The Fiscal Year 2009 Department of Defense

Internet Protocol Version 6

Test and Evaluation Report

September 2009

Assistant Secretary of Defense for Networks and Information Integration/
Department of Defense Chief Information Officer

THIS PAGE INTENTIONALLY LEFT BLANK.

The Fiscal Year 2009 Department of Defense Internet Protocol Version 6 Test and Evaluation Report

September 2009

Submitted by: RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

Approved by: RONALD C. STEPHENS
Colonel, USA
Commander

THIS PAGE INTENTIONALLY LEFT BLANK.

Table of Contents

Executive Summary **1**

1 Introduction **3**
1.1 Purpose 3
1.2 Test and Evaluation Objectives 3
1.3 Scope 3
1.4 FY 2005 - FY 2008 Cumulative Results and Recommendations 4

2 FY 2009 IPv6 Test and Evaluation Results **5**
2.1 Overview 5
2.2 Cumulative Analysis Methodology 5
2.3 Impact of FY 2009 Test and Evaluation Reports on Demonstration of Joint Staff IPv6 Operational Criteria 8
2.3.1 Criterion 1: Demonstrate security of unclassified network operations, classified network operations, black backbone operations, integration of HAIPE, integration of IPsec, and integration with firewalls and intrusion detection systems 9
2.3.2 Criterion 2: Demonstrate end-to-end interoperability in a mixed IPv4 and IPv6 environment 12
2.3.3 Criterion 3: Demonstrate equivalent to, or better performance than, IPv4 based networks 13
2.3.4 Criterion 4: Demonstrate voice, data, and video integration 13
2.3.5 Criterion 5: Demonstrate effective operation in low-bandwidth environment 14
2.3.6 Criterion 6: Demonstrate scalability of IPv6 networks 15
2.3.7 Criterion 7: Demonstrate support for mobile terminals (voice, data, and video) 16
2.3.8 Criterion 8: Demonstrate transition techniques 17
2.3.9 Criterion 9: Demonstrate ability to provide network management of networks 18
2.3.10 Criterion 10: Demonstrate tactical deployability and ad hoc networking 19

3 FY 2009 Conclusions **20**

4 Recommendations **22**

5 Summary **24**

Appendix A - References **25**

Appendix B - Terms and Definitions **26**

Appendix C - Acronym List **29**

List of Tables

Table 2-1 Cumulative Test and Evaluation Matrix 7
Table 2-2 Joint Staff IPv6 Operational Criterion 1 Status 9
Table 2-3 Joint Staff IPv6 Operational Criterion 2 Status 12
Table 2-4 Joint Staff IPv6 Operational Criterion 3 Status 13
Table 2-5 Joint Staff IPv6 Operational Criterion 4 Status 13
Table 2-6 Joint Staff IPv6 Operational Criterion 5 Status 14
Table 2-7 Joint Staff IPv6 Operational Criterion 6 Status 15
Table 2-8 Joint Staff IPv6 Operational Criterion 7 Status 16
Table 2-9 Joint Staff IPv6 Operational Criterion 8 Status 17
Table 2-10 Joint Staff IPv6 Operational Criterion 9 Status 18
Table 2-11 Joint Staff IPv6 Operational Criterion 10 Status 19
Table D-1. 2009 T&E Reports and Related Operational Criteria 38
Table D-2. 2009 T&E JITC IPv6 Special Certifications 39
Table D-3. IPv6 Capable Device Requirements for Testing 43
Table D-4. Test Configuration Hardware and Software 51
Table D-5. MO3 Targeted Set of Applications 68
Table D-6. IPv6 Compatibility of Various FTP Applications 70
Table D-7. IPv6 Compatibility of Various HTTP Applications 71
Table D-8. DNS Transaction Times for Host Resolution 73
Table D-9. Address Selection for Windows Applications 74
Table D-10. Address Selection for Linux Applications 74
Table D-11. DSCP Assignment Scheme 77
Table D-12. Tested System Configuration 90
Table D-13. VTC Objectives 95
Table D-14. Summary of Joint Staff Operational Criteria Results 96
Table D-15. IPv6 IA Requirements Summary Without RAE and With RAE Findings 105
Table D-16. Tested System Configuration 106
Table D-17. IPv6 IA Requirements Summary Without RAE and With RAE Findings 113
Table D-18. Tested System Configuration 113
Table D-19. Tested System Configuration 121
Table D-20. Tested System Configuration 126

Table D-21. Tested System Configurations 131
Table D-22. Test Objective Scores 137
Table D-23. MO3 Interoperability Results 152
Table D-24. MO3 Test Result Failures 153

List of Figures

Figure D-D-1. JITC Simulated DISN IP Core Network 42
Figure D-D-2. NIPRNet IPv6 Core Network Connectivity 53
Figure D-D-3. NIPRNet IPv6 External Network Connectivity 54
Figure D-D-4. DNS Test Bed Topology Diagram 59
Figure D-D-5. DNS Test Bed Logical Diagram 60
Figure D-D-6. IPv6 Single Domain Multicast 64
Figure D-D-7. IPv6 Inter-Domain Multicast 65
Figure D-D-8. Lab Test Environment 69
Figure D-D-9. IPv6 Test Configuration 81
Figure D-D-10. IPv6 Test Configuration 85
Figure D-D-11. Test Configuration 89
Figure D-D-12. JUICE 09 IPv6 Network 94
Figure D-D-13. RANGE Hybrid Airborne Scenario 101
Figure D-D-14. Test Configuration 105
Figure D-D-15. Test Configuration 112
Figure D-D-16. SUT Test Configuration 120
Figure D-D-17. SUT Test Network 130
Figure D-D-18. IPv6 Test Configuration 135
Figure D-D-19. Joint Staff Operational Criteria 5 Configuration for EPLRS 140
Figure D-D-20. JITC MO3 Dual-Stack Test Network 151

THIS PAGE INTENTIONALLY LEFT BLANK.

Executive Summary

This report is compiled from field tests, exercises, demonstrations, experiments, simulations, and analyses conducted by Department of Defense (DoD) Components over the last five years, with emphasis on the most recent year test results (June 2008 through September 2009). This report is an update to the report submitted to Congress in October 2008.

The DoD Internet Protocol (IP) Version 6 (IPv6) Transition Office (DITO) established a repository of IPv6 Test and Evaluation (T&E) reports provided by DoD Components in response to requests from the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD (NII)/DoD CIO). The Joint Interoperability Test Command (JITC) evaluated the data contained in these reports with respect to the principal T&E objectives of the DoD IPv6 Master Test Plan Version 2.0 (MTPv2.0). Following guidance set forth in the DoD IPv6 MTPv2.0, the DoD Components have developed, conducted, and reported on T&E for their specific Joint Staff IPv6 Operational Criteria. The Army, Navy, Air Force, National Security Agency (NSA), and Defense Information Systems Agency (DISA), henceforth referred to as DoD Components, provided 223 reports. For Fiscal Year (FY) 2009, DITO received 82 reports from the DoD Components, and 60 of these are IPv6 Special Interoperability Certifications.

The DITO facilitates the sharing of IPv6 T&E results among DoD Components and other federal IPv6 working groups through a Defense Knowledge Online (DKO) web portal available at https://www.us.army.mil/suite/folder/11858739. Based on a cumulative analysis of all reports submitted in prior years, 4 of the 10 Joint Staff IPv6 Operational Criteria demonstrated successfully. These are Interoperability (Criterion 2), Performance (Criterion 3), Scalability (Criterion 6), and Transition Techniques (Criterion 8). This year, testing showed progress on Security (Criterion 1); however, its overall status is unchanged. Low-Bandwidth (Criterion 5) testing supported changing its overall status from red to yellow.

The availability of IPv6 commercial and open-standard products and services has increased markedly during the past several years. It appears all features, functions, and services available using IPv4, currently are, or will soon be available with IPv6. IPv6 features that will provide capabilities beyond what IPv4 can provide are under development.

The NSA-certified commercial products for encryptors, firewalls, Intrusion Protection Systems and Intrusion Detection Systems became available during this reporting period. The availability of these devices should facilitate the demonstration of the un-demonstrated IPv6 security features. Full demonstration of Security (Criterion 1) is necessary to allow DoD wide deployment of IPv6.

Congress directed the Chairman of the Joint Chiefs of Staff to provide certification that conversion of DoD networks to IPv6 would "provide equivalent or better performance and capabilities than that which would be provided by any other combination of available technologies and protocols." The successful demonstration of the remaining Joint Staff IPv6 Operational Criteria will support the full deployment of IPv6 on DoD networks.

THIS PAGE INTENTIONALLY LEFT BLANK.

Introduction

1.1 Purpose

The publication of the 2009 Department of Defense (DoD) Internet Protocol (IP) Version 6 (IPv6) Test and Evaluation (T&E) Report provides an assessment of IPv6 T&E activities carried out by the DoD Components with respect to the T&E objectives of the DoD IPv6 Master Test Plan Version 2.0 (MTPv2.0). This report is also provides input to the congressionally directed IPv6 certification by the Chairman of the Joint Chiefs of Staff.

1.2 Test and Evaluation Objectives

The DoD IPv6 T&E Report provides consolidated test results and assessments in support of the DoD transition to IPv6. It identifies what is complete and what T&E is still required to demonstrate the remaining criteria. Assessment of the individual IPv6 T&E reports furnished by the DoD Components address the progress in meeting the objective of demonstrating the functionality of IPv6 as delineated in the Joint Staff IPv6 Operational Criteria.

The Joint Staff enumerated 10 operational criteria to demonstrate support of the DoD's transition of networks to IPv6. These criteria provide top-level operational and technical capabilities necessary to verify IPv6 fulfills the needs of the DoD. Each criterion was decomposed to provide two subordinate levels of measurable and verifiable functional elements.

- Level 1 decomposition identifies capabilities required for each criterion.
- Level 2 decomposition identifies the specific technology, infrastructure, and/or functionality to demonstrate Level 1 decomposition.

Responsibility for Level 1 and Level 2 decomposition elements, as well as further decomposition levels associated with each Joint Staff IPv6 Operational Criteria, has been distributed among the DoD Components, as outlined in the DoD IPv6 MTP v2.0.

Congress also directed the Chairman of the Joint Chiefs of Staff to provide certification that conversion of the DoD networks to IPv6 would "provide equivalent or better performance and capabilities than that which would be provided by any other combination of available technologies and protocols." The successful demonstration or approved disposition of the Joint Staff IPv6 Operational Criteria will support this certification.

1.3 Scope

The scope of analysis in this report is limited to T&E reports submitted during the reporting period of June 2008 through September 2009. The DoD Components submitted these reports in response to requests from the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD (NII)/DoD CIO) in a memo dated

June 12, 2009. The DoD IPv6 Transition Office (DITO) received 82 reports from DoD Components in response to the memo. The evaluation team for this report consisted of the Defense Information Systems Agency (DISA) Joint Interoperability Test Command (JITC) and Director Operational Test and Evaluation (DOT&E) representatives. This report provides the results of analyses for the FY09 reports and integrates the analyses of previously submitted reports to provide a cumulative status for IPv6 T&E.

1.4 FY 2005 - FY 2008 Cumulative Results and Recommendations

The FY 2008 report provided cumulative results from the previous reports. Based on T&E results over the last four years, Interoperability (Criterion 2), Performance (Criterion 3) Scalability (Criterion 6), and Transition Techniques (Criterion 8) fully demonstrated capability for transition to IPv6. The 2008 T&E report recommended further research, development, and testing necessary to ensure the DoD's networks can transition without affecting mission critical operations. The lack of IPv6 Capable Information Assurance (IA) products (Criterion 1) and High Assurance IP Encryptor (HAIPE) devices delayed enterprise-wide implementation of IPv6. Voice, Data, and Video Integration (Criterion 4) and Operation in Low-Bandwidth Environment (Criterion 5) need technical guidelines, defined standards, and would benefit from testing over satellite links. Lastly, the 2008 T&E Report stated Mobility (Criterion 7) and Tactical Deployability and Ad Hoc Networking (Criterion 10) lacked vendor development and implementation, resulting in limited T&E, as well as suggesting that Network Management (Criterion 9) should be a key objective of any major exercise utilizing IPv6.

2 FY 2009 IPv6 Test and Evaluation Results

2.1 Overview

This section provides overall status of DoD IPv6 T&E in 2009 in support of DoD's transition to IPv6, and summarizes IPv6 T&E results reported by DoD Components for the period June 2008 through September 2009. There were 82 T&E reports, of which 60 were Special Interoperability Test Certifications, analyzed for the current reporting period. Appendix D contains a summary for each report and certification.

Results indicate IPv6 Capable HAIPE devices are available and ready for use in DoD networks. Testing in low-bandwidth environments showed IPv6 is functionally equivalent to IP Version 4 (IPv4) in similar bandwidth ranges. Finally, testing of network management tools reveals no additional progress in the demonstration of Network Management (Criterion 9).

In prior years, T&E successfully demonstrated Interoperability (Criterion 2), Performance (Criterion 3), Scalability (Criterion 6), and Transition Techniques (Criterion 8). All reports used for this analysis are on the DoD IPv6 (Unrestricted) Knowledge Center on the Defense Knowledge Online (DKO): https://www.us.army.mil/suite/folder/11731042[1]. This year, testing showed progress on Security (Criterion 1); however, its overall status is unchanged. The Special IPv6 Interoperability Test Certifications (primarily Criterion 2) provided an indication of increased commercial availability of IPv6 products. Low-Bandwidth (Criterion 5) testing supported changing its overall status from red to yellow.

2.2 Cumulative Analysis Methodology

Table 2-1 provides the cumulative status of each Joint Staff IPv6 Operational Criterion in pie charts with slices colored red, yellow, or green to represent the progress to date. Each slice of a criterion's pie represents one Level 2 decomposition element for that criterion. The basis for the status color of each Level 2 element is an analysis and evaluation of the test results for underlying decomposition elements.

The color-coded rating scale for the Level 2 decomposition elements is:

- Red - Limited progress made. A red slice indicates a Level 2 decomposition element had little or no T&E, or existing T&E results are inconclusive or unsatisfactory. Significant T&E needs to be conducted.

- Yellow - Significant progress made. A yellow slice indicates a Level 2 decomposition element had considerable T&E and multiple, independent tests provided substantially similar, positive results. A yellow slice shows that some additional analysis and testing is required

[1] Access to the DKO requires a DoD Common Access Card (CAC) and registration with the DoD IPv6 (Unrestricted) Knowledge Center.

- Green - Successfully demonstrated. A green slice indicates a Level 2 decomposition element successfully demonstrated, or the decomposition has an approved disposition. The evaluation type, relevance, and scope (considered with the number of tests) provide enough data to yield a high confidence factor.

Table 2-1 presents the total number of T&E reports applicable to each criterion for the entire transition effort, categorized by the evaluation method (counts for this reporting period are in parentheses). A comparison of cumulative pie chart for 2008 to cumulative pie chart for 2009 provides an indication of progress made in FY 2009 for each criterion. A cumulative pie chart that includes red slices indicates the demonstration of the underlying functional or technical elements is incomplete. A cumulative pie chart that includes yellow with no red slices indicates the underlying elements had considerable progress. A cumulative pie chart that is all green indicates all underlying elements for that criterion fully tested and the criterion demonstrated. The expected completion date to fully demonstrate each criterion is also in Table 2-1.

Table 2-1 Cumulative Test and Evaluation Matrix

	Joint Staff IPv6 Operational Criteria	Test Methods							Cumulative Status Thru		Expected Completion Date
		Engineering Analyses	Modeling & Simulation	Experiments	Demonstrations	Pilots	Exercises	Field Tests	2008	2009	
1	Demonstrate security of unclassified network operations, classified network operations, black backbone operations, integration of HAIPE, integration of IP security (IPsec), and integration with firewalls and intrusion detection systems	22	1	19	14 (2)	2	17 (5)	2			4th QTR FY 2010
2	Demonstrate end-to-end interoperability in a mixed IPv4 and IPv6 environment	11	2	17	27 (14)	1	25 (6)	8			4th QTR FY 2009
3	Demonstrate equivalent to, or better performance than, IPv4 based networks	2	2	10	20 (8)		10 (2)				4th QTR FY 2009
4	Demonstrate voice, data, and video integration	6		2	6 (3)		6 (2)	1			4th QTR FY 2010
5	Demonstrate effective operation in low-bandwidth environment	2	2		6 (3)		8 (2)				4th QTR FY 2010
6	Demonstrate scalability of IPv6 networks	1		1	1	1					1st QTR FY 2009
7	Demonstrate support for mobile terminals (voice, data and video)	5	1	1	3		9 (2)	1			4th QTR FY 2010
8	Demonstrate transition techniques	16	4	23	38 (14)	2	31 (6)	7			4th QTR FY 2009
9	Demonstrate ability to provide network management of networks	3		6	6		1 (1)				4th QTR FY 2010
10	Demonstrate tactical deployability and ad hoc networking	7	1	2	3		1 (1)	1			4th QTR FY 2010

Key:
- Successfully demonstrated
- Significant progress
- Limited progress

Quarter (QTR), Fiscal Year (FY) Total Events (Current Fiscal Year Events)
IPv6 Special Certifications are not included in this years total

2.3 Impact of FY 2009 Test and Evaluation Reports on Demonstration of Joint Staff IPv6 Operational Criteria

This section provides the evaluation of each Joint Staff IPv6 operational criterion at Level 1 and Level 2 of the decomposed functional or technical elements. The DoD Components responsible for each criterion recommended status updates based on testing performed this year. The evaluation team used the recommendations and test reports to determine the decomposition status.

The color-coded rating scale used in the individual criterion's decomposition table is:

⊗ Red - Limited progress. Criteria require more T&E and/or development to certify the decomposition elements as demonstrated, or T&E to date demonstrates limited or no satisfactory results.

⊕ Yellow - Significant progress. T&E indicates limited successful demonstration of some portions of the decomposition element, or confidence in previous T&E results is low. Criteria require more T&E to certify the decomposition element as demonstrated.

⊘ Green - Indicates a successfully demonstrated element or has an approved disposition. T&E provided enough data to assure the decomposition element demonstrated with a high confidence factor.

The rating symbols in the 2008 columns are the status reported in the 2008 T&E report for Level 1 and Level 2 criterion decomposition. Rating symbols in the 2009 columns are status for each criterion. Specific T&E observations follow each table.

The estimated completion column lists the expected completion date of the Level 1 decomposition element. The responsible DoD Components provided the estimated completion dates.

2.3.1 Criterion 1: Demonstrate security of unclassified network operations, classified network operations, black backbone operations, integration of HAIPE, integration of IPsec, and integration with firewalls and intrusion detection systems

Table 2-2 Joint Staff IPv6 Operational Criterion 1 Status

Level 1 Decomposition (Capabilities to be demonstrated)	Cumulative Status Thru		Estimated Completion Date	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Cumulative Status Thru	
	2008	2009			2008	2009
1.1 Ensure that information is not disclosed to unauthorized persons, processes, or devices.	⊕	⊕	4th Quarter FY 2010	**1.1.1** Verify the implementation of IPsec with Encapsulating Security Protocol (ESP) in IPv6 hosts and routers. Verify integration with Public Key Infrastructure (PKI).	⊕	⊕
1.2 Ensure information received is the same as that which was sent (protect against unauthorized modification or destruction of information).	⊕	⊕	4th Quarter FY 2010	**1.2.1** Verify implementation of Authentication Header (AH) in IPv6 hosts and routers. Verify integration with PKI.	⊕	⊕
1.3 Ensure Authentication, Authorization, and Accounting (AAA) of persons and processes.	⊗	⊗	4th Quarter FY 2010	**1.3.1** Verify the implementation of an AAA server is able to ensure the Authentication, Authorization, and Accounting of persons, machines, and processes over an IPv6 network.	⊗	⊗
1.4 Ensure availability and mitigate denial of services (timely, reliable access to data, and information services for authorized users).	⊕	⊕	4th Quarter FY 2010	**1.4.1** Verify protection of the IPv6 stack of Hosts and Network Devices from intruders. (Note: Included in this are vulnerabilities that arise from errors in protocol specification or implementation or the associated device firmware).	⊕	⊕
				1.4.2 Demonstrate IPv6 traffic filtering capabilities of routers and firewalls according to security policies.	⊕	✓
1.5 Ensure IPv6 traffic is interoperable with firewalls and Intrusion Detection Systems (IDS).	⊕	✓	4th Quarter FY 2010	**1.5.1** Evaluate Firewalls and IDS functions that can be applied to IPv6 traffic. Evaluate Firewalls and IDS functions that can be applied to tunneled IPv6 traffic.	⊕	✓
1.6 Ensure IPv6 traffic is interoperable with HAIPE devices.	⊗	✓	4th Quarter FY 2010	**1.6.1** Evaluate HAIPE v3's ability to encrypt/decrypt IPv6 packets.	⊗	✓

2009 T&E Observations Criterion 1

- High Assurance IP Encryptor IP Security (HAIPE IS) 3.0 devices are now commercially available from multiple vendors and were successful in large-scale exercises (Joint User Interoperability Communications Exercise (JUICE) report).
  (Test Report D.1 Decompositions 1.4, 1.5, 1.6)

- HAIPE devices implementing the HAIPE IS 3.0.2 specification protected IPv6 and mixed IPv4/IPv6 networks.
  (Test Report D.1 Decompositions 1.4, 1.5, 1.6)

- Many devices fully support IPv6 IP Security (IPsec); host certification tests along with router testing identified last year showed the technology matured.
  (Test Report D.1 Decompositions 1.1.1, 2.1, 2.3, 8.1)

- Testing of Firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) showed support for IPv6 functionality.
  (Test Report D.21 Decompositions 1.4, 1.5)

- Devices configured based on the NSA MO3 IA guidance document were effective at providing IA protection during testing. Furthermore, testing showed the application of NSA MO3 IA guidance does not compromise interoperability or functionality in a mixed IPv4/IPv6 or IPv6-only network.
  (Test Report D.21 Decompositions 1.4, 1.5)

- One of the IPS devices tested was purported by the vendor to be IPv6 Capable, but none of its interfaces were configurable with IPv6 addresses. This limits its functionality.
  (Test Report D.9, D.19 Decomposition 1.4, 1.5)

- One IPv6-Capable firewall scored well in functionality but fared poorly in the areas of documentation, Role Based Access Control (RBAC), and audit/alerts capability.
  Juniper Firewall Report
  (Test Report D.1, D.8 Decompositions 1.4, 1.5)

- One of the IPS devices tested was able to provide only 10 IA functions at any given time even though it had a complete set of functions available.
  (Test Report D.19 Decomposition 1.4, 1.5)

- One of the IPS devices tested could not provide some basic functionality (such as Denial-of-Service detection and Access Control Lists) even though it provides other, more sophisticated functionality (such as Reconnaissance Detection and Quarantine capability).
  (Test Report D.19 Decomposition 1.4, 1.5)

- The Juniper Networks ISG 2000 Firewall is a very stable platform with strong internal functionality. Its strengths are Confidentiality, Integrity, and Availability. This device passed 100 percent of the IPv6 test procedures.
  (Test Report D.8, D.21 Decompositions 1.4, 1.5)

- The McAfee Intrushield 3000 functioned well as an Intrusion Prevention device passing more than 80 percent of the NSA's functional requirements.
  IPv6 Converged Services and Joint Staff Operational Criteria Demonstration
  (Test Report D.19 Decomposition 1.4, 1.5)

2.3.2 Criterion 2: Demonstrate end-to-end interoperability in a mixed IPv4 and IPv6 environment

Table 2-3 Joint Staff IPv6 Operational Criterion 2 Status

Level 1 Decomposition (Capabilities to be demonstrated)	Cumulative Status Thru		Estimated Completion Date	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Cumulative Status Thru	
	2008	2009			2008	2009
2.1 Demonstrate IPv4 application to IPv4 application over a mixed IPv4 and IPv6 network.	✓	✓	1st Quarter FY 2009	**2.1.1** Demonstrate core service interoperability: Domain Name System (DNS), directory services, File Transfer Protocol (FTP), email, web services, Network Time Protocol (NTP), and PKI.	✓	✓
				2.1.2 Demonstrate network core application interoperability: Voice over IP (VoIP) and video over IP.	✓	✓
				2.1.3 Demonstrate Commercial Off The Shelf (COTS) application interoperability (transaction, database access, and web services).	✓	✓
				2.1.4 Demonstrate Government Off The Shelf (GOTS) applications/systems interoperability.	⊕ 4	⊕ 4
2.2 Demonstrate IPv6 application to IPv4 application over a mixed IPv4 and IPv6 network.	✓	✓	1st Quarter FY 2009	**2.2.1** Demonstrate core service interoperability: DNS, Directory, FTP, email, web services, NTP, and PKI.	✓	✓
				2.2.2 Demonstrate network core application interoperability: VoIP and video over IP.	✓	✓
				2.2.3 Demonstrate COTS application interoperability (transaction, database access, and web services).	✓	✓
				2.2.4 Demonstrate GOTS application/system interoperability.	⊕ 4	⊕ 4
2.3 Demonstrate IPv6 application to IPv6 application over a mixed IPv4 and IPv6 network.	✓	✓	1st Quarter FY 2009	**2.3.1** Demonstrate core service interoperability: DNS, Directory, FTP, email, web services, NTP, and PKI.	✓	✓
				2.3.2 Demonstrate network core application interoperability: VoIP and video over IP.	✓	✓
				2.3.3 Demonstrate COTS application interoperability (transaction, database access, and web services).	✓	✓
				2.3.4 Demonstrate GOTS application/system interoperability.	⊕ 4	⊕ 4

2009 T&E Observations Criterion 2

- All planned IPv6 Interoperability T&E was complete and reported in the 2008 T&E Report.
  (General Observation)

2.3.3 Criterion 3: Demonstrate equivalent to, or better performance than, IPv4-based networks

Table 2-4 Joint Staff IPv6 Operational Criterion 3 Status

Level 1 Decomposition (Capabilities to be demonstrated)	Cumulative Status Thru		Estimated Completion Date	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Cumulative Status Thru	
	2008	2009			2008	2009
3.1 Demonstrate IPv6 throughput equivalent to or better than IPv4.	✓	✓	1st Quarter FY 2009	**3.1.1** Same as Level 1	✓	✓
3.2 Demonstrate IPv6 latency equivalent to or better than IPv4.	✓	✓	1st Quarter FY 2009	**3.2.1** Same as Level 1	✓	✓
3.3 Demonstrate IPv6 packet loss equivalent to or better than IPv4.	✓	✓	1st Quarter FY 2009	**3.3.1** Same as Level 1	✓	✓
3.4 Demonstrate IPv6 service availability equivalent to or better than IPv4.	✓	✓	1st Quarter FY 2009	**3.4.1** Same as Level 1	✓	✓

2009 T&E Observations Criterion 3

- All planned IPv6 Performance T&E was complete and reported in the 2008 T&E Report. (General Observation)

2.3.4 Criterion 4: Demonstrate voice, data, and video integration

Table 2-5 Joint Staff IPv6 Operational Criterion 4 Status

Level 1 Decomposition (Capabilities to be demonstrated)	Cumulative Status Thru		Estimated Completion Date	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Cumulative Status Thru	
	2008	2009			2008	2009
4.1 Demonstrate simultaneous voice, data, and video (or any combination thereof) over shared IPv6 networks.	⊕	⊕	4th Quarter FY 2010	**4.1.1** Demonstrate Quality of Service (QoS) capabilities of IPv6 networks using Differentiated Services (DiffServ) and Resource Reservation Protocol (RSVP).	⊕	⊕
				4.1.2 Demonstrate transport control capabilities of IPv6 networks using Real Time Control Protocol (RTCP).	⊕	⊕
				4.1.3 Demonstrate session signaling capabilities of IPv6 networks using the Session Initiation Protocol (SIP).	⊕	⊕

2009 T&E Observations Criterion 4

- Results showed significant bandwidth savings with multicast, compared to unicast; the savings was proportional to the number of receivers.
  (Test Report D.4 Decompositions 4.1)

- Recently released Video Teleconferencing (VTC) products have IPv4/IPv6 dual-stack capabilities and can integrate IPv4 and IPv6 VTC sessions.
  (Test Report D.7 Decompositions 4.1)

- Cisco Voice over Internet Protocol (VoIP) phones established IPv6 calls, IPv4/IPv6 calls, and IPv6 three-way calls.
  (Test Report D.7 Decompositions 4.1)

- A single chat server was able to provide chat services for both IPv4 and IPv6 clients using open source and tactically fielded chat applications.
  (Test Report D.7 Decompositions 4.1)

2.3.5 Criterion 5: Demonstrate effective operation in low-bandwidth environment

Table 2-6 Joint Staff IPv6 Operational Criterion 5 Status

Level 1 Decomposition (Capabilities to be demonstrated)	Cumulative Status Thru		Estimated Completion Date	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Cumulative Status Thru	
	2008	2009			2008	2009
5.1 Demonstrate ability to establish and maintain applications in low-bandwidth IPv6 environments.	⊗	⊕	4th Quarter FY 2010	**5.1.1** Demonstrate ability to establish and maintain applications (voice, data, and video) in low-bandwidth IPv6 environments.	⊗	⊕
				5.1.2 Demonstrate ability to maintain network operations (i.e., Network Management, DNS, Dynamic DNS, and Security) in low-bandwidth IPv6 environments.	⊗	⊕

2009 T&E Observations Criterion 5

- Results showed significant bandwidth savings with multicast, compared to unicast, the saving was proportional to the number of receivers.
  (Test Report D.4 Decompositions 5.1.1)

- Multicast is a technique to optimize overall bandwidth requirements and mitigate bandwidth limitations.
  (Test Report D.4 Decompositions 5.1.1)

- Testing shows IPv6 reacts to “low-bandwidth” environments the same as IPv4.
  (Test Report D.4 Decompositions 5.1.1)

- Data analysis indicates that IPv6 performs as well as IPv4 in low and moderate conditions of bandwidth loading. However, when capacity reaches the 80 percent range, the additional overhead associated with IPv6 begins to become a factor.
  (Test Report D.11 Decompositions 5.1.1)

- For connection-oriented data transfers such as File Transfer Protocol, IPv6 performance (effective data rate, transfer time, and error rate) in all bandwidth ranges tested, 64 to 1024 kilobits per second (kbps), was within 10 percent of IPv4 performance.
  (Test Report D.20 Decompositions 5.1.1)

- At a bandwidth of 512 kbps or greater, average bit rate and packet loss of streaming video over IPv6 was equivalent to IPv4.
  (Test Report D.20 Decompositions 5.1.1)

- Testing of a Low-Bandwidth network using a topology containing six DNS domains was successful.
  (Test Report D.20 Decompositions 5.1.1)

2.3.6 Criterion 6: Demonstrate scalability of IPv6 networks

Table 2-7 Joint Staff IPv6 Operational Criterion 6 Status

Level 1 Decomposition (Capabilities to be demonstrated)	Cumulative Status Thru		Estimated Completion Date	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Cumulative Status Thru	
	2008	2009			2008	2009
6.1 Demonstrate ability to add more network resources, services, and users without negatively impacting existing users.	✓	✓	1st Quarter FY 2009	**6.1.1** Demonstrate the ability to build IPv6 networks comparable in size to existing IPv4 networks, with equal or better performance.	✓	✓
				6.1.2 Demonstrate the ability to populate IPv6 subnets with network elements of comparable numbers to existing IPv4 subnets, with equal or better performance.	✓	✓
				6.1.3 Demonstrate the ability to create IPv6 multicast sessions whose sizes are comparable to existing IPv4 multicast sessions, with equal or better performance.	✓	✓
				6.1.4 Demonstrate the ability to create IPv6 core services (DNS, Directory, FTP, email, Web, NTP, and PKI) where the number of users is comparable to existing IPv4 core services, with equal or better performance.	✓	✓

2009 T&E Observations Criterion 6

- All planned IPv6 Scalability T&E was complete and reported in the 2007 T&E Report.
  (General Observation)

2.3.7 Criterion 7: Demonstrate support for mobile terminals (voice, data, and video)

Table 2-8 Joint Staff IPv6 Operational Criterion 7 Status

Level 1 Decomposition (Capabilities to be demonstrated)	Cumulative Status Thru		Estimated Completion Date	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Cumulative Status Thru	
	2008	2009			2008	2009
7.1 Demonstrate ability to establish and maintain IPv6 applications (voice, data, and video) on the move.	⊗	⊗	4th Quarter FY 2010	**7.1.1** Demonstrate ability to initiate and maintain voice, data, or video applications using mobile terminals.	⊗	⊗
				7.1.2 Demonstrate ability to maintain network operations of mobile terminals (i.e., Network Management, DNS, Dynamic DNS, and Security).	⊗	⊗
				7.1.3 Demonstrate the ability to maintain connectivity of Mobile Nodes (MN) while On-The-Move (OTM) and network management of MN while OTM.	⊗	⊗

2009 T&E Observations Criterion 7

- Testing showed the Proxy-Mobile IPv6 (MIPv6) module produced IPv6 performance that was slightly better than IPv4 using the MIPv4 protocol.
  (Test Report D11. Decompositions 7.1)

- Little operationally realistic testing has been attempted in tactical environments.
  (General Observation)

2.3.8 Criterion 8: Demonstrate transition techniques

Table 2-9 Joint Staff IPv6 Operational Criterion 8 Status

Level 1 Decomposition (Capabilities to be demonstrated)	Cumulative Status Thru		Estimated Completion Date	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Cumulative Status Thru	
	2008	2009			2008	2009
8.1 Demonstrate DoD recommended network transition techniques.	✓	✓	4th Quarter FY 2010	**8.1.1** Demonstrate the interoperability of IPv4 and IPv6 network transition techniques: • Dual stack everywhere in an autonomous system • Configured tunnels • Tunnel Broker	✓	✓
				8.1.2 Demonstrate the performance of IPv4 and IPv6 network transition techniques: • Dual stack everywhere in an autonomous system • Configured tunnels • Tunnel Broker	✓	✓
				8.1.3 Demonstrate the security of IPv4 and IPv6 network transition techniques: • Dual stack everywhere in an autonomous system • Configured tunnels • Tunnel Broker	**N/A**[2]	**N/A**[2]

2009 T&E Observations Criterion 8

- All planned IPv6 Transition Techniques T&E was complete and reported in the 2008 T&E Report.
  (General Observation)

[2] Responsibility for Decomposition 8.1.3 is being transferred to the NSA.

2.3.9 Criterion 9: Demonstrate ability to provide network management of networks

Table 2-10 Joint Staff IPv6 Operational Criterion 9 Status

Level 1 Decomposition (Capabilities to be demonstrated)	Cumulative Status Thru		Estimated Completion Date	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Cumulative Status Thru	
	2008	2009			2008	2009
9.1 Demonstrate ability to monitor, configure, and account for IPv6 network resources.	⊗	⊕	4th Quarter FY 2010	**9.1.1** Demonstrate that IPv6 devices can be monitored by Network Management Systems (NMS) commonly used by the DoD.	✓	✓
				9.1.2 Demonstrate that NMS commonly used by the DoD can conFigure D-IPv6 devices.	✓	✓
				9.1.3 Demonstrate that IPv6 devices can be accounted for by NMS commonly used by the DoD.	⊕	⊕

2009 T&E Observations Criterion 9

- Network management tools tested provided discovery and monitoring for IPv6 devices, but were unable to provision and conFigure D-those devices using IPv6 transport. (Test Report D.22. Decompositions 9.1, 9.2, 9.3)

- No single network management tool is capable of performing all required network management functions on an IPv6-only network. (Test Report D.11. Decompositions 9.1)

- While IPv6 services and applications on dual-stack nodes are manageable with current tools using IPv4 transport, this requires more network bandwidth. (Test Report D.22. Decompositions 9.1, 9.2, 9.3)

- During large-scale exercise testing, one tool provided discovery and monitoring functionality of IPv6-only nodes using IPv6 transport. (Test Report D.22. Decompositions 9.1, 9.2, 9.3)

- Some HAIPE devices employed during large-scale exercise testing could not be managed using IPv6 tools over IPv6 transport. **(**Test Report D11. Decompositions 9.1)

2.3.10 Criterion 10: Demonstrate tactical deployability and ad hoc networking

Table 2-11 Joint Staff IPv6 Operational Criterion 10 Status

Level 1 Decomposition (Capabilities to be demonstrated)	Cumulative Status Thru		Estimated Completion Date	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Cumulative Status Thru	
	2008	2009			2008	2009
10.1 Demonstrate ability to move IPv6 networks as a whole, without reconfiguration.	⊗	⊗	4th Quarter FY 2010	**10.1.1** Demonstrate the ability to move networks to other locations while maintaining connectivity via the original IPv6 addresses, using Network Mobility (NEMO).	⊗	⊗
10.2 Demonstrate ability to support IPv6 networking without fixed router infrastructure.	⊗	⊗	4th Quarter FY 2010	**10.2.1** Demonstrate ability of IPv6 hosts to forward packets from peers, while on the move, using Mobile Ad hoc Networks (MANET) routing protocols.	⊗	⊗

2009 T&E Observations Criterion 10

- No reports were submitted for Criterion 10 testing.
  (General Observation; Decomposition 10.2)

3 FY 2009 Conclusions

The following conclusions resulted from the review and analysis of the reports received for FY 2009. The DoD made significant progress in successfully demonstrating Joint Staff IPv6 Operational Criteria during this reporting period. Low-Bandwidth (Criterion 5) is sufficiently mature and will support the Department's implementation of IPv6 and the Chairman of the Joint Chiefs Of Staff certification of equivalent performance and capability compared to other protocols. The few certified IPv6-Capable IA devices advanced the status of Criterion 1, but not enough to fully demonstrate the criterion.

Specific conclusions for individual criterion are:

Criterion 1: Demonstrate security of unclassified network operations, classified network operations, black backbone operations, integration of HAIPE, integration of IPsec, and integration with firewalls and intrusion detection systems.

- Lack of HAIPE devices is no longer the major obstacle for demonstration of this criterion.
- Authentication, Authorization, and Accounting (AAA) is now the primary shortfall to demonstration of this criterion.
- Although some progress occurred on Firewalls, IDS, and IPS the limited number of vendors offering these products and immaturity of these systems is still a significant obstacle to the demonstration of this criterion.
- IPsec needs development, although many devices now support IPv6 IPsec.
- The NSA IA MO3 guidance requirements do not compromise interoperability or functionality in a mixed IPv4/IPv6 or IPv6-only network.

Criterion 2: Demonstrate end-to-end interoperability in a mixed IPv4 and IPv6 environment.

- All planned T&E to support demonstration of this criterion was complete in FY 2008.

Criterion 3: Demonstrate equivalent to, or better performance than, IPv4-based networks.

- All planned T&E to support demonstration of this criterion was complete in FY 2008.

Criterion 4: Demonstrate voice, data, and video integration.

- Session Initiated Protocol (SIP) appears to be mature and functions properly in an IPv6 environment.
- Differentiated Services (DiffServ) is an effective method to provide quality VTC voice, data, and video integration.

Criterion 5: Demonstrate effective operation in low-bandwidth environment.

- Using multicast mitigates bandwidth limitations.
- Low-Bandwidth environments are equally challenging for IPv4 and IPv6 communications.
- Testing revealed that Low-Bandwidth environments support IPv6 network applications.

Criterion 6: Demonstrate scalability of IPv6 networks.

- All planned T&E to support demonstration of this criterion was complete in FY 2007.

Criterion 7: Demonstrate support for mobile terminals (voice, data, and video).

- The small amount of testing done indicates IPv6 sometimes outperforms IPv4 in mobile applications.

Criterion 8: Demonstrate transition techniques.

- All planned T&E to support demonstration of this criterion was complete in FY 2008.

Criterion 9: Demonstrate ability to provide network management of networks.

- Total network management is not currently possible using IPv6 network management over IPv6 transport.

Criterion 10: Demonstrate tactical deployability and ad hoc networking.

- Mobility applications (Network Mobility (NEMO) and MANET) continue to be emerging technologies. Future T&E for this criterion is dependent upon continued standards and mobile applications development.

4 Recommendations

Analysis of T&E results combined with DoD Components' inputs provides the following recommendations. These recommendations will support the Chairman of the Joint Chiefs of Staff certification and assist in ensuring a smooth transition to IPv6 for the DoD.

> *Recommendation 1: Continue to sanction and resource operationally realistic use of IPv6 in large exercise environments. This will provide: opportunity to employ IA products and guidance; visibility and experience with IPv6 for personnel outside the transition community; a venue for testing additional IPv6 functionality as it is developed; and a stable, long-term, easily accessible environment that can be used to test user-level applications.*

> *Recommendation 2: Encourage deployment of IPv6 on operational networks in selected enclaves with operators who desire to experiment with IPv6 or who have a need met by the base IPv6 protocol, such as a need for a larger address space or better aggregated hierarchical routing.*

The DoD CIO established a policy for requiring IPv6 Capable Products in acquisition programs. Adherence to these polices is essential for the development of IPv6.

> *Recommendation 3: Enforce this policy in current and future acquisition programs.*

Performance of IPv6 (with bandwidth of 512 kbps or higher) was demonstrated to be equivalent to IPv4. Testing completed this year shows that IPv4 and IPv6 behave similarly in low-bandwidth environments. Effective operation of IPv6 in Low-Bandwidth environments below 512 kbps (Criterion 5) lacks full demonstration.

> *Recommendation 4: Continue testing in low-bandwidth environments representative of operational tactical networks.*

To date, vendor IPv6 implementations focus on basic functionality. Future development and T&E is required for network management tools, IA products, and devices. A full suite of IA products, tools, and policies is required before IPv6 implementation DoD-wide.

> *Recommendation 5: Require full IPsec functionality in products procured by DoD.*

> *Recommendation 6: Continue IPv6 T&E efforts for IA capabilities.*

> *Recommendation 7: Develop and test IPv6-Capable AAA and Public Key Infrastructure (PKI) within DoD.*

> *Recommendation 8: Encourage vendors to accelerate production of IPv6 - Capable IA devices.*

Network management functionality is gradually improving. However, current capabilities provide network management only through the dual-stack phase of IPv6 transition. IPv6-only management will eventually be necessary with the elimination of IPv4 from DoD networks.

> *Recommendation 9: Stress to vendors the need for greater IPv6 functionality in network management tools.*

> *Recommendation 10: Continue network management testing during large-scale exercises to demonstrate the criterion. These exercises will allow testing in an operational environment and expose the tools to systems that go beyond the challenges offered in a laboratory setting.*

The remaining criteria, support for Mobile Terminals (Criterion 7) and Tactical Deployability and Ad-hoc Networking (Criterion 10), still require significant development and T&E.

> *Recommendation 11: Identify use cases and mission threads, and utilize large-scale exercises to focus on undemonstrated criteria as key testing objectives.*

> *Recommendation 12: Encourage vendors to develop and improve IPv6 functionality and performance for mobile terminals, tactical deployability and ad-hoc networking.*

The DoD needs standardized requirements documents to allow for distributed testing. This testing will reduce the cost of systems and accelerate the delivery to the warfighter.

> *Recommendation 13: Incorporate the NSA MO3 IA guidance requirements into the Unified Capabilities Requirements 2008 and other applicable requirements documents for certification testing. Establish standards by releasing these requirements documents to industry.*

5 Summary

The current state of IPv6 products and services does not support full implementation DoD-wide. T&E activities demonstrate vendor devices, operating systems, and network services do not fully support network requirements. Basic features required to enable information exchange using IPv6 are mature and suitable to enable basic connectivity, though many are not optimized.

Important steps were made in implementing IPv6 in the DoD during this reporting period. HAIPE 3.0 IPv6 Capable devices became commercially available and successfully tested. However, the few commercially available IPv6-Capable IA products (specifically IPS and IDS devices) and immaturity of AAA and PKI delays enterprise-wide deployment of IPv6. Although IPv6 is sufficiently mature, IPv6 implementations in software and hardware devices is deficient.

Successful implementation of IPv6 by DoD will require IPv6 features and IA capabilities that are currently underdeveloped. Further research, development, and testing are necessary to ensure that DoD's networks can transition without affecting mission critical operations

Appendix A - References

- Public Law 109-163 National Defense Authorization Act for Fiscal Year 2006, January 6, 2006.
  http://www.defenselink.mil/dodgc/olc/docs/PL109-163.pdf

- Public Law 108-375 National Defense Authorization Act for Fiscal Year 2005, October 28, 2004.
  http://www.defenselink.mil/dodgc/olc/docs/PL108-375.pdf

- Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Master Test Plan version 2.0 (MTP v2.0), September 2006.
  https://www.us.army.mil/suite/doc/8958812

- DoD IPv6 Generic Test Plan Version 3 (GTPv3), August 2007.
  https://www.us.army.mil/suite/doc/9523305

- DoD IPv6 Definitions
  https://www.us.army.mil/suite/doc/11706660

- DoD Information Technology Standards Registry
  https://disronline.disa.mil/

- DITO IA Guidebook Version 1-1
  https://www.us.army.mil/suite/doc/7253350

Appendix B - Terms and Definitions

Demonstration: Testing that is limited to a combination of related, perhaps interdependent, features or functions. It is usually an ordered sequence of tasks and is restricted from any operational network traffic.

Engineering Analysis: Category of testing based on engineers' previous experience with the technology, as well as use of equipment specifications to speculate about the performance or capability.

Exercise: Environment is a functional, operationally realistic network with controlled traffic and realistic loading. The test administrators and users are sympathetic to IPv6. Tests focused on network and communications testing, perhaps with some training goals. This includes automated test generators running scripted test cases a large number of times. The test is well defined and of a limited duration.

Experiment: Testing that consists of a scope that is restricted to a single question or theory with a test network isolated from operational network traffic. Few repetitions of test cases and a limited number of participants are involved.

Field Test: Testing that uses an operationally realistic network with common protocol traffic and assumed loading conditions. Focus is on the devices or systems operating within the environment in which it deploys. A well-defined, limited duration is set for testing.

IPv6 Base Requirements: Requirements mandated for each specific device type in the IPv6 product profile in the DoD Information Technology Standards Registry (DISR).

IPv6-Capable Product: Products (whether developed by commercial vendor or the government) that can create or receive, process, and send or forward (as appropriate) IPv6 packets in mixed IPv4/v6 environments. IPv6-Capable Products shall be able to interoperate with other IPv6-Capable Products on networks supporting only IPv4, only IPv6, or both IPv4 and IPv6 and shall:

- Conform to the requirements for the DoD IPv6 Standards Profiles for IPv6-Capable Products document contained in the DISR.
- Possess a migration path and/or commitment to upgrade from the developer (company Vice President, or equivalent, letter) as the IPv6 standards evolve.
- Ensure product developer IPv6 technical support is available.
- Conform to National Security Agency (NSA) and/or Unified Cross Domain Management Office requirements for Information Assurance (IA) and products.

IPv6 Generic Test Plan (GTP) Versions 3 and 4: A plan developed to provide IPv6 conformance, interoperability, and performance test procedures.

Joint Staff IPv6 Operational Criteria: The 10 criteria the Joint Staff identified to show full IPv6 functionality.

Milestone Objective 1 (MO1): DoD Components can implement and operate IPv6 within an enclave. At MO1, the evaluation of the IPv6 protocol is sufficient, and the policy, procedures, and technical guidance developed to authorize DoD Components to operate in a single network domain or enclave environment within operational networks. The single domain or enclave requires strict access controls be maintained under a single administrative authority for IA and security policy. Information flow requires tight control to prevent IPv6 packets from entering or leaving the domain. The border device shall not translate nor permit the transit of native or tunneled IPv6 packets. MO1 allows the use, familiarization, and testing of IPv6 protocol and applications to ascertain issues and derive migration strategies for this new protocol. Authorized use of MO1 began October 1, 2005.

Milestone Objective 2 (MO2): DoD Components can implement and operate IPv6 across cooperative domain boundaries. At MO2, the policies, procedures, and technical guidance developed to expand the operation of IPv6 across cooperative domain boundaries, but limited to within DoD networks (no internet exchange of IPv6 packets, native or tunneled). MO2 will provide the ability to evaluate the scalability and further evaluate the IPv6 IA implications using tunneling and native IPv6 routing, as available. IPv6 traffic, which crosses cooperative domain boundaries, requires approval in accordance with the Defense Information Systems Network (DISN) connection-approval process to ensure compliance with IA policies. Multiple certification and accreditation authorities may be involved in MO2. MO2 permits applications to test IPv6-specific end-to-end capabilities and routing schema efficiencies. Limiting operation to within the DoD and only at approved locations reduces risk to IA and operational impacts on existing IPv4 networks. Authorized use of MO2 began October 1, 2006.

Milestone Objective 3 (MO3): DoD Components are authorized to implement and operate IPv6 enterprise-wide. At MO3, policy, planning, and technical transition guidance provided to allow tunneled and native IPv6 traffic to exist on DoD operational networks. DISN and DoD Component core IP infrastructures authorized to accept, route, and process IPv6 protocol traffic while maintaining interoperability with IPv4. Boundary protection and other security mechanisms to assure IA requirements shall be available and implemented to protect the DISN. MO3 permits applications and data owners to complete operational transition to IPv6 with at least the same functionality (parity) as currently found in IPv4. Target date for MO3 is FY 2009.

Mixed IPv4 and IPv6 Environment: A mixed IPv4 and IPv6 environment includes the situations of tunneling IPv4 over IPv6 native network, tunneling IPv6 over an IPv4 native network, providing protocol translation at various points, and dual-stack operation.

Modeling and Simulation (M&S): Testing that uses a completely virtual environment to predict system or network performance. Software used to simulate all involved devices and protocols.

Pilots (i.e., Pilot Testing): Testing that uses a functional, operational network with a limited number of administrators and users, but is realistic for the size of the network. There is no set time limit in conducting pilots, and all traffic is non-scripted (routine traffic).

Appendix C - Acronym List

6in4	IPv6 in IPv4
6PE	IPv6 PE
A	DNS A record for an IPv4 Address
AAA	Authorization, Authentication, and Accounting
AAAA	DNS AAAA record for an IPv6 Address
ACL	Access Control List
ADNS	Automated Digital Network System
AFATDS	Advanced Field Artillery Tactical Data System
AFB	Air Force Base
AFIOC	Air Force Information Operations Center
AFRL	Air Force Research Laboratory
AFSN	Air Force System Networking
AH	Authentication Header
AIPTL	Advanced IP Technology Laboratory
ARP	Address Resolution Protocol
ASA	Adaptive Security Appliance
ASBR	Autonomous System Border Routers
ASD	Assistant Secretary of Defense
ASLAN	Assured Services Local Area Network
AS-SIP	Assured Services-SIP
APL	Approved Products List
AODV	Ad hoc On Demand Distance Vector Routing
AT&L	Acquisition Technology and Logistics
BER	Bit Error Rate
BGP	Border Gateway Protocol
BIND	Berkeley Internet Name Domain
CA	Certificate Authority
CAC	Common Access Card
CAT	Categories
CDS	Cross Domain Solutions
CERDEC	Communications Electronics Research Development and Centers
CIO	Chief Information Officer
CLI	Command Line Interface
CONUS	Continental United States
COI	Community of Interest
COTS	Commercial Off-The-Shelf
CPU	Computer Processor Unit
CJCS	Chairman of the Joint Chiefs of Staff
CVE	Common Vulnerabilities and Exploits
DAA	Data Acquisition Agent

DCP-ETSI	Distribution and Communication Protocol-European Telecommunications Standard Institute
DDoS	Distributed Denial of Service
DFS	Data Fusion Server
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DiffServ	Differentiated Services
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISR	DoD IT Standards Registry
DITO	DoD IPv6 Transition Office
DKO	Defense Knowledge Online
DMZ	Demilitarized Zone
DNS	Domain Name System
DoD	Department of Defense
DoS	Denial of Service
DOT&E	Director, Operational Test and Evaluation
DREN	Defense Research and Engineering Network
DSCP	DiffServ Code Points
DTRA	Defense Threat Reduction Agency
DUT	Device Under Test
E2E	End to End
EIGRP	Enhanced Interior Gateway Routing Protocol
EPLRS	Enhanced Positioning Location Reporting System
ERD	Electronic Report Distribution
ESP	Encapsulating Security Payload
EUI-64	Extended Unique Identifier - 64
FA	Foreign Agent
FE	Fast Ethernet
FSO	Field Security Operations
FTP	File Transfer Protocol
FW	Firewall
FY	Fiscal Year
Gbps	Gigabits per second
GES	Ground Entry Sites
GIG	Global Information Grid
GHz	Giga Hertz
GN	Ground Node
GNTF	GIG Network Test Facility
GOTS	Government Off-The-Shelf
GRE	Generic Routing Encapsulation
GTP	Generic Test Plan

HA	Home Agent
HAIPE	High Assurance Internet Protocol Encryptor
HAIPE IS	High Assurance IP Encryptor IP Security
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I3MP	Installation Information Infrastructure Modernization Program
IA	Information Assurance
IATT	Information Assurance Team
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
IDS	Intrusion Detection System
IE	Internet Explorer
IETF	Internet Engineering Task Force
IIS	Internet Information Services
IKE	Internet Key Exchange
INE	In-Line Encrytors
INSC	Interoperable Network for Secure Communications
IOS	Internetwork Operating System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	IP security
IPTV	Internet Protocol Television
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISATAP	Intra-Site Automatic Tunneling Address Protocol
ISP	Information Support Plan
ISR	Integrated Services Router
IT	Information Technology
ITA	Information Technology Agency
ITAG	IPv6 Information Assurance Group
ITP	Interoperability Test Plan
JCAN	Joint Capability for Airborne Networking
JCS	Joint Chiefs of Staff
JITC	Joint Interoperability Test Command
JSTARS	Joint Surveillance Target Attack Radar Systems
JTEN	Joint Tactical Edge Networks
JUICE	Joint User Interoperability Communications Exercise
Kb	Kilobit
Kbps	Kilobits per second
KPP	key Performance Parameters
L2	Layer-2

L3	Layer-3
LAN	Local Area Network
LoC	Letter of Conformance
LDAP	Lightweight Directory Access Protocol
LSP	Label Switched Paths
M&S	Modeling and Simulation
MAC	Media Access Control
MANET	Mobile Ad hoc Networks
Mb	Megabit
Mbps	Megabits per second
MEXT	Mobility Extensions for IPv6
MGEN	Multi-Generator
MLD	Multicast Listener Discovery
MLDv2	Multicast Listener Discovery Version 2
ms	Microseconds
MIB	Management Information Base
MIP	Mobile IP
MN	Mobile Node
MO	Milestone Objective
MO1	Milestone Objective 1
MO2	Milestone Objective 2
MO2v2	Milestone Objective 2 version 2
MO3	Milestone Objective 3
MOB1	Main Operating Base 1
MOS	Mean Opinion Score
MP-BGP	Multiprotocol–Boarder Gateway Protocol
MPLS	Multi Protocol Label Switching
MPEG	Motion Picture Expert Group 2
MR	Mobile Router
MRD	Minimum Requirements Document
ms	milliseconds
MTP	Master Test Plan
MTP v2.0	Master Test Plan Version 2.0
MTU	Maximum Transmission Unit
NAP	Network Access Points
NAT-PT	Network Address Translation-Protocol Translation
NBMA	Non-Broadcast Multi-Access
NCOW	Net-Centric Operations Warfare
NFS	Network File System
NIC	Network Information Center
ND	Neighbor Discovery
NEMO	Network Mobility
NIDS	Network Intrusion Detection System
NII	Networks and Information Integration

NIPRNet	Unclassified but Sensitive Internet Protocol Router Network
NM	Network Management
NMI2	Network Management IPv6 Initiative
NM/OPS	NM Operations
NMS	Network Management Systems
NOC	Network Operations Center
NS2	Network Survivability Double Link Failure
NS	Name Server
NS	Neighbor Solicitation
NSA	National Security Agency
NSM	NetScreen Secutiy Manager
NRL	Naval Research Laboratory
NTP	Network Time Protocol
OAM	Operation, Administration, and Maintenance
OLSR	Optimized Link State Routing
OMB	Office of Management and Budget
OS	Operating System
OSPF	Open Shortest Path First
OTM	On The Move
P	Provider
PAC	Pacific
PAT	Port Address Translation
PC	Personal Computer
PIC	Physical Interface Card
PIM	Protocol Independent Multicast
PIM-SIM	Protocol Independent Multicast – Sparse Mode
PIM-SSM	Protocol Independent Multicast – Source Specific Multicast
PKI	Public Key Infrastructure
PO	Participating Organization
PoE	Power over Ethernet
POP3	Post Office Protocol version 3
PPP	Point-to-Point Protocol
PT	Port Translation
PTP	Point to Point
QFY	Quarter Fiscal Year
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Ancillary Equipment
RAE	Required Ancillary Equipment
RBAC	Role-Based Access
RF	Radio Frequency
RFC	Request for Comment

RHEL	Red Hat Enterprise Linux
RIM	Radio Interface Module
RIP	Routing Information Protocol
RO	Route Optimization
RP	Rendezvous Point
RR	Resource Record
RSA	Rivest-Sharir-Adleman
RSVP	Resource Reservation Protocol
RTCP	Real Time Control Protocol
RTP	Reliable Transport Protocol
RTSP	Real Time Streaming Protocol
SAAT	Security Architecture Analysis and Testing
SATCOM	Satellite Communications
SDC	Standard Desktop Configuration
SDP	Service Delivery Points
SDP	Shelf Discovery Protocol
SEND	Secure Neighbor Discovery
SIIT	Stateless IP/Internet Control Message Protocol Translation
SIMR	Serial Interface to Military Radios
SIP	Session Initiation Protocol
SISTM	Simulator-Simulator
SLAAC	Stateless Address Auto-configuration
SM	Sparse Mode
SMF	Simplified Multicast Forwarding
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP	Service Pack
SPSS	Statistical Package for Social Sciences
SSM	Source Specific Multicast
STIG	Secure Technical Implementation Guide
STP	System Tracking Program
SUP	Supervisor
SUT	System Under Test
SYN	Synchronize
T&E	Test and Evaluation
TCP	Transmission Control Protocol
TDC	Theater Deployable Communications
TDR	Test Discrepancies Reports
TEWG	Test and Evaluation Working Group
TIC	Technology Integration Center
TOC	Tactical Operation Center
TNT	Tactical Network Topology
TRPR	TCPDUMP Rate Plot Real Time
TSIG	Transaction Authentication

UC	Unified Capabilities
UCR	Unified Capabilities Requirements
UDP	User Datagram Protocol
UDS	User Defined Signatures
UPE	Unclassified Provider Edge
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VLC	VLAN Client
VoIP	Voice over IP
VPN	Virtual Private Network
VTC	Video Teleconferencing
WAN	Wide Area Network
WWW	World Wide Web

THIS PAGE INTENTIONALLY LEFT BLANK.

Appendix D – Department of Defense Internet Protocol Version 6 2009 Test and Evaluation Report Summaries

This appendix provides summaries for the 83 Internet Protocol (IP) Version 6 (IPv6) Test and Evaluation (T&E) reports that Department of Defense (DoD) Components submitted since June 2008. Table D-1 summarizes the applicability of each report to the IPv6 Joint Staff Operational Criteria. The alphanumeric designator that precedes each report title in this table corresponds to the section number of the appendix that summarizes the report. Each report summary is comprised of the following eight elements: title, testing organization and publication date, summary, T&E method, relevant IPv6 Joint Staff Operational Criteria (including Level 1 and Level 2 decomposition relevancy), configuration, results, and conclusions/recommendations. Because of the similarity in results, summary D-1 combines all 61 Joint Interoperability Test Command (JITC) IPv6 Special Interoperability Certification Reports into one summary. This summary contains a table that defines Request for Comments (RFCs) found in the DoD Information Technology Standards Registry (DISR) available at https://disronline. disa. mil.

Table D-1. 2009 T&E Reports and Related Operational Criteria

Section	Test Report Short Title	IPv6 Joint Staff Operational Criteria									
		1	2	3	4	5	6	7	8	9	10
D.1	Special Interoperability Test Reports	x	x						x		
D.2	NIRPNet IPv6 Demonstration Report		x	x					x		
D.3	DSN Test Plan II	x	x	x					x		
D.4	IPv6 Multicast Test Report		x		x	x	x		x		
D.5	ITA IPv6 client and server application test		x	x					x		
D.6	ITA MO3 IPv6 DNS & Interoperability Test Plan & Report		x	x					x		
D.7	(JCS) Criteria 4 Testing	x	x	x	x	x			x		
D.8	Juniper ISG 2000 Firewall Internet Protocol Version Six Test Report	x	x						x		
D.9	Cisco Systems IPS 4260 Series Sensor Intrusion Prevention System IPv6 Test Report	x	x						x		
D.10	Cisco Assured Services Local Area Network (ASLAN) Version (v) 6 (Tracking Number 0821001		x	x	x				x		
D.11	IPv6 Converged Services and Joint Staff Operational Criteria Demonstration	x	x		x	x		x	x	x	
D.12	JCS Criteria 10 Test Plan		x		x	x		x	x		x
D.13	Force10 networks E300, C300, C150 and S50V Force10 Operating System (FTOS)Version (V)7.8.1.0.E (Tracking Number 0831101)		x	x					x		
D.14	Defense Threat Reduction Agency Demonstration Test Report to Support Defense Threat Reduction Agency IPv6 Compliance		x						x		
D.15	Information Assurance IPv6 Findings Summary		x						x		
D.16	Foundry-Brocade Assured Services Local Area Network (ASLAN) and Non-ASLAN Version 6 (V6) With Specified Software Releases (Tracking Number 0833804)		x	x					x		
D.17	Juniper MX240/480/960 and EX4200/3200		x	x					x		
D.18	Motorola Point to Point (PTP) 600 Network Element With Software Release 08-32		x	x					x		
D.19	McAfee IntruShield 3000 Intrusion Prevention System Internet Protocol Version Six Test Report		x						x		
D.20	Joint Staff IPv6 Operational Criteria Test Report Criterion #5: Demonstrate Effective Operation In Low-bandwidth Environment		x			x			x		
D.21	Evaluation of Joint Chiefs of Staff Criteria #9: IPv6 Network Management		x						x		
D.22	National Security Agency Milestone Objective 3 Information Assurance Guidance Validation Test Report	x	x						x		

Table D-2 lists the IPv6 Special Certifications combined into one summarized report in D.1.

Table D-2. 2009 T&E JITC IPv6 Special Certifications

Test Report Short Title	Device Type
Xerox Phaser 6360DT Running System Firmware 1.3.7.P/Operating System 8.26/Post Script 4.12.0/Engine 12.11.0/Newtwork 37.58.03.03,2008 Family of Color Printers for IPv6 Capability	**Simple Server**
Cisco 3845 Integrated Services Router Running Internetworking Operating System (IOS) Version 12.4(11)T bundled with the 7600 Family of Routers Running IOS Version 12.2(33) SRBI System for Internet Protocol Version 6 (IPv6) Capability	**Router**
Cisco 2811 Integrated Services Router Running Internetworking Operating System (IOS) Version 12.4(11)T bundled with the 7600 Family of Routers Running IOS Version 12.2(33) SRBI System for Internet Protocol Version 6 (IPv6) Capability	**Router**
Dell PowerVault Storage System TL2000 and Dell PowerVault Storage System TL4000 Tape Libraries with an Embedded Transmission Control Protocol/Internet Protocol (TCP/IP) Dual-Stack Core Running Firmware Version 6.60 for Internet Control Protocol Version 6 (IPv6) Capability	**Simple Server**
Microsoft Windows Server 2008 Standard Service Pack 1 Build 6.0.6001 Running on the Dell Power Edge R900, Dell Power Edge 2950, and Dell Power Edge 1950 Servers for Internet Protocol Version 6 (IPv6) Capability	**Advanced Server**
Hewlett-Packard Jet Direct 635n/690n Print Server Card Firmware Version (V).38.05 for Internet Protocol Version 6 (IPv6) Capability	**Simple Server**
Dell 5110CN Printer Family for Internet Protocol Version 6 (IPv6) Capability	**Simple Server**
Dell OptiPlex 749 Family of Host/Workstations Running Microsoft Windows Vista, Service Pack 1, Operating System for Internet Protocol Version 6 Capability	**Host/Workstation**
Dell 5330DN Printer Family for Internet Protocol Version 6 (IPv6) Capability	**Simple Server**
Dell OptiPlex 755 Family of Host/Workstations Running Microsoft Windows Vista, Service Pack 1, Operating System for Internet Protocol Version 6 Capability	**Host/Workstation**
Dell Latitude D630 Family of Host/Workstations Running Microsoft Windows Vista, Service Pack 1, Operating System for Internet Protocol Version 6 Capability	**Host/Workstation**
Broadcom Transmission Control Protocol (TCP)/Internet Protocol (IP) Offload Engine (TOE) part number BCM5709 and BCM57710 Network Interface Cards for IP Version 6 (IPv6) Capability	**Advanced Server**
McAfee IntruShield I-Series and M-Series Sensors for Internet Protocol Version 6 Capability	**Simple Server**
IBM AIX Server and AIX Virtual Input/Output Server Running Version 0833A-611PV661b Service Pack 1 for Internet Protocol Version 6 Capability	**Advanced Server**
Dell EqualLogic PS Series Array, Firmware Version 4.0.0 for Internet Protocol Version 6 Capability	**Network Appliance**
Brocade SilkWorm 200E Fiber Channel Switch Running Fabric Operating System Version 6.2 Software for Internet Protocol Version 6 Capability	**Network Appliance**
Polycom HDX 9000x Product Family, Running Software Version 2.0.5_J for Internet Protocol Version 6 Capability	**Network Appliance**
Juniper NS-5400 Firewall Running ScreenOS Version 6.2 Software for Internet Protocol Version 6 Capability	**Firewall**
Tandberg Video Communication Server Running Software Version X2.0 for Internet Protocol Version 6 Capability	**Simple Server**
Tandberg Management Suite Version 11.9.1, Running on Microsoft Windows Server 2033 Enterprise Service Pack 2, Build 5.2.3790, for Internet Protocol Version 6 Capability	**Simple Server**
Tandberg 3000MXP Running Software Version F7.1 Family for Internet Protocol Version 6 Capability	**Simple Server**
Tandberg MPS 800 Running Software Version J4.4 Family for Internet Protocol Version 6 Capability	**Simple Server**
Fortinet FortiGate 400A and 3600, 3.00, Build 0726.080716 Family of Information Assurance Devices for Internet Protocol Version 6 Capability	**Firewall**
2330DN Printer running Software Version FPN. APS. F001abd-0 for Internet Protocol Version 6 Capability	**Simple Server**
Dell Latitude E6500 32-bit and 64-bit Family of Notebook Computers Running Microsoft Windows Vista, Service Pack 1, Operating System for Internet Protocol Version 6 Capability	**Host/Workstation**
Dell 3130CN Running Software Version 2.1.0(0/9), Printer Family for Internet Protocol Version 6 Capability	**Simple Server**
Dell Precision M6400 64-bit Notebook Computer Running Microsoft Windows Vista, Service Pack 1, Operating System for Internet Protocol Version 6 Capability	**IA Device**
Dell OptiPlex 960 32-bit and 64-bit Family of Desktop Computers Running Microsoft Windows Vista, Service Pack 1, Operating System for Internet Protocol Version 6 Capability	**IA Device**
Dell OptiPlex 360 32-bit and 64-bit Family of Desktop Computers Running Microsoft Windows Vista, Service Pack 1, Operating System for Internet Protocol Version 6 Capability	**IA Device**
Dell OptiPlex 160 32-bit Desktop Computer Running Microsoft Windows Vista, Service Pack 1, Operating System for Internet Protocol Version 6 Capability	**IA Device**
Dell Latitude E5500 and Precision M6400 32-bit Family of Notebook Computers Running Microsoft Windows Vista, Service Pack 1, Operating System for Internet Protocol Version 6 Capability	**IA Device**
Hewlett-Packard LaserJet P2055, Firmware Version V3.07. SD, Family of Printers for Internet Protocol Version 6 Capability	**Simple Server**

Table D-2. 2009 T&E JITC IPv6 Special Certifications (continued)

Test Report Short Title	Device Type
IBM z/OS Version 1.10 Operating System for IBM Mainframe Computer Systems for Internet Protocol Version 6 Capability	**Advanced Server**
Hewlett-Packard (HP) Integrity RX2660 Systems Family of Servers Running the HP-UX 11i v3 Operating System for Internet Protocol Version 6 Capability	**Advanced Server**
Hewlett-Packard Integrity RX2660 Family of Servers Running the SUSE Linux Enterprise Server 10 Service Pack 2, Operating System for Internet Protocol Version 6 Capability	**Advanced Server**
Hewlett-Packard (HP) 9000 RP340 Systems Family of Servers Running the HP-UX 11i v3 Operating System for Internet Protocol Version 6 Capability	**Advanced Server**
Hewlett-Packard xw9400 Workstation Family Running Microsoft Windows Vista Service Pack 1 Operating System for Internet Protocol Version 6 Capability	**Host/Workstation**
Hewlett-Packard ProLiant DL380 Family of Servers Running the Windows Server 2008 Service Pack 1 Operating System for Internet Protocol Version 6 Capability	**Advanced Server**
Hewlett-Packard ProLiant DL380 Family of Servers Running the SUSE Linux Enterprise Server 10 Service Pack 2 Operating System for Internet Protocol Version 6 Capability	**Advanced Server**
Hewlett-Packard ProLiant DL380 Family of Servers Running the Red Hat Enterprise Linux RhEL5.2 Operating System for Internet Protocol Version 6 Capability	**Advanced Server**
Secure Computing 1100 and 2150 Sidewinder Family of Firewalls Running Software Version 7.0.1.00 for Internet Protocol Version 6 Capability	**Firewall**
Infoblox 550 DNSOne Family of Network Services Appliances Running Infoblox NIOS Version 4.3r2 Operating System for Internet Protocol Version 6 Capability	**Simple Server**
Dell PowerConnect 5424 Family of Gigabit Ethernet Layer-2 Switches with Marvell Prestera-DX Application- Specific Integrated Circuits Running the Marvell ROS-7.47 Software Package for Internet Protocol Version 6 Capability	**Network Appliance**
Dell PowerConnect 3524 Family of Fast Ethernet Layer-2 Switches with Marvell Prestera-DX Application- Specific Integrated Circuits Running the Marvell ROS-7.47 Software Package for Internet Protocol Version 6 Capability	**Network Appliance**
Zebra S4M Family of Printers Running Software Version ZSP1189A Using the Zebra SHE PS105-Z External and Zebra SHE PS102-Z Internal Print Servers Running Software Version 10.2.z for Internet Protocol Version 6 Capability	**Simple Server**
Zebra 110XiIIIPlus Family of Printers Running Software Version ZSP1190A Using the Zebra SHE PS105-Z External and/or Zebra SHE PS 102-Z Internal Printer Servers Running Software Version 10.2. z for Internet Protocol Version 6 Capability	**Simple Server**
Securify Monitor Version 6. Family of Information Assurance/Integrated Security Devices Running CentOS Version 5 Operating System for Internet Protocol Version 6 Capability	**IA Device**
Dell PowerVault MD3000i Storage Array Running the Modular Disk Storage Manager Version 03.35.G6.37 and Controller Firmware Version 07.35.22.60 for Internet Protocol Version 6 Capability	**Network Appliance**
Dell PowerVault MD3000 Storage Array Running the Modular Disk Storage Manager Version 03.35.G6.37 and Controller Firmware Version 07.35.22.60 for Internet Protocol Version 6 Capability	**Network Appliance**
NetApp FAS3020 Family of Storage Systems Running the NetApp Data ONTAP Version 7.3.1 Software for Internet Protocol Version 6 Capability	**Simple Server**
Integrated Dell Remote Access Controller 6 – Express and Enterprise, Running the Dell Controller Firmware Version 1.0.36 on the Dell PowerEdge R710 Family of Servers for Internet Protocol Version 6 Capability	**Simple Server**
Dell PowerConnect 6224 Family of layer-3 Switches Running Software Version 3.0.0.0 for Internet protocol Version 6 Capability	**L3-Switch**
TippingPoint Security Management System Version 3.0.0.7063 for Internet Protocol Version 6 Capability	**Simple Server**
TippingPoint 2500N Intrusion Prevention System Running the TippingPoint Operating System Version 3.0.1.1110 for Internet Protocol Version 6 Capability	**IA Device**
IBM Hardware Management Console Version 7 Release 3.4.0 Running the IBM Embedded Linux Operating System, Kernel Version 2.6.5 for Internet Protocol Version 6 Capability.	**Simple Server**
Xerox WorkCentre 4260 Family of Xerox Phaser and WorkCentre Office Multi-Functional Devices and Printers Running the Xerox Internet Protocol (IP) Core Software Version 6.6.3.P Software Platform for IP Version 6 Capability	**Simple Server**
Fluke Networks OptiView Series III Work Group Analyzer Running the OptiView Version 5.3 Operating System for Internet Protocol Version 6 Capability	**Network Appliance**
LGS 7710 Sr-c12 and 7750 SR 7 Family of Service Routers Running the Service Router Operating System Version 6.1 for Internet Protocol Version 6 Capability	**Router**
Sun Storage Tek 6000 Series Family of Disk Storage Arrays Running Software Version 07.15.11.11 for Internet Protocol Version 6 Capability	**Network Appliance**
Sun StorageTek 2500 Series Family of Disk Storage Arrays Running Software Version 07.35.10.10 for Internet Protocol Version 6 Capability	**Network Appliance**

D.1 IPv6 Special Interoperability Certification Reports

Testing Organization and Publication Date

JITC
June 2008 - May 2009

Summary

Testing conducted at JITC certified devices to meet the requirements of the DoD DISR. For IPv6 Special Certification testing, testers identified a device by its Product Class, such as Simple Server or Router. Table D-3 contains a list of the Product Classes and the respective DISR requirements. Testers used the DoD IPv6 Generic Test Plan (GTP) Version (V) 3 or 4, written to provide procedures for testing Product Classes to the DISR requirements. From June 2008 through May 2009, JITC issued 61 IPv6 Special Certifications. This testing contributed to a number of the Joint Staff Operation Criteria and consistently addressed Interoperability (Criterion 2) and Transition Mechanisms (Criterion 8) with the next most commonly tested criterion being Security (Criterion 1).

Test and Evaluation Method

Demonstration

Joint Staff Operational Criteria Tested

1 (1.1.1)
2 (2.1, 2.3)
8 (8.1)

Configuration

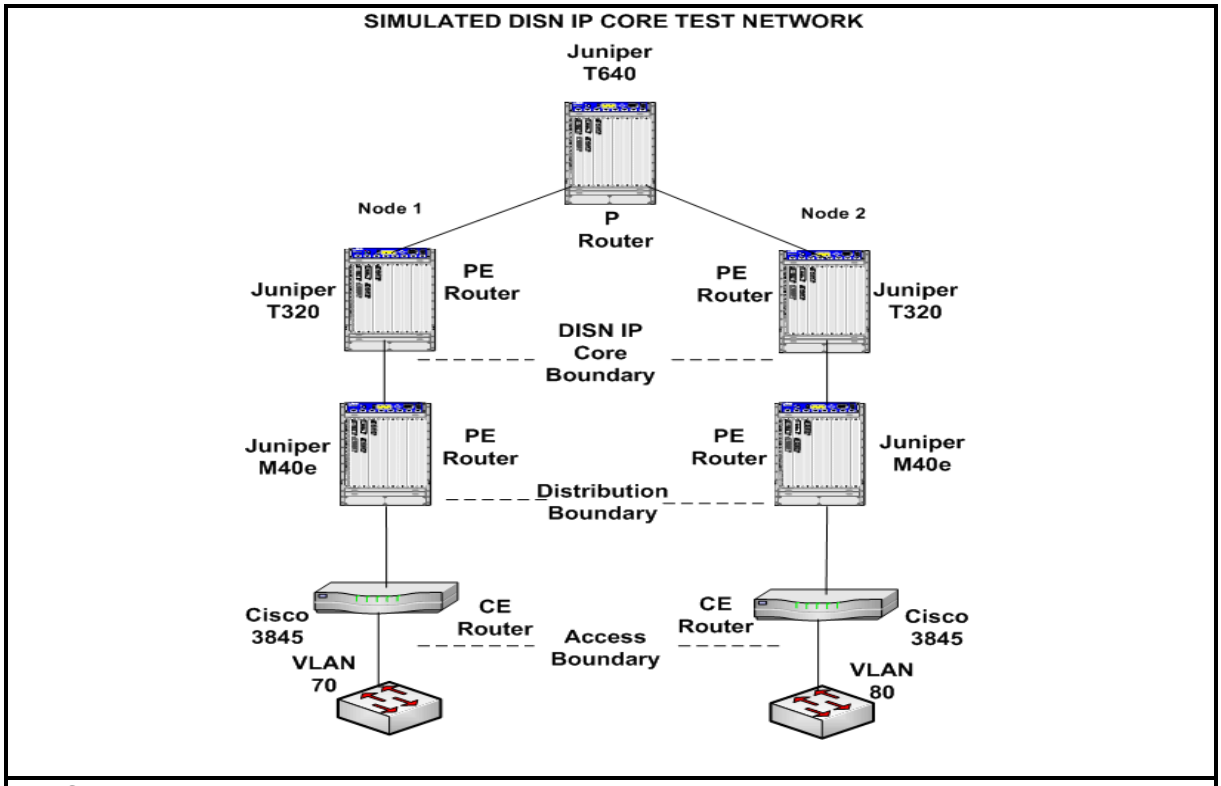
Table D-3 lists the IPv6 Capable DISR requirements for the Product Classes as described in the DoD DISR, "DoD IPv6 Standard Profiles for IPv6 Capable Products V 2.0 or V 3.0." Testers identified the device and Product Class from the requirements in the DISR. Testers evaluated the devices using the procedures listed in the DoD IPv6 GTP V 3/4. If the device passed all the required RFC tests, it was eligible for certification and listed on the Unified Capabilities (UC) Approved Products List (APL) as IPv6 Capable. Certifications expire upon changes that affect interoperability, but no later than 3 years for Joint Chiefs of Staff Instruction (CJCSI) 6212.01D or 4 years for CJCSI 6212.01E from the date of certification. These IPv6 Special Certifications combine IPv6 Capable interoperability testing conducted by JITC at Fort Huachuca, Arizona, and the vendor's Letter of Conformance (LoC) that assures conformance to specific RFCs. In some cases, individual devices provided a representative sample of a device family and the family was certified.

JITC distributes interoperability information via the JITC Electronic Report Distribution system, which uses Unclassified-But-Sensitive IP Router Network (NIPRNet) e-mail. More

comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool at http://jitc.fhu.disa.mil (NIPRNet), or http://199.208.204.125 Secret IP Router Network. Information related to IPv6 Capable testing is on the UC APL at http://jitc.fhu.disa.mil/adv_ip/register/register.html.

Operational Architecture

The operational architecture was the JITC simulated Defense Information Systems Network (DISN) IP Core Network as depicted in Figure D-D-1.



LEGEND:

CE	Customer Edge	LAN	Local Area Network
DISN	Defense Information Systems Network	P	Provider
IP	Internet Protocol	PE	Provider Edge
JITC	Joint Interoperability Test Command	VLAN	Virtual LAN

Figure D-1. JITC Simulated DISN IP Core Network

Required Device Interfaces

All IPv6-capable products to be included on the UC APL must meet the requirements of the DISR, "DoD IPv6 Standard Profiles for IPv6 Capable Products V 2.0 and 3.0," (Product Profile). Testing, in accordance with the procedures identified in the DoD IPv6 GTP, assessed the requirements listed in the DISR. The IPv6 DISR device product class requirements are in Table D-3.

Table D-3. IPv6 Capable Device Requirements for Testing

RFC	RFC Title	Product Class						Effective Date	Comment
		Host/ WS	Network App or Simple Server	Advanced Server	Router	L3 Switch	IA Device		
IPv6 Base									
2460	Internet Protocol, Version 6 (IPv6) Protocol Specification	M	M	M	M	M	M	Current	
5095	Deprecation of Type 0 Routing Headers in IPv6	M	M	M	M	M	M	7/2009	
4443	Internet Control Message Protocol (ICMPv6)	M	M	M	M	M	M	Current	
2461	Neighbor Discovery for IPv6	M	M	M	M	M	M	Current	
4861								7/2009	
2462	IPv6 Stateless Address Autoconfiguration	M	M	M	M	M	M	Current	Note 1
4862								7/2009	
1981	Path MTU Discovery for IPv6	M	S	M	M	M	M	Current	
4291	IPv6 Addressing Architecture	M	M	M	M	M	M	Current	
4007	Scoped Address Architecture	M	M	M	M	M	M	Current	
4193	Unique Local IPv6 Unicast Addresses	O	O	O	O	O	O	Current	
2710	Multicast Listener Discovery for IPv6	M	M	M	M	M	M	Current	
3810	MLDv2 for IPv6	M	S+	M	M	S+	S+	Current	Note 2
2464	IPv6 over Ethernet	CM	CM	CM	CM	CM	CM	Current	Note 3
2492	IPv6 over ATM	CM	CM	CM	CM	CM	CM	Current	Note 3
2472	IPv6 over PPP	CM	CM	CM	CM	CM	CM	Current	Note 3
5072								7/2009	
3572	IPv6 over MAPOS	CM	CM	CM	CM	CM	CM	Current	Note 3
2467	IPv6 over FDDI	CM	CM	CM	CM	CM	CM	Current	Note 3
2491	IPv6 over NBMA	CM	CM	CM	CM	CM	CM	Current	Note 3
2497	IPv6 over ARCnet	CM	CM	CM	CM	CM	CM	Current	Note 3
2590	IPv6 over Frame Relay	CM	CM	CM	CM	CM	CM	Current	Note 3
3146	IPv6 over IEEE 1394 Networks	CM	CM	CM	CM	CM	CM	Current	Note 3
4338	IPv6, IPv4, and ARP Packets over Fibre Channel	CM	CM	CM	CM	CM	CM	Current	Note 3
4944	Transmission of IPv6 Packets Over IEEE 802. 15. 4 Networks	CM	CM	CM	CM	CM	CM	7/2009	
IPsec									
4301	Security Architecture for Internet Protocol	M	S+	M	M	S+	CM	Current	
4302	IP Authentication Header	S	S	S	CM	S	CS	Current	

Table D-3. IPv6 Capable Device Requirements for Testing (continued)

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

Table D-3. IPv6 Capable Device Requirements for Testing (continued)

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

Table D-3. IPv6 Capable Device Requirements for Testing (continued)

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

Table D-3. IPv6 Capable Device Requirements for Testing (continued)

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

Table D-3. IPv6 Capable Device Requirements for Testing (continued)

RFC	RFC Title	Product Class						Effective Date	Comment
		Host/ WS	Network App or Simple Server	Advanced Server	Router	L3 Switch	IA Device		
2858	Multi-Protocol Extensions for BGP-4	N/R	N/R	N/R	CM Note 12	CM Note 7	N/R	Current	
4760								7/2009	
Automatic Configuration									
2462	IPv6 Stateless Address Autoconfiguration (SLAAC)	M Note 1	M Note 1	N/R	M Note 13	N/R	N/R	Current	
4862								7/2009	
3315	DHCPv6 [client]							Current	
3315	DHCPv6 [server]	N/R	CM	CM	CM	N/R	N/R	7/2009	
	DHCPv6 [Relay Agent]		N/R	N/R		CM			
3769	IPv6 Prefix Delegation	N/R	CM	CM	CM	N/R	N/R	7/2009	
3633	IPv6 Prefix Options for DHCPv6	N/R	CM	CM	CM	N/R	N/R	7/2009	
N/A	[disable autoconfiguration]	M	M	M	M	M	M	Current	
5175	Extensions to Router Advertisement Flags	CS+	CS+	CS+	CS+	CS+	CS+	7/2009	
Server									
959	File Transfer Protocol	N/R	O	O	N/R	N/R	N/R	Current	
2428	FTP Extensions for IPv6 and NAT	N/R	O	O	N/R	N/R	N/R	Current	
2821	Simple Mail Transfer Protocol (SMTP)	N/R	O	O	N/R	N/R	N/R	Current	
2911	Internet Printing Protocol	N/R	O	O	N/R	N/R	N/R	Current	
3162	RADIUS (Remote Authentication Dial-In User Service) and IPv6	N/R	O	O	N/R	N/R	CM	Current	
4330	Simple Network Time Protocol (SNTP)	N/R	O	O	N/R	N/R	N/R	Current	
3226	DNS Security and IPv6 A6 Aware Server/Resolver Message Size Requirements	N/R	O	O	N/R	N/R	N/R	Current	
3261	Session Initiation Protocol (SIP)	N/R	O	O	N/R	N/R	N/R	Current	
3596	DNS Extensions to Support IPv6	N/R	O	O	N/R	N/R	N/R	Current	
3053	IPv6 Tunnel Broker	N/R	O	O	N/R	N/R	N/R	Current	
Host									
3484 [Sec 2. 1]	Default Address Selection for IPv6 [Policy Table]	S+	S	S+	N/R	N/R	N/R	Current	
3484 [rest of RFC]	Default Address Selection for IPv6	M	S	M	N/R	N/R	N/R	Current	
3596 resolver	DNS Extensions to Support IPv6	M	S	M	N/R	N/R	N/R	Current	

Table D-3. IPv6 Capable Device Requirements for Testing (continued)

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

LEGEND:

A6	IPv6 Address Record	MIB	Management Information Base
App	Appliance	MLD	Multicast Listener Discovery
ARCnet	Attached Resource Computer Network	MLDv2	MLD Version 2
ARP	Address Resolution Protocol	MPLS	Multi-protocol Label Switching
ATM	Asynchronous Transfer Mode	MTU	Maximum Transmission Unit
BGP-4	Border Gateway Protocol Version 4	N/A	Not Applicable
CM	Conditional Must	N/R	No Requirement
CS	Conditional Should	NAT	Network Address Translation
CS+	Conditional Should Plus	NBMA	Non-Broadcast Multi-Access Network
DHCP	Dynamic Host Configuration Protocol	O	Optional
DHCPv6	DHCP Version 6	OSPF	Opened Shortest Path First
DiffServ	Differentiated Services	OSPFv3	OSPF Version 3
DNS	Domain Name Service	PPP	Point-to-Point Protocol
DoD	Department of Defense	RADIUS	Remote Authentication Dial-In User Service
FDDI	Fiberoptic Digital Data Interface	RFC	Request for Comments
FTP	File Transfer Protocol	RoHC	Robust Header Compression
IA	Information Assurance	RSVP	Resource ReSerVation Protocol
IEEE	Institute of Electrical and Electronic Engineers, Inc.	RTP	Real-Time Transport Protocol
IETF	Internet Engineering Task Force	S	Should
IGMP	Internet Group Multicast Protocol	S+	Should Plus
IKE	Internet Key Exchange	SDH	Synchronous Digital Hierarchy
IKEv1	IKE Version 1	Sect	Section
IKEv2	IKE Version 2	SLAAC	Stateless Address Auto-configuration
IP	Internet Protocol	SN	Should Not
IPsec	Internet Protocol Security	SNMP	Simple Network Management Protocol
IPv4	Internet Protocol Version 4	SONET	Synchronous Optical Network
IPv6	Internet Protocol Version 6	TCP	Transmission Control Protocol
ISAKMP	Internet Security Association and Key Management Protocol	UDP	User Datagram Protocol

Table D-3. IPv6 Capable Device Requirements for Testing (continued)

L3	Layer-3	V	Version
M	Must	VPN-B	Virtual Private Network Suite B
MAC	Media Access Control	WS	Workstation
MAPOS	Multiple Access Protocol Over SONET/SDH		

NOTES:

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

Device Configurations

Table D-4 provides hardware and software components used in the test network.

Table D-4. Test Configuration Hardware and Software

Equipment Name	Model Number	IOS/OS/Version(s)
Hardware		
DUT	DUT Hardware	DUT OS
2 Cisco Routers	Cisco 3845	12.4(11)T
2 Juniper Routers	Juniper M40e	V 7.6R3.6
2 Juniper Routers	Juniper T320	V 7.5R4.4
Juniper Router	Juniper T640	V 7.5R4.4
2 Gateway Notebooks	450ROG	MS Windows XP Professional
Software		
MS Windows XP Professional	N/A	Build 5.1.2600 SP2
MS Windows Server 2003	N/A	Build 5.2.3790 SP1
Wireshark	N/A	V 1.0.3 (SVN Rev 26134)

LEGEND:

DUT	Device Under Test	Rev	Revision
IOS	Internetworking Operating System	SP	Service Pack
MS	Microsoft	SVN	Software Version Number
N/A	Not Applicable	T	New Technology
OS	Operating System	V	Version
R	Release		

Results

Table D-2 lists all the devices certified as a result of IPv6 Special Interoperability Testing.

Conclusions/Recommendations

The devices tested by JITC for IPv6 interoperability met all the RFC requirements listed in the DISR. These tests most commonly addressed Interoperability (Criterion 2), Transition Techniques (Criterion 8), and in some cases included Security (Criterion 1).

D.2 NIPRNet IPv6 Compliance

Testing Organization and Publication Date

Defense Information Systems Agency (DISA)
June 18, 2008

Summary

Devices that make up the operational NIPRNet Backbone Core were configured dual-stack, enabling them to route both IP Version 4 (IPv4) and IPv6 packets through the network. A series of tests performed demonstrated NIPRNet's capability and compliance with Chief Information Officer's (CIO) requirement. Testing demonstrated the ability to route IPv6 packets through the NIPRNet from an external network. IPv6 configured laptops were set up at various node locations, used for initiating and receiving transmitted IPv6 traffic. Utilizing the dual-stacked laptops, testers executed a series of ping and traceroute commands.

Test and Evaluation Method

Exercise

Joint Staff Operational Criteria Tested

2 (2.1, 2.3)
3 (3.1)
8 (8.1)

Configuration

Core Network Connectivity

Testers found host devices capable of generating and terminating IPv6 traffic flows, while directly connected to devices in the operational IPv6 Backbone Core. These interconnected host devices generated and captured IPv6 traffic flow information. The Continental United States (CONUS) Core network diagram in Figure D-2 represents the demonstration's NIPRNet IPv6 Backbone Core topology, composed of Provider (P) (Juniper T640) and Unclassified Provider Edge (UPE) (Juniper T320) routers. The P routers are the highest level of the IP hierarchy and are responsible for high-speed switching of Multi Protocol Label Switching (MPLS) labeled packets within the Backbone. Additionally, certain P routers have the ability to peer with external networks and perform as Autonomous System Border Routers (ASBRs) (i.e., peering routers) as well as route reflectors. These routers are dual-stacked to support IPv4/IPv6 external traffic. In the demonstration, unclassified P and UPE routers interconnected with P router switching labeled packets over an MPLS Core using label switched paths (LSPs). These paths terminated on the UPE routers shown in Figure D-2. The UPE routers were dual-stacked and configured as IPv6 PE (6PE) routers. By configuring the UPE routers to 6PE, routers supported IPv6 routing and packet forwarding over the IPv4 MPLS Core. During the demonstrations, two hosts (PCs/Laptops) configured in dual-stack mode, connected directly to dual-stack NIPRNet

Core: UPE routers via a Fast Ethernet (FE) interface. IPv6 host utilities, such as ping, traceroute, and Screen Capture generated, terminated, and captured IPv6 traffic flow data, as shown in Figure D-2.

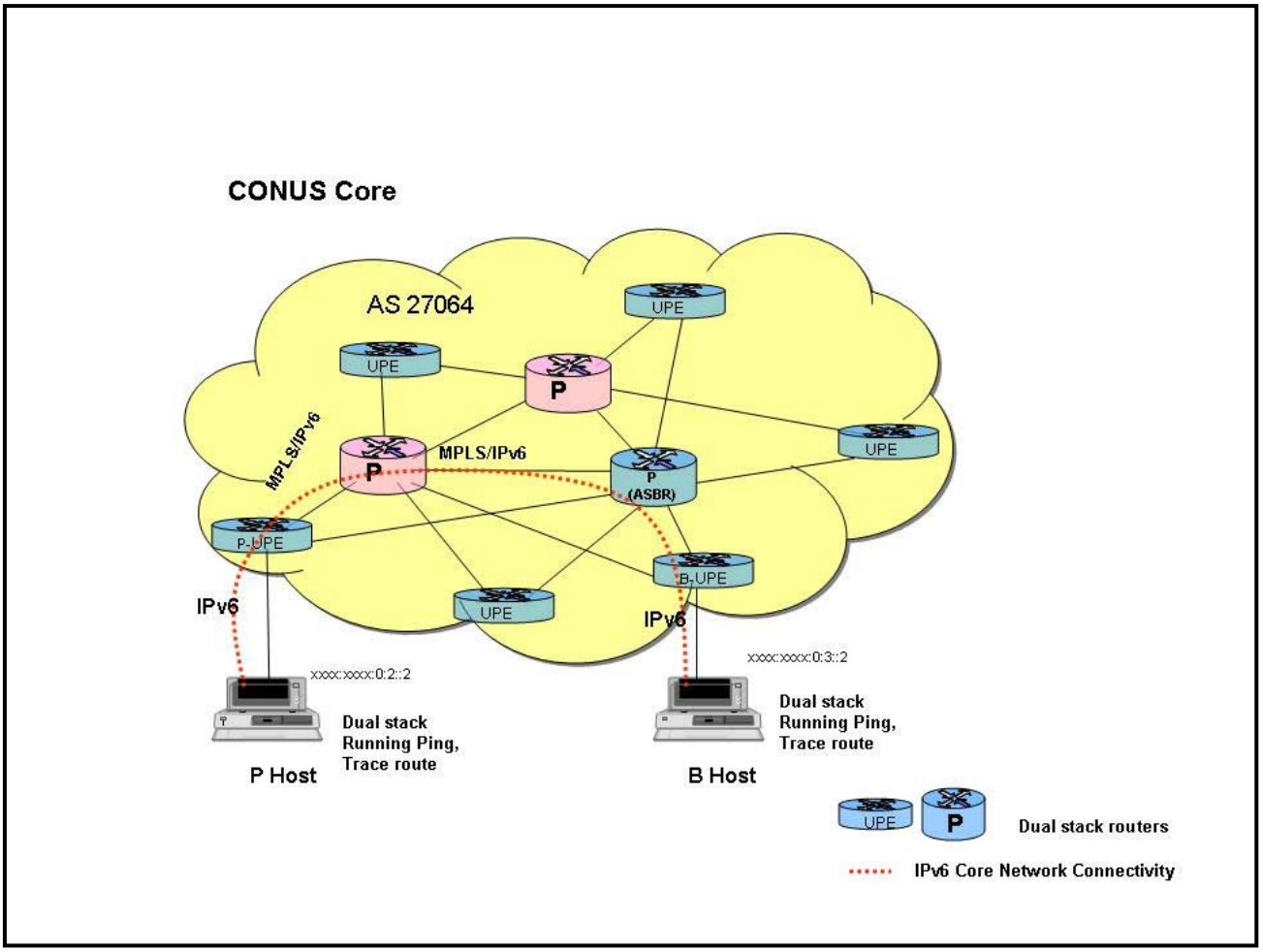


Figure D-2. NIPRNet IPv6 Core Network Connectivity

External Network Connectivity

Figure D-3 illustrates the NIPRNet IPv6 external network connectivity. The identified external network was the Pacific (PAC) Theater Core Backbone, composed of P (Juniper T320), and UPE (Juniper M40e) routers. The PAC Core routers perform various functions such as MPLS on the P routers. In addition some PAC Core routers have the ability to perform as route reflectors and ASBRs. These routers exchange Intermediate System to Intermediate System and Border Gateway Protocol (BGP) respectively. The P and UPE routers interconnected over an MPLS Core with P router switching labeled packets. The MPLS Core used the LSPs that terminate on the UPE routers. The UPE routers were dual-stacked and configured as 6PE routers to support IPv6 routing and packet forwarding over the IPv4 MPLS Core. Only certain P routers of each Backbone Core serve as ASBRs. The ASBRs were dual-stacked to support IPv6/IPv4 external traffic. As shown in Figure D-3, the CONUS operational IPv6 Backbone Core network

connected to the PAC operational Backbone Core network via an Optical Carrier-192 link. The ASBR routers, that form the link, serve as a peering point for interfacing core networks using External BGP and forwarding IPv4/IPv6 traffic between external networks. During the demonstration, a host (PCs/Laptops) at the external network site configured with IPv6 in a dual-stack mode and connected directly to dual-stacked Core - UPE router via an FE interface. IPv6 host utilities, such as ping, traceroute, and Screen Capture used to generate, terminate, and capture IPv6 traffic flow information.

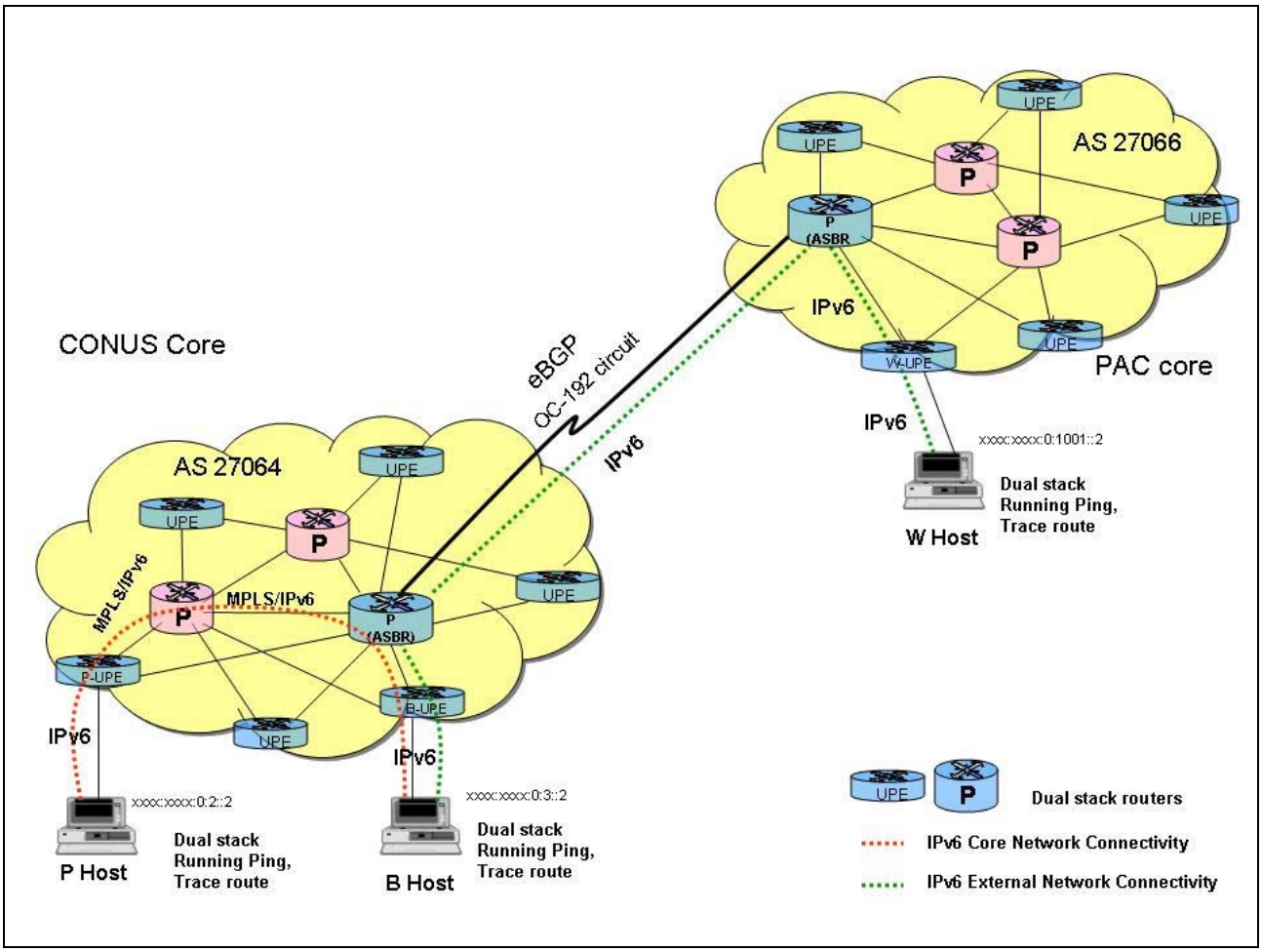


Figure D-3. NIPRNet IPv6 External Network Connectivity

IPv6 Connectivity Demonstration

Core Network IPv6 Connectivity Demonstration

In an attempt to demonstrate the Backbone Core's ability to route IPv6 traffic between two PC/Laptops, testers administered a series of tests. Testers executed a set of 10 *ping* tests via the *ping* script between host P and host B, vice versa. Following 10 *ping* attempts, packet loss was zero. Testers performed this test several more times. A continuous *ping* test was set up for about an hour between the two hosts (P and B), calibrating the responses.

Core Network IPv6 Connectivity with External Network Demonstration

Testers executed set of 10 *ping* tests via the *ping* script between host P, B, and W (connected to the external network). As opposed to the earlier test, this testing involved hosts connecting to one another across separate networks. The procedures involved both host P and B attempting to connect to host W and vice versa. A continuous *ping* test was set up for about an hour between host P and W.

IPv6 Transport Demonstration

Core Network IPv6 Transport Demonstration

To demonstrate the Backbone Core's ability to transport IPv6 traffic between two PC/Laptops, testers executed a series of tests. Testers executed a *traceroute* test with a maximum limit of 10 hops by initiating the *traceroute* script between host P and host B, vice versa. Testers specified a hop limit indicating to the hosts, how many routers the packets could pass through before terminating the search.

Core Network IPv6 Transport with External Network Demonstration

Testers executed multiple *traceroute* tests over a maximum of 10 hops via the *traceroute* script between the hosts P, B, and W. The procedures involved host P and B, attempting to *traceroute* IPv6 packets over to host W and vice versa. The executed *traceroute* command initiated an IPv6 packet that sent from the source host in search of a destination host, while limiting the number of hops to 10.

Demonstration Completeness

Since the CONUS and PAC Backbone Core routers were not available to respond to user *ping* and *traceroute* queries, testers devised a set of tests to assess router performances on each Backbone. These tests illustrated core router IPv6 connectivity and ability to transport IPv6 traffic. Rather than running scripts on the hosts, *ping* and *traceroute* scripts ran on the core routers, directing all requests to neighboring routers. The tests ran on each of the routers connected to host P, B, and W.

Results of IPv6 Connectivity Demonstration

Core Network IPv6 Connectivity Demonstration

The results indicated that for each initiated a 32-byte IPv6 *ping* command, left in one millisecond (ms). Following 10 *ping* attempts, the generated packet, packet loss was zero. The test ran several more times with no errors. A continuous *ping* test was set up for about an hour between the two hosts (P and B), calibrating the responses. The results from the tests indicated that IPv6 connectivity was successful and that the operation of the base Transmission Control Protocol (TCP)/IPv6 stack was working correctly across the CONUS Backbone Core.

Core Network IPv6 Connectivity with External Network Demonstration

Testers executed a set of 10 *ping* tests via the *ping* script between host P, B, and W (connected to the external network). As opposed to the earlier test, confined to one network theatre, another test involved hosts connecting to one another across separate networks. The procedures involved both host P and B attempting to connect to host W and vice versa. The executed *ping* commands that initiated between host B and host W produced 10 responses. The data shown indicated that each *ping* initiated a data packet of 32 bytes and had a connectivity time of 123 ms. Following the transmission of 10 packets, testing found a packet loss of zero. Testers executed the test several more times with no errors. A continuous *ping* test was set up for about an hour between host P and W, with continuous responses showing no errors. The reported response time of 123 ms was expected and attributed to latency between CONUS and PAC. Latency caused by a *ping* initiated at a CONUS east coast host, traversing the Backbone Core, passing into the PAC Core to a PAC host. The results from tests indicated that the operation of the base TCP/IPv6 stack was working correctly between the CONUS Backbone Core and external network.

Results of IPv6 Transport Demonstration

Core Network IPv6 Transport Demonstration

Testers administrated a series of tests to demonstrate the Backbone Core's ability to transport IPv6 traffic between two PC/Laptops. Testers executed a *traceroute* test with a maximum limit of 10 hops by initiating the *traceroute* script between host P and host B and vice versa. Tester specified the hop limit, indicating to the hosts, how many routers the packets could pass through before terminating the search. The results displayed the routes the packets took from the source host through to the CONUS Backbone Core, ending at the chosen destination host. The results also showed that the response times for each hop within CONUS were 1 ms. The notation "* * * Request time out" recorded in the results, indicated that no response was received from the Backbone Core routers. This was due to security configurations preventing the CONUS Backbone Core routers from responding to *traceroute* requests. Although the routers were fully functional, they purposely did not respond to the requests. The results appeared normal and indicated that IPv6 packets successfully transported through the Core network.

Core Network IPv6 Transport with External Network Demonstration

Testers executed multiple *traceroute* tests over a maximum of 10 hops via the *traceroute* script between the hosts P, B, and W. The procedures involved hosts P and B, attempting to *traceroute* IPv6 packets over to host W and vice versa. The executed *traceroute* command initiated an IPv6 packet sent from the source host in search of a destination host, while limiting the number of hops to 10. The results showed that the route taken from the source through the CONUS Backbone Core, to the chosen external destination host was successful. The results indicated that for each hop within CONUS, *traceroute* response times were 1 ms while hop times recorded within the external network found to be 123 ms. This expected latency results because packets have to travel across two separate Backbone Cores. As with the CONUS transport test, the notation "* * * Request time out" found in the results, indicated that both the CONUS and PAC

Backbone Core routers were not responding to *traceroute* requests. The results from test appeared normal, indicating that IPv6 traffic crossed separate networks.

Demonstration Completeness

Since the CONUS and PAC Backbone Core routers were not available to respond to user *ping* and *traceroute* queries, testers assessed router performances on each Backbone. Rather than running scripts on the hosts, *ping* and *traceroute* scripts ran on the core routers, directing all requests to neighboring routers. The tests ran on each of the routers connected to hosts P, B, and W. The *ping* tests run on CONUS routers P and B displayed data packets that were 16 bytes with connectivity times fluctuating between 1.22 ms to 84.08 ms. Although data packet sizes were uniform and packet loss was zero, connectivity the latency found within CONUS routers attributed to router proximity. The results indicated a direct relationship between router proximity to the source script and connectivity times. The further away a router was from the source script the longer the connectivity time. When the *ping* test ran on PAC router W, the main difference found between the tests was higher connectivity latency found between the source and its neighboring routers. As with the CONUS test, connectivity latency was attributed to router proximity to one another. To illustrate IPv6 transport between routers, each designated router initiated a *traceroute* script to an affiliated backbone router. In each case the number of hops between the routers was one, indicating directly connected backbone routers.

Conclusions/Recommendations

The results indicated the NIPRNet Core network was fully capable of routing IPv6 traffic. The results showed that IPv6 connectivity and transport through the NIPRNet was consistent with that of IPv4. By showing IPv4 parity, the demonstration successfully met the conditions outlined in the DoD CIO's 9 June 2003 memo, establishing a policy for IPv6 on the NIPRNet.

D.3 IPv6 DNS Phase II Test Report

Testing Organization and Publication Date

DISA
June 26, 2008

Summary

The goal of the test plan was to demonstrate the coexistence of IPv4 and IPv6 Domain Name Service (DNS) functionality within a Wide Area Network (WAN) environment. DNS provided support to IPv4 and IPv6 DNS Resource Record (RR) Sets, name resolution, and reverse lookups. The IPv6 DNS Support Team working in collaboration with the DoD Network Information Center (NIC) developed the DNS infrastructure, simulating NIPRNet's .mil DNS hierarchy. Testers configured devices to route both IPv4 and IPv6 traffic in a dual-stacked approach. Administrators introduced Transaction Authentication (TSIG), a type of authentication key, to the DNS test plan, providing a secure means of transferring DNS zone files. In addition, testers added security features such as IPv6 Capable firewalls, web servers, and traffic monitoring servers, in an attempt to assess IPv6 DNS functionality. Testers deployed and monitored IPv6 at three levels identified by: Root, Top-Level, and Sub-Level Domains (Army, Navy, and NIC) under the WAN environment in an attempt to evaluate and assess IPv6 DNS functionality.

Test and Evaluation Method

Exercise

Joint Staff Operational Criteria Tested

1 (1.1, 1.1.1, 1.2.1, 1.4.1, 1.4.2, 1.5.1)
2 (2.1, 2.3)
3 (3.1)
8 (8.1)

Configuration

Testers replicated the NIPRNet's .mil DNS infrastructure to assess its ability to route IPv6 queries as shown in Figure D-4.

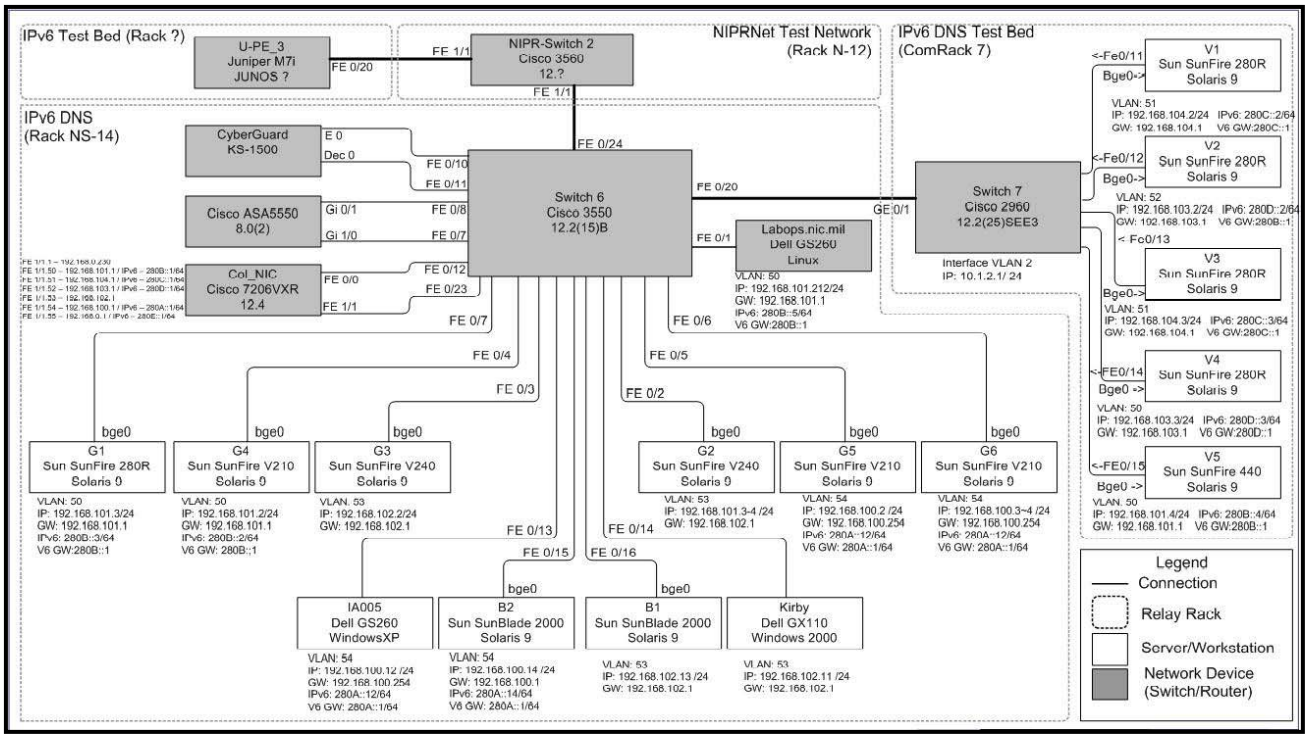


Figure D-4. DNS Test Bed Topology Diagram

General Equipment Listing

- Cisco router 7206VXR 12.4(17)
- Cisco switch 3550 12.2(15) Switch, Switch 6
- Cisco ASA 5550 8.0(2) Sun Solaris, Solaris 9 Servers
- Windows XP Service Pack (SP) 2 Professional
- Linux Ubuntu 7.10 Bind 9.4.1.P1, Apache 2.2.8, NIC .mil DNS server

IPv6 Implementation Procedures

Administrators enabled IPv6 on the Premise Router (Columbus_NIC) to ensure interior and exterior routing supported both native IPv4 and IPv6 routing protocols. This environment mirrored the operational DNS NIPRNet infrastructure managed by the DoD NIC. Administrators added name servers to evaluate the expanded scope of the study. Administrators added a number of these name servers to the existing sub-level domains. This provided queries with an in-depth DNS tree to traverse and the ability to better assess DNS functionality. Testers implemented DNS server configuration changes in Phase II of the test plan. Testers introduced DNS server zone authentication capabilities to determine whether they would have a nominal effect on IPv6's implementation. DNS name server functionality distinguished, dedicated DNS master servers to be authoritative, and DNS slave servers to be caching servers. In an effort to enhance the test plan's security footprint and bolster Information Assurance (IA) capabilities, testers added a number of features. Testers strategically placed an IPv6 Capable firewall to provide a security barrier in front of the TLD.mil DNS server and the Root Server. The addition

of the Web Server and the Traffic Monitoring Server provided a means to run and control the test plan's implementation. Figure D-5 is a logical diagram of the network that was tested.

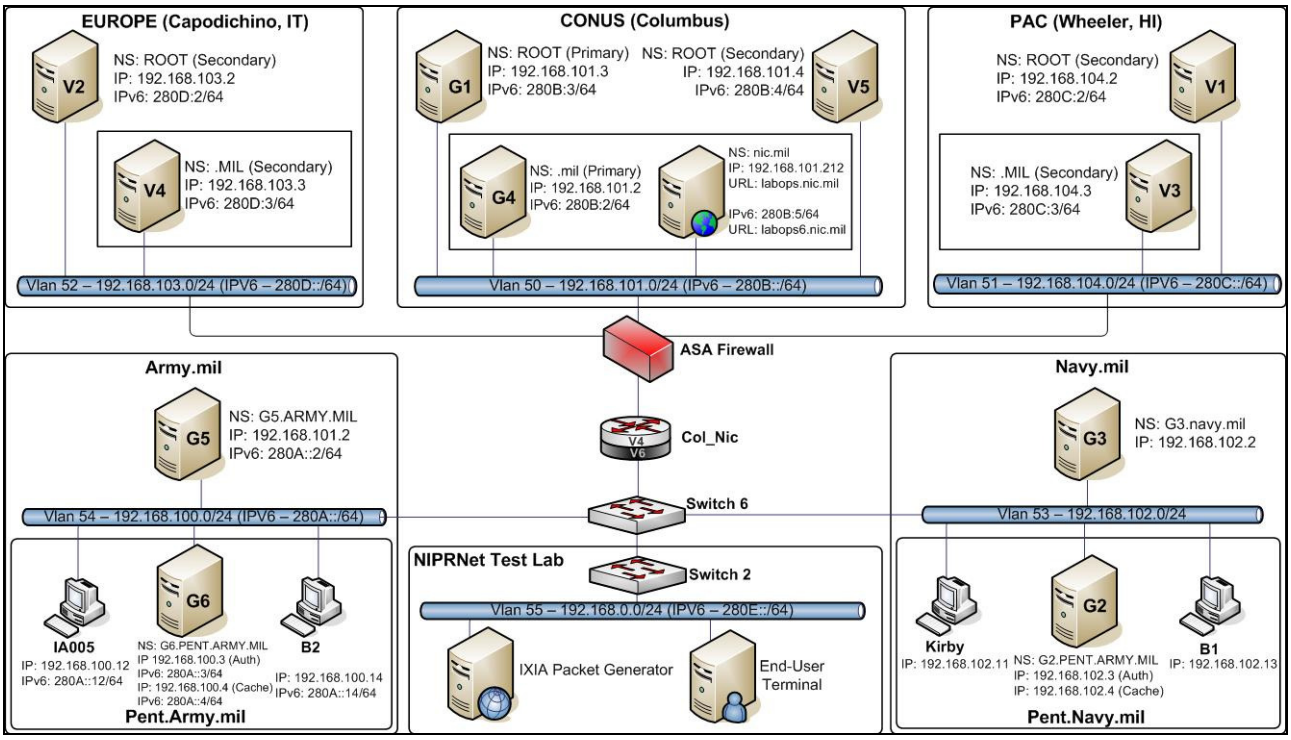


Figure D-5. DNS Test Bed Logical Diagram

Name Spaces

Three domain name spaces used in Phase II contained a series of name servers forming sub-level domains. Testers assigned each of the domain name spaces to different Virtual Local Area Network (LAN) (VLAN), with IPv6 turned on selectively. Testers configured the navy.mil domain name space to utilize only native IPv4 address space.

IPv6 Test Tools (Security Evaluation)

The selected IPv6 Test Tools was a suite of software and/or checklist used to ensure the security level and functionality of network resources within the test network. The test network simulated the operational DISN NIPRNet Core. The IPv6 Test Tools suite consisted of but was not limited to the following:

- NSLOOKUP
- DIG
- Gold Disk

Results

Testers successfully demonstrated zone file transfers using TSIG. The zone files analyzed, showed both IPv4 and IPv6 DNS RR sets successfully transferred. In addition zone transfer log files reflected various server zone transfer attempts, logging all activities.

The results confirmed that in each case the dual-stacked server resolved the specified query type. Both IPv4 and IPv6 DNS queries routed over TCP, providing complete resolutions between the servers.

Testers analyzed the Central Processing Unit (CPU) utilization baseline with the same amount of native IPv4 queries in trial number 1 and native IPv6 queries tested in trial number 2. The combined IPv4 and IPv6 dual-stacked queries testing culminated during trial numbers 3 and 4. The Distributed Denial of Service (DDoS) attack took place during trial number 5, the CPU utilization level shows about the same CPU performance range as monitored in trial numbers 3 and 4. However, in observing the server's CPU activities each servers began swapping between CPU0 and CPU1 extremely rapidly, which indicates a sign of a server under attack. Eventually this rapid swapping state would cause the G-Root server to deny service.

Testers configured DNS forward-queries on .mil production servers to field around 6,000 queries per minute; Trial 1 used native IPv4 queries, with trial 2 using native IPv6 queries. In both cases, the CPU utilization appeared negligible. When the DNS traffic load doubled, combining IPv4 and IPv6 interfaces as with trial 4, the CPU utilization doubled with linear proportionality. When testers subjected the server to the DDoS attack, in trial 5, the CPU utilization level almost tripled compared with trial 4.

The results indicated that the .mil DNS server's (*G4*) CPU utilization increased substantially once the server encountered a large amount of bogus queries. In third time interval which represents the beginning of the simulated DDoS attack, the server appears to labor considerably, doubling its CPU utilization during the attack. In observing the results there appears to be a linear correlation between CPU utilization and the number of queries presented to *G4*. Testers generated more bogus queries and sent the queries to *G4*, causing CPU swapping. This continued through the fourth time interval trials, however, it did not actually cause *G4* to deny service.

From the test results the *G-Root* appeared to be having a difficult time addressing normal IPv4 and IPv6 traffic flows. With CPU utilization above 50 percent the *G-Root* server did not seem to have the capacity to address additional traffic. At the third and fourth time intervals, simulating a DDoS attack, the *G-Root* server's CPU utilization slightly increased by three percent. This was unusual because unlike the other cases, *G-Root's* utilization did not appear to be proportional to the amount of DNS queries and did not spike. The CPU did however begin to swap back and forth between CPU0 and CPU1, eventually resulting in a Denial of Service (DoS) to incoming traffic.

Conclusions/Recommendations

Testers decided during the testing period, to work on a low cost, practical, yet effective method to curtail possible attacks against the *G-Root* and TLD .mil Servers. The best method was to incorporate Access Control Lists (ACL) at the ingress interface on the NIPRNet Premise Router, the proposed DNS Edge Router, or the IPv6 compatible firewall. The ACL proved to be vitally effective in filtering out known sources behind the mock attacks during test trials simulating pre and post transition scenarios. However, as requirements for IPv6 increase the logistical challenges in the production environment, to manage dedicated resources for distinguishing and restricting multiple sources behind such attacks, may prove beneficial but unrealistic.

Testing during both Phase I and Phase II demonstrated that DNS was able to operate successfully within a native IPv4, IPv6, and/or dual-stacked environment. In testing the basic concepts behind a resolver forwarding a query to a DNS server for a response, the observed process uniquely yet independently worked with minimal configuration enhancements. The server accepted queries, conducted lookups and forwarded response resource records to hosts, regardless of the selected protocol. Complexities that involve protocol selection and transport remain specific to the host rather than the DNS server.

The tests conducted by the DNS Support Team attempted to cover several design considerations and operational requirements, identified by various internal support divisions and outside agencies. Testers addressed and thoroughly tested each concept that fell within the scope of DNS services, relating to IPv6, with the exception of application-based protocol selection and DNS Security.

Testers analyzed mitigation-capable devices that included firewalls, network security devices, and software-based products for compatibility. Several vendors have provided demonstrations and presented IPv6 protection solutions that detect and thwart network security threats such as NX Domain DDoS attacks. These tools would be ideal in automating and protecting DNS servers by incorporating deep packet inspection polices within future security design models. Such concepts would prove effective in providing a more granular inspection of malicious IPv6 packets. After researching most product offerings, the tools were either still undergoing developmental testing or were not scheduled to support advance IPv6 policy filters until late 2008 or early 2009.

D.4 IPv6 Multicast Test Report

Testing Organization and Publication Date

Space and Naval Warfare Systems Center
August 28, 2008

Summary

Multicast protocols and IPv6 route summarization together have great potential for conserving bandwidth, a 'must' on constricted Radio Frequency links. Together with stateless autoconfiguration, these improve scalability of a network architectures and reduce an administrative requirement; autoconfiguration enabled nodes conFigure D-their own IPv6 address automatically, plug-and-play fashion. Our main goal was to provide a proof-of-concept IPv6 multicast implementation and qualify its benefits in the Navy IPv6 architecture.

Test and Evaluation Method

Demonstration

Joint Staff Operational Criteria Tested

2 (2.3)
4 (4.1, 4.1.1.2.1, 4.1.1.2.2, 4.1.2)
5 (5.1, 5.1.1.2.1, 5.1.1.3.1.1, 5.1.1.4.2.1)
6 (6.1, 6.1.1.1, 6.1.2.2)
8 (8.1)

Configuration

Figure D-6 illustrates a typical single-domain multicast architecture which consists of a Network Operations Center (NOC) serving two ships. In this example, the Navy assigns the entire prefix 2080:10::/28 to the NOC, which in turn assigns the entire prefix 2080:13:40::/42 to ship 1 and prefix 2080:14:80::/42 to ship 2. Realistically, there should be an additional Community of Interest (COI) or so-called enclave router, which provides the interface between the Automated Digital Network System (ADNS) router and the various enclaves on each ship. The enclaves/COIs are defined as the local networks on the ship, and would each normally exist behind High Assurance IP Encryptors (HAIPE). Without the HAIPE devices in our architecture, the single enclave/COI considered General Service operating at secret classification level. In this case, ship 1 should assign the prefix 2080:13:41::/48 to its enclave, and ship 2 assigns the prefix 2080:14:81::/48 to its enclave. Due to limited of resources, we did not include the enclave/COI router; however, this should not have impacted our test in any significant way. The enclave LAN on ship 1 is assigned a 2080:13:41::/64 prefix, and the enclave LAN on ship 2 is assigned a 2080:14:81::/64 prefix. Figure D-6 shows the single domain multicast diagram used in testing.

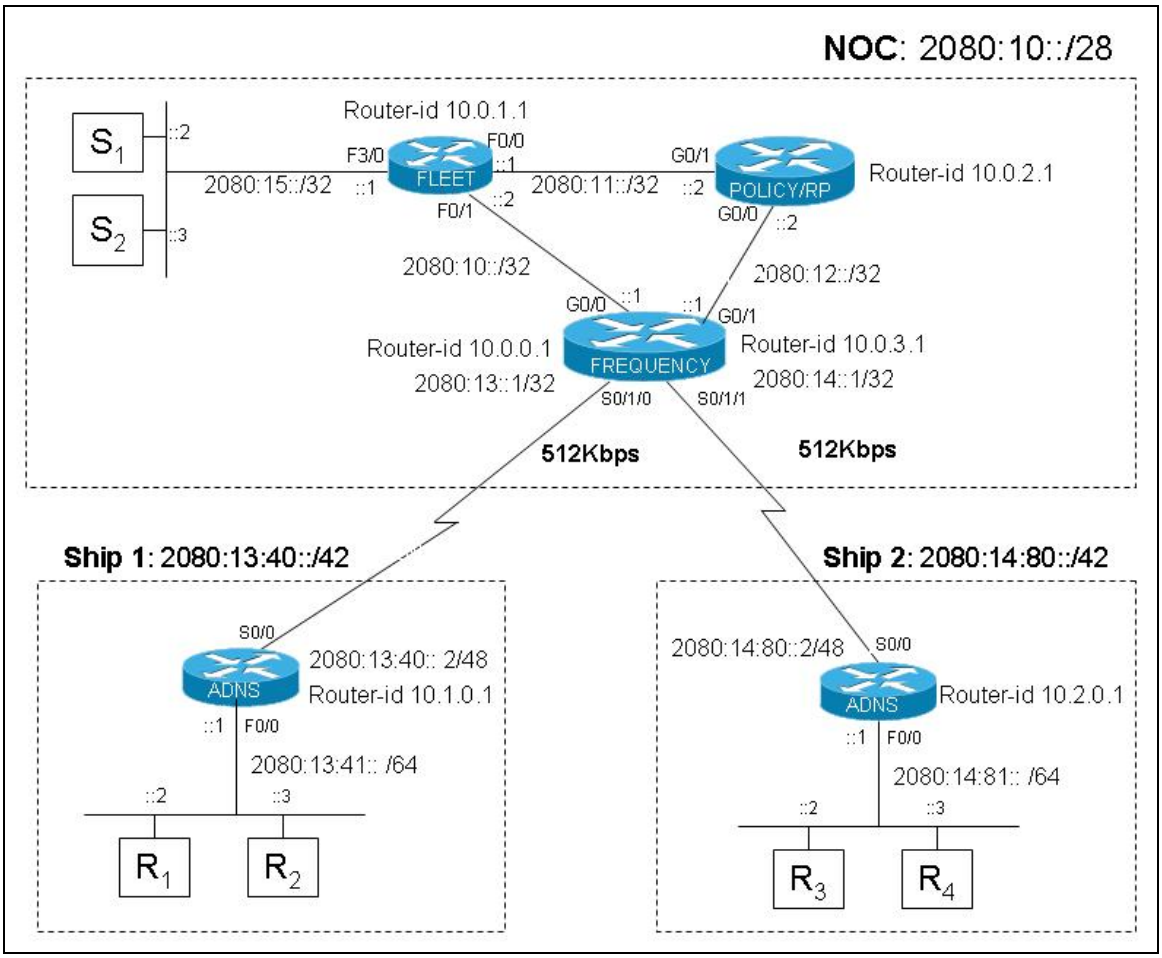


Figure D-6. IPv6 Single Domain Multicast

Figure D-7 illustrates a typical inter-domain multicast architecture consisting of two NOCs each serving a ship in its own operating domain. In this example, NOC 1 assigns the prefix 2080:13:40::/42 to ship 1, and NOC 2 assigns the prefix 2080:21:80::/42 to ship 2. Ship 1 then assigns the prefix 2080:13:40::/48 to its enclave, and ship 2 assigns the prefix 2080:21:80::/48 to its enclave. As aforementioned, there should be an additional COI router, providing an interface between the ADNS router and each enclave on the ship, but again it was not included due to resource limits.

Each Enclave then assigns /64 address blocks to 65,536 subnets. Users and applications would reside on these individual subnets. The ADNS router on each ship summarizes the prefix /64 as a single /42 prefix and advertises it to its respective NOC, where the Policy router then summarizes the /42 prefix as its own /28 prefix and only announces the aggregated /28 prefix across domain to the peering NOC. Thus, completed route aggregation achieved to prevent IPv6 route explosion on the Navy networks.

The Multiprotocol Extensions for BGP Version 4 [8], also called Multiprotocol BGP, is an inter-domain multicast routing protocol that enables multicast routing policy to connect multicast

topologies within and between BGP autonomous systems. Section 5.5 provides detailed descriptions of IPv6 multicast operating over inter-domain network architecture.

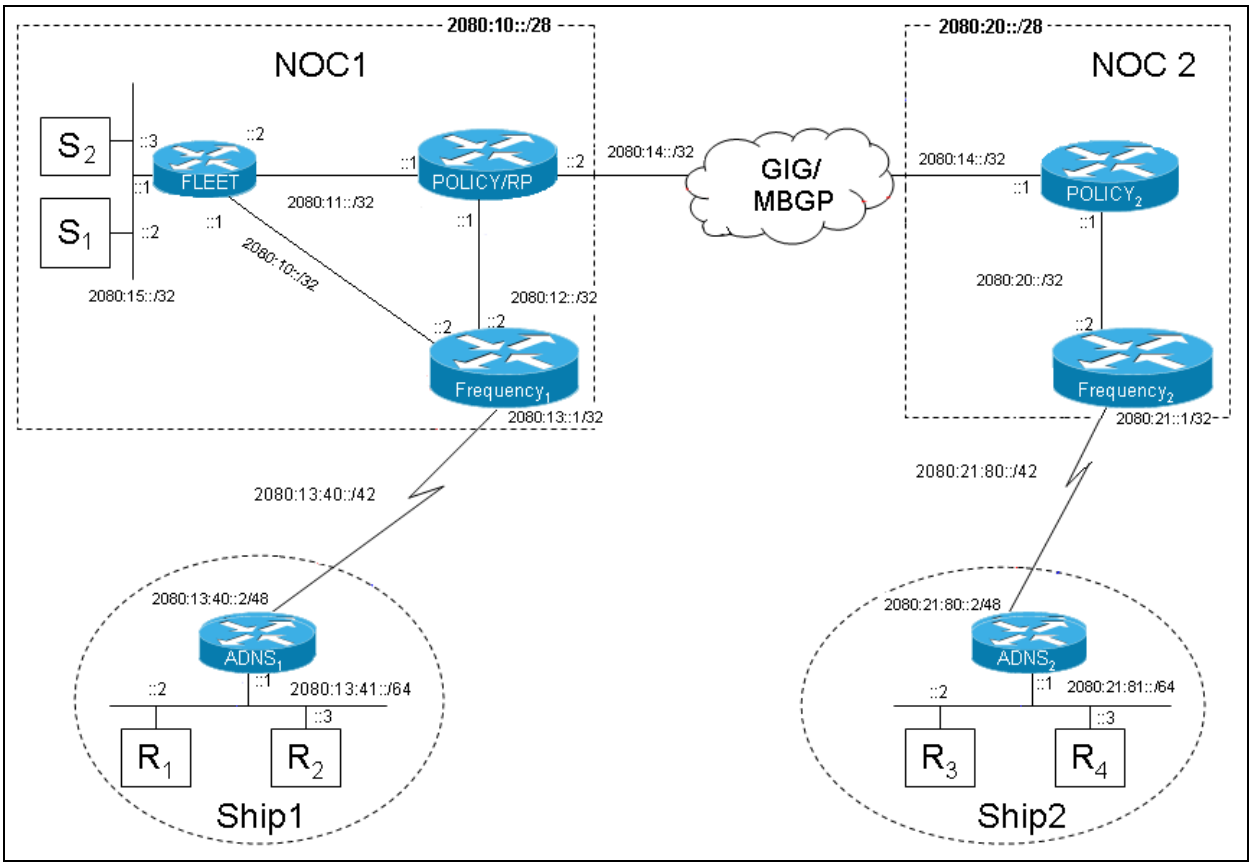


Figure D-7. IPv6 Inter-Domain Multicast

Results

The processes successfully tested are:

- Stateless autoconfiguration
- Neighbor Solicitation
- Neighbor Advertisement
- Router Solicitation
- Router Advertisement
- IPv6 Stateless Autoconfiguration
- Reach ability Verification
- Unicast and Multicast Comparison
- Unicast Testing and Multicast Testing
- Multicast Comparisons
- Single Source – Multiple Groups Multicast
- Multiple Sources – Multiple Groups Multicast

- Protocol Independent Multicast (PIM) – Sparse Mode (SM) (PIM-SM) Testing source/SHORTEST PATH TREE
- PIM – Source Specific Multicast (SSM) (PIM-SSM) Testing
- Inter-Domain IPv6 Multicast Testing
- Route Summarization
- Inter-Domain Multicast PIM-SM
- Inter-Domain Multicast PIM-SSM

Conclusions/Recommendations

Our results showed significant bandwidth savings using multicast, when compared to unicast, and especially so when the number of receivers increased. Therefore, multicast optimized overall bandwidth requirements and mitigated bandwidth limitations present in the network infrastructure.

We found similar performance between PIM-SM and PIM-SSM. The PIM-SSM is better for single source transmission such as (video) broadcasting. PIM-SSM uses the reserved address range FF3x::/32 for multicast groups, and uses Multicast Listener Discovery (MLD) Version 2 (MLDv2) for group membership registration. Unless specified, the Cisco routers will run MLDv2 by default, which is backward compatible with MLD Version 1 used by PIM-SM.

The test showed only a single Rendezvous Point (RP) router is needed for a given global group across multiple (two in our test) PIM-SM domains. We configured the RP statically, and we recommend this approach, since it is simple and convenient. PIM-SSM can support interdomain multicast without the need of the RP; however, the decision whether to choose PIM-SM or PIM-SSM depends on the applications, network architecture design, and security requirements. The PIM-SM and PIM-SSM can co-exist to complement each other in providing scalable and flexible network architecture.

Use of the Navy IPv6 addressing scheme to reduce routing overhead and prevent IPv6 route explosion was verified through the use of “show IPv6 route bgp” command on BGP routers. Routes were shown to be summarized as a single aggregated prefix at the highest level of the address space (e. g., /28 at each NOC), and only then advertised across domain to the peering NOC or Autonomous Systems. Also, the stateless autoconfiguration mechanism’s default use of the Extended Unique Identifier-64 (EUI-64)’s 64 bits as the host portion of a global IPv6 address was proved a straightforward operation; however, it did require IPv6 hosts to operate on a subnet that assigned a /64 prefix in order to work properly.

Finally, the proof-of-concept IPv6 networks consistently operate according to the Internet Engineering Task Force (IETF) RFC specifications of the IPv6 protocols under test, and we have proved this using the Wireshark protocol analyzer. Our results strongly show that IPv6 multicast, stateless autoconfiguration, and route summarization can be implemented in Navy IPv6 networks to improve scalability, performance, and conserve bandwidth, while reducing configuration needs.

In conclusion, testers successfully demonstrated the proof-of-concept of certain IPv6 features as working consistently with their IETF RFC specifications using the Wireshark network protocol analyzer. Results showed that stateless autoconfiguration, IPv6 multicast and route summarization can be implemented as part of the Navy's IPv6 transition to optimize Navy network designs and performance, and as useful bandwidth conservation techniques.

D.5 ITA IPv6 Client and Server Application Test

Testing Organization and Publication Date

Information Technology Agency (ITA)
September 18, 2008

Summary

Milestone Objective 3 (MO3) is an important step for the DoD to begin operational use of IPv6. MO3 will allow IPv6 traffic to flow within the DoD networks, which will require interoperability of many different operating environments. This report describes the steps taken to test the various MO3 scenarios as indicated in the MO3 testing support document provided to ITA. The tests will focus on the specific client and server applications listed in this document.

Test and Evaluation Method

Demonstration

Joint Staff Operational Criteria Tested

2 (2.1, 2.3)
3 (3.1, 3.2, 3.3, 3.4)

Configuration

The testing focused on verifying the IPv6 functionality of the applications listed in Table D-5.

Table D-5. MO3 Targeted Set of Applications

Applications
File Transfer Protocol (FTP)
Network File System (NFS)
Hypertext Transfer Protocol (HTTP) / Hypertext Markup Language (HTML)
Network Time Protocol (NTP)

Since most applications rely on DNS to resolve hostnames, the testing environment will utilize a dual-stacked Infoblox DNS server for this purpose. The DNS server only contains Authentication, Authorization, Accounting, and Auditing (AAAA) records since the application tests focused on IPv6 communication only. If the dual-stack client successfully communicates with the DNS server, it should return the appropriate IPv6 address that the application can use to contact the server. Figure D-8 depicts the test environment that tested the various IPv6 applications.

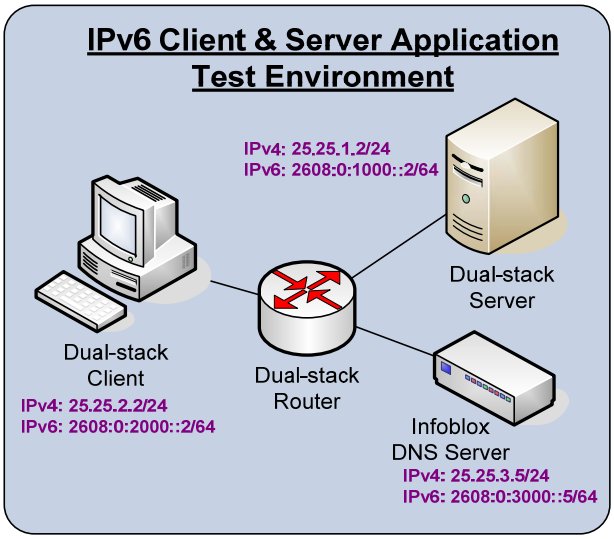


Figure D-8. Lab Test Environment

The test environment represented a transitional network environment where dual-stack is the selected IPv6 transition mechanism.

File Transfer Protocol (FTP)

For this test, the FTP server was a Linux Fedora 9 server running FTPd, both Windows and Linux Ubutnu 7.10, and Fedora 9 were dual-stacked clients. Using different clients allowed testing of different versions of FTP in order to verify compliance with RFC 2428.

Network File System (NFS)

NFS is a protocol originally developed by Sun Microsystems to provide transparent remote access to shared files across networks. RFC 3530 provides the all the details of this latest version, including the use of IPv6 with the protocol.

Hypertext Transfer Protocol (HTTP)

HTTP is an application-level protocol used on the Internet for transfer of information. Testers chose HTTP/1.1 since this version is today's predominant protocol. Testers analyzed both Apache and Microsoft Internet Information Services (IIS) to ensure that HTTP clients can successfully retrieve Hypertext Markup Language (HTML) pages over IPv6. Testers chose various web browsers including Internet Explorer, Mozilla Firefox, and Google Chrome for testing. The HTML pages included IPv6 links to ensure that the web browser can successfully access linked images and websites.

Network Time Protocol (NTP)

The purpose of running NTP is to synchronize all the system clocks in a given network. It uses User Datagram Protocol (UDP) as its transport protocol on port 123. For this test, NTP ran over

IPv6 to verify its functionality. The test environment remained the same as depicted in Figure D-8. The Fedora 9 server will serve as the NTP server for the test network. The Windows and Linux clients will attempt to synchronize their system clock with the Fedora NTP server.

Results

FTP

The test results proved that FTP successfully utilized IPv6. Table D-6 lists the unsuccessful results.

Table D-6. IPv6 Compatibility of Various FTP Applications

FTP Client	Operating System	Result	Comments
WinXP FTP	Windows XP SP2	Unsuccessful	Does not support IPv6 – Received error message: "FTP connect: Unknown error number"
SmartFTP	Windows XP SP2	Partially successful	Cannot connect using hostname because it never queries for AAAA record, but can use IPv6 address instead of hostname to connect.
Vista FTP	Windows Vista	Successful	No problems found.
Ubuntu FTP	Ubuntu 7.10	Unsuccessful	Does not support IPv6 – Received error message: "FTP: fedorapc. lab.pentagon. mil: Unknown host. " Using the IPv6 address instead of the hostname does not work either.
Command-Line FTP	Ubuntu 7.10	Successful	No problems found.
Fedora FTP	Fedora 9	Successful	No problems found.

Testers found some noncompliant RFC 2428 FTP applications. The standard FTP client on Windows XP and Ubuntu Linux 7.10 did not support IPv6 addressing. However, administrators can use third-party FTP applications on these operating systems to connect to IPv6 FTP servers. Our tests did not find a suitable IPv6 FTP client for Window XP. Testers found SmartFTP only partially successful in Table D-6 because it was able to connect to the IPv6 FTP server using its IPv6 address, but could not use DNS to obtain the AAAA record for the hostname. On the other hand, Command-Line FTP on Ubuntu, along with the standard FTP clients on both Windows Vista and Fedora Linux 9, fully support IPv6.

NFS

When setting up the Fedora NFS server, the '/etc/exports' file required a list of the folders being shared and the clients authorized to mount them. After specifying the necessary information using IPv6 addresses for the clients, the 'exportfs' command was run to maintain the current table of NFS exported file systems. This generated an error because it would not accept an IPv6 address as the authorized client. Next, the IPv6 address was replaced with the hostname of the client, but this was not accepted either. Additionally, the output of the nslookup command proved the DNS server is able to resolve the client hostname.

The packet captures revealed that the 'exportfs' command only queried the DNS server for A records, and not for the AAAA of the given hostname. Additionally, the Linux client could not specify an IPv6 address with the 'mount' command. The mount command also queries for the A record only. To ensure the NFS configuration was correct, the same NFS configuration

successfully tested using IPv4. This shows that the current versions of NFS commands do not support IPv6.

HTTP

The test results proved that HTTP clients successfully communicated over IPv6 to both Apache and Microsoft IIS web servers. All web browsers behaved identically when obtaining the HTML information from the IPv6 server, although there were some minor differences in the way they queried the DNS server.

NTP

Test results showed that both ntpdate and ntpd supported IPv6 on the Linux hosts. It was clear the NTP client used IPv6. Similarly, the NTP daemon was also able to update the system clock using the IPv6 NTP server. Since the daemon runs in the background, no output exists, but the updated time along with the packet capture verified that it worked properly over IPv6.

Table D-7 summarizes the results from the NTP testing:

Table D-7. IPv6 Compatibility of Various HTTP Applications

IPv6 Application	Operating Systems			
	Windows XP SP2	Windows Vista	Ubuntu Linux 7. 10	Fedora Linux 9
NTP	FAIL*	☑	☑	☑

** Windows XP host could not utilize the built-in NTP client to query the NTP server using IPv6. It never queries for the IPv6 record, and it cannot use the server's IPv6 address instead of the hostname in the NTP configuration. A third party NTP application should solve this problem, but none were available in the ITA lab.*

Conclusions/Recommendations

The ITA testing revealed that IPv6 support is present in many client and server applications. Since IPv6 is an add-on to the Windows XP operating system, the IPv6 client applications running on XP experienced more issues than any other operating system. It does not seem feasible to have Windows XP end-users in an IPv6-only environment since they cannot query an IPv6-only DNS server. Windows Vista and Linux operating systems will be necessary to completely transition from a dual-stack to an IPv6-only network. However, as seen during the NFS testing, not all applications are fully IPv6-compliant, so a dual-stack network will be required until the majority of applications fully support IPv6

D.6 ITA MO3 IPv6 DNS & Interoperability Test Plan & Report

Testing Organization and Publication Date

ITA
June 23, 2008

Summary

MO3 is an important step for the DoD to begin operational use of IPv6. MO3 will allow IPv6 traffic to flow within the DoD networks, which will require interoperability of many different operating environments. This report describes the steps taken to test the various MO3 scenarios as indicated in the MO3 testing support document provided to ITA. The tests will focus on the DNS and interoperability scenarios outlined in the document.

Test and Evaluation Method

Demonstration

Joint Staff Operational Criteria Tested

2 (2.1, 2.3)
3 (3.1, 3.4)
8 (8.1)

Configuration

The test focused on two main areas – DNS-only and IPv4/IPv6 interoperability. The DNS-only test required configuration of DNS servers capable of handling requests for IPv4 and IPv6 records. In previous DNS testing at ITA, testers verified the Berkeley Internet name Domain (BIND) version used at that time (9.3.2) supported the AAAA IPv6 records. Testers used BIND 9.5 during this DNS-only testing. Additionally, testers introduced Microsoft DNS into the test environment to check for any IPv6 compatibility issues. Testers chose Apache and Microsoft web servers to determine any differences in the way the web clients resolve their Uniform Resource Locator via DNS.

The IPv4/IPv6 interoperability testing initially dealt with a targeted set of applications to determine operations in IPv4-only, IPv6-only, and dual-stack environments. The applications contacted their respective DNS servers to resolve the destination hostnames. When contacting the DNS servers, if a given hostname contained IPv4 and IPv6 records, the specific application and/or operating system determined the address to use based on its configured rule set. The final interoperability test determined the best method of transitioning from an IPv4-only environment to an IPv6-only environment without breaking operational capability.

Results:

Testing RFC 4074

The test results showed the DNS server did not misbehave as indicated in RFC 4074. The Response Code (RCODE) received for each of the test scenarios was as expected. Additionally, the web browser successfully resolved the hostname containing only an A record, even though it queried for the AAAA record first. This proved the DNS server did not send an inappropriate response to the initial AAAA query, causing it to fail.

DNS Reachability

The Windows XP SP2 client could not resolve hostnames using IPv6. Windows XP provides a "netsh" command to conFigure D-an IPv6 DNS server, but tests showed the client never used this address for DNS queries. Without a defined IPv4 DNS server, all of the DNS requests failed even with a configured IPv6 server. Therefore, testers replaced the client with a Windows Vista PC when sending IPv6 DNS queries.

Although Windows Vista queried over IPv6, the "nslookup" command defaults to IPv4. However, issuing the nslookup "server" command followed by the IPv6 address of the DNS server fixes this issue. Even if testers removed the IPv4 DNS server address from the network configuration, nslookup does not use the IPv6 DNS address configured by default. However, applications such as Internet Explorer successfully use the IPv6 DNS address configured in Windows Vista.

The forwarding BIND DNS server successfully received requests over IPvx and resolved them over IPvy. Since the authoritative server does not have an AAAA record for this domain, it sends a no error response (also seen during the RFC 4074 testing). The DNS server then attempts to resolve this domain via an IPv4 record and successfully receives the A record.

DNS Records: Shared or Unique?

This test utilized the Windows XP SP2 client running Internet Explorer 7 as the host generating the DNS query. The tests showed the transaction times for resolving the AAAA and dual-stack hosts were about the same. The reason for the increased response time for the A record is because XP prefers IPv6 over IPv4, it first tries to obtain an AAAA record before querying for an A record. This causes a minor delay in the DNS resolution for the IPv4-only hostname.

Table D-8. DNS Transaction Times for Host Resolution

Query Type	Transaction Time
apache-vista4. lab.pentagon.mil (A record)	1.191 ms
apache-vista6. lab.pentagon.mil (AAAA record)	0.279 ms
apache-vista6. lab.pentagon.mil (dual records)	0.427 ms

Although Table D-8 shows a delay in the A record hostname resolution, this is only a minor issue, since the magnitude of this is less than 1 ms. The major drawback of using separate

hostnames for IPv4 and IPv6 is the host cannot fallback to the secondary protocol if the interface with the primary protocol failed. Testers removed the IPv6 address on the web server itself, leaving the AAAA record in the DNS database. The host once again attempted to resolve the AAAA hostname first, and when it received a successful reply, it attempted to connect to the IPv6 address. When the TCP connection failed because of the missing IPv6 address, it used the IPv4 address and successfully connected to the web server. The root hints file for the DNS servers also use shared DNS records when defining the IP addresses for the 13 Internet root server groups.

IPv4/IPv6 Interoperability Testing

As expected, the IPv4-only client could not contact the IPv6-only client and vice versa. The failures in these cases did not cause the application to hang.

Address Selection with Dual DNS Records

The applications shown in Table D-9 and Table D-10 took the operating system's preference when querying the DNS server and connecting to the destination server.

Table D-9. Address Selection for Windows Applications

Windows XP, 2003, and Vista

Application	Protocol Preference
Internet Explorer 7	IPv6
FireFox 3	IPv6
FTP	IPv6

** The only difference with Windows Vista versus the other Windows platforms is that it queries for the A record before the AAAA record, but it still prefers IPv6 over IPv4. Additionally, the Windows Vista applications query the dual-stack DNS server via IPv6 first, then IPv4.*

Table D-10. Address Selection for Linux Applications

Fedora 9 and Ubuntu 7.10 Linux

Application	Protocol Preference
FireFox 2	IPv6
FTP (Fedora only)	IPv6

** The Linux applications query the dual-stack DNS server via IPv6 first, then IPv4.*

Transition Walkthrough Test

The results from the test case verified the best approach to transitioning from IPv4-only to IPv6-only, utilizing a dual-stack intermediate period. The reasoning behind the recommended transitioning approach will be determined after all the previous tests are completed.

Conclusions/Recommendations

Based on the results, dual-stack clients and servers communicate with each other via either protocol. For the applications tested, the operating systems determined the protocol preference. A slight delay exists when a client was dual-stacked enabled, but did not communicate using IPv6. The tests have also shown the DNS servers do not need to be dual-stacked to resolve AAAA queries from the clients. However, even though the DNS servers do not need to be dual-stacked to transition to an IPv6-only network, dual-stacking of DNS servers must take place. This is the only way true native IPv6 communication can take place. Dual-stacking the network will not break operational capability, but may introduce new security vulnerabilities for the network.

D.7 Test Plan (JCS) Criteria 4 Testing

Testing Organization and Publication Date

Navy Project Office
June 11, 2009

Summary

The end state of this specific laboratory testing is to successfully demonstrate the following segments of Joint Staff Operational Criteria 4: 4.1.1.1, 4.1.1.2, 4.1.1.3, 4.1.1.5, 4.1.1.6, and 4.1.1.7. Segments 4.1.1.1 through 4.1.3.1, 4.1.3.2, and 4.1.3.3 cover Quality of Service (QoS) capabilities of IPv6 networks using Differentiated Services (DiffServ). Segments 4.1.1.5 through 4.1.1.7 cover QoS capabilities of IPv6 using Resource ReSerVation Protocol (RSVP). Specifically, the objectives of this demonstration are three fold. The first objective is to demonstrate that IPv6 supports Session Initiated Protocol (SIP) to setup the transport Voice, Video, and Data traffic over independent and shared IPv6 environments. The second objective is to modify the first objective and add end-to-end security with IP Security (IPsec) based encryptors to verify if SIP can work end-to-end on a secure IPv6 network. The third objective is to compare the performance of SIP over IPv4 and IPv6 based environments.

Test and Evaluation Method

Demonstration

Joint Staff Operational Criteria Tested

1 (1.1, 1.2, 1.3)
2 (2.1, 2.3)
3 (3.1, 3.2, 3.3)
4 (4.1)
5 (5.1.1)
8 (8.1, 8.2)

Configuration

This test will access the proposed Global Information Grid (GIG) DiffServ Code Points (DSCP) Assignments as DiffServ is the basis of the GIG QoS architecture. The IP packets generated by the GIG applications and systems will be marked by either end user applications or edge networks based on a standard code point table to indicate the desired service class and possibly precedence level to the GIG networks. GIG standard QoS classes establish a base for consistent expectation of a set of services provided by the GIG transport End to End (E2E) in terms of forwarding behavior and performance objectives. To ensure E2E QoS interoperability, a set of DSCP needs standardization for the GIG service classes across the GIG. Table D-11 provides a DSCP assignment scheme proposed by the GIG QoS Working Group for the GIG.

Table D-11. DSCP Assignment Scheme

Per Hop Behavior (PHB)			DiffServ Code Point (DSCP)	IP Precedence	
Assured Forwarding		**Low Drop Probability**	**Medium Drop Probability**	**High Drop Probability**	
	Class 1	AF11	AF12	AF13	1
		001010	**001**100	**001**110	
	Class 2	AF21	AF22	AF23	2
		010010	**010**100	**010**110	
	Class 3	AF31	AF32	AF33	3
		011010	**011**100	**011**110	
	Class 4	AF41	AF42	AF43	4
		100010	**100**100	**100**110	
Expedited Forwarding		**101**110			
DSCP	**Binary**	**Decimal**			
Default	000000	0			
CS1	001000	8			
AF11	001010	10			
AF12	001100	12			
AF13	001110	14			
CS2	010000	16			
AF21	010010	18			
AF22	010100	20			
AF23	010110	22			
CS3	011000	24			
AF31	011010	26			
AF32	011100	28			
AF33	011110	30			
CS4	100000	32			
AF41	100010	34			
AF42	100100	36			
AF43	100110	38			
CS5	101000	40			
EF	101110	46			
CS6	110000	48			
CS7	111000	56			

The test report lists detailed procedures for the following test cases. Test cases also list the Applicable Criteria Decompositions.

- Test Case For Diffserv Concept And Performance Verification Demonstration (4.1.1.1 and 4.1.1.3)
- Test Case for RSVP Concept and Performance Verification Demonstration (4.1.1.5 and 4.1.1.7)
- Test Case for RSVP Extension for the Reduction of Bandwidth of Reservation Flow (4.1.1.6)
- Test Case for SIP Session Signaling Concept and Performance Verification Demonstration (4.1.3.1 and 4.1.3.3)
- Test Case for SIP E2E Security between IPv6 Networks (4.1.3.2)
- Test Procedure
- Test Case for Real Time Protocol (RTP) Transport Control Concept and Performance Verification Demonstration (4.1.2.1 and 4.1.2.2)

Conclusions/Recommendations

Test Case for Diffserv Concept and Performance Verification Demonstration (4.1.1.1 and 4.1.1.3)

- Pass criteria equal IPv6 Video Teleconferencing (VTC) quality equivalent to IPv4.
- Performance metrics at close parity between IPv4 and IPv6.

Test Procedure to Mark and Prioritize Traffic Based On Various QoS Strategies and Policies

- RSVP reserves bandwidth in an IPv6 environment.
- Performance metrics at close parity between IPv4 and IPv6.

Test Case for RSVP Concept and Performance Verification Demonstration (4.1.1.5 and 4.1.1.7)

- Endpoints negotiate a new lower bandwidth that falls at or below the specified new bandwidth maximum allocated by the network.

Test Case for RSVP Extension for the Reduction of Bandwidth of Reservation Flow (4.1.1.6)

- Pass criteria equals SIP working in an IPv6 environment.
- Performance metrics at close parity between IPv4 and IPv6.

Test Case for SIP Session Signaling Concept and Performance Verification Demonstration (4.1.3.1 and 4.1.3.3)

- Pass criteria equal successful VTC call over Virtual Private Network (VPN) tunnel.

Test Case for SIP E2E Security between IPv6 Networks (4.1.3.2)

- Pass criteria equal successful VTC call over VPN tunnel.

Test Case for RTP Transport Control Concept and Performance Verification Demonstration (4.1.2.1 and 4.1.2.2)

- RTP in coordination with RTCP gathers control statistics in IPv6 environment.
- Performance metrics at close parity between IPv4 and IPv6.

ITA recommends that IPv6 packets be marked with DiffServ code that simulates the GIG DiffServ policy. RFCs 2475, 2205, 2207, 2210, 2750, 4495.

D.8 Juniper ISG 2000 Firewall Internet Protocol Version Six Test Report

Testing Organization and Publication Date

National Security Agency (NSA)
August 12, 2008

Summary

The T&E objective that this report supports is the functional demonstration of the Joint Staff Operational Criteria; specifically Criterion 1. This test assesses the conformance, functionality, and performance of the Juniper ISG 2000 Firewall.

Test and Evaluation Method

Demonstration

Joint Staff Operational Criteria Tested

1 (1.1.1, 1.2.1, 1.3.1, 1.4.1, 1.4.1, 1.6.1)
2 (2.1, 2.3)
8 (8.1)

Configuration

Testers developed the ISG 2000 test configuration to emulate a realistic enclave boundary device on an operational network while remaining in a controlled non-operational environment. Traffic and Threat generators were used in-line with actual clients and servers to provide a test environment as operationally realistic as possible for testing IA devices. The diagram illustrated in Figure D-9 is an example of a test scenario used in completing the ISG 2000 evaluation.

The Interoperability Test Plan (ITP) defines the test procedures to evaluate the conformance, functionality, and performance of IA devices. It includes 51 procedures to fully evaluate the firewall requirements in the ITP. The conformance section met by a LoC provided by Juniper Networks addresses their private testing of RFC conformance. The functional testing of the ISG 2000 included evaluation of eight functional areas. Testers assessed performance in accordance with the ITP.

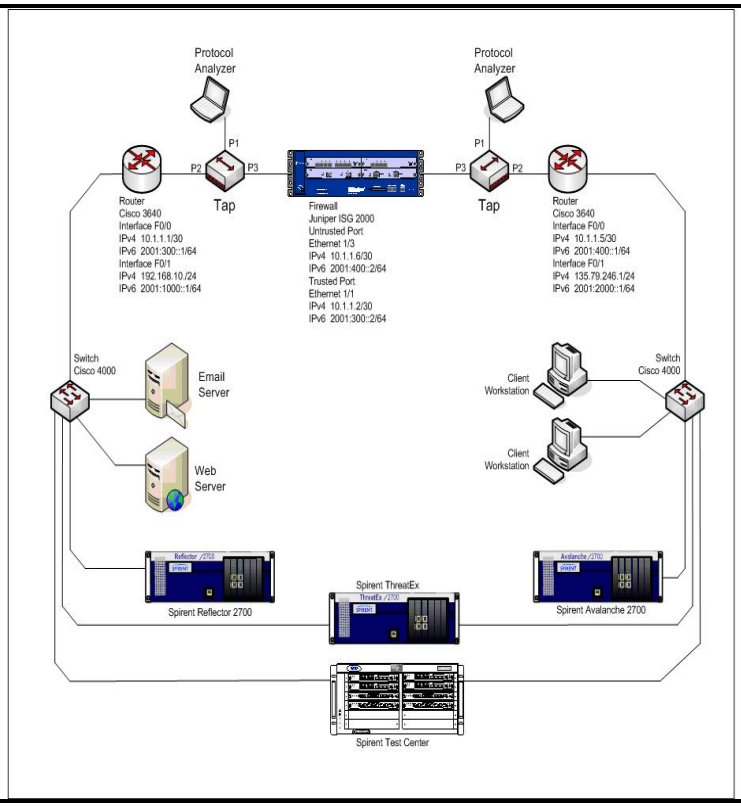


Figure D-9. IPv6 Test Configuration

Results

Conformance

Juniper passed 16 out of 20 RFC conformance requirements. They were lacking in Stateless Address Auto-configuration (SLAAC), IPsec Policy Management, and Internet Key Exchange (IKE) V 2. For SLAAC, they only implement section 5.5 of the RFC. For IKE, they support V 1 for both IPv4 and IPv6, but they only support V 2 on their IPv4 protocol stack.

Confidentiality/Integrity/Availability Triad

The ISG 2000 passed 31 of 32 Confidentiality, Integrity, and Availability requirements for a 97 percent success rate. The ISG 2000 failed only the requirement to have a conditioned, battery-backed power supply adequate to allow a soft fail of the system.

Role-based Access Control (RBAC)

Juniper failed 22 of the 23 RBAC requirements. This was due to the firewall having only two roles, a super user with read/write privileges, and a read-only administrator role. The only internal authentication method is passwords. Juniper also provided for the testing a role-based firewall administration product that provided for RBAC called NetScreen Security Manager (NSM). The NSM provided for (at least) 17 configurable roles with a granularity of 220

different permissible functions. This would have permitted the ISG 2000 firewall to pass nearly every requirement if packaged with the ISG 2000. The NSM was not included in the results because it is a separate Juniper Networks product and not automatically packaged with the firewall. The ISG 2000 is able to use Remote Authentication Dial-In User Service (RADIUS).

Basic Firewall Functionality

Juniper passed a majority of the basic firewall functionality requirements. In ports, protocols, and services it was able to block on a per-interface basis, 59 of 59 filtering requirements. It also defaulted to block known threat ports. The default configuration had the known threat services disabled. The ISG 2000 passed all of the inactivity guard, traffic integrity, and TCP traffic enforcement requirements. The ACL management was convenient and worked in IPv4, IPv6, and dual-stack environments. Stateful inspection of captured packets was decipherable up to layer-7 on common applications and layer-4 on less used protocols and 3rd party applications. Recursive tunnel inspection, a known insider threat in IPv6, was not possible with the current code.

Advanced Firewall Functionality

The Juniper ISG 2000 passed 66 of the 77 advanced functionality requirements tested. One testable requirement was at the discretion of a Designated Approval Authority (DAA) and was not tested. There were no notable shortcomings, but a testing of environmental variables showed failures in temperature and humidity controls/alarms. Five of the seven procedures in this section passed with 90 percent or better results.

Audit and Alert Mechanisms

The Juniper ISG 2000 met 68 of the 87 auditing requirements and had a robust system for viewing audit reports. They passed only 4 of the 9 alert/alarm requirements, failing redundant alerts and an audible alarm. The ISG 2000 logging system works best if exported to an external server.

IPv6 and IPsec Functionality

Juniper did very well in this category, passing 34 of 34 IPv6-specific requirements. They also passed every Internet Control Message Protocol (ICMP) Version 6 (ICMPv6) and IPsec requirement (total 28 of 28). This category included Hop-by-Hop header review, default router advertisements, and specific transition mechanism blocking.

Common Attack Defense

The ISG 2000 is very resistant to today's known attack methods. Testers subjected the firewall to numerous attacks including the Smurf and Synchronize (SYN) Flood varieties of DoS. It passed 30 of 36 DoS requirements, 9 of 9 Man-in-the-Middle attack requirements, 11 of 12 Start/Shutdown vulnerability requirements, and 4 of 4 Tiny Fragmentation attack requirements in both IPv4 and IPv6. When tested against the most current set of Common Vulnerabilities and

Exploits (CVEs), the ISG 2000 passed 100 percent. The Juniper was also Penetration-tested with unclassified tools and passed all requirements with the exception of not requiring strong passwords.

Documentation

Juniper provided only the documentation that was available on the Internet such as User and Administration Guides. As such, they did poorly in the documentation procedures, meeting only 169 of the 319 requirements. They did best in firewall development and cryptography (88 percent and 79 percent respectively). Their administration guide passed 11 of 21 requirements.

Performance

The Juniper ISG 2000 passed 100 percent of the performance requirements in the ITP. The interfaces were able to maintain gigabit, 1 Gigabits per second (Gbps), speeds even with Stateful Packet Inspection in process. Testers recorded TCP Sessions in excess of 25,000 per second.

Conclusions/Recommendations

The Juniper Networks ISG 2000 Firewall is a very stable platform with strong internal functionality. Its strengths are the security triad of Confidentiality, Integrity, and Availability. The IPv6 developers at Juniper have produced a network protection device that was able to pass 100 percent of the IPv6 test procedures. Built for speed on its interfaces, the Juniper Networks ISG 2000 Firewall's only recorded delay resulted from longer ACLs and signatures for its deep packet inspection being negligible. It did well defending itself and the test network from common attacks. While strong, the ISG 2000 does have weaknesses. Juniper has not made significant effort to make the development documentation or the results of their own vulnerability assessments of the ISG 2000 available. Increased availability of the firewall's documentation would enable the DAA to make a more informed decision. Additionally, Juniper does not include their NetScreen Security Manager as part of the firewall management package, which limits their identification and authentication mechanisms on the firewall itself to passwords.

D.9 Cisco Systems IPS 4260 Series Sensor Intrusion Prevention System Internet Protocol Version Six Test Report

Testing Organization and Publication Date

NSA
January 22, 2009

Summary

The NSA Information Assurance Directorate tests and evaluates IPv6 network protection devices (firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS)) in order to satisfy the objectives of the DoD IPv6 Master Test Plan (MTP), V 2.0 (MTPv2.0), Section 2.7. The T&E objective that this report supports is the functional demonstration of the Joint Staff Operational Criteria specifically Criterion 1: Demonstrate security of unclassified network operations, classified network operations, black backbone operations, integration of HAIPE, integration of IPsec, and integration with firewalls and IDS.

Test and Evaluation Method

Exercise

Joint Staff Operational Criteria Tested

1 (1.1.1, 1.2.1, 1.3.1, 1.4.1, 1.6.1)
2 (2.1, 2.3)
8 (8.1)

Configuration

The Cisco IPS 4260 System Sensor test configuration emulated a realistic enclave boundary device on an operational network while remaining in a controlled non-operational environment. The test scenarios used routers, switches, and other devices (web, email, and AAA servers). Traffic and Threat generators were used in-line with actual clients and servers to provide a test environment as operationally realistic as possible for testing IA devices. The diagram illustrated in Figure D-10 is an example of a test scenario used in completing the Cisco IPS 4260 System Sensor evaluation.

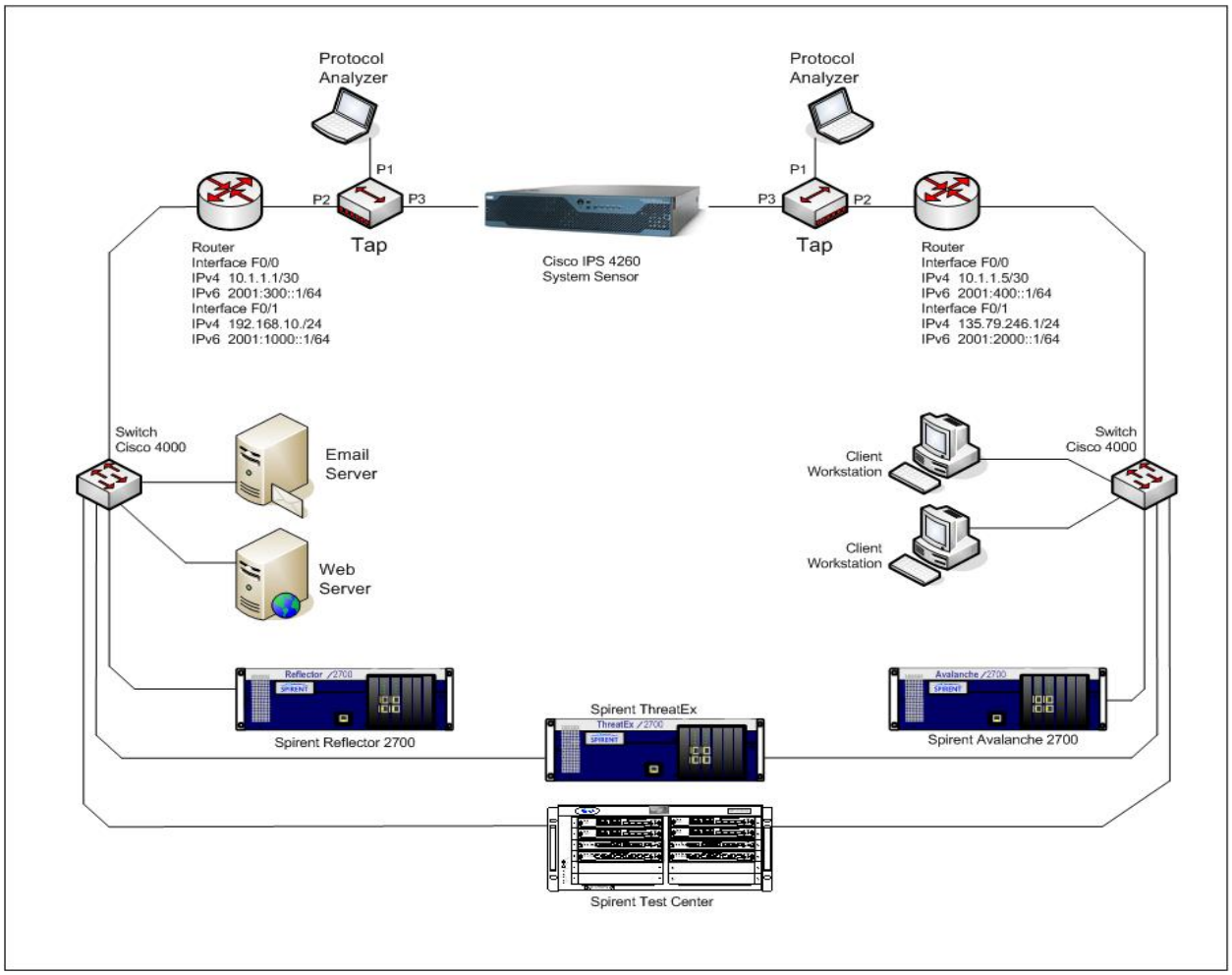


Figure D-10. IPv6 Test Configuration

Results

Conformance

The Cisco IPS 4260 System Sensor failed all 20 RFC conformance requirements. All of the traffic interfaces are promiscuous and parse traffic either off a tap or in an IPS connect-thru mode. They do not respond to attempts to communicate directly with the ports either via IPv4 or IPv6. The management port is currently IPv4-only.

Confidentiality/Integrity/Availability Triad

The Cisco IPS 4260 System Sensor passed 24 of 31 Confidentiality, Integrity, and Availability requirements for a 77 percent success rate. In Availability, the device does not have battery backup, but it does have the option of having a redundant power supply (though this too is AC-based).

Role-Based Access Control

Cisco IPS 4260 System Sensor failed 15 of the 23 RBAC requirements. This was due to the IPS having only two roles, a super user with read/write privileges and a read-only role. The only internal authentication method is passwords. The basis of the configurable roles is Mandatory Access Control security and not RBAC. The Cisco IPS 4260 System Sensor is able to use RADIUS authentication services.

Basic IPS Functionality

Cisco IPS 4260 System Sensor passed a majority of the basic IPS functionality requirements. In ports, protocols, and services it was able to block on a per-interface basis, 59 of 59 filtering requirements. It also defaulted to block known threat ports. The default configuration had the known threat services disabled. The Cisco IPS 4260 System Sensor passed all of the inactivity guard, traffic integrity, and TCP traffic enforcement requirements. The ACL management was convenient and worked in IPv4, IPv6, and dual-stack environments. Stateful inspection of captured packets was decipherable up to Layer-7 on common applications and Layer-4 on less used protocols and third party applications. Recursive tunnel inspection, a known insider threat in IPv6, was not possible with the current code.

Advanced IPS Functionality

The Cisco IPS 4260 System Sensor passed 33 of the 53 advanced functionality requirements tested. Five requirements were at the discretion of a DAA and were not tested. There were no notable shortcomings, but a testing of environmental variables showed failures in temperature and humidity controls/alarms.

Audit and Alert Mechanisms

The Cisco IPS 4260 System Sensor met 77 of the 120 auditing requirements and had a robust system for viewing audit reports. They failed all of the 9 alert/alarm requirements. The web dashboard for alerting human monitors to problems do not update to show new attacks or require acknowledgements that attacks have been recognized. Administrators should export the Cisco IPS 4260 System Sensor logging system to an external server, so management of the logs and tweaking of the rule sets are simultaneous.

IPv6 and IPsec Functionality

Cisco IPS 4260 System Sensor did very well in this category, passing 30 of 34 IPv6-specific requirements with 2 not tested. They passed nearly all of the ICMPv6 and IPsec requirements (total 23 of 26). This category included Hop-by-hop header review, default router advertisements, and specific transition mechanism blocking.

Common Attack Defense

The Cisco IPS 4260 System Sensor is very resistant to today's known attack methods. Testers subjected the firewall to numerous attacks including the Smurf and SYN Flood varieties of DoS. It scored above 90 percent on three of the five attack categories. When tested against the most current set of CVEs, the Cisco IPS 4260 System Sensor passed 100 percent. The Cisco IPS 4260 System Sensor was also Penetration-tested with unclassified tools and passed all requirements with the exception of not requiring strong passwords.

Performance

The Cisco IPS 4260 System Sensor passed 100 percent of the performance requirements in the ITP. The interfaces were able to maintain 1 Gbps speeds even with Stateful Packet Inspection in process. Testers recorded TCP Sessions in excess of 25,000 per second.

Conclusions/Recommendations

The Cisco Systems IPS 4260 Series Sensor is a very good IPv4 IPS. It does everything expected of IDS/IPS in today's network environment. However, it is difficult to call the 4260 Sensor an IPv6 IPS as no interfaces are addressable or configurable with IPv6 functionality. This in turn means that IPv6 support protocols, such as ICMPv6, Neighbor Discovery, and Duplicate Address Detection do not produce action/reaction on the box. The two ports that act as sensing ports are promiscuous and are able to read IPv6 traffic that passes through them. The management port is IPv4-only.

The IPS 4260 was able to read, filter, and react to IPv6 traffic on monitored network segments. It rated above 80 percent in basic functionality and an 88 percent in IPv6/IPsec functionality. The only category the IPS 4260 scored perfectly on was performance. It was able to maintain line rate on its interfaces even when it was parsing attack traffic. Another point to note is that the Cisco IPS 4260 Series Sensor has a web interface with three settings designed like a speed gauge. There is no reasonable way to differentiate between scans and all-out attacks unless the tester wants to relegate scans to a minimal security rating and alarm to the critical attacks. This is dangerous in DoD networks as these networks face some 3 million attacks per day.

D.10 Cisco Assured Services Local Area Network (ASLAN) V6 (Tracking Number 0821001)

Testing Organization and Publication Date

JITC
February 2009

Summary

This test resulted in the certification of the following devices: Catalyst 6524, Catalyst 6509 with Supervisor (Sup) 32, Catalyst 6509 with Sup 720; Catalyst 4507 with Sup 6E, Cisco 7609 – 2, Cisco 7609 – 1, Catalyst 4507R-E with Sup 6E, Catalyst 4900M, Catalyst 3560-E Small Form factor Pluggable, Catalyst 4507 with Sup II+, Catalyst 3560-E, and Catalyst 3750-E. Testers analyzed these devices for functionality against applicable requirements in the Unified Capabilities Requirements (UCR) 2008.

Test and Evaluation Method

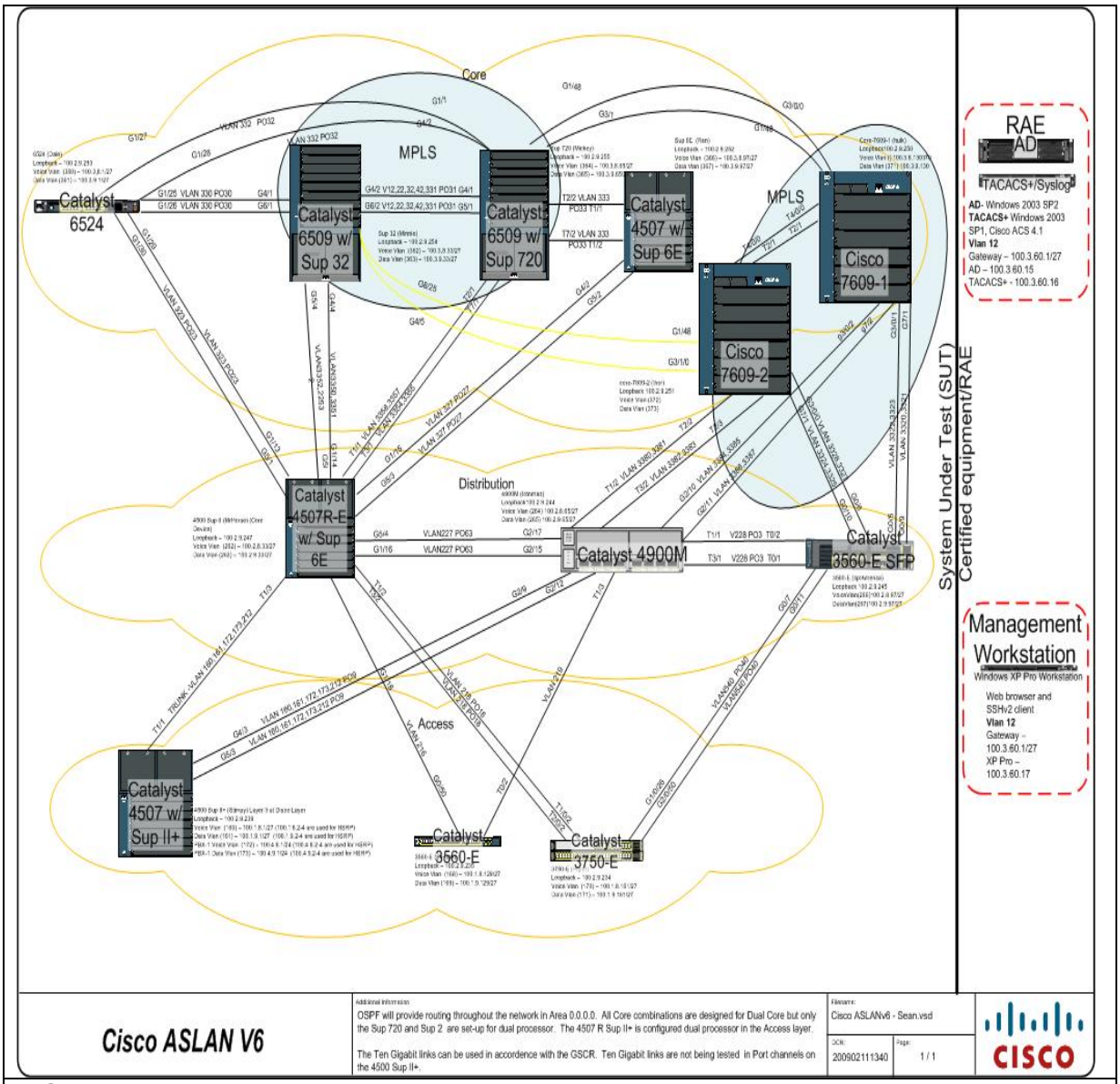
Demonstration

Joint Staff Operational Criteria Tested

2 (2.1, 2.3)
3 (3.1, 3.2, 3.3)
4 (4.1)
8 (8.1.1, 8.1.2, 8.1.3)

Configuration

Figure D-11 is the test configuration used for this test.



LEGEND:

ACS	Access Control Server	SFP	Small Form factor Pluggable
AD	Active Directory	SP	Service Pack
ASLAN	Assured Services Local Area Network	SSH	Secure Shell
DSN	Defense Switched Network	Sup	Supervisor
IP	Internet Protocol	T1	Transmission-Carrier 1
LAN	Local Area Network	TACACS+	Terminal Access Controller Access-Control System Plus
MPLS	Multi Protocol Label Switching		
OSPF	Open Shortest Path First	V	Version
PBX	Private Branch Exchange	VLAN	Virtual Local Area Network
PRI	Primary Rate Interface	w/	With
Pro	Professional	XP	Experience
RAE	Required Ancillary Equipment		

Figure D-11. Test Configuration

System Configurations

Table D-12 provides the system configuration and the hardware and software components tested.

Table D-12. Tested System Configuration

System Name	Hardware/Software Release			
Required Ancillary Equipment	Active Directory			
	Management Client			
	SysLog Server			
	TACACS+			
ASLAN Version 6	**Layer**	**Hardware**	**Card Name / Part Number/ Name**	**Software/ Firmware**
	Core	Catalyst 6524	ME-C6524GS-8S	IOS s6523-advipservicesk9-mz.122-33.SXI
		Catalyst 6509 w/ Sup 32	WS-X6148X2-45AF, 96-port 10/100 Mbps RJ45	IOS s3223-adventerprisek9_wan-mz.122-33.SXI
			WS-X6148-RJ45V, 48-port 10/100 mb RJ45	
			WS-X6516-GBIC, SFM-capable 16 port 1000mb GBIC	
			WS-SUP32-GE-3B, Supervisor Engine 32 8GE (Active)	
			WS-SUP32-GE-3B, Supervisor Engine 32 8GE (Active)	
			WS-X6148-FE-SFP, 48-port 100FX SFP Ethernet Module	
			WS-X6548-GE-TX, SFM-capable 48 port 10/100/1000mb	
			WS-X6148V-GE-TX, 48 port 10/100/1000mb EtherModule	
		Catalyst 6509 w/ Sup 720	WS-X6748-SFP, CEF720 48 port 1000mb SFP	IOS s72033-adventerprisek9_wan-mz.122-33.SXI
			WS-X6704-10GE, CEF720 4 port 10-Gigabit Ethernet	
			WS-X6148A-GE-45AF, 48-port 10/100/1000 RJ45 EtherModule	
			WS-X6816-GBIC, Pure SFM-mode 16 port 1000mb GBIC	
			WS-SUP720-3BXL, Supervisor Engine 720 (Active)	
			WS-SUP720-3BXL, Supervisor Engine 720 (Standby)	
			WS-X6708-10GE, CEF720 8 port 10GE with DFC	
			WS-X6148-45AF, 48-port 10/100 mb RJ45	
			WS-X6548-GE-TX, SFM-capable 48 port 10/100/1000mb RJ45	
		Catalyst 4507 w/ Sup 6E	WS-X4516-10GE, Sup V-10GE 10GE (X2), 1000BaseX (SFP) (Active)	IOS cat4500e-entservicesk9-mz.122-46.SG
			WS-X4516-10GE, Sup V-10GE 10GE (X2), 1000BaseX (SFP) (Standby)	
			WS-X4148-RJ45V, 10/100BaseTX (RJ45)V	
			WS-X4306-GB, 1000BaseX (GBIC)	
			WS-X4306-GB, 1000BaseX (GBIC)	
			WS-X4148-FX-MT, 100BaseFX (FX-MT)	
			WS-X4232-GB-RJ, 10/100BaseTX (RJ45), 1000BaseX (GBIC)	
		Cisco 7609 – 2	RSP 720-3CXL-10GE	IOS c7600rsp72043-adventerprisek9-mz.122-33.SRD
			WS-X6708-10GE	
			7600-ES20-2X10G	
			WS-6748-GE-TX	
			WS-6748-SFP	
			WS-6708-10GE	
			WS-X6548-AF	

Table D-12. Tested System Configuration (continued)

System Name	Hardware/Software Release			
	Layer	Hardware	Card Name / Part Number/ Name	Software/ Firmware
ASLAN Version 6 (continued)	Core (continued)	Cisco 7609 – 1	WS-Sup720-3B	c7600s72033-adventerprisek9-mz.122-33.SRD
			7600-SIP-600	
			7600-SIP-400	
			SPA-5X1GE-V2	
			SPA-1X10GE-L-V2	
			WS-X6748-SFP	
			WS-X6708-10GE	
	Distribution	Catalyst 4507R-E w/ Sup 6E	WS-X4606-X2-E,10GE (X2), 1000BaseX (SFP)	IOS cat4500e-entservicesk9-mz.122-46.SG
			WS-X4648-RJ45V-E, 10/100/1000BaseT PoE E Series	
			WS-X45-SUP6-E, Sup 6-E 10GE (X2), 1000BaseX (SFP)	
			WS-X4306-GB, 1000BaseX (GBIC)	
			WS-X4548-GB-RJ45, 10/100/1000BaseT (RJ45)	
			WS-X4248-RJ45V, 10/100BaseTX (RJ45)V, Cisco/IEEE	
		Catalyst 4900M	WS-C4900M	IOS cat4500e-entservices-mz.122-50.SG
			WS-4920-GB-RJ45	
			WS-X4908-10GE	
		Catalyst 3560-E SFP	WS-C3560E-12SD	IOS c3560-universalk9-mz.122-46.SE
	Access	Catalyst 4507 w/Sup II+	WS-X4013+10GE, Sup II+10GE 10GE (X2), 1000BaseX (SFP)	IOS cat4500-ipbasek9-mz.122-46.SG
			WS-X4013+10GE, Sup II+10GE 10GE (X2), 1000BaseX (SFP)	
			WS-X4248-RJ45V, 10/100BaseTX (RJ45)V, Cisco/IEEE	
			WS-X4306-GB, 1000BaseX (GBIC)	
			WS-X4306-GB, 1000BaseX (GBIC)	
			WS-X4548-GB-RJ45V, 10/100/1000BaseT (RJ45)V, Cisco/IEEE	
		Catalyst 3560-E	WS-C3560E-48PD	IOS c3560-universalk9-mz.122-46.SE
		Catalyst 3750-E	WS-C3750E-24PD	IOS c3750-universalk9-mz.122-46.SE
			WS-C3750E-48PD	

LEGEND:

ASLAN	Assured Services Local Area Network	ME	Metro Ethernet
CEF	Cisco Express Forwarding	RJ	Registered Jack
DFC	Dotter Feature Card	PoE	Power over Ethernet
E	Ethernet	SFM	Switch Fabric Module
FX	Foreign exchanges	SFP	Small Form factor Pluggable
GB	Gigabyte	SIP	Serial Interface Port
GBIC	Gigabit Interface Converter	SPA	Special Access
GE	Gigabyte Ethernet	Sup	Supervisor
IEEE	Institute of Electrical and Electronics Engineers	TACACS+	Terminal Access Controller Access-Control System Plus
IOS	Internetworking Operating System		
Mb	Megabit	w/	with
Mbps	Megabits per seconds	WS	Work group Switch

When a finding is present within the System Under Test (SUT), requirements are verbatim from the UCR IA IPv6 section. Findings from the UCR IA IPv6 fall into three categories (CAT) based on the following definitions:

- **CAT I.** A failed test objective assigned high risk when the test objective is critical to the secure operation of the system. The violation of security policy results in information leakage or the passing of malicious code.
- **CAT II.** A failed test objective assigned medium risk when the failure affects the secure operation of the system. There is a lower level of assurance in the system, but the violation of security policy does not result in information leakage or the passing of malicious code.
- **CAT III.** A failed test objective assigned low risk when the failure has minimal effect on the secure operation of the system.

Results

The Cisco ASLAN IPv6 test environment permitted functionality test procedures against the UCR 2008**.** The Information Assurance Test Team (IATT) was able to capitalize on existing test results from the IPv6 Special Interoperability Certification from DISA in accordance with the DoD IPv6 MTPv2.0.

CAT I. None.

CAT II. None.

CAT III. None.

Conclusions/Recommendations

Cisco Assured Services Local Area Network (ASLAN) met the requirement for certification.

D.11 IPv6 Converged Services and Joint Staff Operational Criteria Demonstration

Testing Organization and Publication Date

Army
July 2009

Summary

During Joint User Interoperability Communications Exercise (JUICE) 09, the main focus was to test or demonstrate as many of the Joint Staff Operational Criteria as possible. The exercise showcased new or emerging applications using IPv6-enabled products. The objective of this test demonstrated coexistence, interoperability, or compatibility with IPv4 and IPv6.

Test and Evaluation Method

Exercise

Joint Staff Operational Criteria Tested

1 (1.2, 1.2, 1.3)
2 (2.1, 2.3)
4 (4.1.1, 4.1.2)
5 (5.1)
7 (7.1)
8 (8.1)
9 (9.1)

Configuration

The IPv6 Effort for JUICE 09 Included Four Objectives

The first objective tested or demonstrated as many aspects of the IPv6 Joint Staff Operational Criteria as possible. The task originated from Lt. Col. Peifer, Chairman of the Joint Chiefs of Staff (CJCS) IPv6 Tiger Team, to "identify venues for operationally realistic testing. This testing will support the CJCS's certification of IPv6 performance and capability parity with IPv4" and to "link warfighters with IPv6 requirements, to venues for experimenting, demonstrating and testing commercial off-the-shelf (COTS) and government off-the shelf IPv6 capabilities, and track progress of Joint Staff Operational Criteria leading to CJCS parity certification and enabling IPv6 on DoD networks."

The second objective extended the IPv6 demonstration beyond the DoD, to include non-DoD federal agencies, local civil agencies, emergency services, and first responders.

The third objective showcased new or emerging applications that are using IPv6 to enhance their capabilities and to illustrate tactical operational use of IPv6-enabled products.

The fourth objective heightened awareness among senior DoD leadership that IPv6 products and applications are available and can be easily integrated into current and future force architectures without impact to the mission.

IPv6 Joint Staff Operational Criteria

Key personnel selected 14 technical objectives for demonstration during JUICE 09, and mapped each objective and its sub-objectives to the IPv6 Joint Staff Operational Criteria. JUICE 09 tested or demonstrated all 10 Joint Staff Operational Criteria, except Scalability (Criterion 6) and Mobile Networks (Criterion 10). Figure D-12 shows the network diagram for the IPv6 portion of JUICE 09.

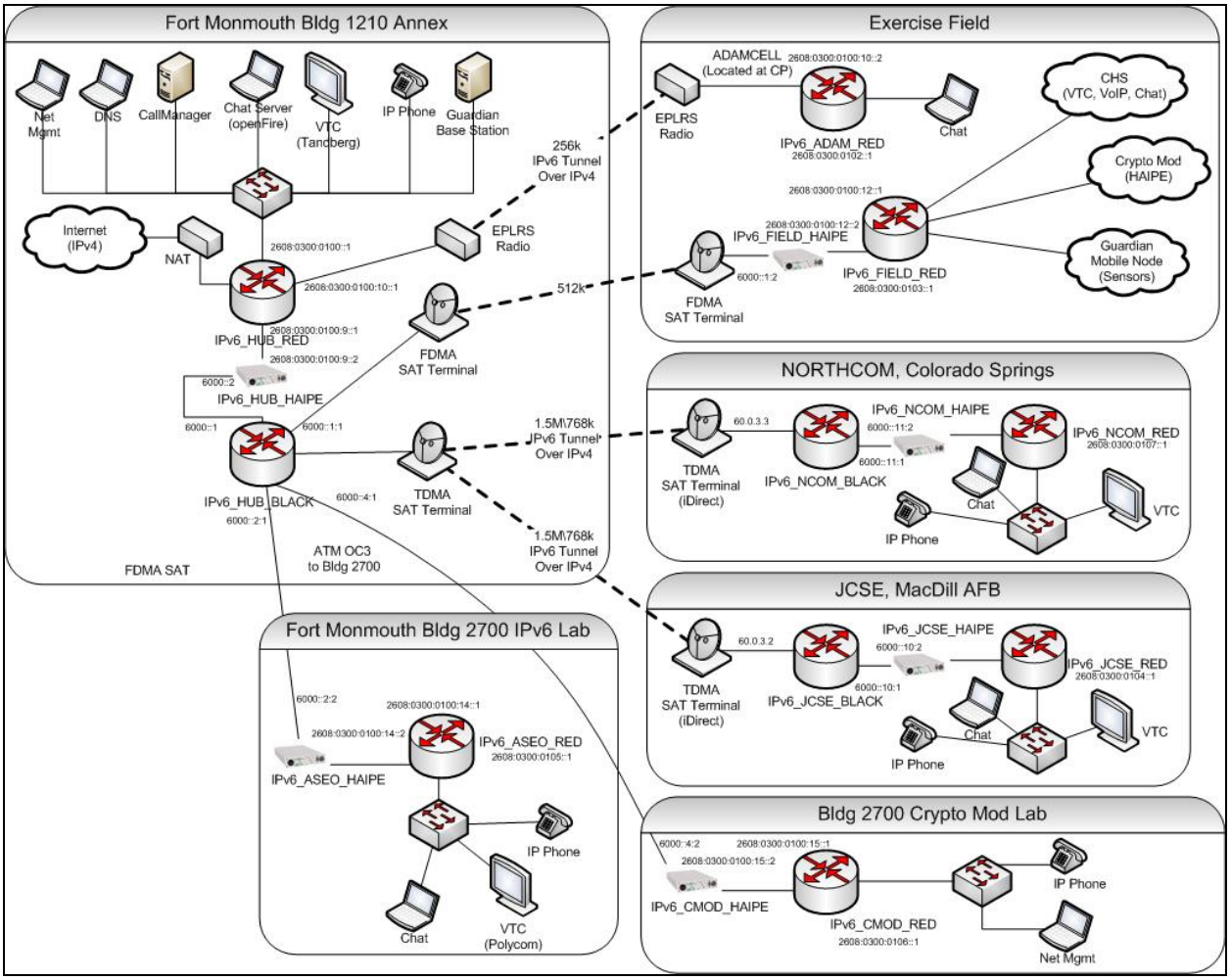


Figure D-12. JUICE 09 IPv6 Network

The network used hub/spoke architecture to support the Black Core configuration. Fort Monmouth served as the hub supporting four remote locations.

Table D-13 lists the VTC objectives.

Table D-13. VTC Objectives

Description	Date Completed	JS Criteria
VTC		2,4,8
Demonstrate interoperability between diverse systems/vendors: BVTC, Polycom, Tandberg		2,4
Demonstrate IPv4-to-IPv6 transition of BVTC using Datatek transformer	12 Jun 09 test failed	2,4,8
BVTC / Polycom Interoperability	pending	2,4
BVTC / Tandberg Interoperability	pending	2,4
Polycom / Tandberg Interoperability	5 Jun 09	2,4
Conduct multipoint conference to 4 or more sites	5 Jun 09	2,4
Demonstrate integrated collaboration using VTC system		2,4
BVTC acting as server	pending	2,4
Polycom acting as server	pending	2,4
Tandberg acting as server	pending	2,4

Results

The focus of the IPv6 effort during JUICE 09 demonstrated, tested, and evaluated as many of the IPv6 Joint Staff Operational Criteria as possible. For each objective and sub-objective, a cross-reference listed its relevance to a Joint Staff Operational Criteria. All objectives except for Objectives 8 and 14 either partially or fully met the requirements.

Of the remaining 12 objectives, testers successfully performed all of the most critical sub-tests. Most noteworthy were the results of Objective 4, Encryption. In cooperation with the Cryptographic Modernization Program Management Office (CM PMO), testers successfully installed a multi-site IPv6-only Black Core network, marking the first time the DoD has ever demonstrated and exercised such a configuration.

Other highly significant objectives included Objective 1, Video Teleconferencing; Objective 2, Voice over Internet Protocol (VoIP) telephony; and Objective 3, Chat. All three objectives demonstrated full interoperability between IPv4 and IPv6 user applications with full IPv4/IPv6 transparency to the user and no adverse affects in performance.

Table D-14 lists the summary results of testing.

Table D-14. Summary of Joint Staff Operational Criteria Results

#	Description	Type of Test	Results	JUICE Objective
1	Security	Tactical Black Core • HAIPE IS 3.0.2 • ViaSat KG-250, L-3 KG-245A	Pass	4, 14
2	Interoperability	IPv4/IPv6 Interoperability Chat, VoIP	Pass	1, 2, 3, 10, 11, 13
3	Performance	Stress Testing over Satellite and ELPRs	Partial	All
4	Voice, Data, & Video Integration	Multi-Vendor Video Conferencing • Cisco, Polycom, Tandberg	Pass	1, 2, 3, 13
5	Low-Bandwidth	Stress Testing over Satellite and ELPRs	Pass	12
6	Scalability	Not Tested	Not Tested	N/A
7	Mobile Node	Session Continuity and Performance while On-The-Move	Pass	5
8	Transition Mechanisms	Tunneling • 4-over-6 & 6-over-4 Translation	Pass	1, 10, 14
9	Network Management	Name Server Autoconfiguration DopplerVUE	Pass	6, 7, 9
10	Mobile Networks	Not Tested	Not Tested	N/A
* In depth testing of IPv6 Joint Staff Operational Criteria 5 was conducted during April/May 2009 and its results are available in a separate report. An over-the-air EPLRS test was run during JUICE to provide additional data points.				

Joint Staff Operational Criteria 1: Security

There are two primary aspects to IPv6 security, encryption and network protection. During this exercise, encryption was tested using NSA certified KG-245As and KG-250s running High Assurance IP Encryptor Internet Protocol Security (HAIPE IS) V 3.0.2, the first version of HAIPE to ever support IPv6. A five-node Black Core network was established and remained operational throughout the entire exercise, functioning flawlessly. The IPv6 Black Core test marked the first time that such a test was run on a DoD network.

Joint Staff Operational Criteria 2: Interoperability

Testers analyzed various aspects of IPv4/IPv6 interoperability throughout the exercise. Testers set up a VTC link between an IPv4 Polycom system and a dual-stacked Tandberg system running on the IPv6 network. Voice interoperability tests used IPv4 and IPv6 Cisco phones and Cisco Call Manager v7.1.1. Interoperability chat sessions used the OpenFire chat server, an open source Jabber/XMPP chat server currently used in the Army-fielded tactical systems. This is possibly the first time such IPv4/IPv6 interoperability tests were run on a DoD network of this type. Previous tests had used simulation, emulation, soft-phones, and soft-video products due to the unavailability of commercial IPv6 products.

Joint Staff Operational Criteria 3: Performance

Testers listed the pass/fail status of IPv6 performance as “partial” because of the lack of rigorous performance testing. However, under the normal operating conditions of the JUICE 09 IPv6

network, which included satellite links between three locations, voice, data, and video traffic routinely passed without incident.

Joint Staff Operational Criteria 4: Voice, Data, & Video Integration

A single VTC session qualifies as an example of a voice, data, and video integration demonstration. The voice, data, and video integration tests ran flawlessly using a variety of Tandberg VTC systems. Other types of integration, such as using chat sessions to transmit streaming video, also ran successfully. To a lesser extent, experiments attempted using Cisco Call Manager v7.1.1 to integrate VTC and VoIP calls.

Joint Staff Operational Criteria 5: Low-Bandwidth

In-depth testing of Joint Staff Operational Criteria 5, conducted during April and May 2009 yielded results available in a separate report. An over-the-air Enhanced Positioning Location Reporting System (EPLRS) test was conducted by the Software Engineering Center at Fort Monmouth during JUICE 09 to provide additional data points. Preliminary indications from both sets of data indicate that IPv6 performs as well as IPv4 in low and moderate conditions of bandwidth loading. However, when capacity reaches the 80 percent range, the addition overhead associated with IPv6 begins to become a factor.

Joint Staff Operational Criteria 7: Mobile Node

Telcordia tested IPv6 mobile node capabilities and performance. Using the Proxy-Mobile IPv6 module, IPv6 performed slightly better than IPv4 using the Mobile IPv4.

Joint Staff Operational Criteria 8: Transition Mechanisms

Testers analyzed various forms of IPv6 transition mechanisms, including translation as well as 4-over-6 and 6-over-4 tunneling. All worked flawlessly in support of the particular application. Other forms of transition mechanisms, such as the integrated dual-stack features of the Tandberg video server, Cisco Call Manager, and OpenFire chat server ran successfully.

Joint Staff Operational Criteria 9: Network Management

All three areas of the network management tests (DNS, autoconfiguration, and DopplerVUE) ran properly without incident throughout the duration of the exercise. The DNS running BIND 9.5 properly handled all queries for IPv4 and IPv6 resolution. The engineering team used DopplerVUE daily and found it useful, accurate, and easy to use.

Joint Staff Operational Criteria 10: Mobile Networks

JUICE 09 did not test IPv6 mobile network or ad-hoc networking. However, the Army Communications-Electronics Research Development and Centers (CERDEC) will be conducting a collaborative test with the French Ministry of Defense in Aug/Sept that will include IPv6 Mobile Ad-hoc Networking (MANET). A report will be available in October 2009.

Conclusions/Recommendations

The single most significant event during this exercise was the successful demonstration of an IPv6 Black Core network using HAIPE IS 3.0.2 In-Line Encryptors. In preparing for IPv6 readiness and implementation, it is imperative throughout the DoD that all of the IPv6 security requirements be completely satisfied. The demonstration and use of the IPv6 Black Core network during JUICE 09 was a major step forward towards the deployment of IPv6 in operational DoD networks.

In addition to the great progress in IPv6 security, it was evident by the extent of the testing during this exercise the availability of IPv6 COTS products and services has increased markedly during the past several years. Moreover, these products are addressing the basic needs of the DoD for voice, data, and video integration. By all indications, it appears that all features, functions, and services currently available using IPv4, currently are, or will soon be available with IPv6.

D.12 JCS Criteria 10 Test Plan

Testing Organization and Publication Date

Department of the Navy
June 19, 2009

Summary

The Department of the Navy is the process of testing IPv6 Joint Staff Operational Criteria 10. Testers modified the original plan to clarify the test procedures. Testing will use network emulators generating traffic over Ethernet and wireless links. The objective of this test is to evaluate the use of Network Mobility (NEMO), Optimized Link State Routing (OLSR), Ad hoc On Demand Distance Vector Routing (AODV) and Simplified Multicast Forwarding (SMF) for MANET in an IPv6 network.

Test and Evaluation Method

Planned Exercise

Joint Staff Operational Criteria Tested

2 (2.3)
4 (4.1)
5 (5.1.1, 5.1.2)
7 (7.1.1, 7.1.2)_
8 (8.1.1, 8.1.2, 8 1.3)
10 (10.1 10.2)

Configuration

This test will use network emulation running over Ethernet (with an 802.11-style link model) and/or 802.11b wireless links for most testing. Testers will use the Network Survivability - Double Link Failure (NS2) simulator for scalability studies. Multi-Generator (MGEN) is the traffic generator and receiver for this test, along with some real surrogate applications (e.g., Ivox for VoIP, NormChat, VLAN Client (VLC) for video streaming, MGEN/CMap/ and Software Development Tool for situational awareness). These applications support IPv6, and support setting the Traffic Class and/or Flow Label setting for QoS. The TCPDUMP Rate Plot Real-time (TRPR) analysis tool analyzes MGEN and/or TCPDUMP logfiles.

NEMO Basic Functionality Testing (10.1.1.X)

All completed NEMO testing is in the North Atlantic Treaty Organization Interoperable Networks for Secure Communications (INSC) project. This testing included the use of NEMO across a black transit network of IPsec-encrypted links.

Further investigation is not necessary, because general NEMO development has all but halted since the completion of INSC work. The IETF NEMO Working Group shut down in 2007 without producing a NEMO Extended Support Protocol, and without solving the problems of nested NEMO, multicast support, or most importantly, Route Optimization, which is critical for military use. The IETF Mobility Extensions for IPv6 (MEXT) Working Group continued support for NEMO, but the group has not done much work in the areas of nested NEMO or multicast support for NEMO. Additionally, the MEXT Working Group has focused its NEMO Route Optimization efforts specifically on niche solutions for the aviation and automotive industries, and even there they currently have only problem statements and operational requirements documents, not accepted solutions.

MANET Functionality & Performance Testing (10.2.1.1 & 10.2.1.3)

The MANET network will consist of 10 or more Linux machines connected together in a multi-hop fashion, and the network tested will undergo topology dynamics caused by emulated node motion. MGEN will generate and receive traffic, to ensure that various sets of MANET nodes can communicate across multiple hops in each scenario. For performance testing, MGEN and TRPR will record loss, latency, goodput/reliability, and overhead in both multicast and unicast. Testers will introduce bandwidth constraints and unreliable links for the performance testing portion. Testers will investigate the use of QoS for protecting vital routing protocol traffic investigated in the performance testing section. Also, testers plan to investigate application performance and reliability within the MANET using the representative applications mentioned earlier, though some of that testing may be out of the scope of this document.

Topologies and Scenarios

Testers will analyze the MANET protocol over a variety of topologies throughout the course of each scenario. Testers will use several different scenarios, including a few “random walk” scenarios, in which each node independently walks in a random direction within a box for a random amount of time. Some of these scenarios may involve network partitions and merges.

We will also test a few static topologies that represent unique or interesting situations, including:

- Full mesh: each MANET node connects to every other node.
- Star topology: one MANET node connects to every other node, but those nodes not connected to each other at all (there are possible variations on this as well).
- Line topology: each MANET node connects to only two other nodes, except the end nodes, which connect to one; in such a topology, a packet sent from one end to the other will travel through every MANET node on its way.

An additional set of scenarios comes from the ONR RANGE project. The base scenario, shown in Figure D-13, involves two counter-rotating patterns of Unmanned Aerial Vehicles (UAVs) providing communications reachback capability for a set of ground or surface nodes heading towards some sort of target or goal. At a certain point in this scenario, one of the UAVs leaves its rotational pattern, moves off to provide reachback capability in the target area, and optionally conducts video surveillance of the target area.

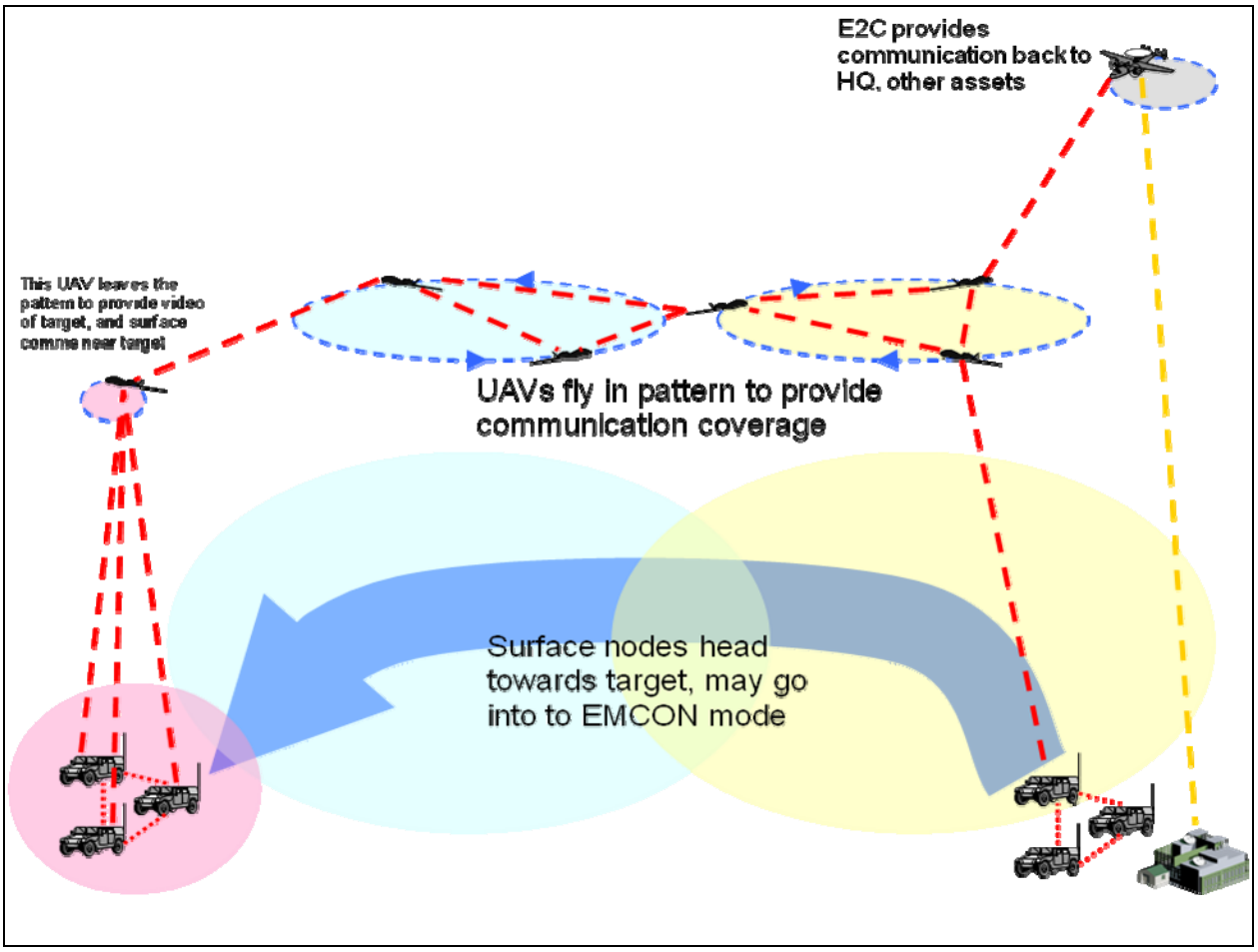


Figure D-13. RANGE Hybrid Airborne Scenario

Proactive Unicast Routing Protocol Testing (10.2.1.1.1)

The OLSR is the dominant and most well-known proactive routing protocol. MANET Opened Shortest Path First (OSPF) is another proactive protocol that has numerous benefits, including easier interoperability with the standard (non-MANET) OSPF Version 3 routing protocol. Testers will use both OLSR and MANET OSPF in the above-listed scenarios with various protocol timer values. For the functionality testing, testers will simply verify they can send unicast data between various nodes across the MANET network. Naval Research Laboratory's (NRL) implementation of OLSR, and Boeing's Quagga-based implementation of MANET OSPF will be tested, along with other popular implementations, such as OLSR org's OLSRd.

For the performance testing, testers will investigate the effects of protocol timer values on latency, loss, and goodput/reliability in each of the previously mentioned scenarios. Testers will also investigate how well the MANET supports multiple flows, as well as the importance of QoS in these scenarios.

OLSR Version 2 is a next generation, standards-track, proactive MANET routing protocol that is under development within the IETF. Now, there are several implementations under development

by various parties, but none released publicly that support IPv6. However, if able to gain access to any implementations, testers will also assess those implementations.

Reactive Unicast Routing Protocol Testing (10.2.1.1.2)

Testers will use AODV in the above-listed scenarios with protocol timer values appropriate for each scenario. Testers will then verify the ability to send unicast data between various nodes across the MANET network. Testers will analyze the popular AODV-UU implementation.

Dynamic MANET On-Demand is a next-generation, standards-track, reactive MANET routing protocol that is under development within the IETF. Now, there are several implementations under development by various parties, but none released publicly that support IPv6. However, if able to gain access to any implementations, testers will also assess those implementations.

Multicast Routing Protocol Testing (10.2.1.1.3)

The SMF is the primary MANET multicast routing protocol under development within the IETF. The SMF will be tested both in "classical flooding" mode (each MANET node forwards every multicast packet exactly once), as well as modes where it receives a more efficient packet forwarder set from the unicast routing protocol. Testers will use the NRL's SMF implementation, which supports receiving forwarder sets from both NRL's OLSR implementation and Boeing's MANET OSPF implementation. Testers will verify the ability to receive multicast packets at every node in the network while under motion in the previously listed scenarios.

For the performance testing, testers will investigate the effects of classical flooding versus intelligent relay sets on latency, loss, and goodput/reliability in each of the previously mentioned scenarios. Testers will also investigate how well the MANET supports multiple multicast flows.

Demonstrate Secure Communications in MANET (10.2.1.2)

Testers will demonstrate MANET communications security in two ways: security of routing control messages and secure data transfer between a pair of MANET nodes. Testers will conduct MANET emulation testing using OLSR and/or MANET OSPF Linux implementations. Those protocols themselves will generate the unsecure routing control traffic. MGEN will generate and receive traffic for user data security.

Routing Control Message Security (10.2.1.2.1)

Testers will use Transport-mode IPsec to encrypt routing control messages. MANET nodes will use pre-shared keys, which is realistic for most military scenarios. The routing protocol will generate the encrypted routing control messages. If the MANET network is still able set up its routes and function properly with encrypted packets, the test will be successful.

User Data Security (10.2.1.2.2)

Testers will use Transport-mode and/or tunnel-mode IPsec to encrypt user data generated by MGEN. If the receiver is able to get the packets back up to MGEN, the test will be successful.

MANET Scalability (10.2.1.4)

Testers will review previous research and conduct a NS2 simulation study of large random networks to investigate scalability testing. Testers will also discuss various methods for improving the scalability of MANET networks.

Conclusions/Recommendations

This test plan offered no conclusions.

D.13 Force10 Networks E300, C300, C150, and S50V Force10 Operating System (FTOS) V 7.8.1.0E (Tracking Number 0831101)

Testing Organization and Publication Date

JITC
April 2009

Summary

The test was to evaluate the Force 10 Network devices with the UCR. The Force 10 Network devices are voice telecommunications equipment and categorized in the UCR IPv6 Profile as LAN Switches. The objective of this test verified the SUT could create or receive, process, and send or forward IPv6 packets in a mixed IPv4/IPv6 environment.

Test and Evaluation Method

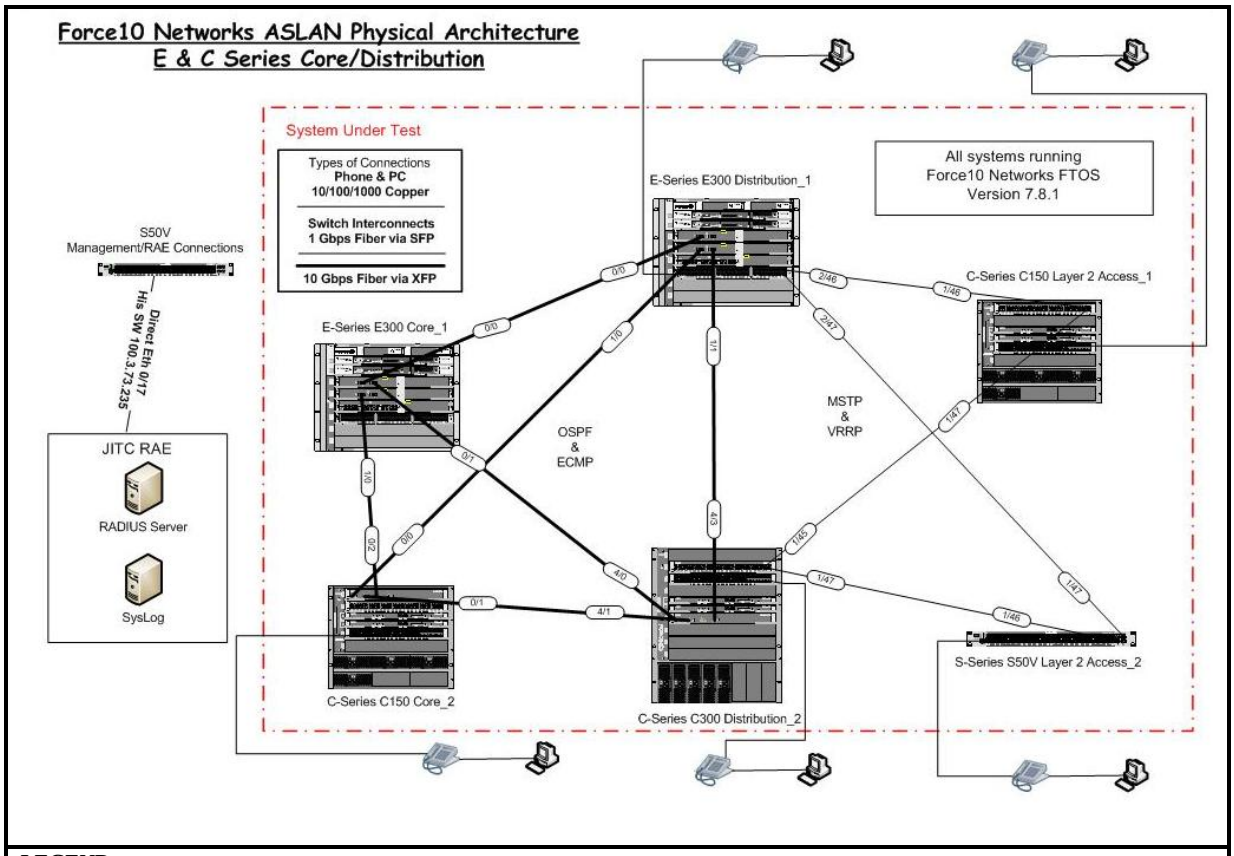
Demonstration

Joint Staff Operational Criteria Tested

2 (2.1, 2.3)
3 (3.1, 3.2, 3.3, 3.4)
8 (8.1, 8.2, 8.3)

Configuration

Figure D-14 was the test configuration used.



LEGEND:

ASLAN	Assured Services Local Area Network	PC	Personal Computer
ECMP	Equal Cost Multi-Path	RADIUS	Remote Access Dial-in User Service
Eth	Ethernet	RAE	Required Ancillary Equipment
FTOS	Force10 Operating System	SFP	Small Form-Factor Pluggable
Gbps	Gigabytes per Second	SW	Software
JITC	Joint Interoperability Command	VRRP	Virtual Router Redundancy Protocol
MSTP	Multiple Spanning Tree Protocol	XFP	10 Gigabit Small Form-Factor Pluggable
OSPF	Open Shortest Path First		

Figure D-14. Test Configuration

Table D-15 provides the requirements source for Required Ancillary Equipment (RAE).

Table D-15. IPv6 IA Requirements Summary Without RAE and With RAE Findings

Requirement (see note)	**Date**	**Testing Status**	**W/O-RAE**	**W-RAE**
IPv6 Requirements	9 Apr 2009	Applied	No CAT I 6 CAT II No CAT III	NA

NOTE: Requirements are derived from UCR 2008 Section 5.3.

LEGEND:

CAT	Category	RAE	Required Ancillary Equipment
IP	Internet Protocol	STIG	Security Technical Implementation Guidelines
NA	Not Applicable	W-RAE	With Required Ancillary Equipment
		W/O-RAE	Without Required Ancillary Equipment

System Configurations

Table D-16 provides the system configuration and the hardware and software components tested.

Table D-16. Tested System Configuration

System Name	Equipment		
Required Ancillary Equipment	Remote Authentication Dial-In User Server		
	SysLog Server		
Force10 Networks E300, C300, C150, S50V	**Hardware**	**Cards**	**Software/Firmware**
	E-Series E300 Distribution and Core	E300 Terascale two port 10Gigabit Ethernet LAN/WAN PHY line card	FTOS V7. 8. 1
		E300 Terascale 24-port Gigabit Ethernet line card	
		E300 Terascale 48-port 10/100/1000Base-T High Density line card	
	C-Series C150 Layer	C-Series four port 10Gigabit Ethernet line-card	FTOS V7. 8. 1
		C-Series 48 port 10/100/1000Base-T line-card with RJ45 interface and inline-power	
		C-Series 48 port 10Gigabit Ethernet line-card	
	S-Series S50V Layer	NA	FTOS V7. 8. 1
	C-Series C300 Distribution and Core	C-Series four port 10Gigabit Ethernet line-card	FTOS V7. 8. 1
		C-Series 48 port 10/100/1000Base-T line-card with RJ45 interface and inline-power	
		C-Series 48 port 10Gigabit Ethernet line-card	

LEGEND:

FTOS	Force10 Operating System	PoE	Power over Ethernet
LAN	Local Area Network	RJ	Registered Jack
NA	Not Applicable	SFP	Small Form-Factor Pluggable
PHY	Physical Layer Device	WAN	Wide Area Network

Testers used the requirements found in the UCR IA IPv6 section to verify that the tested system can create or receive, process, and send or forward (as appropriate) IPv6 packets in mixed IPv4/IPv6 environments. The UCR IA IPv6 requirements have been implemented relating to voice telecommunications equipment specifically IPv6 Profile Category for LAN Switches. The security requirements the system shall meet includes the following: Maximum Transmission Unit (MTU), Flow Label, Address, Dynamic Host Configuration Protocol (DHCP), Neighbor Discovery, Redirect Messages, Router Advertisements, Stateless Address Autoconfiguration and Manual Address Assignment, ICMP, Routing Functions, IPsec, Network Management, IP Version Negotiation, Assured Services SIP (AS-SIP) IPv6 Unique Requirements, and Miscellaneous Requirements.

When a finding is present within the SUT, requirements are verbatim from the UCR IA IPv6 section. Findings from the UCR IA IPv6 fit into three CATs based on the following definitions:

- **CAT I.** A failed test objective assigned high risk when the test objective is critical to the secure operation of the system. The violation of security policy results in information leakage or the passing of malicious code.
- **CAT II.** A failed test objective assigned medium risk when the failure affects the secure operation of the system. There is a lower level of assurance in the system, but the violation of security policy does not result in information leakage or the passing of malicious code.

- **CAT III.** A failed test objective assigned low risk when the failure has minimal effect on the secure operation of the system.

Results

The Force10 Networks ASLAN IPv6 test environment permitted functionality test procedures against the UCR 2008.

- **CAT I** None

- **CAT II** Force10 Networks had six CAT II findings within this requirement:

  - **UCR 2008:** 5.3.5.3.3.8, **RFC** 4291.
    Requirement: The system shall support IPv6 Addressing Architecture as described in RFC 4291.
    Finding: This system does not support the assignment of anycast, site-local, or manual configuration of link-local addressing.
    Vulnerability: A malicious node might send a packet that contains a textual IPv6 non-global address with a zone index, intending to deceive the receiving mode about the zone of the non-global address.
    Components Affected (4): E-Series E300 Distribution 1; C-Series C300 Distribution 2; C-Series C150 Core 2; and E-Series 300 Core 1.
    Force10 Networks Response: Force10 Networks supports RFC 4291; however, Force10 Networks does not currently support the assignment of anycast, site-local or manual configuration of link local addresses.
    Force10 Networks 2nd Response: Force10 Networks supports RFC 4291; however, Force10 Networks does not currently support the assignment of anycast, site-local or manual configuration of link local addresses. According to RFC 4291 a router must recognize and answer on its link-local address and must not forward any packets with link-local source or destination address to other links (section 2.5.6). The format specified in the RFC uses the generic FE80 prefix followed by the interface id (i.e., Media Access Control (MAC)). The RFC does not specify the ability to manually conFigure D-the link-local part of the address.

  - **UCR 2008:** 5.3.5.3.8.20, **RFC** 2710**.**
    Requirement: If the system supports routing functions, the system shall support the MLD process as described in RFC 2710 and extended in RFC 3810.
    Finding: The MLD will not work on C-Series routers, as they do not have a full implementation for IPv6. This also includes a lack of IPsec, Multicast, and IPv6 QoS.
    Vulnerability: The requirement that nodes verify the IPv6 source address of all received MLD messages is a link-local address defends them from action on forged MLD messages originated off-link.
    Components Affected (2): C-Series C300 Distribution 2 and C-Series C150 Core 2.
    Force10 Networks Response: Force10 Networks supports RFCs 2710 and 3810 in the E-Series switch family only. The support for these two RFCs in the C-Series and S-Series switch families is under consideration.

Force10 Networks 2nd Response: Force10 Networks supports RFCs 2710 and 3810 in the E-Series switch family only. The support for these two RFCs in the C-Series and S-Series switch families is under consideration. Force10 Networks will provide the Unified Capabilities Coordination Office with Roadmap information regarding when this feature.

- **CAT III** None

Conclusions/Recommendations

Force10 Networks E300, C300, C150, and S50V Force10 Operating System V 7.8.1.0E met some of the criteria outlined in the UCR for Ethernet switches.

D.14 Defense Threat Reduction Agency Demonstration Test Report to Support Defense Threat Reduction Agency IPv6 Compliance

Testing Organization and Publication Date

Defense Threat Reduction Agency (DTRA)
June 26, 2008

Summary

The DTRA conducted an IPv6 capability demonstration test. The purpose of this test was to provide an initial IPv6 design concept and to develop a better understanding of IPv6 in general. DTRA tested:

- Transmit IPv6 traffic from the Internet and external peers, through the network Backbone Core to the LAN
- Transmit IPv6 traffic from the LAN, through the network Backbone Core out to the Internet and eternal peers
- Transmit IPv6 traffic from the LAN, through the network Backbone Core to another LAN (or another node on the same LAN.

Test and Evaluation Method

Demonstration

Joint Staff Operational Criteria Tested

2 (2.3)
8 (8.1)

Configuration

General

Testers configured router interfaces using EUI–64 MAC addresses so as to allow stateless autoconfiguration for each connecting host. In this way, the interface provided the first 64 bits of the IPv6 address. The connected hosts MAC-Address provided the last 64 bits. The full IP address of the end host was determined during testing.

Phase 1: Layer-2 Host-To-Host IPv6 Demilitarized Zone (DMZ) Traversal

The purpose of this test validated the ability to communicate using only IPv6 addressing through the DTRA Core DMZ enclave. The test demonstrated successful bi-directional pings and traceroutes between the two hosts through the DMZ.

Phase 2: Layer-3 Enclave-To-Enclave IPv6 Traversal

The purpose of this test demonstrated the ability to communicate using only IPv6 addressing through the DTRA Core DMZ environment to a separate DTRA network enclave.

Phase 3: Core Network to External Network IPv6 Traversal

The purpose of this test demonstrated the IPv6 traversal of the Internet cloud. A tunneled approach, created a manual IPv6-in-IPv4 (6in4) tunnel on each site's IPv6 border router to provide site-to-site communication. Testers configured each of the tunnel endpoints explicitly to provide greater ease of implementation and operation.

In addition to showing IPv6 connectivity, the test also fully demonstrated the functionality of the inter-site 6in4 tunnel.

Results

All phases demonstrated successful bi-directional pings and traceroutes between the two hosts through the DMZ.

Conclusions/Recommendations

In addition to showing IPv6 connectivity, the test also fully demonstrated the functionality of the inter-site 6in4 tunnel.

D.15 Information Assurance IPv6 Findings Summary

Testing Organization and Publication Date

JITC
June 2009

Summary

The test evaluated the Cisco Unified Communication Manager with the UCR. The Cisco Unified Communication Manager device is voice telecommunications equipment and categorized in the UCR IPv6 Profile as Router. The objective of this test verified the SUT could create or receive, process, and send or forward IPv6 packets in a mixed IPv4/IPv6 environment.

Test and Evaluation Method

Demonstration

Joint Staff Operational Criteria Tested

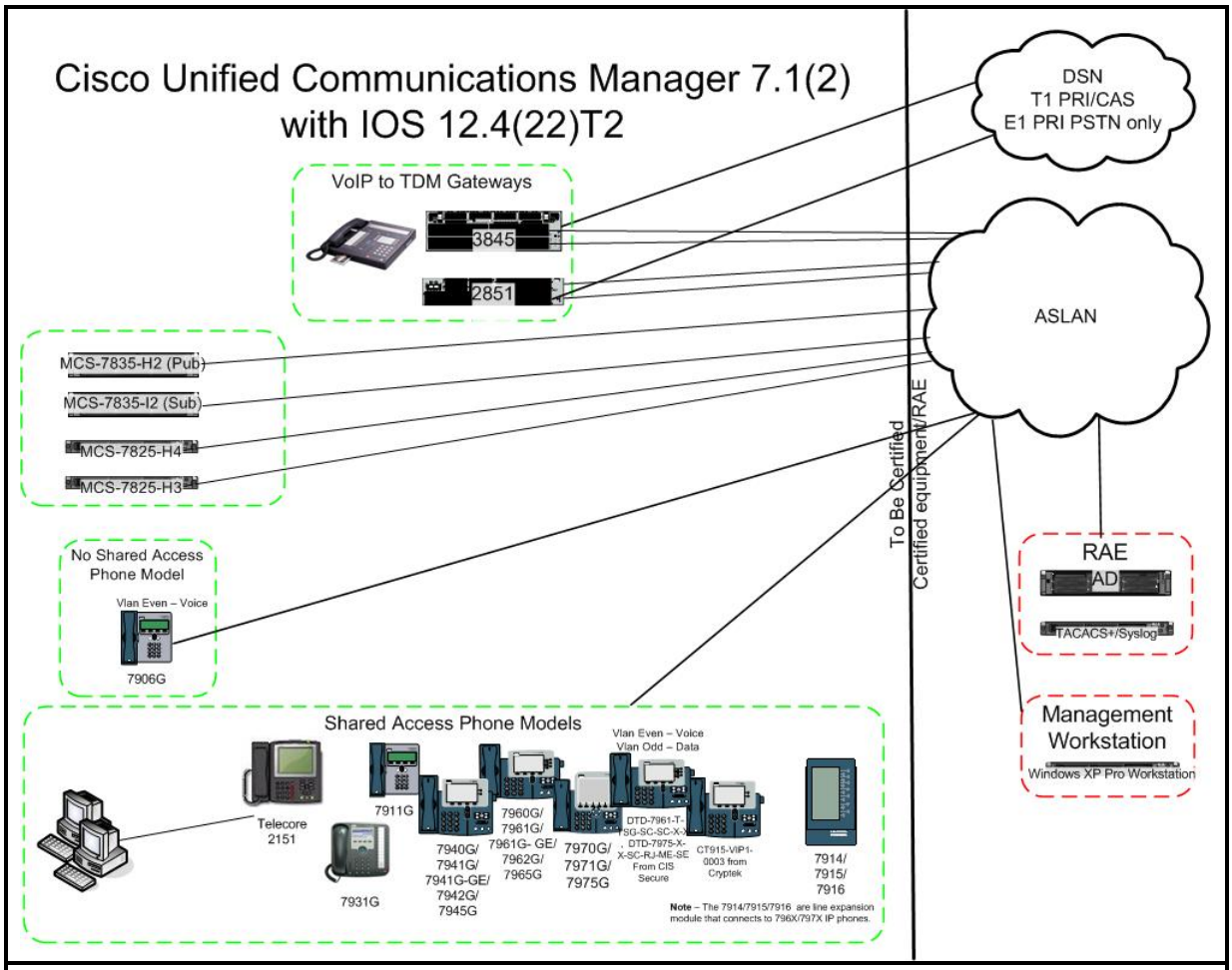
2 (2.3)
8 (8.1)

Configuration

Components

Figure D-15 depicts the system, which consists of the following:

- MCS-7835 Hewlett Packard-(H)2, MCS-7835-I2, MCS-7825-H4, and MCS-7825-H3
- Cisco 3845 and Cisco 2851
- Cisco IP phones
    - 7906G, Telecore 2151, 7911G, 7931G, 7940G, 7941G, 7941G-GE, 7942G, 7945G, 7960G, 7961G, 7961G-GE, 7962G, 7965G, 7970G, 7971G, 7975G
- CIS Secure Data Transfer Device (DTD)-7961-T-Telecommunication Security Group (TSG) - Standard Connector (SC)-SC-X-X
- CIS Secure DTD-7975-X-X-SC-RJ-ME-SE
- Cryptek CT915-VIP-0003
- 7914, 7915, and 7916 Expansion Module



LEGEND:

AD	Active Directory	Pro	Professional
ASLAN	Assured Services Local Area Network	PSTN	Public Switched Telephone Network
CAS	Channel Associated Signaling	Pub	Publisher
DSN	Defense Switched Network	RAE	Required Ancillary Equipment
DTD	Data Transfer Device	Sub	Subscriber
E1	European Standard Line 1	T1	Transmission Carrier 1
G	Gigabyte	TACACS+	Terminal Access Controller Access Control System Plus
GE	Gigabyte Ethernet		
H	Hewlett Packard	TDM	Time Division Multiplexing
I	IBM	TSG-SC	Telecommunication Security Group-Standard Connector
IBM	International Business Machines Corporation		
IOS	Internetwork Operating System	VLAN	Virtual Local Area Network
IP	Internet Protocol	VoIP	Voice over Internet Protocol
MCS	Media Convergence Server	XP	Experience
PRI	Primary Rate Interface		

Figure D-15. Test Configuration

Table D-17 provides the requirements source for RAE.

Table D-17. IPv6 IA Requirements Summary Without RAE and With RAE Findings

Requirement (see note)	**Date**	**Testing Status**	**W/O-RAE**	**W-RAE**
IPv6 Requirements	29 Jun 2009	Applied	No CAT I 6 CAT II No CAT III	NA

NOTE: Requirements are derived from UCR 2008 Section 5.3.

LEGEND:

CAT	Category	UCR	Unified Capabilities Requirements
IA	Information Assurance	v	version
IP	Internet Protocol	W-RAE	With Required Ancillary Equipment
NA	Not Applicable	W/O-RAE	Without Required Ancillary Equipment
RAE	Required Ancillary Equipment		

System Configurations

Table D-18 provides the system configuration and the hardware and software components tested.

Table D-18. Tested System Configuration

System Name	**Hardware/Software Release**		
Required Ancillary Equipment	Active Directory		
	SysLog		
	Terminal Access Control Access-Control System Plus		
Site Provided	Management Workstation		Windows XP Pro SP3
Cisco Unified Communication Manager 7.1(2)	**Hardware**	**Card Name** **Part Number/ Name**	**Software/ Firmware**
	MCS-7835-H2	NA	RedHat 4.6.2, 6.9-67. Elsmp
			Cisco Unified Communication Manager 7.1(2)
	MCS-7835-I2		IBM Informix Dymanic Server version 10.00, UC9X4
	MCS-7825-H4		Apache Tomcat 6.0.18
	MCS-7825-H3		Java 1.6.0_13
	Cisco 3845 Integrated Services Router (Gateway)	VIC 4FXS/DID	IOS 12.4(22)T2
		VIC3 4FXS/DID	
		VWIC2 2MFT T1/E1	
		NM HDV2	
		NM HDV2 2T1/E1	
		EM HDA 8FXS	
		EVM HD 8FXS/DID	
		EVM3 HD 8FXS/DID	
	Cisco 2851 Integrated Services Router (Gateway)	VIC 4FXS/DID (2)	IOS 12.4(22)T2
		VIC3 4FXS/DID	
		VWIC2 2MFT T1/E1	
		EVM3 HD 8FXS/DID	
		EVM HD 8FXS/DID	
		EM HDA 8FXS	

Table D-18. Tested System Configuration (continued)

SUT Telephones		
Telephone type	**Model**	**Firmware**
IP	7906G	SCCP11.8-5-2-2S
	Telecore 2151	2AE-00056-E328
	7911G	SCCP11.8-5-2S
	7931G	SCCP31.8-5-2S
	7940G	P00308010100
	7941G	SCCP41.8-5-2S
	7941G-GE	SCCP41.8-5-2S
	7942G	SCCP42.8-5-2S
	7945G	SCCP45.8-5-2S
	7960G	P00308010100
	7961G	SCCP41.8-5-2S
	7961G-GE	SCCP41.8-5-2S
	7962G	SCCP42.8-5-2S
	7965G	SCCP45.8-5-2S
	7970G	SCCP70.8-5-2S
	7971G	SCCP70.8-5-2S
	7975G	SCCP75.8-5-2S
	CIS Secure DTD-7961-T-TSG-SC-SC-X-X	SCCP41. 8-5-2S
	CIS Secure DTD-7975-X-X-SC-RJ-ME-SE	SCCP75.8-5-2S
	Cryptek CT915-VIP1-0003	SCCP41.8-5-2S
	7914	S00105000400
	7915	B015-1-0-3
	7916	B015-1-0-3

LEGEND:

DID	Direct Inward Dialing
DTD	Data Transfer Device
E1	European Carrier 1
EM	Extension Module
EVM	Extension Voice Module
FXS	Foreign Exchange Station
G	Gigabyte
GE	Gigabyte Ethernet
H	Hewlett Packard
HD	High-density
HDA	High-density Analog
HDV	High-density Digital Voice
I	IBM
IBM	International Business Machines Corporation
IOS	Internetworking Operating System
IP	Internet Protocol
MCS	Media Convergence Server
MFT	Multi-Flex Trunk
NA	Not Applicable
NM	Network Module
Pro	Professional
RJ	Registered Jack
SC	Standard Connector
SCCP	Skinny Client Control Protocol
SP	Service Pack
SUT	System Under Test
T1	Transmission Carrier 1
w/	with
WAN	Wide Area Network
VIC	Voice Interface Card
VWIC	Voice WAN interface Card
XP	Experience

The UCR IA IPv6 (Phase II)

Testers used the UCR IA IPv6 Requirements section to verify the tested system can create or receive, process, and send or forward (as appropriate) IPv6 packets in mixed IPv4/IPv6 environments. The UCR IA IPv6 requirements have been implemented relating to voice telecommunications equipment specifically IPv6 Profile Category for the Routers. The security requirements that the system shall meet include the following: System Requirements, MTU, Flow Label, Address, DHCP, Neighbor Discovery, Redirect Messages, Router Advertisements, Stateless Address Autoconfiguration and Manual Address Assignment, ICMP, Routing Functions, IPsec, Network Management, IP Version Negotiation, AS-SIP IPv6 Unique Requirements, and Miscellaneous Requirements.

Results

When a finding is present within the SUT, requirements are verbatim from the UCR IA IPv6 section. Findings from the UCR IA IPv6 fit into three CATs based on the following definitions:

- **CAT I.** A failed test objective assigned high risk when the test objective is critical to the secure operation of the system. The violation of security policy results in information leakage or the passing of malicious code.
- **CAT II.** A failed test objective assigned medium risk when the failure affects the secure operation of the system. There is a lower level of assurance in the system, but the violation of security policy does not result in information leakage or the passing of malicious code.
- **CAT III.** A failed test objective assigned low risk when the failure has minimal effect on the secure operation of the system.

Testers identified the following CATs.

- **CAT I** None

- **CAT II** Cisco had six CAT II findings within these requirements

  - **UCR 2008:** 5.3.5.3.9.22.12.2, **RFC** 4303
    Requirement: If the SUT supports RFC 4303, the system shall check as its first check after a packet matching to its security associations whether the packet contains a Sequence Number that does not duplicate the Sequence Number of any other packet received during the life of the security association.
    Finding: Packets are duplicating sequence numbers.
    Vulnerability: This prevents an attack where a hacker may try to modify data and re-send the altered IP data for malicious means similar to that seen in the Session Reply attack.
    Components Affected (2): Cisco 3845 and Cisco 2851.
    Cisco's Mitigation: "RFC 4303 is related to IPv6 IPsec which is not being used in the SUT. Cisco Internetworking Operating System (IOS) currently follows RFC 2401 and RFC 2406 to prevent Session Reply attacks."

- **UCR 2008:** 5.3.5.3.10.25, **RFC** 4022.
  Requirement: The system shall support the TCP Management Information Bases (MIB) as defined in RFC 4022.
  Finding: The SUT does not support TCP MIBs as defined in RFC 4022.
  Vulnerability: In addition to MIB vulnerabilities, the tcpConnectionState and tcpConnState objects have a MAX-ACCESS clause of read-write, which allows termination of an arbitrary connection. Unauthorized access could cause a DoS, release of private information, and release of port information without an attacker having to run a port scanner.
  Components Affected (2): Cisco 3845 and Cisco 2851.
  Cisco's Mitigation: "The SUT queries MIBs using Simple Network Management Protocol (SNMP). SNMP is not configured in the SUT. Site policy should state that SNMP should not be configured for these devices."

- **UCR 2008:** 5.3.5.3.10.26 **RFC:** 4113
  Requirement: The system shall support the UDP MIBs as defined in RFC 4113.
  Finding: The SUT does not support UDP MIBs defined in RFC 4113.
  Vulnerability: Failure to properly implement this MIB may result in an intruder altering or creating any management object in the MIB module. Port information is discoverable without an attacker running a port scan.
  Components Affected (2): Cisco 3845 and Cisco 2851
  Cisco's Mitigation: "MIBs are queried using Simple Network Management Protocol (SNMP). SNMP is not configured in the SUT. Site policy should state that SNMP should not be configured for these devices."

- **CAT III** None

Conclusions/Recommendations

Unified Communication Manager met some of the requirement listed in the UCR.

D.16 Foundry-Brocade Assured Services Local Area Network (ASLAN) and Non-ASLAN V6 with Specified Software Releases (Tracking Number 0833804)

Testing Organization and Publication Date

JITC
August 3, 2009

Summary

The test was to evaluate the Foundry-Brocade ASLAN and Non-ASLAN V6 with the UCR. The Foundry-Brocade ASLAN and Non-ASLAN V6 devices are voice telecommunications equipment and categorized in the UCR IPv6 Profile as Switches. The objective of this test was to verify the SUT could create or receive, process, and send or forward IPv6 packets in a mixed IPv4/IPv6 environment.

Test and Evaluation Method

Demonstration

Joint Staff Operational Criteria Tested

2 (2.3)
3 (3.1, 3.2, 3.3, 3.4)
8 (8.1)

Configuration

SUT Description

The SUT transports voice signaling and media as part of an overall VoIP system. All of the SUT switches provide availability, security, and QoS to meet the operational requirements of the network and Assured Services for the warfighter. The SUT components which are bolded and underlined in the tables throughout this certification letter, are the components tested in the JITC laboratory for this certification. The certified ASLAN supports DSN Assured Services over IP.

The SUT is composed of the following components:

The NetIron XMR, NetIron MLX, and BigIron RX series deliver scalable performance and port density across several chassis configurations. The NetIron XMR, NetIron MLX, and BigIron RX series are available in a 4-, 8-, 16-, and 32-slot chassis. These switches feature a range of integrated services modules, including 10-gigabit fiber, 1-gigabit fiber, and 10/100/1000BaseT modules. Users can connect to the LAN for data and voice applications using the 10/100/1000BaseT Ethernet interface on the access devices. The Core distribution and access layer certified NetIron XMR, MLX, and BigIron RX series switches, are deployable as a component in an ASLAN or non-ASLAN. The NetIron XMR, NetIron MLX, and BigIron RX

series were tested for 100/1000/10000 Megabits per second (Mbps) data load throughput. The NetIron XMR, NetIron MLX, and BigIron RX series met all IPv4, IPv6, and Core requirements.

The FastIron Super X chassis series (Super X and SX800/SX1600) delivers scalable performance and port density across two chassis configurations. The FastIron Super X series is available in an 8- or 16-slot chassis. The FastIron Super X series features a range of integrated services modules, including 10-gigabit fiber, 1-gigabit fiber, and 10/100/1000BaseT modules. Users can connect to the LAN for data and voice applications using the 10/100/1000 BaseT Ethernet interface on the access devices. The FastIron Super X series provides QoS and ACL capabilities for control of data entering the network. The Core distribution and access layer certified FastIron Super X series are deployable as a component in an ASVALAN or VALAN. The FastIron Super X series was tested for 100/1000/10000 Mbps data load throughput. The FastIron Super X series met all IPv4 and IPv6 requirements.

The FastIron Edge X series delivers performance and port density across four factory configured standalone units. The FastIron Edge X series is available in a model X424-Power over Ethernet (PoE), X424, X424HF, X448, X648, X624 and X624HF standalone units. The FastIron Edge X series features a range of factory installed services interfaces, including 1-gigabit fiber, 10/100/1000BaseT and 10 Gigabit interfaces. For data and voice applications, users can connect to the LAN using the 10/100/1000BaseT Ethernet interface on these access devices. The FastIron Edge X series provides QoS and ACL capabilities for control of data entering into the network. The Core distribution and access layer certified FastIron Edge X series is deployable as a component in an ASVALAN or VALAN. The FastIron Edge X series was tested for 100/1000/10000 Mbps data load throughput. The FastIron Edge X series met all IPv4 and IPv6 requirements.

The FastIron GS/LS series delivers performance and port density across six factory configured standalone units. The FastIron GS/LS series is available in a model FGS 648P-PoE, FGS 624P-PoE, FGS648, FGS624, FLS648, and FLS624 standalone units. The FastIron GS/LS series features a range of factory installed services interfaces, including 1-gigabit fiber, and 10/100/1000BaseT interfaces. Users can connect to the LAN for data and voice applications, using the 10/100/1000 BaseT Ethernet interface on these access devices. The FastIron GS/LS series provides QoS and ACL capabilities for control of data entering into the network. The Core distribution and access layer certified FastIron GS/LS series is deployable as a component in an ASVALAN or VALAN. The FastIron GS/LS series was tested for 100/1000 Mbps data load throughput. The FastIron GS/LS series met all IPv4 and IPv6 requirements.

The FastIron FWS series delivers performance and port density across six factory configured standalone units. The FastIron FWS series is available in a model FWS 648G-PoE, FWS648G, FWS648, FWS624G-PoE, FWS624G and FWS624 standalone units. The FastIron FWS series features a range of factory installed services interfaces, including 1-gigabit fiber, and 10/100/1000BaseT interfaces. Users can connect to the LAN for data and voice applications using the 10/100/1000 BaseT Ethernet interface on these access devices. The FastIron FWS series provides QoS and ACL capabilities for control of data entering into the network. The Core distribution and access layer certified FastIron FWS series is deployable as a component in

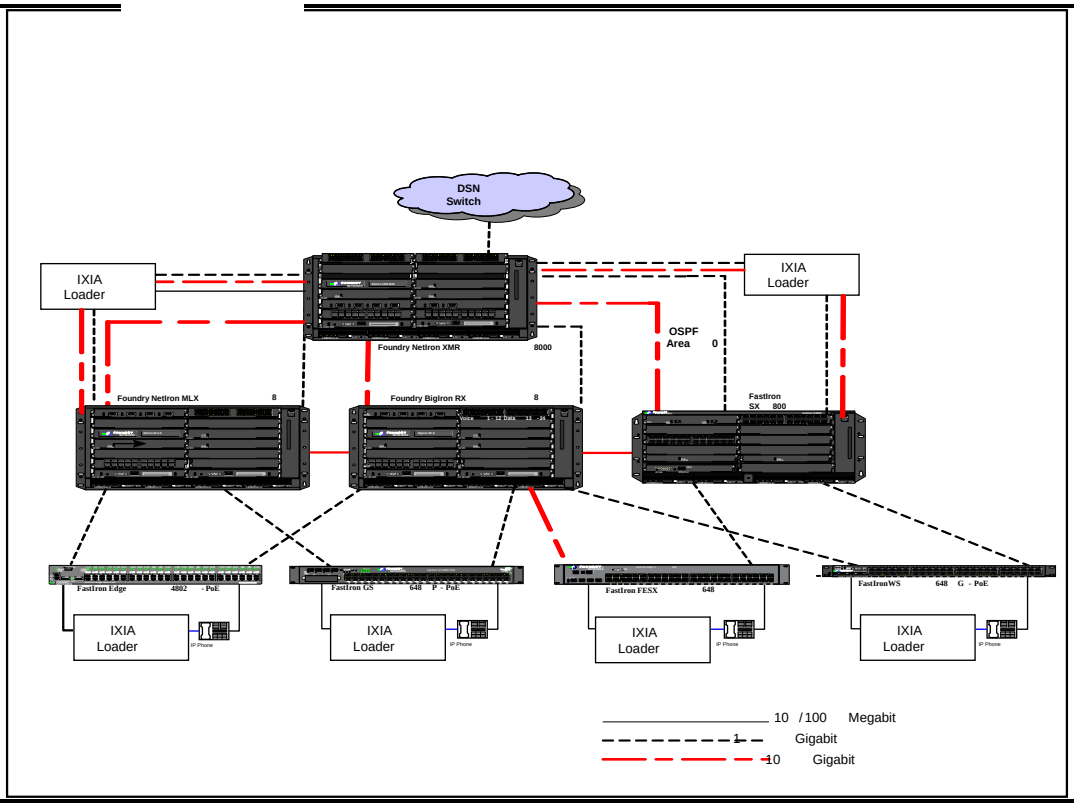
an ASVALAN or VALAN. The FastIron FWS series was tested for 100/1000 Mbps data load throughput. The FastIron FWS series met all IPv4 and IPv6 requirements.
The FastIron Edge series delivers performance and port density across two factory configured standalone units. The FastIron Edge series is available in a model FES2402-PoE, FES4802-PoE, FES2402, FES4802 and FES12GCF standalone units. The FastIron Edge series features a range of factory installed services interfaces, including 1- gigabit fiber and 10/100BaseT interfaces. Users can connect to the LAN for data and voice applications using the 10/100BaseT Ethernet interface on these access devices. The FastIron Edge series provides QoS and ACL capabilities for control of packets entering into the network. The Core distribution and access layer certified FastIron Edge series is deployable as a component in an ASVALAN or VALAN. Testers analyzed the FastIron Edge series for 100 Mbps data load throughput. The FastIron Edge series met all IPv4 and IPv6 requirements.

Operational Architecture

The DSN architecture is a two-level network hierarchy consisting of DSN backbone switches and Service/Agency installation switches. Authorized Service/Agency installation switches, extend voice services over IP infrastructures.

Test Network Description

The JITC's GIG Network Test Facility (GNTF) performed SUT testing in a manner and configuration similar to that of the DSN operational environment. Figure D-16 is the test configuration used.



NOTE: The SUT ASLAN as a Duel processors per chassis and must be deployed with a dual chassis for the Core or distribution layers.

LEGEND:

ASLAN	Assured Services Local Area Network	IP	Internet Protocol
DSN	Defense Switched Network	SUT	System Under Test

Figure D-16. SUT Test Configuration

System Configurations

Table D-20 provides the system configurations, hardware, and software components tested with the SUT. The certified SUT is deployable with switching systems listed on the UC APL for use with a certified ASLAN or non-ASLAN device.

Table D-19. Tested System Configuration

5.1.1.1 System Under Test Components with Current Operating System			
Component (See note 1.)	**Release**	**Sub-component** (See note 1.)	**Function**
Foundry NetIron XMR 4000/8000/16000/32000	FI 4.0.0b	NI-XMR-MR	Core Processor for 4000/8000/16000 system
		NI-XMR-32-MR	Core Processor for 32000 system
		NI-X-SF1	Switch Fabric for 4000 system
		NI-X-SF3	Switch Fabric for 8000/16000 system
		NI-X-32-SF	Switch Fabric for 32000 system
		NI-XMR-10Gx2	2 Port 1/10 Gig fiber module
		NI-XMR-10Gx4	4 Port 1/10 Gig fiber module
		NI-XMR-1Gx20-SFP	20-Port 1 Gig fiber module
		NI-XMR-1Gx20-GC	20-Port 10/100/1000 Mbps copper module
Foundry NetIron MLX 4/8/16/32	FI 4.0.0b	NI-MLX-MR	Core Processor for 4/8/16 system
		NI-MLX-32-MR	Core Processor for 32 system
		NI-X-SF1	Switch Fabric 4 system
		NI-X-SF3	Switch Fabric 8/16 system
		NI-X-32-SF	Switch Fabric 32 system
		NI-MLX-10Gx2	2 Port 1/10 Gig fiber module
		NI-MLX-10Gx4	4 Port 1/10 Gig fiber module
		NI-MLX-1Gx20-SFP	20-Port 1 Gig fiber module
		NI-MLX-1Gx20-GC	20-Port 10/100/1000 Mbps copper module
		NI-MLX-1Gx48-T	48-port 10/100/1000Base-T, MRJ21 module
Foundry BigIron RX 4/8/16/32	FI 2.7.01	RX-BI-MR	Core Processor with 512MB Memory
		RX-BI-MR2	Core Processor with 2GB Memory
		RX-BI-32-MR	Core Processor with 512MB Memory for RX-32
		RX-BI-32-MR2	Core Processor with 2GB Memory for RX-32
		RX-BI-SFM1	Switch Fabric for RX-4
		RX-BI-SFM3	Switch Fabric for RX-8 and RX-16
		RX-BI-32-SFM	*5.1.1.2 Switch Fabric for RX-32*
		RX-BI-BI2XG	*5.1.1.3 2 Port 1/10 Gig fiber module*
		RX-BI-BI4XG	*5.1.1.4 4 Port 1/10 Gig fiber module*
		RX-BI-BI24F	*5.1.1.5 24-Port Gig Ethernet SFP module*
		RX-BI-BI24HF	*5.1.1.6 24-Port 100/1000 Ethernet SFP module*
		RX-BI-BI24C	*5.1.1.7 24-Port 10/100/1000 Mbps copper module*
		RX-BI-16XG	*5.1.1.8 16-port 10GbE SFP+ module*
FastIron SX 800[2]/SX 1600/ FastIron Super X 800/1600	FI 5.0.00	SX-FIZMR	Core Processor SX-800 / SX-1600
		SX-FI12GM-4	12 Port 10/100/1000 Copper / Fiber Core Processor Super X
		FI-FISF	Switch Fabric SX-800 / SX-1600
		SX-FI42XG	2 Port XFP 10 Gig Ethernet module
		SX-FI42XGW	2 Port LAN/WAN XFP 10 Gig Ethernet module
		SX-FI424F	24-Port mini-GBIC based Ethernet module
		SX-FI424C	24-Port 10/100/1000 Ethernet module
		SX-FI424HF	24-Port 10/100/1000 Combo Fiber Ethernet module
		SX-FI424P	24-Port 10/100/1000 Ethernet module with PoE
		SX-FIZMR-6-PREM6	Zero Port Core Processor SX-800 / SX-1600
		SX-FI624HF	24-Port 10/100/1000 Combo Fiber Ethernet module
		SX-FI62XG	2 Port XFP 10 Gig Ethernet module
		SX-FI624P	24-Port 10/100/1000 Ethernet module with PoE
		SX-FI624C	24-Port 10/100/1000 Ethernet module
		SX-24GCPOE	PoE Module to upgrade non PoE copper ports to POE

Table D-19. Tested System Configurations (continued)

Component (See note 1.)	Release	Sub-component (See note 1.)	Function
FastIron SX 800[2]/SX 1600/ FastIron Super X 800/1600	FI 5.0.00	SX-FI8GMR6	4 Port 10/100/1000 Copper + 4 Port 1000 SFP Core Processor SX-800 / SX-1600
		SX-FI8GMR6-PREM6	4 Port 10/100/1000 Copper + 4 Port 1000 SFP Core Processor SX-800 / SX-1600
		SX-FI2XGMR6	2 Port XFP 10 Gig Ethernet Core Processor Module
		SX-FI2XGMR6-PREM6	2 Port XFP 10 Gig Ethernet Core Processor Module
		SX-FI8GMR6	4 Port 10/100/1000 Copper + 4 Port 1000 SFP Core Processor SX-800 / SX-1600
		SX-FI8GMR6-PREM6	4 Port 10/100/1000 Copper + 4 Port 1000 SFP Core Processor SX-800 / SX-1600
FastIron FESX648[2]/ FESX624/FESX624 HF/FESX424/ FESX424-PoE/ FESX424HF/FESX448	FI 5.0.00	Not Applicable	Not Applicable
FastIron Edge 4802-PoE/FES2402-PoE/FES4802/FES2402/ FES12GCF	FI 4.1.01	Not Applicable	Not Applicable
FastIron GS648P-PoE FGS624P-PoE/FGS648P/ FGS624P/FLS648/ FLS624	FI 4.3.02	Not Applicable	Not Applicable
FastIronWS648G-PoE/FWS648G/ FWS648-PoE/FWS648/ FWS624G-PoE/FWS624G/ FWS624-PoE/FWS624	FI 4.3.02	Not Applicable	Not Applicable

NOTES:
1 Components bolded and underlined were tested by JITC. The other components in the family series were not tested; however, they utilize the same software and hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes and they are also certified for joint use.
2 Indicates these switches support one processor and must be configured to failover to a redundant distribution switch.

LEGEND:

CRs	Capability Requirements
E	Enhanced
FRs	Feature Requirements
FX-MT	Foreign Exchange, ATM Term
GB	Gigabit GBIC
IOS	Internetwork Operating System
JITC	Joint Interoperability Test Command
L2	Layer 2
L3	Layer 3
ME	Metro Ethernet
NEB	Network Equipment Building
RJ	Registered Jack
S	Standard
SFP	Small Form Factor Pluggable
SUP	Supervisor
SUT	System Under Test
TX	The designation of a copper RJ-45 connection for Fast Ethernet
WS	Workgroup Switch

Results

Interoperability IPv6 Test Discrepancies

SUT IPv6 compliance is determined by a vendor's LoC. The vendor stated, in writing, compliance to the following criteria:

- Conformant with IPv6 standards profile contained in the DoD DISR.
- Maintaining interoperability in heterogeneous environments and with IPv4.
- Commitment to upgrade as the IPv6 standard evolves.
- Availability of contractor/vendor IPv6 technical support.

Testers noted the following Interoperability IPv6 test discrepancies reports (TDRs) during testing:

- **TDR# F1001**
  Short Title: SUT does not support privacy extensions for stateless address autoconfiguration as defined in RFC 3041.
  Reference: UCR 2007 Appendix 11 Paragraph A11. 3.12.6
  Test Description:
  Per the reference, if the system supports stateless IP address autoconfiguration then the system shall support privacy extensions for stateless address autoconfiguration as defined in RFC 3041. The SUT does not support RFC 3041.
  Note: DISA adjudicated the above discrepancy as having a minor operational impact.

Conclusions/Recommendations

Foundry-Brocade ASLAN and non-ASLAN V6 with specified software releases is certified with switching systems listed on the UC APL that are certified for use with an ASLAN or non-ASLAN.

D.17 Juniper MX240/480/960 and EX4200/3200 Release JUNOS 9.3 (Tracking Number 0907901).

Testing Organization and Publication Date

JITC
August 3, 2009

Summary

The test evaluated the Juniper MX240/480/960 and EX4200/3200 with the UCR. The UC APL categorizes the Juniper MX240/480/960 and EX4200/3200 devices in the UCR IPv6 Profile as Routers and Switches. The objective of this test was to verify the SUT could create or receive, process, and send or forward IPv6 packets in a mixed IPv4/IPv6 environment.

Test and Evaluation Method

Demonstration

Joint Staff Operational Criteria Tested

2 (2.3)
3 (3.1, 3.2, 3.3, 3.4)
8 (8.1)

SUT Description

The Juniper Networks ASLAN provides secure communication using Juniper Networks MX Ethernet Services Routers and EX Ethernet Switches. Deployed on a network behind a firewall and integrated into the data enterprise applications/solution is the Juniper ASLAN. The ASLAN consists of a core layer where the Juniper Networks MX-480 Ethernet Services Routers reside, a distribution layer where the MX-240 and MX-480 Ethernet Services Routers reside, and an access layer for EX-3200 or EX-4200 VC Ethernet switches.

- **MX-480 (Core).** The MX-480 Ethernet Services Router is an Ethernet-optimized edge router that supports both switching and carrier-class Ethernet routing
- **MX-240 (Distribution).** The MX-240 Ethernet Services Router is an Ethernet-optimized edge router that provides both switching and carrier-class Ethernet routing, with a capacity of up to 120 Gbps, full duplex.
- **MX-480 (Distribution).** The MX-480 Ethernet Services Router is an Ethernet-optimized edge router that supports both switching and carrier-class Ethernet routing.
- **EX-3200 (Access).** The EX-3200 switches provide connectivity for low-density environments.
- **EX-4200 (Access).** The EX-4200 switches provide connectivity for medium and high-density environments and scalability for growing networks.

Operational Architecture

The DSN architecture is a two-level network hierarchy consisting of DSN backbone switches and Service/Agency installation switches. Service/Agency authorized installation switches to extend voice services over IP infrastructures.

Test Network Description

Testing occurred at JITC's GNTF in a manner and configuration similar to that of the DSN operational environment.

System Configurations

Table D-20 provides the system configurations, hardware, and software components tested with the SUT. Testing occurred in an operationally realistic environment to determine interoperability.

Table D-20. Tested System Configuration

System Name	Hardware/Software Release		
Required Ancillary Equipment	Active Directory		
	Remote Authentication Dial-In User Service		
	SysLog Server		
Juniper MX240/480/960 EX4200/3200 Rel. JUNOS 9.3	**Hardware**	**Card Name / Part Number/ Name**	**Software/ Firmware**
	Management Workstation (Site Provided)	NA	Windows XP Pro SP3
	MX-480 (Core)	MX-480BASE-DC	JUNOS 9.3 R2.8
		RE-S-2000	
		RE-S-2000	
		DPCE-R-Q-4XGE-XFP	
		DPCE-R-Q-20GE-SFP	
		DPCE-R-2XGE-XFP	
		DPCE-R-40GE-TX	
		MS-DPC	
	MX-240 (Distribution)	MX240BASE-DC	JUNOS 9.3 R2.8
		RE-S-1300	
		RE-S-1300	
		DPCE-R-Q-20GE-SFP	
		DPCE-R-2XGE-XFP	
		DPCE-R-Q-20GE-SFP	
		DPCE-R-2XGE-XFP	
	MX-480 (Distribution)	MX-480BASE-DC	JUNOS 9.3 R2.8
		RE-S-1300	
		RE-S-1300	
		DPCE-R-2XGE-XFP	
		DPCE-R-Q-20GE-SFP	
		DPCE-R-2XGE-XFP	
		DPCE-R-40GE-TX	
		DPCE-R-40GE-TX	
	EX-3200 (Access)	EX-3200-48P	JUNOS 9.3 R2.8
		EX-SFP-1GE-SX	
		EX-SFP-1GE-SX	
	EX-4200 (Access)	EX4200-24F	JUNOS 9.3 R2.8
		EX4200-24F	
		EX4200-48P	
		EX-SFP-1GE-SX	
		EX-SFP-1GE-SX	
		EX-UM-2XFP	
		EX-SFP-1GE-SX	
		EX-SFP-1GE-SX	
		EX-UM-2XFP	

LEGEND:

DC	Direct Current	Rel.	Release
DPCE	Dense Port Concentrators Ethernet	SFP	Small Form Pluggable
FP	Form Factor Pluggable	SP3	Service Pack 3
NA	Not Applicable	TX	Transmission
P	Pluggable	UM	Uplink Module
Pro	Professional	XFP	Small Form Factor Pluggable
R	Release	XP	Experience Professional
RE	Routing Engine		

Interoperability IPv6 Test Discrepancies

The SUT's IPv6 compliance is determined by a vendor's signed LoC. The vendor stated, in writing, compliance to the following criteria:

- Conformant with IPv6 standards profile contained in the DoD DISR.

- Maintaining interoperability in heterogeneous environments and with IPv4.
- Commitment to upgrade as the IPv6 standard evolves.
- Availability of contractor/vendor IPv6 technical support.

Testers noted the following Interoperability IPv6 TDRs during testing:

- **TDR# 93002**
  Short Title: UCR MX-240 (Distro 1) processor failover for IPv4 and IPv6 Exceeds five Seconds or less Requirement.
  Test Results:
  The backup processor took 6.36 seconds to take over as the active processor.
  Expected Results:
  Per the reference, failover to the secondary device must occur within five seconds.

- **TDR# 93003**
  Short Title: Link failover of EX 3200 and EX4200 does not meet five Seconds or fewer requirements.
  Test Setup/Conduct:
  With an Ixia IPv4 and IPv6 bidirectional data load and VoIP "pairs" running, pulled the active link to failover to the secondary link on the EX 3200 and EX-4200 switches.
  Test Results:
  After pulling the primary link, it took 30 seconds for path restoration.
  Expected Results:
  Per the reference, failover to the secondary device must occur within five seconds.

- **TDR# 93006**
  Short Title: Distribution chassis failover exceeds five seconds.
  Test Setup/Conduct:
  With an Ixia IPv4 and IPv6 bidirectional data load and VoIP "pairs" running. Disabling the active distribution (distribution 1, MX-240) forcing the standby chassis (distribution 2, MX-480) to become the primary distribution box.
  Test Results:
  Some of the Ixia Chariot IP streams not originating or terminating in distribution 1, ceased flowing and did not resume until distribution 1 was enabled and assumed Master.
  Expected Results:
  Per the reference, failover to the secondary device must occur within five seconds.

- **TDR# 93007**
  Short Title: OSPF Cost/Metrics are ignored.
  Reference: DISR product profile required RFCs in UCR table 5.3.5-7.
  Test Description:
  Test Setup/Conduct:
  OSPF (V 2 for IPv4 and V 3 for IPv6) configuration included different cost/metric as shown in the test diagram.

Test Results:
Traffic continued to use the high (5) cost/metric link (A) instead of the lower cost/metric path (link B and C) to the Core from the Distribution. Testers verified path utilization by examining buffer utilization within the SUT.
Expected Results:
OSPF protocol should route traffic via the path with the lowest cost/metric. Non-configurable vendor specific features within the router/switch should not override settings configured within OSPF. This causes OSPF to operate in a non-standard/non-interoperable environment.

- **TDR# 93008**
  Short Title: IPv6 Neighbor Discovery requires "Optional" field populated for required failover performance.
  Test Setup/Conduct:
  SUT operating with Ixia IPv4 and IPv6 bidirectional data load, and VoIP "pairs" running.
  Test Results:
  The SUT populates MAC address tables based upon recommended fields. Unlisted fields violate the requirements for Unicast ICMP Neighbor Discovery packets, and causes slow recovery in failover scenarios for IPv6 traffic unless the end instrument also populates the field, which is not mandated in RFC 2461.
  Expected Results:
  Each Unicast frame/packet from the Ixia contains the MAC source, MAC destination, VLAN identifier, IP source, and IP destination address in the header. All the information needed to populate VLAN tables within the SUT is available without additional informational fields. The SUT should populate its tables from the header portion of Unicast frames/packets. Multiple RFCs mandate population of the header fields. The SUT shall conform to the required part of RFC 2461, and populate tables accordingly without dependency on features not required within the RFC.

Conclusions/Recommendations

Juniper MX240/480/960 and EX4200 is on the UC APL of devices certified for use with an ASLAN or non-ASLAN.

D.18 Motorola Point to Point (PTP) 600 Network Element with Software Release 08-32 (Tracking Number 0823901)

Testing Organization and Publication Date

JITC
August 3, 2009

Summary

The test evaluated the PTP 600 Network with the UCR. The UCR categorizes the Motorola PTP 600 Network device as an Ethernet bridge. The objective of this test verified the SUT could create or receive, process, and send or forward IPv6 packets in a mixed IPv4/IPv6 environment.

Test and Evaluation Method

Demonstration

Joint Staff Operational Criteria Tested

2 (2.3)
3 (3.1, 3.2, 3.3, 3.4)
8 (8.1)

Configuration

SUT Description

Motorola PTP 600 is a PTP bridge that supports a variety of fixed and portable communications devices over a high availability wireless Ethernet bridge. The Motorola PTP operates in the 4.4 to 4.8 Giga Hertz (GHz) spectrum (PTP 45600 and 48600) at data rates up to 300 Mbps for the 45600 and 200 Mbps for the 48600 and the 5.4 - 5.8 GHz spectrum (PTP 54600 and 58600) at data rates up to 300 Mbps. The system communicates with Motorola proprietary software, Advanced Encryption Standard, encrypted for securing communications. The PTP 600 Series has a connectorized (for use with external antennas) version and an integrated version (with built-in antenna). All PTP 600 frequency variants and connectorized/integrated variants use the same software. Configuring a given PTP 600 can act as either the Master or Slave end of a link. The PTP 600 device supports three types of network interfaces: an Ethernet interface (10/100/1000 Mbps copper). Although the SUT supports 1000 Mbps, no 1000 Mbps support is available Ethernet because of Layer-3 prioritization, only the 10/100 Mbps copper Ethernet interfaces are certified. The device supports 1000 Mbps Fiber without certification. T1/E1 Time Division Multiplexer interface (1 or 2 T1/E1s supported); both can be active at the same time.

Operational Architecture

The Motorola PTP 600s are PTP devices fielded in pairs. The SUT pairs are employable as a Strategic Network Element in the DSN Backbone.

Test Network Description

Testers analyzed the SUT at JITC's GNTF in a manner and configuration similar to that of the DSN operational environment. Figure D-17 is the test configuration used.

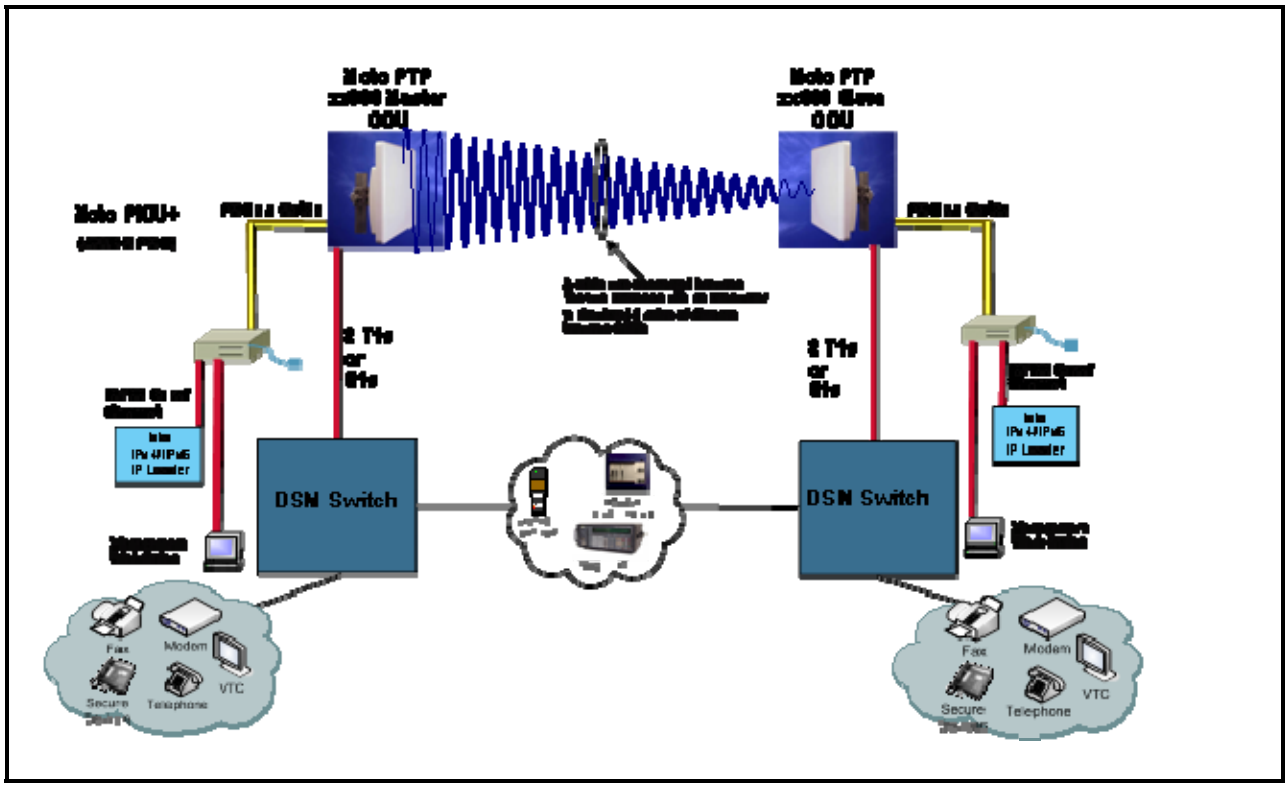


Figure D-17. SUT Test Network

System Configurations

Table D-21 provides the system configurations, hardware, and software components tested with the SUT. Testers analyzed the SUT in an operationally realistic environment to determine interoperability.

Table D-21. Tested System Configurations

System Name	Software
Nortel CS 2100	SE 09.1
Alcatel Lucent 5ESS	5E16 BWM08.0003
Nokia Siemens EWSD	19d Patch Set 46
Avaya S8710	CM 4.0 (R014X.00.2.731.7 Super Patch 14419)

System Under Test			
	Hardware (See note 1)	**Cards/Hardware**	**Software/Firmware**
Motorola PTP 600	Motorola PTP 45600 (4.5 GHz) PIDU & ODU (Master and Slave)	WB3040 (Integrated, Link)[2] WB3041 (Connectorized, Link) WB3044 (Integrated, End) WB3045 (Connectorized, End)	08-32
	Motorola PTP 48600 (4.8 GHz) PIDU & ODU (Master and Slave)	WB3378 (Integrated, Link) WB3379 (Connectorized, Link) WB3382 (Integrated, End) WB3383 (Connectorized, End)	
	Motorola PTP 54600 (5.4 GHz) PIDU & ODU (Master and Slave)	BP5530BH-1 (Integrated, End) BP5530BH-2 (Integrated, Link) BP5530BHC-1 (Connectorized, End) BP5530BHC-2(Connectorized, Link)	
	Motorola PTP 58600 (5.8 GHz) PIDU & ODU (Master and Slave)	BP5830BH -1 (Integrated, End) BP5830BH -2 (Integrated, Link) BP5830BHC-1 (Connectorized, End) BP5830BHC-2 (Connectorized, Link)	

NOTES:

1. All the Motorola PTP xx600 series are certified within the DSN the only difference between them are the radio frequencies of the units, but all have the same software installed.
2. Integrated Link is with a built-in antenna, as a pair.
3. Connectorized Link is use with external antennas, as a pair.
4. Integrated End is a single PIDU and ODU as one.
5. Connectorized End is a single PIDU and the ODU.

LEGEND:

CM	Communication Manager	ODU	Outdoor Unit
CS	Communication Server	PIDU	Power InDoor Unit
EWSD	Elektronisches Wählsystem Digital	PTP	Point-to-Point
GHz	Giga Hertz	5ESS	Electronic Switching System

Results

Interoperability IPv6 Test Discrepancies

The SUT's IPv6 compliance is determined by a signed vendor's LoC. The vendor states, in writing, compliance to the following criteria:

- Conformant with IPv6 standards profile contained in the DoD DISR.
- Maintaining interoperability in heterogeneous environments and with IPv4.
- Commitment to upgrade as the IPv6 standard evolves.
- Availability of contractor/vendor IPv6 technical support.

Testers noted the following Interoperability IPv6 TDR during testing:

- **TDR# 07001**
  Short Title: SUT does not support QoS Queuing with Layer-3 DSCP (IPv4) or Traffic Class (IPv6)
  Test Description:
  The SUT supports Queuing with Layer-2 (Institute of Electrical and Electronic Engineers 802.1p) only. No support for the Layer-3 QoS with DSCP for IPv4 or with Traffic Class (IPv6). Per the UCR reference, the minimum requirement for Video and VoIP systems is to support tagging for the purpose of prioritization queuing at Layer-3 with DSCP (IPv4) and Traffic Class (IPv6). The Layer-2 Tagging/Queuing is conditional.

Conclusions/Recommendations

The Motorola PTP 600 Network met most of the UCR requirements as an Ethernet bridge and listed on the UC APL.

D.19 McAfee IntruShield 3000 Intrusion Prevention System Internet Protocol Version Six Test Report

Testing Organization and Publication Date

NSA
February 2, 2009

Summary

The NSA conducted T&E of the McAfee IntruShield 3000 IPS to verify if it meets the objectives of the DoD IPv6 MTPv2.0, Section 2.7. The test is also a functional demonstration of the SUT for the Joint Staff Operational Criteria.

Test and Evaluation Method

Demonstration

Joint Staff Operational Criteria Tested

2 (2.3)
8 (8.1)

Configuration

Requirements

The IPv6 ITP, V 1.0 derived from DoD Instruction 8500.2, "Information Assurance (IA) Implementation," and Director of Central Intelligence Directive 6/3, "Protecting Sensitive Compartmentalized Information within Information Systems" provided the test requirements for the McAfee IntruShield 3000. It identifies three types of requirements used to assess a vendor's product: Conformance, Functionality, and Performance. The IPS section of the ITP defines 724 requirements that an IPS should perform in order to properly safeguard DoD networks.

Procedures

The ITP defines the test procedures followed by the Test Team to evaluate the conformance, functionality, and performance of IA devices. It includes 42 procedures to fully evaluate the IPS requirements in the ITP. McAfee Inc., provided an LoC to meet the conformance requirements and address their private testing of RFC conformance. The functional testing of the McAfee IntruShield 3000 included evaluation of eight functional areas including verification of the Federal Information Processing Standard 140-2 Certification completed by the National Institute of Standards and Technology as the United States Cryptographic Module Validation Authority. Testers analyzed performance in accordance with the ITP.

Testing Categories

- Conformance: Compliance with the appropriate DISR mandated or emerging standard determined success. If no standard exists and an assessment is still required, then reasonable compliance with industry accepted RFCs constitutes success.
- Functionality: The device or application having the capability to deliver its required/expected services determined success.
- Performance: The device or application meeting the Key Performance Parameters (KPP) as set by the JCOS. In the absence of KPP, obtaining the data necessary for decision-makers to make informed decisions regarding KPP determined success.

Tools

The test platforms used in the McAfee IntruShield 3000 IPS test included clients and servers, which met the Security Technical Implementation Guidelines (STIGs) published by the DISA Field Security Operations (FSO). Other traffic and threat generators included the Spirent Test Center, Avalanche/Reflector, and ThreatEx platforms.

Configuration

The McAfee IntruShield 3000 IPS test configuration emulated a realistic enclave boundary on an operational network while remaining in a controlled non-operational environment. The test scenarios used routers, switches, and other devices (web, email, and AAA servers). Traffic and Threat generators were used in-line with actual clients and servers to provide a test environment as operationally realistic as possible for testing IA devices. The diagram illustrated in Figure D-18 is an example of a test scenario used in completing the McAfee IntruShield 3000 IPS evaluation.

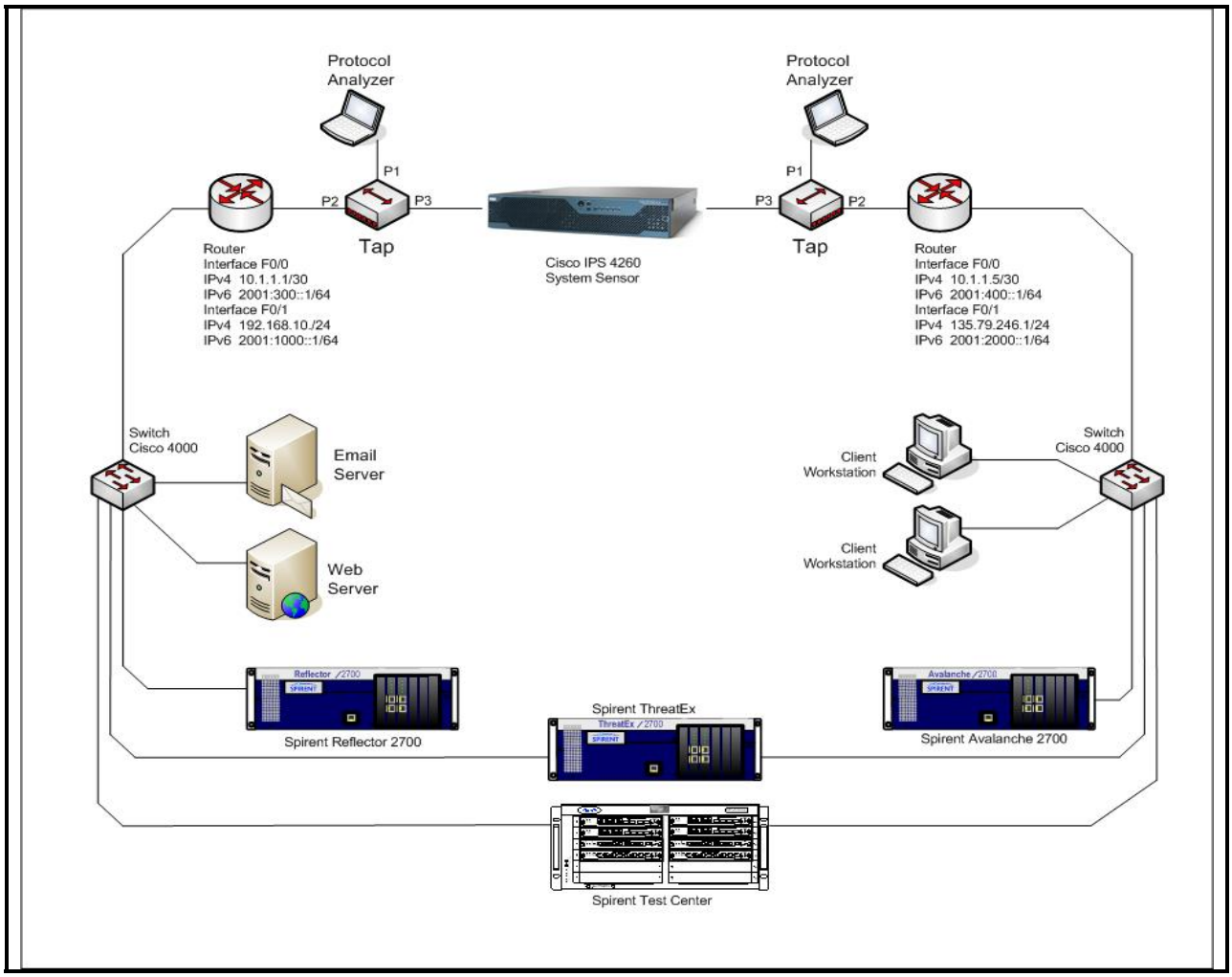


Figure D-18. IPv6 Test Configuration

The Test

The 10 test objectives were:

- Conformance to DISR IPv6-specific RFCs
- Confidentiality/Integrity/Availability Triad
- RBAC
- Basic IPS functionality
- Advanced IPS functionality
- Audit and alert mechanisms
- IPv6 and IPsec functionality
- Common attack defense
- Documentation
- Performance

Results

Conformance

McAfee IntruShield 3000 passed 17 out of 27 RFC conformance requirements. The major areas lacking were IPsec, Neighbor Discovery for IPv6, and MIB for IPv6.

Confidentiality/Integrity/Availability Triad

The McAfee IntruShield 3000 passed 26 of 31 for a success rate of 84 percent. The IntruShield 3000 passed all the Confidentially requirements, all the Integrity requirements except detecting or preventing session hijacking requirements, and all the Availability requirements except battery power backup and preventing or mitigating DoS attacks.

Role-based Access Control

McAfee IntruShield 3000 failed 9 of the 23 RBAC requirements. The IntruShield 3000 does not permit the security administrator to create roles with permissions that are granular enough. If able, it would have scored much higher in this objective.

Basic IPS Functionality

McAfee IntruShield 3000 passed 75 percent of the basic IPS functionality requirements. In ports, protocols, and services, it was able to block on a per-interface basis 59 of 59 filtering requirements. The IntruShield 3000 has the IPv4 and IPv6 functionality, but the implemented IPv6 functionality is in user-defined signatures. The system has a limit of 10 user-defined signatures. This limit restricts the IPS to using a small part of the IPv6 functionality at a time.

Advanced IPS Functionality

The McAfee IntruShield 3000 passed 42 of the 53 advanced functionality requirements tested. There were no notable shortcomings, but a test of environmental variables showed failures in humidity controls/alarms.

Audit and Alert Mechanisms

The McAfee IntruShield 3000 met 99 of the 120 auditing requirements and had a robust system for viewing audit reports. The system performed well on the Alarm requirements by passing all the requirements except the audible alarm requirements. The IntruShield 3000 passed 85 percent of the audit requirement, and none of the failures were significant.

IPv6 and IPsec Functionality

McAfee IntruShield 3000 did very well in this category, passing 28 of 34 IPv6-specific requirements.

Common Attack Defense

The McAfee IntruShield 3000 is very resistant to today's known attack methods. It passed 36 of 48 requirements. The IPS tested against numerous attacks including the Smurf and SYN Flood varieties of DoS and detected and blocked them. When tested against the most current set of CVEs, the IntruShield 3000 passed.

Documentation

McAfee, Inc., provided minimal documentation in addition to the documentation available on the Internet such as User and Administration Guides for the device. They did poorly in the documentation procedures, meeting only 33 of the 169 requirements. Their administration guide passed all the requirements.

Performance

The McAfee IntruShield 3000 passed 100 percent of the performance requirements in the ITP. The interfaces maintained 1 Gbps speeds even with Stateful Packet Inspection in process. Testers recorded TCP Sessions in excess of 25,000 per second.

Grading

Table D-22 provides the grading of all categories tested.

Table D-22. Test Objective Scores

Test Objective	Raw Score	Total Available	Percentage (%)	Weight (%)	Final Tally
Conformance	17	27	62.96	5	3.15
CIA	26	31	83.87	5	4.19
RBAC	9	23	39.13	5	1.96
Basic IPS	76	101	75.24	20	15.05
Advanced IPS	42	53	79.23	10	7.93
Audit/Alert	99	120	82.50	15	12.38
IPv6/IPsec	28	34	82.35	10	8.24
Attack Defense	36	48	75.00	15	11.25
Documentation	33	169	19.53	5	.98
Performance	9	9	100.00	10	10
			Totals	**100**	75.13%
				Grade	C

Conclusions/Recommendations

The McAfee IntruShield 3000 is an excellent IPv4 IDS/IPS. It makes good use of filtering and ACLs and has most of the features one looks for in IPv4 IPS. Built for speed, the IPS keeps its interfaces at line speed 1 Gbps even while under attack.

The biggest weakness in the IntruShield 3000 is the limited level of IPv6 development. Its IPv6 functionality is granular, but not thoroughly developed. Meaning, that IPv6 functionality on the

IPS requires configuration using User-Defined Signatures (UDS), and there is a limit of 10 UDS on the system. So all of the IPv6 functionality (Attack Detection, Reconnaissance Detection, Quarantine capability, Alert Filters) is there, but the device can only use a portion of it at a time. Additionally, functionality like DoS Detection and ACLs, are available only for IPv4 traffic, not IPv6 traffic. Sensor to IntruShield Security Manager communication must use IPv4. Finally, McAfee has not made significant effort to make the IPS development documentation or the results of their own vulnerability assessments of the IntruShield 3000 available. Increased availability of the IPS documentation would enable the DAA to make a more informed decision.

D.20 Joint Staff IPv6 Operational Criteria Test Report Criterion #5: Demonstrate Effective Operation in Low-Bandwidth Environment Test Report

Testing Organization and Publication Date

Army CERDEC Army Systems Engineering Office (ASEO)
August 2009

Summary

The purpose of this test report is to provide DoD leadership and the CJCS an evaluation of how IPv6 performs relative to IPv4 in tactical low-bandwidth environments based on experiments conducted by the Army CERDEC ASEO. The CJCS may use the results, conclusions, and recommendations provided to evaluate the readiness of IPv6 for use in DoD operational networks.

The DoD assigned responsibility to the Army to plan, conduct, and report on the T&E of IPv6 Joint Staff Operational Criteria 5. Two types of applications, FTP and video streaming ran across two different types of low-bandwidth links: satellite and the EPLRS radio. Each series of tests ran at a variety of bandwidth settings ranging from as high as 512 kbps over satellite to as low as 38 kbps over EPLRS. Testers collected and analyzed measurements such as the effective data rate, transfer time, and error rate, to compare the performance of an IPv4-only environment to that of a dual-stacked IPv4/IPv6 environment and an IPv6-only environment. These environments represent the current, and anticipated near-term and future DoD environments, respectively.

Test and Evaluation Method

Demonstration

Joint Staff Operational Criteria Tested

2 (2.3)
5 (5.1.1, 5.1.2)
8 (8.1)

Configuration

In accordance with the Joint Staff Operational Criteria 5 test plan, the three testbed environments created, represented current, near-term, and future tactical network conditions. The current or baseline environment was an IPv4-only mode. The near-term environment was dual-stack mode, and the future environment was IPv6-only mode. To provide a blend of 50 percent IPv4/IPv6 traffic, two clients ran identical applications simultaneously. For the baseline mode, the network infrastructure and the clients were IPv4-only, and the applications ran as IPv4-only. In the near-term the network infrastructure and clients were dual-stacked. To emulate the future environment, both clients ran IPv6 instances of the application.

Since low-bandwidth is a relative term, testers chose two scenarios, as recommended by the Joint Staff Operational Criteria 5 test plan. A satellite link represented reach-back communications operating at T1 speeds or lower, and an Army Combat Net Radio represented a low-bandwidth battlefield communications network operating as low as 38 kbps. In addition, KG-250 In-Line Encryptors (INEs) used with the satellite links more closely emulated a tactical configuration.

Tactical radios, over-the-air satellite links, commercial Cisco routers, and common user applications provided real-world conditions for testing.

The network consisted of two separate, but similar, configurations. One, for testing with EPLRS radios with bandwidth settings of 155 Kilobits per second (Kbps), 115 kbps, and 38 kbps; the other, for testing over the satellite link with bandwidth settings of 256 kbps and 512 kbps. Both of these configurations were also set up to allow switching between an IPv4-only configuration and a dual-stacked configuration for which IPv4 and IPv6 are available simultaneously on the network.

Figure D-19 shows the Joint Staff Operational Criteria 5 test bed configuration for EPLRS. The satellite configuration was the same, except a satellite link and a pair of INEs replaced the EPLRS link.

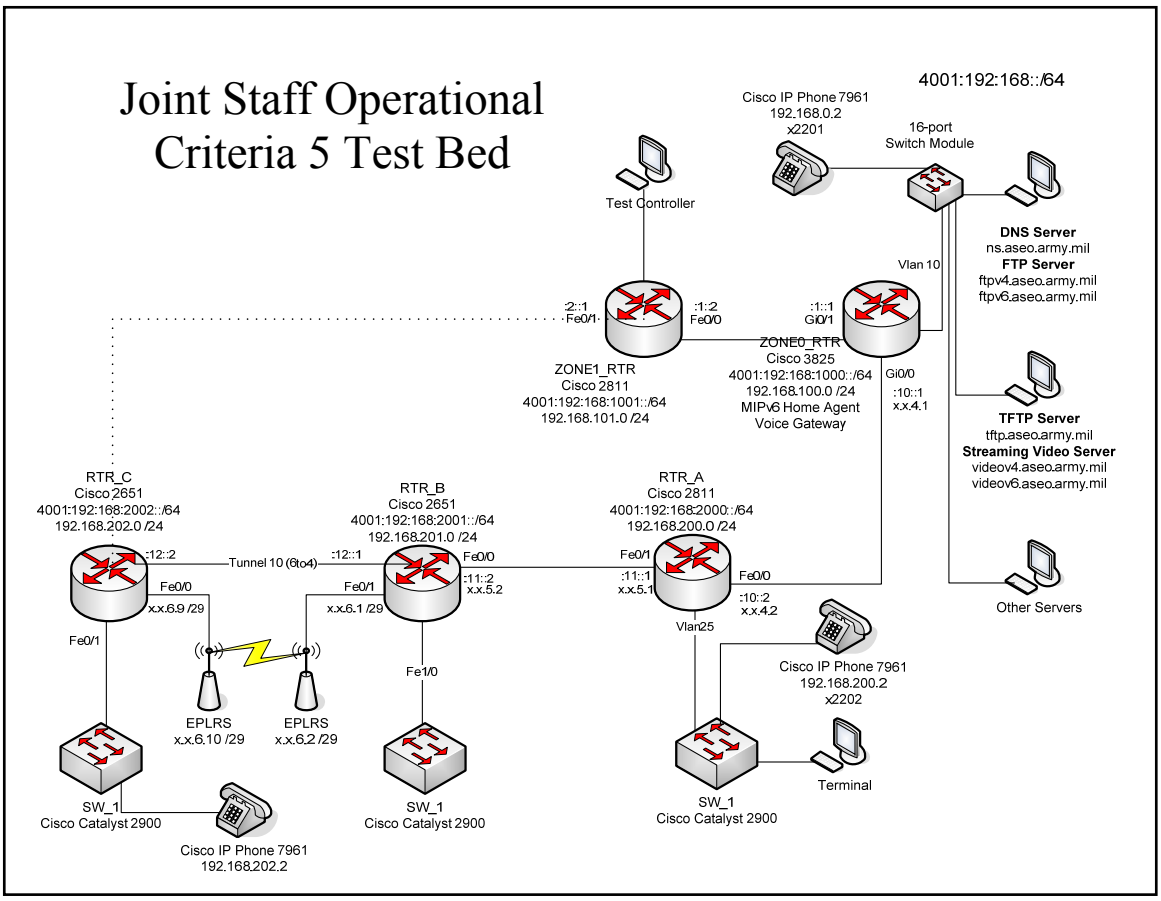


Figure D-19. Joint Staff Operational Criteria 5 Configuration for EPLRS

EPLRS Configuration

The EPLRS configuration consisted of five Cisco routers. Since EPLRS radios are currently not capable of supporting IPv6 traffic natively, testers configured RTR_B and RTR_C with an IPv6-over-IPv4 tunnel to pass IPv6 traffic successfully over the radios. IPv6_RTR_B provides a link to one EPLRS radio. Testers configured two EPLRS radios as IPv4 routers to forward traffic to each other as well as the rest of the network. IPv6_RTR_C was the location where the clients for each test reside. This router provides a link to the other EPLRS radio, thus completing the string from RTR_C to RTR_ZONE0.

Testers enabled OSPF on all routers. Since EPLRS does not support OSPF (and because testers did not want any OSPF traffic flowing over the low-bandwidth link) testers disabled OSPF on the router interfaces facing the EPLRS radios. In those cases, static routers were set up on RTR_B and RTR_C, testers configured OSPF to propagate the static routes from RTR_B to the rest of the network in the direction of RTR_ZONE0.

Satellite Communication (SATCOM) Configuration

Testers configured the SATCOM testbed very similarly to the EPLRS configuration described in Section 3.1.1, with the following changes: A Frequency Division Multiple Access satellite link replaced the EPLRS radio link on both ends. The satellite modems configured, to use a "quick setup" mode which created a Layer-2 connection across the SATCOM link. This made the IP addressing of the satellite modems irrelevant to the tests.

A KG-250 INE at each end of the SATCOM link provided encryption. These devices utilized an addressing scheme and routing table identical to the previous configuration of the EPLRS radios. Even though this version of the KG-250 could support IPv6 traffic, testers configured these devices to operate in IPv4 mode only, thus preserving the same IPv6-over-IPv4 tunnel used in the EPLRS test above. The rest of the network remained configured exactly as described. Two types of applications represented typical data that might flow over a tactical network: FTP and streaming video. Both of these applications consume significant bandwidth and provide a worst-case analysis for a stressed low-bandwidth network.

Streaming Video Testing

Streaming video was tested using a video file that was encoded using an H. 264 codec and without an audio stream. Testers used VLC as the Real-Time Streaming Protocol server which listened for connection requests from a client and then automatically started sending the video stream information using the RTP. Two instances of the video server were running, one for IPv4 and one for IPv6. When started, the client would connect to the server, request the video stream, and then play back the received video.

For each test environment (current, near-term, and future), five streaming video trials were run. Each trial used two clients controlled by the script to launch simultaneous video sessions. For the first series of trials, testers used a video file encoded at a bit-rate of 32 kbps. The second

series of trials used a video file encoded at 64 kbps. The third series of trials used a video file encoded at 96 kbps. The same high-definition quality source video encoded each file.

Using the automated script, the full battery of tests ran unattended and Wireshark collected the data. After completion, testers reconfigured the network for a different bandwidth, and the process repeated.

Results

The findings for FTP traffic indicated IPv6 performs within 10 percent of IPv4 under all conditions. Thus, for this particular type of traffic, IPv6 meets the Joint Staff Operational Criteria 5 requirement. For video streaming, high failure rates were found for both IPv4 and IPv6 when running over EPLRS at all tested bandwidth settings (38, 115, and 155 kbps), leading to the conclusion that EPLRS is not suitable for video streaming regardless of the IP version. At a bandwidth of 255 kbps over satellite, there were two critical and unexpected anomalies within the dual-stacked environment and the IPv6-only environment in which the IPv6 streaming applications exhibited unacceptable amounts of delay in launching.

In all but one case, IPv6 performance was within 10 percent of the IPv4 performance. In general, the performance of the near-term environment was within 4 percent and the future environment was within 7 percent. Header compression techniques, which are expected to become commonplace with IPv6 implementations, should improve the performance to the point where IPv6 performs better than IPv4.

It is clear that a problem exists when attempting to simultaneously launch an IPv4 and IPv6 video stream over a 256 kbps satellite link. It is not clear if this is a race condition, or if this condition occurs in an IPv4-only environment with other timing parameters modified. It is also not clear why delayed-start failures consistently occurred when running IPv6-mode over a 256 kbps satellite link.

Conclusions/Recommendations

Overall, IPv6 instances of FTP in a dual-stack and IPv6-only environment performed within the 10 percent range of the Joint Staff Operational Criteria 5 requirements for low-bandwidth operations. As the development of IPv6 compression techniques continues, the performance disparity should improve.

Video streaming over EPLRS for IPv4 and IPv6 performed poorly in all cases. Testers do not recommended permitting video streaming applications over EPLRS or similar types of tactical radio systems.

Issues with video streaming also exist when mixed IPv4/IPv6 traffic is present on a dual-stacked network using a 256 kbps satellite link, as there was a high incidence of parallel-run failures. As expected interleaving of the two video streams occurred, especially at a bandwidth of 256 kbps.

The consistent occurrence of delayed-start failures for video streaming of IPv6-only traffic across a 256 kbps satellite link is another concern. Waiting 15-20 seconds for a video streaming session to start is generally unacceptable.

Testers provided the following recommendations:

- In keeping with current practices for network traffic engineering, permit FTP using IPv6 on low-bandwidth tactical networks in accordance with the same policies and practices that are currently in effect for IPv4.
- Do not permit IPv4 and IPv6 streaming video on EPLRS networks.
- Permit IPv6 streaming video on tactical satellite links of 512 kbps or greater.
- Conduct additional testing of IPv6 streaming video in a dual-stack environment over a 256 kbps satellite link to resolve delayed-start and parallel-run failure conditions.
- Do not permit other IPv6 applications such as VoIP, VTC, and streaming video with integrated sound, on tactical low-bandwidth networks until properly tested.
- Continue to test common applications, such as VoIP, VTC, and chat, within IPv6 low-bandwidth tactical environments.
- Test and evaluate next generation IPv6 products, such as cell phones and personal electronic devices, to assess tactical feasibility.
- Continue to monitor the capabilities and availability of IPv6 compression techniques.

D.21 Evaluation of Joint Chiefs of Staff Criteria #9: IPv6 Network Management

Testing Organization and Publication Date

Air Force
June 2008

Summary

This document provides a current Network Management (NM) "snapshot" of the IPv6 advancement into the network management realm. It includes application functionality and transition capabilities of network management servers and clients. Testers also assessed the overall effects on the network through the interaction of IPv6 with the major network management protocol SNMP. Ultimately, NM capability of devices capable of using either protocol will occur over IPv4 during the dual-stack transition. In later years, as the transition continues, the trend will reverse with IPv6 being the most dominate IP used. NM is continuing to evolve and change and will eventually entail larger areas of control such as policy based management, mission-driven management, and a more involved information management role.

Test and Evaluation Method

Demonstration

Joint Staff Operational Criteria Tested

2 (2.1, 2.2)
9 (2.1, 2.2, 9.1, 9.2, 9.3)

Configuration

This report is the result of testing and the analysis of other reports submitted (some already included in this T&E report. The Network Management tools and clients tested were:

- What's Up Gold v11.01 Windows Server 2003
- Smarts InCharge 6.5.1 Windows Vista (Ultimate)
- NeuralStar 8.0.3 Cisco 3845 router (IOS 12.4(13R)T)
- HP Openview's Network Node Manager 7.5
- Cisco 2621XM (12.3(14)T3)
- CiscoWorks LAN Management 2.5.1 Juniper M7i router (JUNOS 8.4R1.13)
- Solaris 10
- Fedora Core 6 (zod) (Linux 2.6.18-1.2798.fc6)

Results

Testers successfully tested the following IPv6 Joint Staff Operational Criteria:

- JS 9.1.1.1: NM tool support for SNMP
- JS 9.1.1.2: SNMP version support within the monitored client
- JS 9.1.2.1: NM tool generates SNMP query and displays results
- JS 9.1.2.2: Dual-stack client responds to NM query
- JS 9.1.2.3: Dual-stack client generates trap
- JS 9.1.2.4: NM tool receives and displays basic trap
- JS 9.1.3.1: Availability of help support for NM tool
- JS 9.1.3.2: Availability of help support for dual-stack client
- JS 9.1.4.1: Identify how dual-stack autodiscovery is accomplished
- JS 9.1.4.2: Compare discovery approach between IPv4-only and dual-stack
- JS 9.1.4.3: Compare discovery results of IPv4-only versus dual-stack
- JS 9.1.5.1: Test ability of tool to manage 1000s of nodes
- JS 9.1.6.1: Compare and contrast how tool displays MIB information
- JS 9.2.1.2: Client sets the value as identified in SNMP Set
- JS 9.2.1.3: Client capable of being configured as dual-stack
- JS 9.2.2.1: Tool capable of recognizing change from IPv4-only to dual-stack
- JS 9.3.1.1: Tool identifies/correctly displays dual-stack client's information
- JS 9.3.1.2: Tool correctly identifies IPv4 only versus dual-stack clients
- JS 9.3.3.1: Compare IPv4 versus dual-stack using tool default MIB queries
- JS 9.3.3.2: Compare IPv4 versus dual-stack using default MIB traps
- JS 9.3.3.1: Compare IPv4 versus dual-stack using equal mappings of queries

Testers did not test the following IPv6 Joint Staff Operational Criteria:

- JS 9.1.7.1: Tool capable of displaying large enterprise of IPv4/dual-stack clients
- JS 9.3.3.2: Compare IPv4 versus dual-stack using equal mappings of traps
- JS 9.3.3.2: Compare IPv4 versus dual-stack using equal mappings of traps

Conclusions/Recommendations

It is important to reiterate here the purpose of the network management analysis conducted. As the IPv6 transition continues, it is important to maintain equivalent levels of performance in all categories of functionality with an immediate focus being on achieving this for the NIPRNet. To do this for network management, it was critical to obtain a snapshot of the current IPv6 state of NM tools and clients with the understanding that this is a baseline determination and not the end all state. This is due to the tendency that vendors are continually upgrading their software with added features to provide more functionality to meet present requirements of their customers.

General Observations

Conclusions gathered from the entirety of the work performed in this research:

- NM polling in a LAN performed over the IPv6 protocol will take a shorter amount of time than equivalent polling done over the IPv4 protocol.
- Network usage requirement for NM is higher for IPv6 than for IPv4.
- In general, much more traffic exists on the wire for IPv6 MIB requests polled over IPv4 compared to IPv4 requests polled over IPv4. There is still more traffic on the wire for MIB requests made over IPv6 compared to the same requests made over IPv4, but to a much lesser degree.
- The commercial world's definition of "IPv6 Capable" is not consistent among vendors, and thus, does not necessarily mean that products make full use of IPv6 for every feature they support.
- Implementation of the full use of the IPv6 address space available (i.e., having a large number of network nodes) may not be an issue in the area of network management since the current paradigm is to manage only a small number of critical nodes. If managing a large number of clients becomes the norm, then there would very likely be a problem with both IPv4 and IPv6.
- Controlling the amount and type of management traffic requested will act as a protection against large and burdensome traffic loads. The SNMP MIB structure easily allows flexibility when choosing what management information is necessary for each mission area or system managed. If the wrong environment requests the wrong information, the result may be an increase in the traffic load to a wasteful and perhaps unacceptable level.
- A possible explanation for higher polling times for network management traffic over IPv4 is that increased packet processing time within the NM systems. The increased processing time may be due to parsing the extra fields inherent in IPv4 headers when taking in and sending out NM traffic.
- Continuous NM testing is necessary as more advanced IPv6 NM products gain greater capabilities. Such testing should be the responsibility of the respective Program Management Office for the network or system to ensure the capturing of the necessary requirements and test results. The current snapshot gives a good perspective on the state of network management for an IPv6 transition.

In this research, there were 13 overall categories looked at, broken up into 25 subcategories. Of those subcategories tested, 19 related to network management tools while the remaining 6 involved aspects tested with various types of clients. Testers considered the objective and threshold goals met if the majority of the tools met the goal. Testers listed only server tool results. Within the monitoring and configuration categories, all subcategories tested met either the objective or threshold goals. Within the accounting category, there was an even split of those areas meeting threshold goals versus those areas meeting no goal at all. The areas not meeting desired goals in the accounting category refer to the increase in usage of the network for IPv6 to send equivalent data (since it has a bigger header), which means it essentially requires more time on the wire.

The relatively high current and future data rates on DoD LANs, WANs, and the fact that network management traffic is not used in any overwhelming degree, gives a high degree of protection against a degradation of performance by using IPv6 for network management. In summary, 72 percent of the subcategories looked at resulted in acceptable results (either objective or threshold goals being met). Testers did not examine the other 20 percent. Tools/clients and the threshold goals were in a "good enough" state. Either category was sufficient for representing acceptable results for the ability to execute equivalent network management during an IPv6 transition as seen today.

In a dual-stack environment, both tools and clients need to continue to support SNMP Version 1 and SNMP Version 2, since SNMP Version 3 is not widely implemented within the DoD at this time. For NM server tools in a dual-stack environment, it is necessary for a tool to continue to send requests to clients for information needed for management, and also to receive "alert" messages (called traps). It is also necessary for the tools to continue to discover the presence of devices on the network, either automatically or through the use of a seed file. Since network managers often know their IP address ranges as well as machines on the network either method of discovery is acceptable to strive for in a dual-stack environment. It is additionally necessary for a NM server tool to send requests to a client in order to change a parameter, to visually display properly the status and information of a discovered dual-stack client, and allow network managers to determine which displayed nodes are IPv4 and which are dual-stack. As long as a tool can poll a node over IPv4, it can maintain the capability to accomplish all of these features even in a dual-stack environment.

It is important for a NM server making use of IPv6 to use a similar amount of available network bandwidth as it does when using IPv4. If this is not the case, then the impact of this inequality must not be detrimental to the larger mission as a whole. This, in most cases, is not easily quantifiable since different missions require different bandwidth levels. However, at this stage of examination, there are enough baseline statistics within the NIPRNet from which to draw a conclusion.

It is necessary for clients to, at a minimum, provide similar information that users are accustomed to. This includes responses to queries of information from the Generic MIB, the IPv6 MIB, and Private MIBs. In addition, clients must respond to ICMP traffic (ICMPv6 for IPv6) and generate traps to send to NM servers. It is also important, though not critical, for an NM client to continue to be configurable when necessary by a NM server tool.

Despite the fact that the abilities mentioned are not completely integrated into the tools and clients used today in the DoD, the overall network management capability will not be impacted. The present goal is to move towards a dual-stacked NIPRNet. This being the case, the result is that an equal state of functionality between IPv6 and IPv4 capabilities need not exist for NM tools and clients in common use today because NM provides a "safety cushion" by its nature. SNMP operates at a different layer of the OSI stack than the stack that IP resides at, there is allowance for either IP protocol to carry requests and responses for gathering NM information. Thus full capabilities are not required for NM tools and clients since information is available for IPv6 devices via the IPv4 protocol. This shows the minimal impact that such a fact has on executing equivalent network management as a whole. However, subsequent vendor upgrades to

some of the products tested has occurred. This will likely continue with commercial vendors competing for customers in the defense market. Additionally, in those cases where some tools and clients have IPv6 support for the functional items listed, it shows that the capability is available even if a DoD organization is currently not using it in its current networking infrastructure.

The performance data gathered from testing has shown that there is more network usage for management traffic over the IPv6 protocol. This is inherently true for the protocol in general due to its header being twice as large as the IPv4 header. This fact does not necessitate a failure for IPv6 since the overall negative impact of this additional traffic on the wire must be significant. Currently, there is very little NM traffic on the wire, web and e-mail traffic is the most prevalent. In any case, the traffic increases involved here are so small that the potential implications to NM performance are minimal.

NM is continuing to evolve and will eventually entail larger areas of control such as policy-based management, mission-driven management, and a more involved information management role. However, in the near term, the overall recommendation is to allow the current network management capabilities in an IPv4-only realm to continue in a dual-stack environment. The recommendation is list IPv6 Joint Staff Operational Criteria #9 with an overall status level of Green.

D.22 National Security Agency Milestone Objective 3 Information Assurance Guidance Validation Test Report

Testing Organization and Publication Date

JITC
September 2009

Summary

NSA MO3 identified requirements for IA devices and systems to ensure the integrity and dependable operational functionality of DoD information systems. It focused on the IA functional requirements for network nodes as defined in the DISR IPv6 Standard Profiles for IPv6 Capable Products document. Specifically, it outlined filtering configuration guidance for network nodes. The IPv6 IA requirements and implementation guidelines for devices and services on DISN use the DoD IPv6 IA Guidance for NSA MO3 V 0.3 Draft 2009. The JITC evaluated the devices in the network for their capability to comply with the requirements of the NSA IA guidance document.

The MO3 validation tested criteria of multiple types including configuration, network, interoperability, and functionality. Configuration testing manually verified configuration requirements listed in the NSA IA guidance document, and traffic testing consisted of sending 112 types of crafted packets to or through the devices. Interoperability and functionality testing showed the MO3 test network was capable of successfully passing the required protocols. The DISA FSO also conducted a Security Architecture Analysis and Testing (SAAT) assessment, which evaluated various aspects of system profiling, security risk analysis, and functional effectiveness based on the requirements in the NSA IA guidance document. The network successfully allowed or blocked 97.3 percent of the crafted packets through the MO3 test network. The failures occurred due to the IA device's inability to block specific packet types. The network blocked and allowed a majority of the packets and still maintained

Test and Evaluation Method

Exercise

Joint Staff Operational Criteria Tested

1 (1.3, 1.4)
2 (2.3)
8 (8.1)

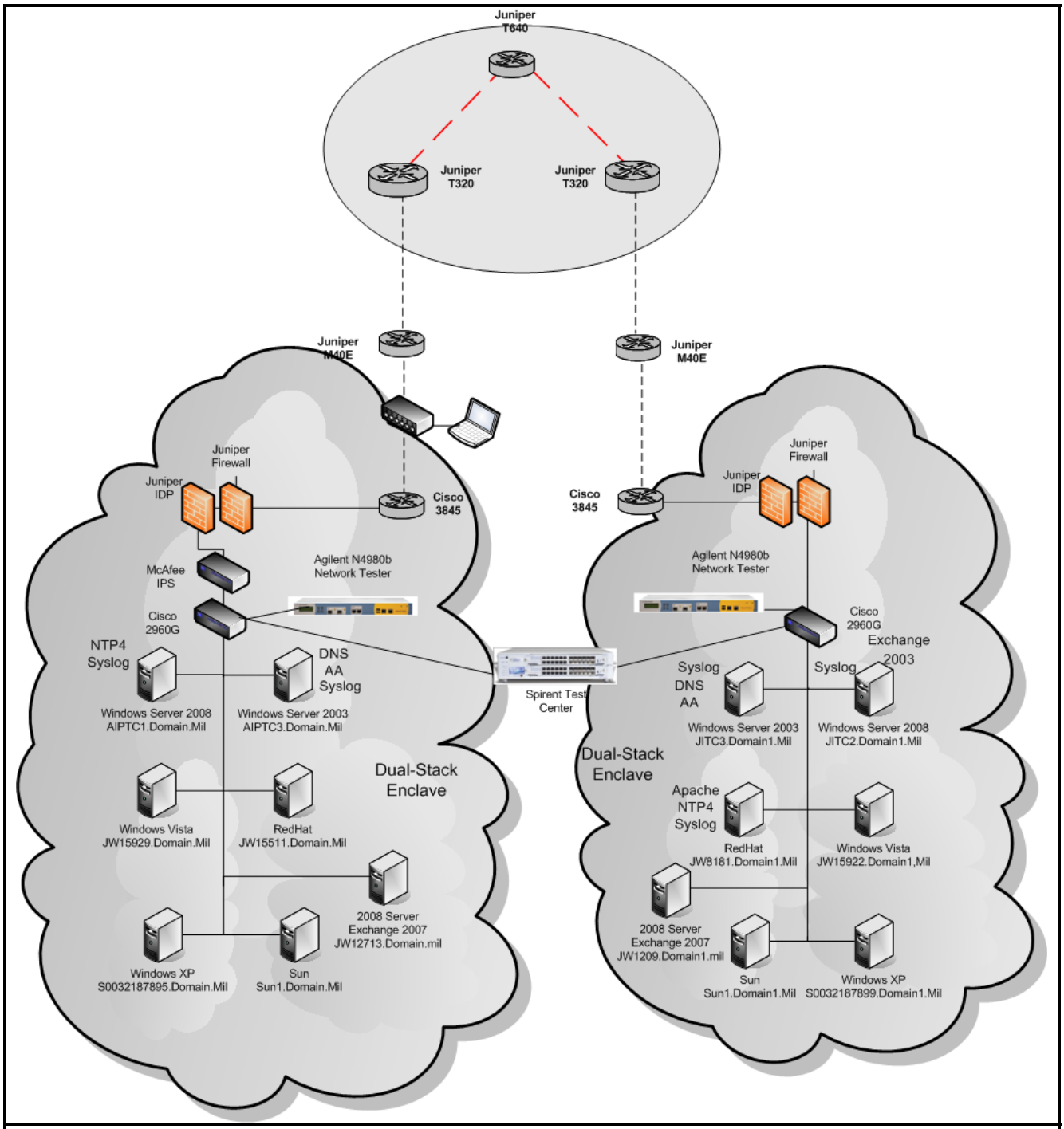
Configuration

Testers configured the devices in accordance with the FSO specifications derived from the NSA MO3 IA guidance requirements. The JITC evaluated the network for its capability to comply with the requirements in the NSA IA guidance document and in addition to interoperability and functionality within the DISN infrastructure. The MO3 test network included the simulated DISN IP Core network and two enclaves. Testers populated two enclaves with hosts protected by IA devices connected to the simulated DISN Core. Both enclaves and the simulated DISN Core were dual-stacked, allowing IPv4 and IPv6 traffic simultaneously. The DISA FSO Team also conducted a SAAT assessment for the MO3 configured test network, servers, and hosts inside the network enclaves.

The devices in the MO3 test network were required to block or allow the individual crafted packets in accordance with the requirements of the NSA IA guidance. The JITC testers initially applied current STIGs to the simulated DISN IP Core network devices. Testers configured all MO3 test network devices to the current STIGs. DISA FSO Team provided additional configuration guidance to address the NSA IA guidance. Testers applied the additional guidance to the test network. The DISA FSO Team then reviewed the network STIGs prior to test. The devices in the MO3 test network included:

- Juniper Integrated Security Gateway - 1000 Intrusion Detection and Prevention
- McAfee IntruShield 2700 IPS
- Cisco 3845 Routers
- Juniper M40, T320, and T640 Routers
- Hosts with the following Operating Systems
    - Microsoft Windows XP Professional
    - Microsoft Windows Vista Enterprise
    - Microsoft Server 2003 R2 Enterprise Edition
    - Microsoft Server 2008 Enterprise
    - Red Hat Enterprise Linux 5.2
    - Sun Solaris 10

Testing identified the crafted packet response of the devices in the network. Interoperability and functionality testing were from two dual-stacked enclaves, as shown in Figure D-20.



LEGEND:

DNS	Domain Name Service	IPv6	Internet Protocol Version 6
FSO	Field Security Operations	JITC	Joint Interoperability Test Command
IAS	Information Assurance System	MO3	Milestone Objective 3
IDP	Intrusion Detection and Prevention	NTPv4	Network Time Protocol Version 4
IPS	Intrusion Prevention System	Syslog	System Log

Figure D-20. JITC MO3 Dual-Stack Test Network

Testing consisted of crafted packets sent to or through the devices in the MO3 test network. Testers used the Spirent Test Center to craft packets to meet the requirements of the NSA IA guidance document. Testers introduced these crafted packets to the test network. Testers sent crafted packets from the Spirent Test Center to the MO3 configured devices in the network. The MO3 test network achieved a score of pass or fail depending on the network's ability to block or allow the crafted packets. The Wireshark network protocol analyzer captured and inspected the traffic for compliance to the NSA IA guidance document. If a device ceased to function after delivery of a crafted packet, testers noted in the results portion of the report.

Results

The MO3 configured IA devices successfully blocked or allowed 109 of the 112 crafted packet types, a 97.3 percent pass rate.

Three failures related to type (0) routing headers, traffic class, and flow label fields. Juniper firewall running ScreenOS 6.2 does not process frames with type (0) routing headers, regardless of whether it has IPsec headers or not. The firewall passed routing header (0) packets to the enclave against the NSA IA guidance. The traffic class and flow label fields are not yet available in ScreenOS 6.2. Juniper Networks is considering the addition of these features to a future release of ScreenOS.

Table D-23 lists interoperability test results.

Table D-23. MO3 Interoperability Results

Application or Service	Interoperable	Protocol Types
Active Directory	Yes	IPv4
Authentication	Yes	IPv4
Domain Name Service	Yes	IPv4/IPv6
Hypertext Transfer Protocol	Yes	IPv4/IPv6
Hypertext Transfer Protocol Secure	Yes	IPv4/IPv6
Microsoft Exchange E-Mail System	Yes	IPv4/IPv6
Network Time Protocol Version 4	Yes	IPv4/IPv6
Syslog Services	Yes	IPv4

LEGEND:

IPv4	Internet Protocol Version 4	MO3	Milestone Objective 3
IPv6	Internet Protocol Version 6	Syslog	System Log

Table D-24 lists the crafted packet test failures. The MO3 test network did not block or allow these packets as required by the NSA IA guidance document.

Table D-24. MO3 Test Result Failures

FSC-ID	Guidance Type	AID	FSC-Name	Results and Comments
SO-C2-2	Primary	1	IPv6 Type (0) Routing Headers	ScreenOS does not process frames with type (0) routing headers, regardless of whether they have IPsec headers or not. There is no administrative control for this. The firewall passed the packet to the enclave against the NSA MO3 Guidance
S0-C2-opt 1	Optional	1	IPv6 *traffic class* field	These features are not yet available in ScreenOS 6. 2. Juniper Networks is considering these features for addition to a future release of ScreenOS. These features are both tracked under Enhancement Request 26951
S0-C2-opt-2	Optional	1	IPv6 *flow label* field	

LEGEND:

AID	Action Identification	IPsec	Internet Protocol Security
FSC	Family Security Control	IPv6	Internet Protocol Version 6
ID	Identification	MO3	Milestone Objective 3

Conclusions/Recommendations

Testing validates the IPv6 IA capability, interoperability, and functionality of COTS IA devices in a MO3 configured test network.

- The DoD IPv6 Transition Office (DITO) should release the results of this test to the participating vendors to help facilitate their compliance with the NSA IA guidance requirements.
- Incorporate the MO3 requirements into the UCR 2008 and any other applicable requirements documents for certification testing.
- Juniper will release ScreenOS 6.3 in the near future. This release will encompass improved capabilities into the firewall operating system. Future testing should evaluate ScreenOS 6.3 for the enhanced capabilities of the Juniper firewall.
- Future MO3 testing should include individual device testing and complete network testing. This will identify which devices properly handle crafted packets.
- The DITO and NSA should review the results and recommendations of this report and the DISA FSO SAAT report before transitioning to IPv6.
- The DITO should seek to participate in working groups or communities of interest who create or influence IPv6 requirements documents.
- The DITO should re-commission the IPv6 T&E Working Group to ensure a community exists for reviewing IPv6 test reports.

THIS PAGE INTENTIONALLY LEFT BLANK.