router B correctly re-routes traffic to Router D via Links B-C, C-D or Links A-B, A-D.
- Restore Link C-D.
- Determine if the DS-3 RAI is removed within 20 seconds.
- Determine if an appropriate Simple Network Management Protocol (SNMP) trap is transmitted by Routers B and D.
- Determine if traffic destined for Router D is restored to Link B-D

Test 11.3. Ethernet Failure Testing

Purpose: To determine if the devices under test will properly process and respond to Gigabit Ethernet and 100 Mbps Ethernet failures.

References: IEEE 802.3.

Resource Requirements: Packet capture tools.

Background:

Test Setup: Set up a four-router network as shown in figure C-11-1**.** Clear any failures that may be present from the previous test.

Procedures: Break link B-C.

- Determine if Routers B and C correctly respond to Gigabit Ethernet link outage by rerouting traffic via each routers least-cost path.
- Restore ling B-C.
- Break link A-B.
- Determine if Routers A and B correctly respond to the 100 Mbps link outage by rerouting traffic via each routers least-cost path.

APPENDIX C ANNEX 12

DOMAIN NAME SYSTEM PRIMARY SERVER FAILURE

Test 12.1. DNS Client Redirect

Purpose: To verify that a client can follow a DNS redirect to a delegated zone server over IPv6.

Resource requirements: Monitor to capture packets.

Background: This test verifies that a DNS root server will send a redirect to a client initiating a redirect request from a delegated zone. The redirect should contain both A and AAAA records for the delegated zone server (assuming a dual stack server). The client will then attempt to contact the delegated zone server over IPv6.

Test setup: Configure a DNS root server on a test server, server under test 1, managing a local zone (e.g. Disa.mil). Delegate a zone to a second test server, server under test 2 (e.g. DNS test.disa.mil). Configure resource records in both zones. Configure a DNS client test machine (TN1). This will require a caching DNS server, which can be run on the client.

Procedures: Test network 1 makes a request for a redirect request (RR) in the delegated zone. This request will go to server under test 1. Server under test 1 will then redirect test network 1 to the delegated zone server, server under test 2.

Observable results: Test network 1 must be able to obtain the redirect request from the delegated zone. The request to server under test 1 and subsequent redirect can be monitored. The redirect will include an IPv6 address for server under test 2. The request over IPv6 to server under test 2 from test network 1 should be monitored and packet captures taken.

Test 12.2. DNS Client Redirect Failover to IPv4

Purpose: To determine if client can fail over to IPv4, when following a DNS redirect to a dual-stack delegated zone server.

Resource requirements: Packet capture tools.

Background: this test verifies that a DNS client will fail over to IPv4, when redirected to a dual-stack delegated zone server. The client will first attempt to connect to the delegated zone server over IPv6, and then fail over to using IPv4.

Test setup: Configure a DNS root server on a test server, server under test 1, managing a local zone (e.g. Disa.mil). Delegate a zone to a second test server, server under test 2 (e.g. Dnstest.disa.mil). Configure resource records in both zones. Configure a DNS client test machine (TN1). This will require a caching DNS server, which can be run on the client. Shut down the IPv6 interface on server under test 2.

Procedures: TN1 makes a request for a redirect request in the delegated zone. This request will go to server under test 1. The server under test 1 will then redirect TN1 to the delegated zone server, server under test 2.

Observable results: TN1 must be able to connect to server under test 2 using IPv4, after failing to connect using IPv6. The request to server under test 1 and subsequent redirect can be monitored. The request over IPv6 to server under test 2 from TN1 and the fail over to IPv4 can be monitored.

APPENDIX D

REFERENCES

[IPv6-SPEC] Hinden, R., S. Deering, IPv6 Specification, RFC 2460, December 1998.

[HTTP-SPEC] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee. Hypertext Transfer Protocol -- HTTP/1.1. RFC 2616, June 1999.

[FTP-SPEC] J. Postel, J.K. Reynolds. File Transfer Protocol, RFC 959, October 1985.

[SMTP-SPEC] J. Klensin. Simple Mail Transfer Protocol, RFC 2821, April 2001.
[DNS-SPEC] M. Crawford, C.Huitema. DNS Extensions to support IPv6 Address Aggregation and Renumbering. RFC 2874, July 2000.

[NFS-SPEC] S. Shepler, B. Callaghan, D. Robinson, R. Thurlow, C. Beame, M. Eisler, D. Noveck. Network File System version 4 Protocol. RFC 3530, April 2003.

[SNTP-SPEC] D. Mills. Simple Network Time Protocol Version 4 for IPv4, IPv6 and OSI. RFC 2030, October 1996.

[RFC 2893] R. Gilligan, E. Nordmark, Transition Mechanisms for IPv6 Hosts and Routers, RFC 2893, August 2000.

[IPv6-SPEC] Hinden, R., S. Deering, Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, December 1998.

[RFC 2461] Narten, T., Nordmark, E., and W. Simpson, Neighbor Discovery for IP Version 6 (IPv6), RFC 2461, December 1998.

[RFC 2462] Thomson, S., T. Narten, IPv6 Stateless Address Autoconfiguration, RFC 2462, December 1998.

[RFC 2463] Conta, A., S. Deering, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, RFC 2463, December 1998.

[path MTU] McCann, J., S. Deering, and J. Mogul, Path MTU Discovery for IPv6, RFC 1981, August 1996.

[MLD] Deering, S., Fenner, W., Haberman, B., Multicast Listener Discovery (MLD) for IPv6, RFC 2710, October 1999.

[T/TCP] R. Braden, TCP Extensions for Transactions Functional Specification, RFC 1644, July 1994.

[FTP] J. Postel, J. Reynolds, File Transfer Protocol (FTP), RFC 959, October 1985.

[RFC 854] J. Postel, J. Reynolds, TELNET Protocol Specification, RFC 854, May 1983.

[RFC 1350] K. Sollins, The TFTP Protocol (Revision 2), RFC 1350, July 1992.

[HTTP] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee, Hypertext Transfer Protocol – HTTP/1.1, June 1999.

[draft-ietf-idr-bgp4-20] "A Border Gateway Protocol 4 (BGP-4)", INTERNET DRAFT.

[RFC 2858] "Multiprotocol Extensions for BGP-4." Request for Comments 2858.

[Mobility Support in IPv6 (draft 24)] Johnson, D., Perkins C., Mobility Support in IPv6 (draft 24), Internet-Draft, June 2003.

[ADDRCONF] Thomson, S., T. Narten, IPv6 Stateless Address Autoconfiguration, RFC 2462, December 1998.

[IPSecArch] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, November 1998.

[AH] S. Kent, R. Atkinson, IP Authentication Header, RFC 2402, November 1998.

[ESP] S. Kent, R. Atkinson, IP Encapsulating Security Payload, RFC 2406, November 1998.

[HMAC-SHA] C. Madson, R. Glenn, The Use of HMAC-SHA-1-96 within ESP and AH, November 1998.

[RFC 2328 – OSPF, Version 2.] Moy, J., Ascend Communications Inc., April 1998.

[RFC 2740 – OSPF for IPv6.] Coltun, R., Siara Systems; Ferguson, D., Juniper Networks; Moy, J., Sycamore Networks. December, 1999.

Joint Technical Architecture (JTA) List of Mandated and Emerging Standards (LMES) Version 5.1 (Draft) dated 21 July 2003.

APPENDIX E

POINTS OF CONTACT

NAME	ADDRESS	PHONE	EMAIL
Major Roswell Dixon (Test Director)			
	ATTN: JTED (Maj. R. Dixon) Building #57305 Joint Interoperability Test Command 2001 Brainard Road Fort Huachuca, AZ 85613-7051	Voice DSN 879-5269 (520) 538-5269 FAX DSN 879-4347 (520) 538-4347	dixonr@fhu.disa.mil
Wallace Ricks (Project Manager)			
	ATTN: INTEROP (Mr. Wallace Ricks) Building #57428 Joint Interoperability Test Command 2001 Brainard Road Fort Huachuca, AZ 85613-7051	Voice DSN 879-5220 (520) 538-5220 FAX DSN 821-9258 (520) 533-9258	ricksw@fhu.disa.mil
Larry Stewart (NIT Lab Manager)			
	ATTN: INTEROP (Mr. Larry Stewart) Building #57435 Joint Interoperability Test Command 2001 Brainard Road Fort Huachuca, AZ 85613-7051	Voice DSN 879-4227 (520) 538-4227 FAX DSN 879-4299 (520) 538-4299	stewartl@fhu.disa.mil
Shawn Smith (IP Task Leader)			
	ATTN: INTEROP (Mr. Shawn Smith) Building #57428B Joint Interoperability Test Command 2001 Brainard Road Fort Huachuca, AZ 85613-7051	Voice DSN 879-0012 (520) 538-0012 FAX DSN 879-1765 (520) 538-1765	shawn.smith@mantech.com

(This page intentionally left blank.)

APPENDIX F

TEST PLAN ANNEX AUTHORS/EDITORS

Table F-1. Test Plan Annex Authors/Editors

TEST PLAN ANNEX	AUTHOR(S)	EDITOR
Appendix C Annex 1: E-Mail	JITC Ft. Huachuca	JITC
Appendix C Annex 2: HTTP	JITC Ft. Huachuca	
Appendix C Annex 3: PKI	JITC Ft. Huachuca	
Appendix C Annex 4: JLWI	Anteon Corporation/JITC Indian Head	
Appendix C Annex 5: VTC	JITC Ft. Huachuca	
Appendix C Annex 6: DCTS	JITC Ft. Huachuca	
Appendix C Annex 7: Mobility	JITC Ft. Huachuca/UNH	
Appendix C Annex 8: Security	JITC Ft. Huachuca /UNH	
Appendix C Annex 9: Router Conformance	Spirent Corporation/Ixia Corporation/Agilent Corporation/JITC Ft. Huachuca	
Appendix C Annex 10: Network Performance and Loading	U.S. Army TIC/JITC Ft. Huachuca	
Appendix C Annex 11: Network Fault Testing	JITC Ft. Huachuca	
Appendix C Annex 12: DNS Primary Server Failure	JITC Ft. Huachuca/Sun Microsystems	

Legend:

DCTS	Defense Collaboration Tool Suite	JITC	Joint Interoperability Test Command
DNS	Domain Name System	JLWI	Joint Logistics Warfighter Initiative
E-mail	Electronic Mail	PKI	Public Key Infrastructure
Ft.	Fort	TIC	Technology Integration Center
HTTP	Hypertext Transfer Protocol	UNH	University of New Hampshire
		VTC	VideoTeleconference

(This page intentionally left blank.)