

# **The Fiscal Year 2006 Department of Defense**

## **Internet Protocol Version 6**

### **Test and Evaluation Report**



**September 2006**

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

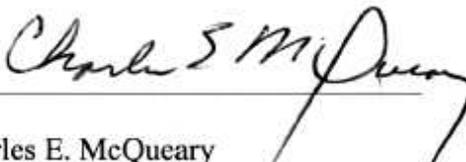
UNCLASSIFIED

The Fiscal Year 2006 Department of Defense  
Internet Protocol Version 6  
Test and Evaluation Report

This report is provided in response to Section 221 of the National Defense Authorization Act for Fiscal Year 2006 (Public Law 109-163). The report provides assessments of the test and evaluation results that the Department of Defense (DoD) Components have submitted to the DoD for the period 1 July 2005 through 30 June 2006 and integrates these assessments with the results previously reported by the DoD to Congress. The assessments follow the processes and methodologies of the test and evaluation strategy set forth in the Department of Defense Internet Protocol Version 6 Master Test Plan Version 2.0.

Approved by:   
John G. Grimes  
Assistant Secretary of Defense for  
Networks and Information Integration/  
DoD Chief Information Officer

Dated: 26 Sept 2006

Approved by:   
Dr. Charles E. McQueary  
Director, Operational Test and Evaluation

Dated: 19 September 2006

## Table of Contents

<b>1 Introduction .....</b>	<b>2</b>
1.1 Purpose .....	2
1.2 Test and Evaluation Objectives .....	2
1.2.1 Demonstration of the Joint Staff IPv6 Operational Criteria .....	2
1.2.2 Approved Products List .....	3
1.3 Scope .....	3
1.4 Previously Reported Results and Recommendations.....	3
<b>2 IPv6 Test and Evaluation Results.....</b>	<b>4</b>
2.1 Overview .....	4
2.2 Cumulative Analysis Methodology .....	4
2.3 Impact of FY 2006 Test and Evaluation Reports on Demonstration of Joint Staff IPv6 Operational Criteria .....	7
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.....	7
2.3.2 Criterion 2: Demonstrate end-to-end interoperability in a mixed IPv4 and IPv6 environment .....	9
2.3.3 Criterion 3: Demonstrate equivalent to, or better performance than, IPv4 based networks .....	11
2.3.4 Criterion 4: Demonstrate voice, data, and video integration .....	12
2.3.5 Criterion 5: Demonstrate effective operation in low-bandwidth environment .....	13
2.3.6 Criterion 6: Demonstrate scalability of IPv6 networks .....	14
2.3.7 Criterion 7: Demonstrate support for mobile terminals (voice, data, and video).....	14
2.3.8 Criterion 8: Demonstrate transition techniques.....	15
2.3.9 Criterion 9: Demonstrate ability to provide network management of networks.....	16
2.3.10 Criterion 10: Demonstrate tactical deployability and ad hoc networking .....	17
2.4 IPv6 Interoperability and Information Assurance Certifications for the DoD Approved Products List.....	18
2.4.1 Interoperability Certifications .....	18
2.4.2 Information Assurance Certifications.....	18
<b>3 Conclusions.....</b>	<b>19</b>
<b>4 Recommendations .....</b>	<b>23</b>
<b>5 Summary .....</b>	<b>24</b>
<b>Appendix A. References .....</b>	<b>25</b>
<b>Appendix B. Terms and Definitions .....</b>	<b>26</b>

<b>Appendix C.</b>	<b>Acronym List .....</b>	<b>28</b>
<b>Appendix D.</b>	<b>DoD IPv6 2006 Test Report Summaries .....</b>	<b>32</b>
<b>Appendix E.</b>	<b>DoD IPv6 2003-2005 Test and Evaluation Summary .....</b>	<b>81</b>

### List of Tables

Table 2-1	Cumulative Test and Evaluation Matrix .....	6
Table 2-2	2006 Reporting Year Joint Staff IPv6 Operational Criterion 1 .....	7
Table 2-3	2006 Reporting Year Joint Staff IPv6 Operational Criterion 2.....	9
Table 2-4	2006 Reporting Year Joint Staff IPv6 Operational Criterion 3.....	11
Table 2-5	2006 Reporting Year Joint Staff IPv6 Operational Criterion 4.....	12
Table 2-6	2006 Reporting Year Joint Staff IPv6 Operational Criterion 5.....	13
Table 2-7	2006 Reporting Year Joint Staff IPv6 Operational Criterion 6.....	14
Table 2-8	2006 Reporting Year Joint Staff IPv6 Operational Criterion 7.....	14
Table 2-9	2006 Reporting Year Joint Staff IPv6 Operational Criterion 8.....	15
Table 2-10	2006 Reporting Year Joint Staff IPv6 Operational Criterion 9.....	16
Table 2-11	2006 Reporting Year Joint Staff IPv6 Operational Criterion 10.....	17
Table D-1	2006 Test Reports and Related Operational Criteria .....	33
Table D-2	Equipment Configuration.....	45
Table D-3	Equipment Configuration.....	53
Table D-4	Equipment Configuration.....	60
Table D-5	Test Results .....	61
Table D-6	Equipment Configuration.....	63
Table D-7	Test Results .....	64
Table D-8	Equipment Configuration.....	65
Table D-9	Test Results .....	66
Table D-10	Equipment Configuration.....	68
Table D-11	Equipment Configuration.....	76
Table E-1	2003-2005 Test and Evaluation Matrix .....	82

## Executive Summary

This report is provided in response to Section 221 of Public Law 109-163. It is based on field tests, exercises, demonstrations, experiments, simulations, and analyses conducted by Department of Defense (DoD) Components over the last four years, with emphasis on the most recent year (July 2005 through June 2006) test results. This report provides an update to the report submitted to Congress at the end of the last fiscal year in response to Section 331 of Public Law 108-375 and presents new findings for this subsequent reporting period.

The DoD Internet Protocol 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)/CIO)). The data contained in these reports have been evaluated with respect to the principal T&E objectives of the DoD IPv6 Master Test Plan Version 2.0 (MTP v2.0). Most of these reports support the objective to demonstrate the Joint Staff IPv6 operational criteria documented in the DoD IPv6 Transition Plan Version 2.0 and decomposed into testable functional elements in the DoD MTP v2.0. A limited number of these reports support interoperability and Information Assurance (IA) certification of IPv6 products that is necessary to place the tested products on the DoD IPv6 Approved Products List (APL).

The DoD Components have reported a substantial amount of IPv6 T&E activities during this reporting period. These activities cover nine of the ten Joint Staff IPv6 operational criteria with emphasis on end-to-end interoperability and transition techniques. However, based on a cumulative analysis of all reports received none of the ten criteria have been fully demonstrated. The cumulative analysis further indicates that the following areas require significantly more T&E effort to adequately demonstrate the criteria: security, low-bandwidth environments, scalability, transition techniques, network management, and ad hoc networking.

The DoD has formalized the process for interoperability and information assurance certification of IPv6 products. Initial interoperability testing of products is proceeding in accordance with the DoD IPv6 Generic Test Plan (GTP).

The DoD Components are developing test plans for their specific IPv6 transition environments and are following the guidance set forth in the DoD IPv6 MTP v2.0. The DoD is facilitating the sharing of IPv6 T&E results among the DoD Components and other Federal IPv6 working groups through DoD web portals.

The results presented in this report indicate that IPv6 technologies continue to progress toward adoption but that there has been insufficient testing on operational networks. Further testing is required to support both the demonstration of the Joint Staff IPv6 operational criteria and APL certification. The development and availability of critical IPv6 capable products may impact DoD's schedule for planned IPv6 T&E and deployment.

# **1 Introduction**

## **1.1 Purpose**

The Fiscal Year (FY) 2006 DoD IPv6 T&E Report is provided in response to Section 221 of Public Law 109-163. This 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 MTP v2.0. This report is also an 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 and helps identify what has been completed and what further testing is required. As defined in the DoD IPv6 MTP v2.0, the DoD IPv6 T&E strategy comprises two objectives:

- Demonstrate the functionality of IPv6 as delineated in the Joint Staff IPv6 operational criteria.
- Establish an APL of IPv6 products that have been certified to meet a set of DoD requirements for interoperability and IA.

Assessment of the individual IPv6 T&E reports furnished by the DoD Components will address the progress in meeting both objectives.

### **1.2.1 Demonstration of the Joint Staff IPv6 Operational Criteria**

The Joint Staff IPv6 operational criteria enumerate the operational and technical capabilities necessary for verifying that IPv6 fulfills operational needs of the DoD. The decomposition of the criteria provides two levels of measurable and verifiable functional elements that can be demonstrated through testing:

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

The mapping of the DoD Components' IPv6 test results to the Joint Staff IPv6 operational criteria will support the Congressionally directed certification by the Chairman of the Joint Chiefs of Staff that the conversion of DoD networks to IPv6 will provide equivalent or better performance and capabilities than that which would be provided by any other combination of available technologies and protocols.

## **1.2.2 Approved Products List**

The DoD APL is a registry of IP products tested by Defense Information Systems Agency (DISA) Joint Interoperability Test Command (JITC) or other DoD entities, validated as IPv6 capable, and certified as meeting specific interoperability and IA criteria. It provides the DoD with a selection of IPv6 products certified to meet the DoD need for interoperability and IA. The addition of an IPv6 product to the APL occurs only after the product has been shown to meet interoperability and IA certification requirements. DoD Components shall purchase IPv6 capable products from the APL, where available. Requirements for IPv6 interoperability certifications are derived from the DISR and the DISR IPv6 Standard Profiles for IPv6 Capable Products. The DISA (JITC) is responsible for interoperability testing processes and procedures. The DISA is responsible for developing processes, procedures, and technical standards for IPv6 IA testing. The DoD APL is located at: [http://jitc.fhu.disa.mil/adv\\_ip/register/register.html](http://jitc.fhu.disa.mil/adv_ip/register/register.html).

## **1.3 Scope**

The scope of the analysis in this report is limited to T&E reports submitted by the DoD Components in response to requests from the ASD(NII)/DoD CIO. The DoD Components (Army, Navy, Air Force, and DISA) provided 19 reports to the DoD for FY 2006 and 39 reports for FY 2005 (for testing conducted FY 2003 through FY 2005). The evaluation team for this report was led by DITO with participation by ASD(NII), Director, Operational Test and Evaluation, and DISA (JITC). This year's report analyzes the 19 reports submitted by the DoD Components and integrates the analysis with the 39 previously submitted reports to provide a cumulative status for IPv6 T&E. This year's cumulative status will be compared with last year's status to assess progress toward IPv6 transition.

## **1.4 Previously Reported Results and Recommendations**

Results from FY 2005 testing indicated that IPv6 technologies, as examined by the DoD Components, had progressed significantly toward the point of adoption. Some aspects of IPv6 appear ready to deploy in a single network domain or enclave environment within operational networks. However, significant issues must be resolved prior to department-wide deployment of IPv6.

Recommendations from the FY 2005 report indicated that additional effort was needed in the areas of performance and scalability, security, creation of an APL, application porting or development, Quality of Service (QoS), transition mechanisms, and network management. All of these areas, with the exception of scalability, are addressed in this year's report. The progress that has been made is discussed in appropriate sections of this report.

## 2 IPv6 Test and Evaluation Results

### 2.1 Overview

This section provides the overall status of DoD IPv6 T&E in support of the DoD's transition to IPv6 and summarizes IPv6 T&E results reported by the DoD Components for the period July 2005 through June 2006. Nineteen T&E reports were analyzed for the current reporting period. Summaries for each of these reports are provided in Appendix D. The 39 reports submitted for the FY 2005 DoD IPv6 T&E report were reanalyzed for relevance to the Joint Staff IPv6 operational criteria. The reanalysis is provided in Appendix E. Reports submitted for the current reporting period address the Joint Staff IPv6 operational criteria more clearly and are generally of higher quality than the previous reports. All reports used for this analysis can be found on the DoD Test and Evaluation Working Group (TEWG) portal: <https://gesportal.dod.mil/sites/JITCIPv6/TEWG>.

### 2.2 Cumulative Analysis Methodology

Each Joint Staff IPv6 operational criterion is assigned a completion status of red, yellow, or green based on analysis of tests conducted by the DoD Components. The status of each criterion was determined through an analysis of all applicable T&E reports.

To date, none of the ten Joint Staff IPv6 operational criteria have been fully demonstrated. However, there has been significant effort in end-to-end interoperability and transition techniques (Criteria 2 and 8). Minimal work was reported for voice, video, and data integration, low-bandwidth environments, scalability, mobility, network operations, and ad hoc networking (Criteria 4, 5, 6, 7, 9, and 10). As highlighted in this report, further testing is needed to adequately demonstrate all of the criteria. Testing of some Level 2 criteria must wait for capabilities to be developed or refined.

A distinction was made between Level 1 and Level 2 decomposition. At Level 2, a subjective engineering judgment is based on analysis and evaluation of three factors as described in Section 2.3 of this document. At Level 1, an objective approach is used to "roll up" the status of the level below. Using this roll-up approach, the lowest status from the level immediately below becomes the status of the intermediate or top level decomposition. A single low-level decomposition element that is red will cause its related criterion to be red, even if all other elements for that criterion are green. Thus, underlying decomposition elements needing additional testing are easily identified. Note that a "red" status at the top level or intermediate decomposition level does not mean that the criterion has not been addressed; it simply means that an element at a lower level still requires significant testing.

The color coded rating scale for the successful demonstration of the criteria is as follows:

⊗ Red - Limited progress has been made. More testing and/or development is needed to allow the criterion to be certified as having been demonstrated.

⊕ Yellow - Significant progress has been made. Some portions of the criterion have not been successfully demonstrated or the confidence in previous test results was low. Additional testing and/or development is needed to allow the criterion to be certified as having been demonstrated.

✔ Green - The criterion has been successfully demonstrated. The evaluation type, relevance, and scope (considered with the number of tests) provide enough data to assure the criterion was demonstrated with a high confidence factor. Adequate testing has been conducted to demonstrate all requirements of the criterion.

The Cumulative Test and Evaluation Matrix (Table 2-1) presents the total number of test reports applicable to each criterion for the entire transition effort, as well as the number of test reports for this reporting period by the Joint Staff IPv6 operational criteria and test method (counts for this reporting period are in parentheses). A cumulative status representing the overall effort regarding each criterion is also presented as well as an expected completion date. The cumulative status for a criterion indicates the lowest completion status for any of the sub-elements of the criterion. Thus, a cumulative status of yellow or red should be viewed as an alert that the demonstration of one or more underlying functional or technical elements is incomplete.

**Table 2-1 Cumulative Test and Evaluation Matrix**

Joint Staff IPv6 Operational Criteria		Test Methods						Cumulative Status	Expected Completion Date	
		Engineering Analyses	Modeling & Simulation	Experiments	Demonstrations	Pilots	Exercises			Field Tests
1	Demonstrate security of unclassified network operations, classified network operations, black backbone operations, integration of High Assurance IP Encryptors (HAIPE), integration of IP security (IPSec), and integration with firewalls and intrusion detection systems	6 (1)	1	9 (2)	6 (1)		6 (1)		⊗	2QFY 2009
2	Demonstrate end-to-end interoperability in a mixed IPv4 and IPv6 environment	3 (1)	1 (1)	14 (3)	5 (2)		14 (5)	1 (1)	⊕	2QFY 2008
3	Demonstrate equivalent to, or better performance than, IPv4 based networks	2	2 (1)	4	2(1)		7 (4)		⊕	1QFY 2008
4	Demonstrate voice, data, and video integration	4		2	1		7 (1)	1 (1)	⊕	4QFY 2008
5	Demonstrate effective operation in low-bandwidth environment	2	2 (1)				2 (2)		⊗	2QFY 2009
6	Demonstrate scalability of IPv6 networks	2			1				⊗	1QFY 2008
7	Demonstrate support for mobile terminals (voice, data and video)	1	1	1	1		7 (1)	1 (1)	⊕	2QFY 2009
8	Demonstrate transition techniques	4 (1)	3 (1)	8 (3)	3 (1)		12 (5)		⊗	4QFY 2008
9	Demonstrate ability to provide network management of networks	1		6 (3)	4 (1)				⊗	4QFY 2008
10	Demonstrate tactical deployability and ad hoc networking	2 (1)	1	1				1 (1)	⊗	2QFY 2010
<p><b>Key:</b>   Criterion has been successfully demonstrated.   Significant progress has been made on this criterion.   Limited progress has been made on this criterion.</p> <p>QFY Quarter Fiscal Year                      Total Events (Current Fiscal Year Events)</p>										

## 2.3 Impact of FY 2006 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 the lowest level of decomposition and is based solely on the test reports submitted during this reporting period. The evaluation of each criterion is performed at the lowest levels of the decomposed functional or technical elements. Three qualitative factors were used to determine the extent to which an individual report contributed to the satisfaction of an element: applicability to the Joint Staff IPv6 operational criteria, qualitative merit based on evaluation type, and scope of each T&E event.

Each T&E event was evaluated for applicability or relevance to each Joint Staff IPv6 operational criterion; and the degree of relevance of each event contributed to determination of the Level 2 status. Next, the type of evaluation was considered and the event results were weighted accordingly. Evaluation types listed in descending qualitative order are: field test, exercise, pilot, demonstration, experiment, modeling and simulation, and engineering analysis. The final factor that contributed to status determination was the scope of each T&E event. Test events that only confirm previous results are considered to contribute less toward status determination than those that cover previously untested areas.

Subsections follow for each criterion. Each subsection provides the status of each criterion's Level 1 and Level 2 decomposition and specific findings related to that criterion. Note that the color status for the decomposed elements in each subsection do not necessarily roll up to the cumulative color status in Table 2-1 because each subsection provides only an incremental analysis of the test reports submitted for this reporting period.

### 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 2006 Reporting Year Joint Staff IPv6 Operational Criterion 1

Level 1 Decomposition (Capabilities to be demonstrated)	Level 1 Status	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Level 2 Status
1.1 Ensure that information is not disclosed to unauthorized persons, processes, or devices.		1.1.1 Verify implementation of IPSec with Encapsulating Security Protocol (ESP) in IPv6 hosts.	
		1.1.2 Verify the implementation of IPSec with ESP in IPv6 routers and switches.	
		1.1.3 Verify integration with Public Key Infrastructure (PKI).	

**Table 2-2 2006 Reporting Year Joint Staff IPv6 Operational Criterion 1 (continued)**

Level 1 Decomposition (Capabilities to be demonstrated)	Level 1 Status	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Level 2 Status
1.2 Ensure information received is the same as that which was sent (protect against unauthorized modification or destruction of information).		1.2.1 Verify implementation of Authentication Header (AH) in IPv6 hosts.	
		1.2.2 Verify implementation of Authentication Header (AH) in IPv6 routers and switches.	
1.3 Ensure authentication of persons and processes.		1.3.1 Verify security of Authentication, Authorization, and Accounting (AAA) servers using IPv6.	
		1.3.2 Verify integration of AAA servers with PKI.	
1.4 Ensure availability and mitigate denial of services (timely, reliable access to data, and information services for authorized users).		1.4.1 Verify protection of the IPv6 resident protocol implementation in hosts, switches, and routers 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).		1.5.1 Evaluate firewalls and IDS functions that can be applied to IPv6 traffic.	
		1.5.2 Evaluate firewalls and IDS functions that can be applied to tunneled IPv6 traffic.	
1.6 Ensure IPv6 traffic is interoperable with HAIPE devices.		1.6.1 Evaluate HAIPE v3 ability to encrypt/decrypt IPv6 packets.	
		1.6.2 Evaluate HAIPE v3 ability to encrypt/decrypt tunneled IPv6 packets.	

T&E Observations:

- No HAIPE was tested because IPv6 capable HAIPE devices are still under development.
- An IPv6 test network using a commercially available secure wireless gateway effectively provided Advanced Encryption Standard (AES) Layer 2 encryption with no performance degradation.
- A test network was configured for black backbone operation with serial bulk encryption to secure IPv6 traffic. To load the black network, pre-defined automated test scripts were initiated from automated test tools. There was no performance degradation when passing IPv6 traffic via serial encryption devices.

- Vendor implementations of IPSec for IPv6 continue to be immature.
- The state of commercially available IPv6 firewalls and IDS appears to be far behind the DoD's need for network protection.
- Further commercial development and T&E is required for security devices such as firewalls, IDS, HAIPE, and other network security appliances.

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

**Table 2-3 2006 Reporting Year Joint Staff IPv6 Operational Criterion 2**

Level 1 Decomposition (Capabilities to be demonstrated)	Level 1 Status	Level 2 Decomposition (Specific technology/infrastructure/functionality to be demonstrated)	Level 2 Status
2.1 Demonstrate IPv4 application to IPv4 application over a mixed IPv4 and IPv6 network.	⊕	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.	⊕
2.2 Demonstrate IPv6 application to IPv4 application over a mixed IPv4 and IPv6 network.	⊕	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	⊕

**Table 2-3 2006 Reporting Year Joint Staff IPv6 Operational Criterion 2 (continued)**

Level 1 Decomposition (Capabilities to be demonstrated)	Level 1 Status	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Level 2 Status
2.3 Demonstrate IPv6 application to IPv6 application over a mixed IPv4 and IPv6 network.	⊕	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	⊕

T&E Observations

- Tests indicate native IPv6 applications can be successfully used in mixed IPv4 and IPv6 environments including protocols. Some of the tested application examples are:
  - Hypertext Transfer Protocol (HTTP)
  - Hypertext Transfer Protocol Secure (HTTPS)
  - Post Office Protocol version 3 (POP3)
  - Simple Mail Transfer Protocol (SMTP)
  - File Transfer Protocol (FTP)
  - Secure Shell (SSH)
  - Telnet
  - Real Time Streaming Protocol (RTSP).
- Many tests demonstrated the use of “tunneling”, so that IPv4 end nodes and their associated applications can still be employed across an IPv6 network.
- Dynamic Host Configuration Protocol version 6 (DHCPv6) duplicates the functionality of Dynamic Host Configuration Protocol (DHCP) in IPv4, but it is not yet implemented in any of the Windows operating systems.
- The IPv6 capable Ethernet switch blocked Domain Name Service (DNS) query traffic over IPv6 by default. Therefore, testers manually configured this network on the Ethernet switch in order for DNS traffic to pass through. Only then could the Vista client perform DNS lookups.
- Internet Explorer 6 can browse Web pages over IPv6, but it will not accept IPv6 Uniform Resource Locators specified by address.

- Windows networking and sharing of drives worked without issue over IPv6.
- Some tests demonstrated interoperability on par with IPv4 as long as the application supported IPv6, and the equipment met IPv6 minimum system requirements.
- While these initial results are positive, further testing and evaluation is required to adequately demonstrate interoperability in mixed IPv4 and IPv6.

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

**Table 2-4 2006 Reporting Year Joint Staff IPv6 Operational Criterion 3**

Level 1 Decomposition (Capabilities to be demonstrated)	Level 1 Status	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Level 2 Status
3.1 Demonstrate IPv6 throughput equivalent to or better than IPv4.	⊕	3.1.1 Same as Level 1.	⊕
3.2 Demonstrate IPv6 latency equivalent to or better than IPv4.	⊕	3.2.1 Same as Level 1.	⊕
3.3 Demonstrate IPv6 packet loss equivalent to or better than IPv4.	⊕	3.3.1 Same as Level 1.	⊕
3.4 Demonstrate IPv6 service availability equivalent to or better than IPv4.	⊕	3.4.1 Compare service provisioning times.	⊕
		3.4.2 Compare service recovery times.	⊕

**T&E Observations**

- Bit level performance measured throughput, frame loss, latency, standard deviation, and packet sequencing that showed superior single and dual stack IPv6 performance utilizing Application-Specific Integrated Circuit (ASIC) based routers over programmable processor based routers.
- Certain tests demonstrated the ability to ping from a device's IPv4 and IPv6 interfaces to another device's IPv4 and IPv6 interfaces with a quicker response time on the IPv6 interfaces.
- One test ran a continuous ping for one hour with no loss of packets. Additionally, three separate tests of 1,000 ping tests were performed with a 100 percent success rate. A

network tap was used to capture the continuous ping packets and examine them for Request For Comment (RFC) compliance.

- Layer 3 switch testing showed high-end switches from several vendors have equivalent performance when passing IPv4 and IPv6 traffic. The majority of Layer 3 switches, however, have much lower performance (1 to 5 percent) of the speed of their IPv4 capabilities.
- Most edge switches consistently passed IPv6 traffic at/or near the line rate. Core switches passed traffic normally below the line rate.
- Further development and T&E is required for ASIC-based IPv6 routers and Layer 3 switches to adequately demonstrate IPv6 performance equivalent to, or better than, IPv4.

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

**Table 2-5 2006 Reporting Year Joint Staff IPv6 Operational Criterion 4**

Level 1 Decomposition (Capabilities to be demonstrated)	Level 1 Status	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Level 2 Status
4.1 Demonstrate simultaneous voice, data, and video (or any combination thereof) over shared IPv6 networks.		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 Protocol (RTP).	
		4.1.3 Demonstrate session signaling capabilities of IPv6 networks using the Session Initiation Protocol (SIP).	

#### T&E Observations

- One test demonstrated data and video integration with all data transfers completing error-free and streaming video maintaining high quality throughout the testing.
- Further development and T&E of integrated IPv6 voice, data, and video products is required to adequately demonstrate this criterion.
- The DoD must agree on technical guidelines for voice, data, and video integration.

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

**Table 2-6 2006 Reporting Year Joint Staff IPv6 Operational Criterion 5**

Level 1 Decomposition (Capabilities to be demonstrated)	Level 1 Status	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Level 2 Status
5.1 Same as the criterion itself.		5.1.1 Demonstrate ability to compress IPv6 headers using Robust Header Compression (ROHC) techniques.	
		5.1.2 Demonstrate ability to maintain IPv6 connectivity under low-bandwidth conditions. (Note: Point to Point Protocol will be added to demonstrate IPv6 connectivity.)	

#### T&E Observations

- During this reporting period the lowest bit rate tested using IPv6 was 2.4 Kilobits per second (Kbps). Testing demonstrated IPv6 traffic can operate effectively in low-bandwidth IPv6 native environments. However, there were performance penalties at bandwidth rates lower than 16 Kbps.
- In dual stack configuration, performance within limited bandwidth links degraded. At circuit speeds of 2 Megabits per second (Mbps) or higher, dual stack configurations produced only minor adverse effects. Below 2 Mbps, the network showed an appreciable decline in throughput performance and increase in frame loss.
- Results for low-bandwidth environments varied according to test configuration.
- Further development of Robust Header Compression (ROHC) and T&E within tactical environments are required to fully demonstrate this criterion.

**2.3.6 Criterion 6: Demonstrate scalability of IPv6 networks**

**Table 2-7 2006 Reporting Year Joint Staff IPv6 Operational Criterion 6**

Level 1 Decomposition (Capabilities to be demonstrated)	Level 1 Status	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Level 2 Status
6.1 Demonstrate ability to add more network resources, services, and users without negative impact on existing users.	⊗	6.1.1 Demonstrate ability to build IPv6 networks comparable in size to existing IPv4 networks, with equal or better performance.	⊗
		6.1.2 Demonstrate ability to populate IPv6 subnets with network elements in comparable numbers to existing IPv4 subnets, with equal or better performance.	⊗
		6.1.3 Demonstrate ability to create IPv6 multicast sessions whose sizes are comparable to existing IPv4 multicast sessions, with equal or better performance.	⊗
		6.1.4 Demonstrate ability to create IPv6 core services (DNS, Directory, FTP, email, web services, NTP, and PKI) where the numbers of users are comparable to existing IPv4 core services, with equal or better performance.	⊗

T&E Observations

- There were no tests conducted on scalability of IPv6 networks during this reporting period.
- Development of data for network models and simulations, combined with T&E, is required to adequately demonstrate this criterion.

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

**Table 2-8 2006 Reporting Year Joint Staff IPv6 Operational Criterion 7**

Level 1 Decomposition (Capabilities to be demonstrated)	Level 1 Status	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Level 2 Status
7.1 Demonstrate ability to maintain IPv6 applications on the move.	⊗	7.1.1 Demonstrate ability to maintain an existing voice, data, or video session on the move using SIP and Mobile IPv6 (MIPv6).	⊗
		7.1.2 Demonstrate ability to initiate or accept new voice, data, or video sessions on the move using SIP and MIPv6.	⊗

T&E Observations

- Testing was conducted with operating system beta software. However, a client would not establish a relationship with the Home Agent in the router. It was later determined this mobility feature is no longer supported.
- Limited mobility testing was conducted this reporting period and attempts to use IPv6 mobility were unsuccessful. Vendor implementation immaturity is a serious and systemic problem in fielding MIPv6, Network Mobility (NEMO), and Mobile Ad Hoc Networking (MANET).
- Development, implementation, and T&E of IPv6 mobility standards and features are required for mobile environments to adequately demonstrate this criterion.

**2.3.8 Criterion 8: Demonstrate transition techniques**

**Table 2-9 2006 Reporting Year Joint Staff IPv6 Operational Criterion 8**

Level 1 Decomposition (Capabilities to be demonstrated)	Level 1 Status	Level 2 Decomposition (Specific technology/infrastructure/functionality to be demonstrated)	Level 2 Status
8.1 Demonstrate DoD recommended network transition techniques.		<b>8.1.1</b> Demonstrate feasibility of IPv4 and IPv6 network transition techniques: <ul style="list-style-type: none"> <li>• Dual stack everywhere in an autonomous system</li> <li>• Configured tunnels</li> <li>• Dual Stack Transition Mechanism (DSTM)</li> <li>• Tunnel Broker.</li> </ul>	
8.2 Demonstrate DoD recommended application transition techniques.		<b>8.2.1</b> Demonstrate the feasibility of the IPv4 and IPv6 application transition techniques: <ul style="list-style-type: none"> <li>• Stateless IP/Internet Control Message Protocol Translation (SIIT)</li> <li>• Bump in the Application Program Interface (BIA)</li> <li>• Bump in the Stack (BIS).</li> </ul>	

T&E Observations

- The following five methods of tunneling IPv6 traffic over IPv4 networks were used during T&E: manual IPv6 tunnels, automatic IPv4 compatible tunnels, Generic Routing Encapsulation (GRE) tunnels, automatic 6to4 tunnels, and Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnels.
- Some testing with tunneling IPv4 traffic over IPv6 networks decreased throughput and increased frame loss when compared to previous tunneling tests over IPv4 networks.

- Common network applications and network management appeared to be unaffected in a dual stack environment.
- Tests involved dual stack and tunneling transition techniques. The maturity of vendor implementations resulted in successful testing of these transition mechanisms.
- Dual stack transition techniques appear to create the most flexible strategy to allow the coexistence of IPv4 and IPv6 applications.
- Further development and implementation of Dual Stack Transition Mechanism (DSTM) and application transitions techniques are required to adequately demonstrate this criterion.

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

**Table 2-10 2006 Reporting Year Joint Staff IPv6 Operational Criterion 9**

Level 1 Decomposition (Capabilities to be demonstrated)	Level 1 Status	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Level 2 Status
9.1 Demonstrate ability to monitor, configure, and account for IPv6 network resources.		9.1.1 Demonstrate that Network Management Systems (NMS) commonly used by the DoD can monitor IPv6 devices.	
		9.1.2 Demonstrate that NMS commonly used by the DoD can configure IPv6 devices.	
		9.1.3 Demonstrate that IPv6 devices can be accounted by NMS commonly used by the DoD.	

#### T&E Observations

- The scope of the testing was insufficient to provide conclusive results.
- Results from testing have uncovered many major drawbacks to IPv6 implementation of Network Management Systems (NMS). These drawbacks include limited support for Simple Network Management Protocol (SNMP) in operating systems and networking devices.
- As tested, the Command and Control Resource Management System (C2RMS) could effectively monitor resources for status via IPv6 oriented ping monitor and an IPv6 oriented SNMP monitor.

- Further development and T&E of IPv6 capable network management tools and systems are required to adequately demonstrate this criterion.

### 2.3.10 Criterion 10: Demonstrate tactical deployability and ad hoc networking

**Table 2-11 2006 Reporting Year Joint Staff IPv6 Operational Criterion 10**

Level 1 Decomposition (Capabilities to be demonstrated)	Level 1 Status	Level 2 Decomposition (Specific technology/infrastructure/ functionality to be demonstrated)	Level 2 Status
10.1 Demonstrate ability to move IPv6 networks as a whole, without reconfiguration.		10.1.1 Demonstrate the ability to move networks to other locations while maintaining connectivity via the original IPv6 addresses, using Network Mobility (NEMO).	
		10.1.2 Demonstrate ability to move network elements to other locations while maintaining connectivity via the original IPv6 addresses, using MIPv6.	
10.2 Demonstrate ability to support IPv6 networking without fixed router infrastructure.		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.	

#### T&E Observations

- In testing the Warfighter Information Network-Tactical (WIN-T) prototype, IPv6 was tactically deployed throughout the WIN-T test network. Simulated IPv6 voice, data, and video traffic were sent through the network. Although the communications success rate was low, other factors heavily influenced this low percentage.
- Significantly more work remains for testing the tactical deployability and ad hoc networking capabilities of IPv6.
- Further development, vendor implementation, and T&E of MIPv6, NEMO, and MANET are required to adequately demonstrate this criterion.

## **2.4 IPv6 Interoperability and Information Assurance Certifications for the DoD Approved Products List**

### **2.4.1 Interoperability Certifications**

Requirements for interoperability certifications for IPv6 are derived from the DISR and from the DISR IPv6 Standard Profiles for IPv6 Capable Products. Using these requirements, DISA (JITC) has developed the DoD IPv6 GTP and associated APL process to certify vendor products as IPv6 capable. Products that are on the schedule for IPv6 interoperability certification this year can be found on the APL website: [http://jitc.fhu.disa.mil/adv\\_ip/register/register.html](http://jitc.fhu.disa.mil/adv_ip/register/register.html).

### **2.4.2 Information Assurance Certifications**

DISA is responsible for developing processes, procedures, and technical standards for IPv6 IA testing. Responsibilities include documenting the system mission, environment, and architecture, identifying vulnerabilities, defining levels of effort, and documenting the security requirements needed for IPv6 IA certification. Processes, procedures, and technical standards are to be developed.

### 3 Conclusions

The following conclusions are based upon reviewing and integrating the results of the 19 FY 2006 test reports. The DoD has made progress in IPv6 T&E. However, further work is required. The conclusions are summarized according to the Joint Staff IPv6 operational criteria.

#### **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.**

- The IPv6 extension headers for IPsec have been successfully loaded with Public Key Infrastructure (PKI) certificates and secure end-to-end communications have been demonstrated.
- Security functions of routers (vulnerability scanning, support of SSH, secure management, password protection, and product integrity) have been successfully tested on routers selected for implementation.
- Access Control Lists for IPv6 routers and firewalls have been successfully demonstrated.
- No testing of HAIPE devices was performed. The National Security Agency (NSA) has developed technical specifications for HAIPE (version 3). Technical analysis of the specifications was performed and recommendations were provided to NSA. HAIPE T&E by NSA requires the delivery of version 3 prototypes.
- IPv6 packet inspection by firewalls has not been demonstrated. T&E will occur when firewall vendors produce IPv6 capable products.
- IDS have not been tested. T&E will occur when IDS vendors produce IPv6 capable products.
- IA certification and accreditation of IPv6 products and systems have not been accomplished.

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

- Numerous tests were performed that analyzed the performance and interoperability of IPv6 implementations in hosts and routers. The results of the tests varied, depending on the router and its operating system. Newer routers and operating systems support the basic IPv6 features but require further development to satisfy DoD IPv6 capable requirements.

- The following features were successfully demonstrated in a mixed IPv4 and IPv6 environment:
  - Stateless autoconfiguration
  - IPv6 routing protocols [Open Shortest Path First version 3 (OSPFv3) and Border Gateway Protocol 4+(BGP4+)]
  - Internet control messages [Internet Control Message Protocol version 6 (ICMPv6)]
  - Common network applications (HTTP, SMTP, and FTP)
  - Network services [DNS/Berkeley Internet Name Domain 9 (BIND 9) and Network Time Protocol (NTP)].
- IPv6 mobility and multicasting features experienced problems in the beta version of the operating system tested.
- Interoperability of IPv4 and IPv6 applications in mixed environments was demonstrated. The performance of the applications was on par with IPv4 only networks compared with IPv4 and IPv6 mixed environments.

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

- Several high-end Layer 3 Ethernet switches and some routers deliver IPv4 and IPv6 performance parity. Software implementations of IPv6 Layer 3 Ethernet switches demonstrate lower performance when using IPv6 than when using IPv4.
- The lack of IPv6 capable satellite IP modems and accelerators prevents deployment in a manner equivalent to IPv4. Overall, the current state of IPv6 used in tactical networks is immature and needs additional development and T&E before performance comparisons can be made with IPv4.
- Bandwidth constrained IPv6 links, with bandwidths higher than 16 Kbps, demonstrate parity with IPv4.

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

- Limited testing of voice, data, and video integration was performed using a voice/video emulation test tool with routers from a single vendor. The routers operated properly in interpreting the IPv6 DiffServ code points and provided the required quality of service.
- Further development and T&E is required to adequately demonstrate integration of voice, data, and video on IPv6 networks.

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

- Test results for low-bandwidth environments were not conclusive. Conclusions drawn from two test reports were contradictory and indicate that further testing is needed.
- Bandwidth constrained links with bandwidths higher than 16 Kbps are not negatively affected using native IPv6 in comparison to IPv4 over the same network. For bit rates below 16 Kbps, IPv6 throughput was much lower than IPv4.
- Use of dual stack techniques appeared to degrade performance on links below 2 Mbps. IPv6 parity with IPv4 was demonstrated using dual stack techniques with links above 2 Mbps.

**Criterion 6: Demonstrate scalability of IPv6 networks.**

- No scalability analysis of IPv6 networks has been performed, as there is currently insufficient data to populate network models and simulations.

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

- Limited mobility testing was conducted this reporting period and attempts to use IPv6 mobility were unsuccessful. Immature vendor implementations are a serious and systemic problem in fielding MIPv6, NEMO, and MANET.

**Criterion 8: Demonstrate transition techniques.**

- Five transition mechanisms are recommended: dual stack (within host OS and network devices), manual configured tunnel, automatic tunneling, Application Layer Gateway (ALG), and Stateless IP/ICMP Translation (SIIT).
- Dual stack transition techniques appear to create the most flexible strategy to allow coexistence of IPv4 and IPv6 applications.

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

- Testing shows that IPv6 network management tools have been implemented to a limited extent. More development of IPv6 network management tools and T&E is required to demonstrate this criterion.
- The Government Off The Shelf (GOTS) network management tool C2RMS, as modified by the Air Force, resulted in important lessons learned in transitioning applications to IPv6.

- Of the routers and switches tested, the majority did not support the SNMPv3 Management Information Base (MIB).

**Criterion 10: Demonstrate tactical deployability and ad hoc networking.**

- Simplified Multicast Forwarding (SMF) T&E indicates that further development is required to support MANET multicasting.
- The WIN-T prototype nodes demonstrated IPv6 connectivity on the move and at the halt.
- Significantly more work remains for T&E of the tactical deployability and ad hoc networking capabilities of IPv6.

## 4 Recommendations

Since IPv4 and IPv6 devices are expected to co-exist for some time, thorough testing of interoperability, security, and performance is key for a smooth transition to IPv6. Several issues need to be resolved before IPv6 is implemented in DoD networks. Areas requiring further emphasis are:

- Commercial development and T&E is required for IPsec and security devices such as firewalls, IDS, HAIPE, and other network security appliances. *(Criterion 1)*
- T&E is required to adequately demonstrate network and application interoperability in mixed IPv4 and IPv6 environments. *(Criterion 2)*
- Development and T&E is required for ASIC-based IPv6 routers and Layer 3 switches to adequately demonstrate IPv6 performance equivalent to, or better than, IPv4. *(Criterion 3)*
- Development and T&E of integrated IPv6 voice, data, and video products is required. The DoD must also agree on technical guidelines for integration of voice, data, and video. *(Criterion 4)*
- Development of ROHC and T&E for use within tactical environments is required. *(Criterion 5)*
- Development of data for network models and simulations, combined with T&E, is required to adequately demonstrate scalability. *(Criterion 6)*
- Development, implementation, and T&E of IPv6 mobility standards and features are required for mobile environments. *(Criterion 7)*
- Development and implementation of DSTM and application transition techniques are required. *(Criterion 8)*
- Development and T&E of IPv6 capable network management tools and systems are required. *(Criterion 9)*
- Development, vendor implementation, and T&E of MIPv6, NEMO, and MANET are required. *(Criterion 10)*

## 5 Summary

IPv6 protocols and products, critical to the IPv6 transition for the DoD, are still under development. The availability of IPv6 capable commercial products, that meet the DoD's performance, interoperability, and IA requirements, continues to be key to the transition. Pacing items for T&E and subsequent implementation of IPv6 across the DoD include: HAIPE devices, network management systems, firewall appliances, intrusion detection/prevention systems, PKI implementation, and key distribution systems. T&E and operational deployment of IPv6 capabilities may be delayed until the critical equipment and devices are commercially available.

Test and evaluation of interoperability (Criterion 2) and network transition techniques (Criterion 8) have progressed sufficiently to allow use of the base protocol and the major transition mechanisms (dual stack and tunneling) to support broader testing in more operationally realistic environments. Elements of Criteria 2 and 8 have not been completely demonstrated, but have matured to form the basis for further testing of criteria such as security (Criterion 1), performance (Criterion 3), and voice, data, and video integration (Criterion 4). Development of IPv6 capabilities for other criteria [low-bandwidth operation (Criterion 5), scalability (Criterion 6), and tactical deployability and ad hoc networking (Criterion 10)] is still immature. As a result, there has been limited T&E in these areas. More development and T&E directed at these criteria is needed to improve the current "red" status ratings in Table 2-1.

Although the Joint Staff IPv6 operational criteria divide capabilities into separate categories, many of the functional capabilities required for one criterion have a significant impact on others. As a result, integrated T&E will be required. T&E of sufficient breadth and scope to address the performance and scalability of IPv6 in multi-vendor networks, of the size that the DoD employs, needs to be conducted. Further, all IPv6 capabilities, including the relatively mature areas of interoperability and transition techniques, will need to be tested in conjunction with IPv6 security solutions once developed. This integrated T&E is needed to ensure that performance in secure environments, using these IPv6 solutions, still meets the user's operational requirements.

## Appendix A. References

1. 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>
2. 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>
3. Department of Defense Internet Protocol Version 6 Master Test Plan, Version 2.0, September, 2006.  
<https://gesportal.dod.mil/sites/JITCIPv6/tewg/Document%20Library/Forms/AllItems.aspx?RootFolder=%2fsites%2fJITCIPv6%2ftewg%2fDocument%20Library%2f%2fIPv6%20Master%20Test%20Plan&View=%7b98E2C58D%2d809C%2d4EE4%2d82C%2d949D777469A2%7d>
4. Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Plan Version 2.0, June 2006.  
<https://gesportal.dod.mil/sites/JITCIPv6/tewg/Document%20Library/Forms/AllItems.aspx?RootFolder=%2fsites%2fJITCIPv6%2ftewg%2fDocument%20Library%2f1%2fIPv6%20Transition%20Plan&View=%7b98E2C58D%2d809C%2d4EE4%2d892C%2d949D777469A2%7d>
5. DoD IPv6 Generic Test Plan, Version 2, June 2006.  
[http://jitic.fhu.disa.mil/adv\\_ip/register/docs/ipv6\\_gtp\\_v2.pdf](http://jitic.fhu.disa.mil/adv_ip/register/docs/ipv6_gtp_v2.pdf)

## Appendix B. Terms and Definitions

**Approved Products List (APL):** A registry of products tested by DISA (JITC), or other DoD entities, and validated as IPv6 capable by DISA (JITC).

**Demonstration:** The use of controlled laboratory test environments to verify the results of experiments in a more complex network environment.

**DoD Components:** The Office of the Secretary of Defense, Military Departments, Chairman of the Joint Chiefs of Staff, Combatant Commands, Office of the Inspector General of the Department of Defense, Defense Agencies, DoD Field Activities, and all other organizational entities in the Department of Defense.

**Engineering Analysis:** The use of analytical techniques to predict the compliance of the design based on system modeling and calculated or derived data.

**Exercise:** A simulated peacetime or wartime operation involving DoD Components in a mix of live and M&S environments.

**Experiment:** The use of controlled laboratory test environments to prove technical principles and/or collect detailed data.

**Field Test:** The use of operational network test environments with controlled and uncontrolled user traffic to verify that the Joint Staff IPv6 operational criteria are being met.

**IPv6 capable:** An IPv6 capable system or product shall be capable (once IPv6 enabled) of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4.

**IPv6 Generic Test Plan (IPv6 GTP):** A plan developed to specify interoperability and performance procedures that IPv6 products must successfully complete in order to be certified for interoperability by DISA (JITC).

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

**Joint Staff IPv6 operational criteria:** Criteria that must be successfully demonstrated to support a decision to initiate DoD transition to IPv6 and identify key operational and technical capabilities at a high level.

**Milestone Objective 1 (MO1):** DoD Components are authorized to implement and operate IPv6 within an enclave. At MO1, the evaluation of the IPv6 protocol is sufficient, and the policy, procedures, and technical guidance have been 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 will be tightly controlled 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. MO1 was authorized as of October 1, 2005.

**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):** The use of computer modeling and simulations to predict system performance based on key technical performance elements.

**Pilot:** The use of a controlled, live network in accordance with the DoD CIO policy and guidance to demonstrate performance in a more realistic environment than a laboratory.

## Appendix C. Acronym List

AAA	Authorization, Authentication, and Accounting
ACL	Access Control List
AD	Active Directory
ADNS	Automated Digital Network System
AES	Advanced Encryption Standard
AFB	Air Force Base
AFCA/IN	Air Force Communications Agency Integration Engineering
AFRL	Air Force Research Laboratory
AFSN	Air Force Systems Networking
AH	Authentication Header
ALG	Application Layer Gateway
API	Application Programming Interface
APL	Approved Products List
ASD	Assistant Secretary of Defense
ASIC	Application-Specific Integrated Circuit
ATEC	Army Test and Evaluation Command
ATH	At The Halt
BGP	Border Gateway Protocol
BIA	Bump in the Application Programming Interface
BIND	Berkeley Internet Name Domain
BIS	Bump in the stack
C2	Command and Control
C2RMS	Command and Control Resource Management System
C4ISR	Command, Control, Communications, and Computers, Intelligence, Surveillance, and Reconnaissance
CERDEC	Communications-Electronics Research, Development, and Engineering Center
CIO	Chief Information Officer
COTS	Commercial Off The Shelf
CPU	Computer Processor Unit
CSR	Communications Success Rate
CT	Cipher Text
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol Version 6
DiffServ	Differentiated Services
DISA	Defense Information Systems Agency
DISR	DoD IT Standards Registry
DITO	DoD IPv6 Transition Office
DNS	Domain Name System
DoD	Department of Defense

DPD	Duplicate Packet Detection
DSCP	Differentiated Service Code Point
DSTM	Dual Stack Transition Mechanism
DT/OT	Development Test/Operational Test
DUT	Device Under Test
EPLRS	Enhanced Position Location Reporting System
ESP	Encapsulating Security Payload
FALCoN	Forward Area Lightweight Communications Node
FTP	File Transfer Protocol
FY	Fiscal Year
GIG	Global Information Grid
GOTS	Government Off The Shelf
GRE	Generic Routing Encapsulation
GTP	Generic Test Plan
HAIPE	High Assurance Internet Protocol Encryptor
HP	Hewlett Packard
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I3MP	Installation Information Infrastructure Modernization Program
IA	Information Assurance
ICE	IPv6 Capable Exercise
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol Version 6
IDM	Information Dissemination Management
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IM-PEPD	Implicit Peer Enclave Prefix Discovery protocol
IOS	Inter-network Operating System
IP	Internet Protocol
IPSec	IP Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISATAP	Intra-site automatic tunnel addressing protocol
IT	Information Technology
JITC	Joint Interoperability Test Command
JUICE	Joint User Interoperability Communications Exercise
Kbps	Kilobits per second

LCS	Live Communications Server
M&S	Modeling and Simulation
MANET	Mobile Ad hoc Networks
Mbps	Megabits per second
MIB	Management Information Base
MIPv6	Mobile Internet Protocol Version 6
MLD	Multicast Listener Discovery
MO1	Milestone Objective 1
MTP	Master Test Plan
NAT	Network Address Translation
NEMO	Network Mobility
NETTION	Network Testing and Operational Environment
NIC	Network Card
NII	Networks and Information Integration
NM	Network Management
NMINIT-6	Network Management Initiative for IPv6
NMS	Network Management Systems
NNM	Network Node Manager
NSA	National Security Agency
NTP	Network Time Protocol
OS	Operating System
OSPF	Open Shortest Path First
OSPFv2	Open Shortest Path First Version 2
OSPFv3	Open Shortest Path First Version 3
PIM	Protocol Independent Multicast
PIM-SM	Protocol Independent Multicast – Sparse Mode
PKI	Public Key Infrastructure
POP3	Post Office Protocol Version 3
PPP	Point-to-Point Protocol
PT	Plain Text
QFY	Quarter Fiscal Year
QoS	Quality of Service
RFC	Requests for Comment
RIPng	Routing Information Protocol Next Generation
ROHC	Robust Header Compression
RSVP	Resource Reservation Protocol
RTP	Real Time Protocol
RTSP	Real Time Streaming Protocol

SIIT	Stateless IP/Internet Control Message Protocol Translation
SIP	Session Initiation Protocol
SMF	Simplified Multicast Forwarding
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPAWAR	Space and Naval Warfare Systems
SSH	Secure Shell
T&E	Test and Evaluation
TCP	Transmission Control Protocol
TEWG	Test and Evaluation Working Group
TIC	Technology Integration Center
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USAISEC	U.S. Army Information Systems Engineering Command
VECP	Virtual Encryptor Configuration Protocol
VMW	Virtual Machine Ware
VoIP	Voice over IP
VPN	Virtual Private Network
VTC	Video Teleconference
WAN	Wide Area Network
WIN-T	Warfighter Information Network-Tactical
WWW	World Wide Web

## **Appendix D. DoD IPv6 2006 Test Report Summaries**

This appendix provides summaries for the 19 IPv6 T&E reports that DoD Components submitted for this year. The applicability of each report to the Joint Staff IPv6 operational criteria is summarized in Table D-1 on the next page. 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 Joint Staff IPv6 operational criteria (including Level 1 and 2 decomposition relevancy), configuration, results, and conclusions/recommendations.

**Table D-1 2006 Test Reports and Related Operational Criteria**

Section	Test Report Title	Joint Staff IPv6 Operational Criteria									
		1	2	3	4	5	6	7	8	9	10
D.1	Addendum to the NMINIT-6 Effort									X	
D.2	Air Force Participation In Moonv6, Phase IV		X	X					X		
D.3	IPv6 Study Final Report		X	X		X			X		
D.4	Network Management-Initiative For IPv6								X	X	
D.5	System Assessment for the Warfighter Information Network-Tactical (WIN-T)		X		X			X			X
D.6	Internet Protocol Version 6 Product Capabilities Assessment Report		X	X					X		
D.7	Forward Area Lightweight Communications Node Assessment Report		X						X		
D.8	Joint User Interoperability Communications Exercise 2005 Internet Protocol Version 6 Assessment Report Annex		X	X	X	X		X	X		
D.9	Milestone Objective 1 Implementation Report	X	X						X		
D.10	Capabilities and Lessons Learned from IPv6 Migration of the Command and Control Resource Management System (C2RMS)									X	
D.11	Internet Protocol Version 4 (IPv4) to IPv6 Transition Mechanisms for Tactical Networks		X						X		
D.12	Milestone Objective 1 Internet Protocol version 6 Capable Evaluation Base, Control		X								
D.13	Milestone Objective 1 Internet Protocol version 6 Capable Evaluation Base, Transition Mechanisms, Applications		X						X		
D.14	Milestone Objective 1 Internet Protocol version 6 Capable Evaluation Information Assurance	X									
D.15	2005 Ethernet Switch Comparison Report		X	X						X	
D.16	ADNS HAIPE Interface Requirements (Including IM-PEPD, VECP and Route redistribution)	X									
D.17	Simplified Multicast Forwarding for MANET										X
D.18	Special Interoperability Test Certification of the Hewlett Packard Laser Jet 2420d Printer with Jetdirect Card for Internet Protocol Version 6 (IPv6) Capability	X	X	X		X			X		
D.19	IPv6 Transitioning: Not Ready For Prime Time	X	X						X		
<b>Total Test Reports by Joint Staff IPv6 Operational Criteria</b>		<b>5</b>	<b>13</b>	<b>6</b>	<b>2</b>	<b>3</b>	<b>0</b>	<b>2</b>	<b>11</b>	<b>4</b>	<b>2</b>

## **D.1 Addendum to the NMINIT-6 Effort**

### **Testing Organization and Publication Date**

Air Force Research Laboratory (AFRL) Rome Research Site  
January 2006

### **Summary**

This report documents the results of additional testing to the Network Management Initiative for IPv6 (NMINIT-6) effort. Testing was conducted from November 2005 to January 2006 at the Rome Research Site, New York. The purpose was to determine the interaction/relationship between the IPv6-enabled router and the IPv6-enabled Network Node Manager (NNM) software in a dual stack environment.

### **Test and Evaluation Method**

Experiment

**Joint Staff IPv6 Operational Criteria Tested** (relevant Level 1 and 2 decomposition items)

**9** (9.1, 9.1.1, 9.1.3)

### **Configuration**

A Cisco 2621XM router, Internetwork Operating System (IOS) 12.3(14)T3, with an IPv4 and IPv6 addressed interface, was networked to the same Local Area Network as the server running Hewlett Packard (HP) Openview's NNM version 7.5 used in the original effort.

### **Results**

- Cisco and HP do not use (by default) similar Message Information Base(s) (MIBs) regarding IPv6 parameters.
- Cisco does not support the generic IPv6 RFC known as RFC 2465 (from which the IPv6 forwarding request is derived from) and will likely not be implemented in the near future.
- IPv6 MIBs are implemented by Cisco based upon the "draft-ipngwg-rfc2096-update-00.txt" and "draft-ietf-ipngwg-rfc2011-update-00.txt" documents and usually created under the Cisco enterprise branch (1.3.6.1.4.1.9) of the object id tree hierarchy.
- Cisco supports the following eight MIBs:
  - CISCO-CONFIG-COPY-MIB
  - ENTITY-MIB
  - CISCO-FLASH-MIB
  - NOTIFICATION-LOG-MIB

- CISCO-CONFIG-MAN-MIB
  - CISCO-DATA-COLLECTION-MIB
  - SNMP-TARGET-MIB
  - CISCO-SNMP-TARGET-EXT-MIB.
- However, five of the eight MIBs did not contain IPv6 references; the three that did have IPv6 references were in the (Cisco 2621XM) IOS under test.

### **Conclusions/Recommendations**

More testing is needed in the area of IPv6 network management. The knowledge of new MIBs within an IOS version is misleading. One way to find issues is to poll from the management server to the device running the IOS using IPv6 desired parameters. This action can keep MIBs up to date. A newer version of IOS may also be needed to obtain MIBs that are not in that current version of code. It is recommended that DoD be more specific with vendors concerning network management MIBs.

## **D.2 Air Force Participation In Moonv6, Phase IV**

### **Testing Organization and Publication Date**

Air Force Communications Agency Integration Engineering Directorate (AFCA/EN), Scott Air Force Base, Illinois  
January 2006

### **Summary**

This report documents the results of the Air Force's participation in Moonv6, Phase IV. Testing was conducted from 24 October to 18 November 2005. This test focused primarily on testing to the draft DoD IPv6 GTP. Conformance and performance testing of IPv6 hardware and software were evaluated in AFCA/EN's participation in Moonv6, Phase IV.

### **Test and Evaluation Method**

Exercise

**Joint Staff IPv6 Operational Criteria Tested** (relevant Level 1 and 2 decomposition items)

**2** (2.1, 2.2, 2.3)

**3** (3.1, 3.2, 3.3, 3.4, 3.1.1, 3.2.1, 3.3.1, 3.4.1, 3.4.2)

**8** (8.1, 8.1.1)

### **Configuration**

The Air Force used the Defense Satellite Communications Service to connect to JITC-Fort Huachuca, Arizona during the Moonv6 exercise. Equipment included:

- Cisco 3725 Router – IOS version 12.4(3) with the Advanced Enterprise Services feature pack
- Cisco 7206 VXR Router – IOS 12.3(14)T5
- Cisco 2621 XM Router – IOS 12.3(16) with Advanced Enterprise Services feature pack
- Cisco 3650 Switch
- Microsoft Windows Server 2003
- Microsoft Windows XP Workstation
- Spirent SmartBits 600.

## Results

### *Conformance*

The following tests were conducted and recorded during Moonv6, Phase IV. Equipment used in each test was optimized prior to test in order to meet the Ixia and Spirent test scripts.

- Cisco 7206 VXR Router was tested to comply with IPv6 standards for features such as Extension Headers, Neighbor Discovery, Path Maximum Transmission Unit Discovery, Internet Control Message Protocol version 6, IPv6 Stateless Address Autoconfiguration, connection of IPv6 domains via IPv4 clouds, Jumbograms, general, and aggregatable global unicast address. Three separate configurations and two operator intervention scenarios were run for each standard. The Cisco 7206 VXR did not pass 100 percent of any tested feature.
- A Cisco 2621 XM Router was tested to meet IPv4 IPsec standards by running test suites that included IPSEC AH, Internet Key Exchange (IKE), and IPsec ESP. The Cisco 2621 XM did not pass 100 percent of the requirements of any test.

### *Performance*

Performance features tested included four separate configurations. The list below identifies all the tested configurations and their results.

- IPv4 traffic only - Average recorded throughput was 17 megabits per second (Mbps), 118 microseconds (usec) of latency, and 49 usec of jitter.
- Dual stack (IPv4 –only traffic) - Average throughput recorded was 17 Mbps, 119 usec of latency, and 50 usec of jitter.
- Dual stack (50 percent IPv4 traffic and 50 percent IPv6 traffic) – Average recorded throughput was 14 Mbps, 130 usec of latency, and 50 usec of jitter.
- Dual stack (IPv6-only traffic) – Average recorded throughput was 13.5 Mbps, 140 usec of latency: no jitter statistics were recorded.

## Conclusions/Recommendations

Based on the Air Force's participation during Moonv6, Phase IV, the tested commercial products are unable to meet all the conformance and performance requirements. The inability to meet all standards are partly due to vendor interpretation of the standards. Continued work to improve dual stack and IPv6 traffic handling is indicated by these results. Identifying critical interoperability and functional requirements to develop an appropriate IPv6 capable definition for procurement of commercial products will assist the DoD's transition to IPv6.

## **D.3 IPv6 Study Final Report**

### **Testing Organization and Publication Date**

Air Force Systems Networking (AFSN), Headquarters Operations and Sustainment Systems Group, Maxwell AFB-Gunter Annex, Alabama  
25 January 2006

### **Summary**

The AFSN Program Office conducted a study on the effects of using IPv6 on standard network equipment utilized to provide Wide Area Network (WAN) connectivity on the Unclassified-But-Sensitive IP Router Network and Secret IP Router Network. All testing was conducted at the Test and Integration Facility at Maxwell Air Force Base (AFB)-Gunter Annex, AL. The test simulated three AFBs passing traffic over a simulated DISA WAN. The AFSN testing primarily focused on three areas: dual stacking (IPv4 and IPv6), tunneling (both IPv6 within IPv4 and IPv4 within IPv6), and the effect of running IPv6 over limited bandwidth circuits. The purpose of this study was to determine the impact of implementing IPv6 in existing Air Force networks, as well as in future Air Force networks.

### **Test and Evaluation Method**

Modeling and Simulation

**Joint Staff IPv6 Operational Criteria Tested** (relevant Level 1 and 2 decomposition items)

**2** (2.1, 2.2, 2.3)

**3** (3.1, 3.2, 3.1.1, 3.2.1)

**5** (5.1, 5.1.1)

**8** (8.1, 8.1.1)

### **Configuration**

Equipment involved in this testing includes Cisco 3700, 3600, 2600, and 7200 series routers running IOS 12.4 and Spirent SmartBits test equipment within a dual stack environment.

### **Results**

#### *Dual Stack*

As the most likely implementation for the Air Force, dual stack enables legacy (IPv4) devices to communicate within an IPv6 environment. Equipment involved in this testing included Cisco 3700, 3600, 2600, and 7200 series routers. However, the smaller routers (3600 and 2600) limited the amount of testing that could be conducted, due to their lack of available memory. All testing used Spirent SmartBits automated test tool to generate traffic and record results.

The following list conveys the test results:

- Some significant losses were shown during testing (45 percent overall for throughput and frame loss). This represented an increase in loss of approximately 17 percent over initial baseline testing. However, there was no significant difference in the loss numbers between IPv4 traffic flows and IPv6 traffic flows.
- Limited bandwidth paths showed more sensitivity to loss due to dual stack implementation than larger bandwidth paths.

### *Tunneling*

The test team evaluated passing IPv4 traffic over newly implemented IPv6 networks. This can occur where some enclaves of IPv4 traffic still exist and can't immediately upgrade to IPv6, while other parts of the WAN have been converted to IPv6 addressing. This test used the following two examples to assess tunneling.

- IPv6 traffic over IPv4 network - No significant losses of traffic were caused by this mode of tunneling. A slight increase in loss (approximately 28 percent to 34 percent for IPv6 traffic tunneled) compared to the initial baseline test was recorded. Furthermore, there was only a small increase in loss when comparing the previous IPv6 baseline to tunneling (from 33 percent in the IPv6 baseline test to approximately 34 percent loss overall in the tunneling test). This was apparent in both throughput and frame loss tests.
- IPv4 traffic over IPv6 network - Increase in both throughput loss and frame loss in this tunneling test was noted when compared to the previous tunneling test over IPv4 networks. Even though only one IPv6 tunnel was implemented, losses increased from the previous tunneling test from about 34 percent to roughly 50 percent overall loss.

### *Limited Bandwidth*

Testing limited bandwidth circuits are extremely beneficial for tactically deployed Air Force units, Navy ships at sea, and other units or agencies unable to support large bandwidth links. This portion of testing evaluated limited bandwidth circuits using IPv6 addressing. AFSN varied data rates from 1200 bits per second (bps) up to 1.28 Megabits per second (Mbps) for testing. The results are listed below:

- As bandwidth was reduced towards 1200 bps, throughput decreased to almost zero in these limited bandwidth paths.
- The use of the dual stack configuration in some tests seemed to degrade performance within limited bandwidth links. At circuit speeds of 2 Mbps or higher dual stack configurations produced only minor effects. Below 2 Mbps, the network showed an appreciable decline in throughput and increase in frame loss.

- Overall losses approximately 55 percent were routinely seen on circuits under 38.4 Kbps, with consistent losses approaching 100 percent on the limited bandwidth paths.
- Losses only slightly decreased for circuits above 38.4 Kbps.

Losses decreased by a couple percent for 56 Kbps circuits and another couple percent for 64 Kbps circuits. With 1.28 Mbps circuits, losses dropped a significant 5 percent.

### **Conclusions/Recommendations**

This study examined several possible IPv6 implementations (dual stacking, tunneling IPv6 traffic over IPv4 networks, tunneling IPv4 traffic over IPv6 networks, and limited bandwidth). The configurations used were somewhat limited in scope (only three base architectures were used, with limited traffic flowing between bases) and not all facets of possible future implementations were observed (dual stack Access Control Lists, Virtual Private Network (VPN) tunnels using IPv6, Border Gateway Protocol, and Open Shortest Path First Protocol, etc.). The results of the study made some basic conclusions on possible impacts of deploying IPv6 in current and future Air Force networks, such as selecting the proper IOS for a router. This allows the device to support all the features given in an IPv6 network. Merely running IPv6 traffic over the network did increase throughput and frame loss. Comparing the results of the IPv4 baseline and IPv6 baseline tests shows a 5-6 percent increase in throughput and frame loss. The only configuration that perhaps causes reason for alarm is the use of very limited bandwidth circuits.

## **D.4 Network Management-Initiative For IPv6**

### **Testing Organization and Publication Date**

AFRL Rome Research Site  
September 2005

### **Summary**

This report documents the results of testing Network Management capabilities in an IPv4, IPv6, and dual stack environment. Testing was conducted from May to September 2005, at the Rome Research Site. The Network Management Initiative for IPv6 (NM-INIT6) effort encompassed designing and implementing a dual stack test bed and evaluating NM tools to determine whether effective/equivalent NM could be performed. This effort tested applications/clients running IPv4-only, IPv6-only, and/or both, Commercial Off The Shelf (COTS), and GOTS NM applications and protocols. The following section presents results, analysis, and a conclusion on all conducted testing. Three primary foci of this effort included testing functionality, scalability, and C2RMS transitions.

### **Test and Evaluation Method**

Experiment

**Joint Staff IPv6 Operational Criteria Tested** (relevant Level 1 and 2 decomposition items)

**8** (8.1, 8.1.1)

**9** (9.1, 9.1.3)

### **Configuration**

The test bed consisted of HP Openview's Network Node Manager version 7.5, VMWare ESX Server, a hub, and a sniffer used to monitor packets. Twenty eight virtual machines were also created from the VMWare ESX Server to represent an adequate number of managed, critical machines at a given DoD site. The test bed clients were originally loaded with Windows XP Operating System. However, due to Window XP's inability to recognize a general IPv6 MIB, test bed clients were changed to Windows 2003 Server.

## **Results**

### *Functionality*

The NM-INIT6 effort assessed functionality and scalability of NM tools. The NM tools were not compared against each other during testing, but verified individual tool performance in a dual stack environment.

- Compared to similar IPv4 requests, three to five times more data exists on the wire for IPv6 MIB requests.
- A larger number of clients likely results in a higher usage of available bandwidth by network management traffic, thus slowing mission essential data.
- No conclusive evidence exists as to whether IPv6 network management will be harmful.
- Knowing what is being requested via SNMP can reduce traffic loads.
- Computer Processor Units (CPUs) affect NM performance with IPv4 and IPv6.

### **Conclusions/Recommendations**

Based on AFRL's NMINIT-6 effort, continuous NM testing is necessary to ensure future NM products effectively make full use of IPv6. Preliminary results have not found major drawbacks to IPv6 implementation, but planning and network knowledge can assist a network manager to maintain a fully functional and scalable IPv6 network. Initial assessments indicate that network management tools must be further developed in order to fully support IPv6 capabilities.

## **D.5 System Assessment for the Warfighter Information Network-Tactical (WIN-T)**

### **Testing Organization and Publication Date**

Army Test and Evaluation Command (ATEC)  
March 2006

### **Summary**

As the replacement for the current Mobile Subscriber Equipment and Tri-Services Tactical Communications Program systems, WIN-T will be the future Army communications backbone architecture for years to come. From 3 to 18 November 2005, at Fort Huachuca, Arizona, and Fort Monmouth, New Jersey, ATEC evaluated automated IPv6 voice, data, and video traffic through the WIN-T Developmental Test/Operational Test (DT/OT) network.

### **Test and Evaluation Method** (relevant Level 1 and 2 decomposition items)

Field Test

### **Joint Staff IPv6 Operational Criteria Tested**

**2** (2.1, 2.2, 2.3, 2.1.1, 2.2.1, 2.3.1)

**4** (4.1, 4.1.1)

**7** (7.1, 7.1.1, 7.1.2)

**10** (10.1.1)

### **Configuration**

The Voice/Video Emulation Test Tool instrumentation and NETTION were placed throughout the entire WIN-T DT/OT network at various systems within the test network. Devices within the test network included:

- Cisco 3745,3725 Routers – IOS 12.3(11T)
- Cisco PIX 525 Firewall – IOS 6.3(4)

### **Results**

The result of IPv6 testing is presented by a Communications Success Rate (CSR). The CSR was calculated by dividing the number of communications completed by the total number of communications sent. Data collection from 15 runs served as the basis for the CSR assessment. Category 1 through 4 messages were sent throughout the entire assessment.

The following list explains the definition of the categories:

- Category 1 (survival information) communications  $\leq 5$  seconds.
- Category 2 (time-sensitive) communications  $< 8$  seconds.
- Category 3 (routine) communications  $< 30$  seconds.
- Category 4 (non-time sensitive) communications  $< 15$  minutes.

The following list is the specific results for all IPv6 traffic sent during the assessment:

- At The Halt (ATH) excursions of communication Categories 2, 3, and 4, the data message CSR was 82 percent.
- The CSR estimates for the eight excursions with movers for communication Categories 2, 3, and 4, the data message CSR was only 65 percent, significantly lower than IPv4 CSR of 80 percent.
- The Voice CSR for ATH nodes was 64 percent.
- The CSR estimates and 90 percent confidence interval based on Analysis of Variance of ATH excursions was 82 percent.
- The Information Dissemination Management (IDM) estimates for ATH excursions of communication Categories 2, 3, and 4 demonstrated a data message IDM rate of 79 percent versus 90 percent for IPv4.
- IDM estimates for ATH communication Category 1 messages were 89 percent.
- IDM estimates for the eight excursions with movers of communication Categories 2, 3, and 4 was 62 percent for data messages. This was much lower than IPv4, which demonstrated an IDM rate of 78 percent.

Operating system limitations and incorrect marking of Differentiated Services Code Points (DSCP) caused all IPv6 traffic to be sent at lower precedence than intended (Routine or Best Effort). Due to this problem, all IPv6 traffic had to be treated as routine or best effort traffic during the analysis. Other factors decreasing the CSR of IPv6 involved nominal satellite communications and Unmanned Aerial Vehicle coverage.

### **Conclusions/Recommendations**

While operating in the developmental phase of production, the WIN-T network was able to pass IPv6 and demonstrate the potential to meet the requirements. Instrumentation limitations of incorrect DSCP and operating system problems degraded the IPv6 results.

## D.6 Internet Protocol Version 6 Product Capabilities Assessment Report

### Testing Organization and Publication Date

JITC, Fort Huachuca, AZ  
June 2006

### Summary

The IPv6 Capable Exercise (ICE) focused on an extensive technical analysis of the implementation of IPv6 within COTS equipment critical to the IPv6 DoD transition. The DoD IPv6 Generic Test Plan was designed to evaluate the implementation level of IPv6 within a product by analyzing the conformance, performance, and interoperability of the protocol implementations. This information will be used to populate the recently created APL.

### Test and Evaluation Method

Exercise

**Joint Staff IPv6 Operational Criteria Tested** (relevant Level 1 and 2 decomposition items)

**2** (2.1, 2.2, 2.3, 2.1.1, 2.1.3, 2.2.1, 2.2.3, 2.3.1, 2.3.3)

**3** (3.1, 3.2, 3.1.1, 3.2.1)

**8** (8.1, 8.1.2)

### Configuration

The following table lists the devices under test during ICE. Not included in the table are Agilent, Ixia, and Spirent Automated Test tools that were used for the assessment.

**Table D-2 Equipment Configuration**

Device Under Test	IOS Version #
Cisco 3725	12.3(11)T
Cisco 3845	12.3(11)T5
Cisco 3845	12.4(11)T (Not Available for Test)
Cisco ONS 15454	12.0(3)
Cisco 2621XM	12.3(16)
Juniper M5	6.4R2.4
Juniper M40e	6.4R2.4
Juniper T320	6.4R2.4
Juniper T640	6.4R2.4

## Results

### *Conformance Testing*

The results from IPv6 conformance test efforts conducted by JITC, Cisco, and Juniper test labs support the same conclusions; automated IPv6 conformance testing to date, suffers from:

- Lack of adopted IPv6 RFCs.
- Lack of industry implemented IPv6 RFCs.
- Lack of joint development efforts between automated test vendors and original equipment manufactures.

The IPv6 conformance test suites are not presently mature enough in development or stable enough to yield conclusive data now.

An unusually large number of inconclusive results from the conformance test suites from of all three vendors may be declared a result of either unrealistic timer values not associated with the tested RFCs or improper setup. There were many instances where a timer value was declared as a default setting by the manufacturer of the Device under Test, and not implemented within the conformance test suite.

### *Performance Testing*

Automated performance testing focused on two areas: protocol performance and bit level performance. Protocol performance delivered a trend that indicates close parity between IPv4 and IPv6. Bit level performance was tested for throughput, frame loss, latency, standard deviation, packet sequencing. Superior single and dual stack IPv6 performance utilizing ASIC based routers over programmable processor based routers was shown.

### *Interoperability Testing*

Protocol level performance tests were conducted emulating 150 individual user sessions. Each session initiating and terminating connections utilized a 7 in 1 automated protocol test script that requested transactions in the following IPv6 protocols: HTTP 1.1, HTTP Secure (HTTPS) 1.1, Real Time Streaming Protocol (User Datagram Protocol streaming video), DNS A, DNS AAAA, FTP, and Telnet.

Interoperability was on par with IPv4 if the application that supported the service in question supported IPv6 and the equipment met IPv6 minimum system requirements.

## **Conclusions/Recommendations**

The following conclusions were made with respect to IPv6 conformance, performance, and interoperability testing. Automated conformance testing should not be considered a valid alternative until IPv6 conformance test suites are more complete. Automated performance testing focused on two areas: protocol performance and bit level performance. Protocol level performance showed close parity between IPv4 and IPv6. Bit level performance showed superior single and dual stack IPv6 performance utilizing ASIC based routers over programmable processor based routers. Interoperability was on par with IPv4 if the application that supported the service in question supported IPv6 and the equipment met IPv6 minimum system requirements.

## **D.7 Forward Area Lightweight Communications Node Assessment Report**

### **Testing Organization and Publication Date**

JITC, Fort Huachuca, AZ  
22 May 2006

### **Summary**

The JITC assessed the Forward Area Lightweight Communications Node (FALCoN) at Fort Huachuca, Arizona, from 14 to 24 March 2006 during DoD Interoperability Communications Exercise 2006. The assessment included IPv6 interoperability, performance, and functionality testing in a dual-protocol environment. The test evaluated core IPv6 functionality, transition mechanisms, routing protocols, common network applications, and network operations. The FALCoN was tested for its capabilities in both a wired and wireless network.

### **Test and Evaluation Method**

Exercise

**Joint Staff IPv6 Operational Criteria Tested** (relevant Level 1 and 2 decomposition items)

**2** (2.1, 2.2, 2.3, 2.1.1, 2.1.3, 2.2.1, 2.2.3, 2.3.1, 2.3.3)

**8** (8.1, 8.1.1)

### **Configuration**

The FALCoN was tested in both a wired and wireless network using the following equipment.

- Cisco Mobile Access Radio Card - IOS 12.4(2)T1 fc3
- Access Points, 3201 Wireless Mobile Interface Card - IOS 12.2(15)JK4 fc1
- AirFortress Secure Gateway - Software Version 3.0.2900AQ.

### **Results**

#### *Security*

- The AirFortress Secure Gateway effectively provided security and did not inhibit network operations.

#### *Core IPv6 Functionality*

- Stateless Auto Configuration - The FALCoN demonstrated the ability to auto configure and function within an IPv6 test network in either a wired or a wireless mode.

- Internet Control Message Protocol Version 6 (ICMPv6) - The FALCoN successfully pinged a known address within a IPv6 test network in wired and wireless mode. While operating in IPv6, the pings returned quicker than when in IPv4 mode.

#### *Transition Mechanisms*

- Dual stack and 6to4 Static Tunnels - The FALCoN was able to ping from both its IPv4 and IPv6 interfaces to another device's IPv4 and IPv6 interfaces. The IPv6 interfaces returned a quicker time than the IPv4 interfaces.

#### *Routing Protocols*

- BGP Multi-protocol Extensions - Every FALCoN and router within the test network ran BGP correctly, updated its routing table, and forwarded traffic accordingly. The FALCoN supports the BGP routing protocol.
- RIPng – Every FALCoN and router within the network allowed other routing protocols to enter one of the devices running RIPng. The FALCoN and the router propagated other protocols through RIPng and its routing table updated accordingly. The FALCoN successfully implemented RIPng within the test network.

#### *Common Network Applications*

- The FALCoN transferred combined 77 HTTP, POP3, SMTP, and FTP files successfully in an IPv6 network. All transfers were completed error-free. Therefore, the FALCoN supports common network applications as also used in IPv4 networks.

#### *Network Operations*

- DNS for IPv6 - The IPv6 128-bit address record name was resolved on the FALCoN's host machine. This demonstrates the FALCoN's ability to conduct network operations within an IPv6 environment.

### **Conclusions/Recommendations**

The FALCoN can provide core IPv6 functionality, support transition mechanisms and routing protocols, provide common network applications, and sustain network operations in either a wired or wireless environment.

## **D.8 Joint User Interoperability Communications Exercise 2005 Internet Protocol Version 6 Assessment Report Annex**

### **Testing Organization and Publication Date**

JITC, Fort Huachuca, AZ  
December 2005

### **Summary**

The JITC performed an assessment of the JUICE 2005 IPv6 network. The IPv6 assessment took place at in August of 2005. The assessment determined to what extent current vendor implementations of IP systems including routing mechanisms, security, mobility, operating systems, and applications interoperated in a dual IPv4 and IPv6 environment. Emphasis was placed on using IPv4 as the backbone transport mechanism.

### **Test and Evaluation Method**

Exercise

### **Joint Staff IPv6 Operational Criteria Tested** (relevant Level 1 and 2 decomposition items)

**2** (2.2, 2.3, 2.1.1, 2.2.1, 2.3.1)

**3** (3.1, 3.1.1)

**4** (4.1)

**5** (5.1, 5.1.1)

**7** (7.1)

**8** (8.1, 8.1.1)

### **Configuration**

The base network was IPv4 with IPv6 riding over that existing network. Testing was restricted to assessing dual stack configurations and transition mechanisms. Serial encryption (KIV-19s) was used and is currently the preferred encryption method for IPv6 circuits. The following equipment was used during testing.

- Cisco 3725, 3745, 3845 - IOS 12.3(7)T, later upgraded to 12.4(2) for mobility testing and Spirent SmartFlow Test Equipment.

## Results

### *Network Performance over Bandwidth Constrained Links*

A four-router network was used during testing. The bandwidth on the link under test was varied from 9.6 Kbps to 1544 Kbps. Automated traffic generators provided traffic to congest the link, as approximately 100 million packets were captured across the bandwidth constrained links using IPv6 over IPv4 tunnels. Results were as follows:

- Links maintained a high level of service as demonstrated by meeting the criteria of 100, 99, 95, and 90 percent packet completion on unsaturated links at all assessed bandwidths using transmission control protocol (TCP), HTTP, and FTP packets.
- Testing demonstrated IPv6 traffic can operate effectively in low-bandwidth environments.
- All other scenarios (99, 95, 90 percent packet completion) produced data rate throughput higher than the KHz rate of the transmission media.
- Some bandwidth scenarios showed duplicate packets on links of 16 Kbps or less.

### *Security*

The network was configured for black backbone operation with bulk encryption to secure IPv6 traffic. Pre-built automated test scripts were performed from automated test devices. The bulk encryption was successful and inserting serial encryption devices in the system had no negative impact. HAIPE devices do not currently have the ability to encrypt IPv6.

### *End to-End Interoperability in a Mixed IPv4 and IPv6 Environment*

Traffic was transferred across 6to4 tunnels in accordance with RFCs 2893 and 2473. When the link was not saturated, the circuit maintained a 99 percent or greater completion rate. Latency across the tunnel averaged less than 10 milliseconds longer than the same circuit without a tunnel. The measured administrative overhead for the IPv6 tunnel was less than 10 percent of the allotted bandwidth.

### *Integration of Services*

The network was required to transport voice, data and video between two networks separated by a bandwidth constrained IPv4 network.

- Voice testing was not conducted, as the Cisco CallManager was unable to be configured in time for IPv6 testing.
- Data transfers between the computers maintained a 100 percent completion rate.

- An IPv6 capable camera was connected to the network using both IPv4 and IPv6 to allow remote monitoring of the JITC laboratory from anywhere in the JUICE network using streaming video.
- The video maintained high quality when used on high bandwidth circuits. No IPv6 capable video teleconference (VTC) systems were available for the test.

### *Mobile IPv6*

Subscriber mobility was tested across a network consisting of IPv4 bandwidth constrained links. The following list presents the results of testing mobile IPv6:

- Attempts to use IPv6 mobility were unsuccessful.
- Troubleshooting determined that the Internetworking Operating System for the Cisco routers required a minimum software version of 12.3(14)T for the mobility function.
- After loading version 12.4(2), the file was found to be too large for installation via Trivial File Transfer Protocol. Therefore, an FTP server was used to successfully upgrade the Cisco router.
- A Microsoft Windows Vista personal computer was upgraded with beta mobility software from Microsoft, but would not establish a relationship with the Home Agent in the router. The mobility features within Microsoft Windows Vista (beta) is no longer supported and will not be fielded.
- Due to the fact that the warfighter will not have the beta version of the Microsoft software, troubleshooting was suspended.

### *Network Management Traffic*

Network management features from a remote location using either SNMP or proprietary management systems were not tested, due to time constraints. The IPv6 SNMP management system was not brought online during testing, but routers were instead managed successfully via telnet.

### **Conclusions/Recommendations**

The current state of IPv6 used in a tactical network is immature and needs additional development and testing before full deployment. Tunneling IPv6 over IPv4 operated correctly as a method to allow transmission of IPv6 traffic over IPv4 circuits. The lack of HAIPE for IPv6 will require special planning and procedures that vary from the current network planning methods. Bandwidth constrained links with bandwidths higher than 16 Kbps are not negatively affected using IPv6 in comparison to IPv4 over the same system.

## D.9 MO1 Implementation Report

### Testing Organization and Publication Date

SI International  
30 March 2006

### Summary

This report documents Milestone Objective (MO1) pilot testing. This testing took place in a DoD IPv6 test bed that modeled common existing DoD enterprise networks using COTS hardware and software. The hardware and software demonstrated the conversion of IPv4 to a system running IPv6 within a test bed. Testing focused on post transition aspects of the test bed in the following areas:

- Documented configuration of test bed before and after transition.
- Baseline of test bed configuration after transition to IPv6:
  - Application layer compatibility with IPv6
  - Workarounds and Lessons Learned.

### Test and Evaluation Method

Demonstration

**Joint Staff IPv6 Operational Criteria Tested** (relevant Level 1 and 2 decomposition items)

**1** (1.5)

**2** (2.1, 2.2, 2.3, 2.1.1, 2.2.1, 2.3.1)

**8** (8.1, 8.1.1)

### Configuration

**Table D-3 Equipment Configuration**

Device Under Test
Cisco 2600 Router – IOS 12.3
Cisco PIX 515e Firewall - PIXOS 7.0(1), 7.0(4)
Cisco 2900 Switch – IOS 12.1
Cisco 2950 – IOS 12.1
Cisco Switch – IOS 12.2
HP ProCurve Switch 2524
Servers
Dell PowerEdge 2800
Windows Server 2003 Enterprise Edition
Sun Fire V20Z

**Table D-3 Equipment Configuration (continued)**

<b>Device Under Test</b>
Solaris 10
Windows XP Professional
VMWare
Fedora Core 4
Dell Optiplex GX300, GX150
Dell 8400 Dimension
Dell Dimension L1000R

## **Results**

### *Firewalls*

The firewall successfully supported dual stack; all native, translated, and tunneled IPv6 traffic was blocked. The firewall device passed all required tests.

## **Routing**

### (1) Open Shortest Path First Version 3 (OSPFv3)

The OSPF database and routing table included all subnets in the test bed. A ping from one laptop to a distant end laptop was successfully conducted through the network; therefore, verifying both routers used all prefixes in the lab. The router correctly ran OSPFv3.

### (2) Open Shortest Path First Version 2 (OSPFv2)

As with OSPFv3 tests, a ping from one laptop to a distant end laptop was successfully conducted through the network; therefore, verifying both routers used all prefixes in the lab. The router correctly ran OSPFv2.

## **Protocol Independent Multicast-Sparse Mode (PIM-SM)**

The PIM-SM did not function, due to the firewall and/or the modification of the PIXOS required utilizing PIM-SM with IPv6 in the test bed. To support PIM-SM, the IPv4 multicast infrastructure must be maintained.

## **Network Services**

Common network services were tested in two phases. First, IPv4 services were verified while running dual stack configuration and ensured all criteria were met before testing within IPv6. These services included: Network Address Translation, DHCP, DNS, NTP, SSH, FTP, Remote Login, VPN, HTTP, and HTTPS. Only VPN was unable to function properly in this setup.

After the transition to IPv6, DNS, SSH, FTP, HTTP, HTTPS, and Remote Login were successfully verified for functional operation. DHCP Version 6 (DHCPv6) and NTP both failed to operate correctly. Streaming Media partially passed the set criteria set.

### **Lessons Learned**

- Windows 2003 Server and XP Service Pack 2 Client do not support NTP using IPv6 transport.
- E-mail: Microsoft Exchange 2003 was not capable of communicating with IPv6 addresses.
- Orenosv FTP Server v.1.0 supports IPv6 and was successfully installed on Windows XP machines to run as FTP server.
- Windows Server 2003 does not support DHCPv6.
- DNS: Bind 9 supports and understands AAAA records and communicates using IPv6 protocol.
- Windows Server 2003 supports WWW service in IPv6 as part of their IIS services Network News Transfer Protocol in IPv6. But once IPv6 transport is enabled on a server running IIS 6.0, all web pages on the computer are available to IPv6 clients. Individual pages or virtual directories cannot be configured to respond to either IPv4 or IPv6 requests only.
- Linux supports SSH server using IPv6 transport.

### **Conclusions/Recommendations**

In the initialization of the network systems, the base network services were brought online and basic functionality was provided to each of the workstations independent of the internal networks of which they were a part. The servers and workstations were all properly configured and documented to allow for standard operational network procedures. The routers, firewalls, servers, and hosts were all properly configured and documented. This dual stack implementation of the test bed was completed successfully. The current configuration to support IPv6 is the standard DoD IPv4 enterprise architecture.

## **D.10 Capabilities and Lessons Learned from IPv6 Migration of the Command and Control Resource Management System (C2RMS)**

### **Testing Organization and Publication Date**

Adroit Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Center, SRA International, Inc.  
19 September 2005

### **Summary**

The C2RMS program monitors and manages Command and Control (C2) enterprises in the event of degradation or failure of mission critical components. The C2RMS program rapidly initiates corrective measures, both manually and automatically, to ensure continued mission effectiveness in a rapidly changing environment that may cross service, coalition, and DoD agency boundaries. This report documents capabilities and lessons learned during C2RMS migration. Previous versions of C2RMS had limited IPv6 capability. This migration now enables C2RMS to have more IPv6 features.

### **Test and Evaluation Method**

Experiment

**Joint Staff IPv6 Operational Criteria Tested** (relevant Level 1 and 2 decomposition items)

**9** (9.1, 9.1.1, 9.1.2, 9.1.3)

### **Configuration**

The configurations were tested in a dual stack environment with the IPv6 enabled version of C2RMS.

### **Results**

The C2RMS has the following IPv6 capabilities:

- Resources (any IP addressable device) can be created in C2RMS with an Pv4 or IPv6 address.
- C2RMS can monitor resources for status via IPv6-oriented ping monitor and an IPv6-oriented SNMP monitor.
- Monitors report back to the C2RMS server via IPv4 or IPv6, depending on which address (IPv4/v6) within the host was queried.

## Lessons Learned

The following list presents lessons learned from the IPv6 migration of C2RMS:

- Auto configuration is not yet implemented across all platforms.
- Windows does not provide SNMP daemon support for IPv6.
- Windows Server 2003 operating system's (OS) SNMP agent shipped with the OS does not work with IPv6.
- Outbound network interfaces must be specified for link local IP addresses.
- Many OSs currently do not provide much support for common networking protocols such as DHCP.
- Java 1.5 provides IPv6 support.
- An IPv6 address does not have a set prefix and subnet like an IPv4 address. Therefore, IPv6 networks must provide multiple scanning ranges, which causes a longer wait-time since the range is much larger than an IPv4 range.
- DHCPv6 servers currently do not meet standards of IPv6, causing an IPv6 network with widely, varied IP addresses.
- Solaris requires no link local address to be assigned to the Ethernet adapter interface.
- In WebLogic 9, IPv6 channels must be configured in order for clients to connect to the Weblogic applications server using the IPv6 address.

## Conclusions/Recommendations

The IPv6 migration of C2RMS is essential to ensure network integrity in service, coalition, and DoD agency boundaries. The migration has enhanced many features of the program, such as allowing the status monitoring of IPv6 host devices using either IPv4 or IPv6. Many lessons learned were taken from testing. Improvements must be made to ensure C2RMS works as well in an IPv6 environment as it does in IPv4.

## **D.11 Internet Protocol Version 4 (IPv4) to IPv6 Transition Mechanisms for Tactical Networks**

### **Testing Organization and Publication Date**

US Army Communications and Electronics Research Development and Engineering Center  
(CERDEC)  
28 Nov 2005

### **Summary**

This report describes various transition mechanisms and transitional architectures to ensure IPv4 and IPv6 interoperability during the Army's transition from IPv4 networking systems to the IPv6 Global Information Grid (GIG). Such mechanisms include dual stack IPv4 and IPv6 TCP/IP stacks, manually configured tunnels, automatic tunnels, and translation mechanisms. The functionality, scalability, and security implications of each mechanism was evaluated. IPv6 transition mechanism architecture is also suggested. In addition, deploying IPv6 capable DNS and address books in tactical networks is discussed.

### **Test and Evaluation Method**

Engineering Analysis

**Joint Staff IPv6 Operational Criteria Tested** (relevant Level 1 and 2 decomposition items)

**2** (2.1.1)

**8** (8.1, 8.2, 8.1.1, 8.2.1)

### **Configuration**

Although no "real" test configuration was used for this analysis, a common DoD network was analyzed.

### **Results**

- Dual Stack:
  - Performance – No major known performance issues.
    - Memory, CPU and network maintenance overhead required to service IP are all increased.
  - Security – New, unproven code into the TCP/IP stack could lead to vulnerabilities.
  - Scalability – Currently seen as a problem as many routers must maintain separate routes for IPv4 and IPv6 networks, creating twice the work as a single stacked network. Overhead penalties of a dual stack can be severe as a network scales up in size.

- Recommendations:
  - All new IPv6 capable devices should be fully dual stacked for maximum network flexibility.
- Configured Tunnels:
  - Performance – Tunnels pay a double penalty for IP header overhead. Configured tunnels must be reconfigured if a network is renumbered by changed addressing.
  - Security – No serious issues were discovered with configured tunnels.
  - Scalability – Time and effort required for administrators to manually configure tunnels to connect each isolated network is an issue.
- IPv4 Compatible IPv6 Addresses:
  - Scalability is deprecated since it requires globally routable IPv4 addresses and creates a node level IPv6 address that is not compatible with hierarchical routing.
- Automatic Host Tunneling Mechanisms:
  - Performance – Like configured tunnels, automatic tunneling has double IP header overhead.
  - Security – This type of tunneling from a host to the outside of a domain provides a possible security breach, especially if the protocol has been designed to bypass NAT and filtering firewalls.
  - Scalability – A single tunneling endpoint router can scale to support several thousand tunnels for a campus-sized network.
  - Examples of Automatic Tunneling Mechanisms:
    - IPv6 Tunnel Broker
    - 6to4
    - Teredo
    - ISATAP
    - DSTM.
- Translators:
  - An on-link bump-in-the-wire translator can sustain specific needs of a device not used for an enterprise-wide service.
- DNS:
  - As the world’s largest network system application, this analysis recommends implementing Berkeley Internet Name Domain (BIND) version 9 or higher for dual stack operations to prepare for IPv6. The BIND-9 supports the new IPv6 resource record type called the “AAAA” record.

## Conclusions/Recommendations

IPv6 can be successfully integrated into tactical networks, but a concentrated engineering effort will be necessary to fully realize the benefits of an IPv6 based network. After initial IPv6 integration via dual stacks and tunnels, an additional effort is necessary to create an “IPv6 dominant” network that can still service IPv4 applications but take advantage of IPv6-only advanced features such as autoconfiguration, mobility, multi-homing, and service discovery.

## D.12 Milestone Objective 1 Internet Protocol version 6 Capable Evaluation Base, Control

### Testing Organization and Publication Date

SI International  
24 October 2005

### Summary

This report is part of a series of testing MO1 requirements. This test pertains to conducted MO1 IPv6 capable evaluation base control. The testing took place in a DoD IPv6 test bed that modeled common existing DoD enterprise networks using COTS hardware and software. Testing focused on detailed functional requirements for IPv6 routing protocols (RIP Next Generation, BGP4+, OSPFv3, and IS-IS) as well as testing fundamental functionalities of the IPv6 protocol (Header format, Stateless autoconfiguration, Multicast Listener Discovery, and Maximum Transfer Unit discovery).

### Test and Evaluation Method

Experiment

**Joint Staff IPv6 Operational Criteria Tested** (relevant Level 1 and 2 decomposition items)

2 (2.2, 2.3)

### Configuration

Table D-4 lists the equipment configuration of the devices under test.

**Table D-4 Equipment Configuration**

Device Under Test
Cisco 2600 Router – IOS 12.3
Cisco PIX 515e Firewall - PIXOS 7.0(1), 7.0(4)
Cisco 2900 Switch – IOS 12.1
Cisco 2950 – IOS 12.1
Cisco 3550 – IOS 12.2
HP ProCurve Switch 2524
Servers
Dell PowerEdge 2800
Windows Server 2003 Enterprise Edition
Sun Fire V20Z
Solaris 10
Windows XP Professional
VMWare
Fedora Core 4
Dell Optiplex GX300, GX150
Dell 8400 Dimension
Dell Dimension L1000R

## Results

The following table gives a summary of MO1 IPv6 Capable Evaluation Base, Control test results while operating in a mixed IPv4 and IPv6 environment.

**Table D-5 Test Results**

Test	Result
Verify that the router supports RIPng routing algorithm	Pass
Verify that routers maintain a routing table entry for every destination	Pass
Verify that each routing table entry, created by a router, contains a route metric	Pass
Verify that each routing table entry contains the IPv6 address of the next router	Pass
Verify that a node's packet format complies with the definition in RFC 2080	Pass
Verify that an address specified in RIPng as a next hop is a link-local address	Pass
Verify that prefix 0:0:0:0:0:0:0:0 is used when specifying the default route	Pass
Verify that the default route is used if the route destination is not listed in the routing table	Pass
Verify that RIPng Requests are sent by a router to ask for a response containing all or part of a neighboring router's routing table	Pass
Verify that RIPng Requests are sent as multicasts by routers which have just come up and are seeking to fill in their routing tables as quickly as possible	Pass
Verify that an (unsolicited) response is received due to a regular update	Pass
Verify that a Response message is received due to a triggered update caused by a route change	Pass
Verify that an interface identifier must be unique on a given link	Pass
Verify that a host must send a multicast listener report when it joins a multicast group or in response to an MLD multicast listener query	Pass
Verify that hosts must request routers to send their address and connection parameters in order to enable autoconfiguration	Pass
Verify that a host must send a neighbor advertisement message in response to neighbor solicitation	Pass
Verify that a host must send a multicast listener done message when it leaves a multicast group	Pass

## Lessons Learned

- Cisco IOS (12.3T):
  - RIPng and OSPFv3 were both supported.
  - RIPng and OSPFv3 should be configured on each router interface and not on the global configuration mode of the router.
- Windows XP (Service Pack 2):
  - When configuring an IPv6 address for any interface, there is no clear way to define the network prefix of the IPv6 address.
- Most Base and Control Plane sections were successfully validated and supported by Windows and Cisco Products.

## **Conclusions/Recommendations**

Any operating system that supports IPv6 should be able to satisfy most of the requirements for the Base and Control section of the IPv6 capable matrix. The routing protocols and fundamental functionalities of the IPv6 protocol were successful during this testing.

## **D.13 Milestone Objective 1 Internet Protocol version 6 Capable Evaluation Base, Transition Mechanisms, Applications**

### **Testing Organization and Publication Date**

SI International  
25 September 2005

### **Summary**

This report is part of a series of testing MO1 requirements. This test pertains to MO1 IPv6 Capable Evaluation Base, Transition Mechanisms, and Applications. The testing took place in a DoD IPv6 test bed that modeled common existing DoD enterprise networks using COTS and software. Tests focused on fundamental functionalities of the IPv6 protocol (Header format, Stateless autoconfiguration, Multicast Listener Discovery, and Maximum Transfer Unit discovery), applications (DNS, HTTP, FTP, Telnet, and SMTP), and transition mechanisms (configured or automatic tunnels, and translation).

### **Test and Evaluation Method**

Experiment

**Joint Staff IPv6 Operational Criteria Tested** (relevant Level 1 and 2 decomposition items)

**2** (2.2, 2.3, 2.2.1, 2.3.1)

**8** (8.1, 8.1.1)

### **Configuration**

Per previous MO1 testing by SI International, the following table lists the equipment configuration.

**Table D-6 Equipment Configuration**

<b>Device Under Test</b>
Cisco 2600 Router – IOS 12.3
Cisco PIX 515e Firewall - PIXOS 7.0(1), 7.0(4)
Cisco 2900 Switch – IOS 12.1
Cisco 2950 – IOS 12.1
Cisco 3550 – IOS 12.2
HP ProCurve Switch 2524
Servers
Dell PowerEdge 2800
Windows Server 2003 Enterprise Edition
Sun Fire V20Z
Solaris 10
Windows XP Professional
VMWare
Fedora Core 4

**Table D-6 Equipment Configuration (continued)**

Device Under Test
Dell Optiplex GX300, GX150
Dell 8400 Dimension
Dell Dimension L1000R
Agilent N4180B Network Tester

**Results**

**Table D-7 Test Results**

Test	Result
Verify that the Web Server is able to send web contents to web clients using IPv6 packets	Pass
Verify that the system supports the extensions of the FTP protocol to move files across networks or the internet using IPv6	Pass
Verify that nodes are able to use Telnet to access IPv6 devices using either the IPv6 address. IPv6 packets must be exchanged during the Telnet session	Pass
Verify that the AAAA Record Type specific to the internet class of a single IPv6 Address is supported	Pass
Verify that systems support the use of SMTP with IPv6	Pass
Verify that the DNS AAAA query returns all associated AAAA resources records in the answer section of a response	Pass
Verify that edge routers can be dual stacked	Pass
Verify that IPv6 device (router) can be configured with configured tunneling transition mechanism (GRE)	Pass
Verify that IPv6 basic header length shall include a destination address (128-bit) field	Pass

**Lessons Learned**

- Windows Server 2003 supports:
  - IPconfig, Ping, Tracert, Netstat, and Route commands.
  - Internet Explorer and the Internet Information Services Web service.
- Apache Web Server running on Windows XP successfully hosted IPv6 web pages.

**Conclusions/Recommendations**

This report documents tested fundamental functionalities of the IPv6 protocol, applications, and transition mechanisms. Although most tests were passed, many common applications are not IPv6 capable yet and do not cover most of the MO1 requirements. More test cases must be executed concentrating on MO1 requirements.

## D.14 Milestone Objective 1 Internet Protocol version 6 Capable Evaluation Information Assurance

### Testing Organization and Publication Date

SI International  
02 September 2005

### Summary

This report documents MO1 testing which took place in a DoD IPv6 test bed that modeled common existing DoD enterprise networks using COTS hardware and software. Conversion of an existing IPv4 system to IPv6 was demonstrated within a test bed. Testing focused purely on IPv6 IA.

### Test and Evaluation Method

Experiment

**Joint Staff IPv6 Operational Criteria Tested** (relevant Level 1 and 2 decomposition items)

1 (1.1, 1.2, 1.4, 1.5, 1.1.1, 1.1.2, 1.1.3, 1.2.1, 1.4.1, 1.4.9, 1.5.1)

### Configuration

Table D-8 lists the equipment configuration of the devices under test.

**Table D-8 Equipment Configuration**

<b>Device Under Test</b>
Cisco 2600 Router – IOS 12.3
Cisco PIX 515e Firewall - PIXOS 7.0(1), 7.0(4)
Cisco 2900 Switch – IOS 12.1
Cisco 2950 – IOS 12.1
Cisco 3550 – IOS 12.2
HP ProCurve Switch 2524
Servers
Dell PowerEdge 2800
Windows Server 2003 Enterprise Edition
Sun Fire V20Z
Solaris 10
Windows XP Professional
VMWare
Fedora Core 4
Dell Optiplex GX300, GX150
Dell 8400 Dimension
Dell Dimension L1000R
Agilent N4180B Network Tester

## Results

**Table D-9 Test Results**

<b>Test</b>	<b>Result</b>
Verify that the IPv6 device (router) could permit and deny packet forwarding based on protocol (http)	Pass
Verify that IPv6 device (router) can properly permit or deny packet forwarding based on source port number 80	Pass
Verify that IPv6 device (firewall) can properly permit or deny packet forwarding based on source port number	Pass
Verify that router must deny or permit packet forwarding based on the IPsec option in the IPsec headers	Pass
Verify that the IPv6 device (firewall) could permit or deny packet forwarding based on TCP info	Pass
Verify that the IPv6 device (router) could permit and deny packet forwarding based on User Datagram Protocol (UDP) info	Pass
Verify that the IPv6 device (firewall) could permit packet forwarding based on UDP info	Pass
Verify that router must require login/password for access to the management function	Pass
Verify that router must recognize the AH fields when they are set to null	Pass
Verify that router must recognize the ESP fields when they are set to null	Pass
Verify that firewall must recognize the AH fields when they are set to null	Pass
Verify that firewall must recognize the ESP fields when they are set to null	Pass

## Lessons Learned

- Windows 2003 Server and XP Service Pack 2 Client:
  - IPsec support for IPv4 traffic is separate from IPsec support for IPv6 traffic. Local or domain-based IPsec policies configured with the IP Security Policies or Group Policy snap-ins are for IPv4 traffic only. These policies have no effect on IPv6 traffic.
  - Windows 2003 Server and XP SP2 Client do not have IPsec Graphical User Interface for IPv6 as all systems have for IPv4; installing and configuring IPsec6 has to be done using command line interface.
  - The current implementation of IPsec for IPv6 is not recommended for use in a production environment because it relies on static keying, which means that it has no provisions for updating encryption keys when sequence numbers are reused.
- Cisco Routers:
  - Cisco IOS IDS is not supported for IPv6.
  - At default, when no IPv6 Access Control Lists (ACLs) are configured on the router all IPv6 traffic is permitted. However, once an IPv6 ACL is configured and applied to an interface, the default action for that interface is to deny all IPv6 traffic not explicitly permitted on the interface.
- Cisco Firewalls:
  - Cisco equipment does not support SNMP management using IPv6 addresses.

## **Conclusions/Recommendations**

This document was created to test MO1 IA requirements, as defined in the IPv6 Capable document, on a simulated DoD enterprise enclave running a dual stack network. The test cases included packet filtering, network management, IPSec, and more. Many requirements were met. However, some IA requirements need further development.

## D.15 2005 Ethernet Switch Comparison Report

### Testing Organization and Publication Date

U.S. Army Information Systems Engineering Command Technology Integration Center  
February 2006

### Summary

The Technology Integration Center (TIC) evaluated Ethernet switches from seven different vendors for possible use in the Installation Information Infrastructure Modernization Program (I3MP). The testing included evaluating core, building, and edge switches in areas of performance, system functionality, network management, and security. The TIC evaluated each switch's strengths and weaknesses in the aforementioned areas.

### Test and Evaluation Method

Demonstration

**Joint Staff IPv6 Operational Criteria Tested** (relevant Level 1 and 2 decomposition items)

**2** (2.2, 2.2.1)

**3** (3.1, 3.2, 3.3)

**9** (9.1)

### Configuration

Table D-10 lists the equipment tested during the 2005 Ethernet switch comparison evaluation.

**Table D-10 Equipment Configuration**

<b>Vendor</b>	<b>Product</b>	<b>Type</b>
3COM	Switch 8814	Core
	Switch 8810	Core
	Switch 8807	Core
	SuperStack 4 5500-48	Edge
	SuperStack 4 5500-24	Edge
	SuperStack 4 5500-48 PWR	Edge
	SuperStack 4 5500-24 PWR	Edge
Alcatel Networks	OmniSwitch 9700	Core
	OmniSwitch 7700	Edge
	OmniSwitch 6800-48	Edge
	OmniSwitch 6800-24	Edge

**Table D-10 Equipment Configuration (continued)**

Cisco Systems	7606	Core
	Catalyst 6509	Core
	Catalyst 4510R	Core
	Catalyst 4507R	Core
	Catalyst 4503	Building
	Catalyst 3750-48	Edge
	Catalyst 3750-24	Edge
	Catalyst 3560-48	Edge
	Catalyst 3560-24	Edge
Enterasys	Matrix N7	Core
	Matrix N5	Core
	Matrix N3	Building
	Matrix E1 WS-48	Edge
	Matrix E1 WS-24	Edge
	Matrix N Series Standalone	Edge
Extreme Network	BlackDiamond 10808	Core
	BlackDiamond 8810	Core
	BlackDiamond 6808	Core
	Alpine 3808	Building
	Alpine 3804	Edge
	Summit 300-48	Edge
	Summit 300-24	Edge
	Summit 200-48	Edge
Summit 200-24	Edge	
Foundry Networks	MG8	Core
	FastIron SuperX	Edge
	FastIron Edge 9604	Edge
	FastIron Edge 4802	Edge
	FastIron 2402	Edge
Nortel Networks	ERS5520-48T-PWR	Edge
	ERS5520-24T-PWR	Edge
	ERS5510-48T	Edge
	ERS5510-24T	Edge

## Results

All switches were tested on stand alone performance (throughput, forwarding, congestion control, Power over Ethernet, multimedia scenarios), system functionality (supports FTP, SMTP, HTTP, and HTTPS), network management (MIB requests, SNMP, capabilities to support NMS), and security (vulnerability scanning, support of SSH, secure management, password protection, and product integrity).

Most edge switches consistently passed IPv6 traffic at/or near the line rate. Core switches passed traffic normally below the line rate. A majority of the switches lacked implemented security and management when operating in IPv6, with few exceptions. No switch met all the current I3MP IPv6 requirements.

## **Conclusions/Recommendations**

Although no switch met all the objectives for IPv6 performance, management, and security, this year's testing saw a dramatic improvement over the 2004 test. As the approving authority for the I3MP Approved Product List, the TIC strongly recommended switches that meet a large number of the IPv6 requirements, as these are necessary for the future I3MP network.

## **D.16 ADNS HAIPE Interface Requirements (Including IM-PEPD, VECP and Route redistribution)**

### **Testing Organization and Publication Date**

SPAWAR Systems Center  
13 February 2006

### **Summary**

This document outlined requirements for the Implicit Peer Enclave Prefix Discovery protocol (IM-PEPD) and associated Virtual Encryptor Configuration Protocol (VECP). The purpose was to propose and document requirements for introduction into the NSA process for inclusion into the High Assurance Internet Protocol Interoperability Specification. The protocol is also applicable to IPsec devices. The goal is to provide a simple, extremely scalable dynamic discovery solution for network encryption.

### **Test and Evaluation Method**

Engineering Analysis

### **Joint Staff IPv6 Operational Criteria Tested** (relevant Level 1 and 2 decomposition items)

**1** (1.6, 1.6.1, 1.6.2)

### **Configuration**

The basic concept of IM-PEPD is that a single network prefix associated with each HAIPE and the addresses of the HAIPEs are administratively pre-determined, making prefix discovery unnecessary.

HAIPE also uses a dynamic discovery protocol, VECP, to support multiple prefixes behind a single HAIPE. This is necessary to support connections to legacy or public networks and for transition between dynamic legacy networks and the planned GIG architecture, where the network encryption is pushed as close to the user as possible.

### **Results (Requirements)**

The following requirements are necessary for HAIPE software implementation:

- HAIPE allows operator configuration of the IM-PEPD prefix length in bits.
- For IPv6 the suggested configuration range is 24-64 bits.
- HAIPE allows configuration of the Cipher Text (CT) Host Identification (ID) for the group.

- HAIPE allows configuration of the CT/Plain Text (PT) interfaces in the same network prefix.
- HAIPE generates the CT destination for key exchanges using the IM-PEPD parameters and the PT destination prefix.
- HAIPE generates the CT header destinations of encrypted packets using the configured IM-PEPD parameters and the PT destination prefix.

The following are proposed HAIPE software requirements for the VECF protocol:

- HAIPE uses a VECF probe/response protocol to discover networks behind other encryptors.
- The receiving HAIPE responds with a message that informs the initiator that it is the gateway for the prefix, when a HAIPE receives a VECF probe.
- HAIPE applies CT destination addresses of remote HAIPEs to encrypted packets according to IM-PEPD parameters, even if the HAIPE for that prefix does not exist.

### **Conclusions/Recommendations**

Using IM-PEPD/VECF for implementation in HAIPE devices could support an IP routing architecture for the network-centric component of the GIG. Further T&E and development are required.

## **D.17 Simplified Multicast Forwarding for MANET**

### **Testing Organization and Publication Date**

Internet Engineering Task Force (IETF) MANET Working Group/Naval Research Lab  
5 March 2006

### **Summary**

This document describes the SMF protocol that provides a basic IP multicast forwarding capability within mobile ad hoc networks (MANET). SMF is designed to have limited applicability as a forwarding mechanism for multicast packets within MANET routing areas. In addition, it provides mechanisms to support interoperability with a connected wired infrastructure. SMF uses a simplified forwarding mechanism that delivers multicast packets to all MANET multicast receivers within a MANET routing area. The core design does not use receiver specific group information in order to reduce complexity and state maintenance within the mobile topology. This document describes the SMF forwarding mechanisms in detail, specifies an optional SMF neighbor discovery protocol, and describes several efficient relay set algorithms that have been implemented in conjunction with SMF.

### **Test and Evaluation Method**

Engineering Analysis

**Joint Staff IPv6 Operational Criteria Tested** (relevant Level 1 and 2 decomposition items)

**10** (10.2, 10.2.1)

### **Configuration**

The following characteristics are desired as an effective MANET flooding algorithm solution for use in SMF:

- Resultant cover set that is small compared to the total number of nodes as the network scales in size and density.
- Robust approach somewhat resilient to network mobility and link dynamics.
- Cover set election/maintenance mechanism that is lightweight, distributed, and adaptive in nature.

### **Results (Recommendations)**

Distributed mechanisms that select and maintain reduced relay node sets have been developed. Wireless contention, topological classes, and robustness of packet delivery and set election under mobility scenarios further complicate design tradeoffs. In addition, the actual protocol

implementation for IP multicast forwarding based upon these flooding algorithms raises additional design tradeoffs and issues, including:

- Protocol state maintenance
- Duplicate packet detection mechanisms
- Packet processing requirements and overhead
- Expected traffic distribution patterns
- Protocol signaling requirements
- Delivery robustness requirements.

SMF should also implement explicit detection of duplicate multicast packets by a temporal packet identification scheme. This is typically implemented by keeping a history of previously received and forwarded packet identifiers for comparison against recently forwarded multicast packets. Different approaches to packet identification have been considered. Possibilities include unique markings within packet header fields, such as packet sequence numbering, or application of hash algorithms or similar techniques to compactly and uniquely describe the history of recently received packets. This document recommends simple, sequence-based schemes that can be accomplished without additional (non-IP) encapsulation of packets and/or their content. Encapsulation approaches are considered out-of-scope so that non-forwarding edge nodes within a MANET area can easily receive flooded content without any additional software beyond a typical IP stack.

Packet hashing approaches for Duplicate Packet Detection (DPD) may be applicable in some cases, but early examination of these approaches indicated that computation complexity may be prohibitive for per-packet processing on many candidate MANET platforms (e.g., PDAs). Additionally, the unavoidable "cache-miss" rates, while possibly low for some algorithms, result in the severe penalty of false DPD (and thus packet loss) rather than the more benign penalty of additional computation cycles as associated with most applications of hashing.

## **Conclusions**

Much work remains on implementing SMF for MANET. The IETF Working Group has designed many possibilities and solutions for SMF implementation. However, areas such as interfacing with exterior multicast routing protocols, multiple gateways, multicast group scoping, and security must be continually worked on and future T&E will be needed to test ideas.

## **D.18 Special Interoperability Test Certification of the Hewlett Packard Laser Jet 2420d Printer with Jetdirect Card for Internet Protocol Version 6 (IPv6) Capability**

### **Testing Organization and Publication Date**

JITC, Ft. Huachuca, AZ  
30 June 2006

### **Summary**

The Device Under Test (DUT) was a Jetdirect network card incorporated in a Hewlett-Packard Laser Jet 2420 Printer providing basic IPv6 capability plus IPsec and certificate based authentication. This card was tested against the GTP version 2, draft test plan for Performance and Interoperability. After completing the certification process, this device will be placed on the IPv6 Approved Products List.

### **Test and Evaluation Method**

Special Interoperability Certification

**Joint Staff IPv6 Operational Criteria Tested** (relevant Level 1 and 2 decomposition items)

**1** (1.1, 1.3, 1.4, 1.1.1, 1.1.3, 1.3.2)

**2** (2.1, 2.2, 2.3, 2.1.1, 2.2.1, 2.3.1)

**3** (3.2, 3.3, 3.2.1, 3.3.1)

**5** (5.1, 5.1.2)

**8** (8.1, 8.1.1)

### **IPv6 APL Result**

This product was given a Special Interoperability Certification awaiting Information Assurance Certification.

### **Configuration**

The network card and printer were connected for testing through the JITC simulated GIG network. The network included encryption capabilities and bandwidth constrained links. The Network Interface Card (NIC) on the printer was tested with laptops that employed Windows XP. The IPv6 type addressing is available on a personal computer that runs Windows XP, Windows Server 2003, Windows Longhorn, Linux Redhat, Linux Fedora Core 4, and Linux Fedora Core 5. Certificates that were used during testing were pulled from a Dell certificate server running Windows 2003 server. Table D-11 lists other equipment used within the test network.

**Table D-11 Equipment Configuration**

<b>EQUIPMENT NAME</b>	<b>MODEL NUMBER</b>	<b>VERSION</b>
Printer	HP Laser Jet 2420d 80 MB RAM	Firmware Datecode 20050203 08.108.3
Network Card	HP Jetdirect 635N J7961A	Firmware V31003.FF
Encryptor	KIV-7HSB	N/A
Cisco Router	CISCO3845	12.3(14)T2
Cisco Router	CISCO3845	12.4(4)T1
Juniper Router	Juniper M40e	v7.4R2.6
Juniper Router	Juniper M40e	v7.4R2.6
Juniper Router	Juniper T 320	v7.3R1.5
Juniper Router	Juniper T 320	v7.3R1.5

## Results

### *Core IPv6 Functionality*

The printer was configured using IPv6. Print jobs were successfully sent across the GIG network and printed via IPv6. The print job was then printed to file and saved. This file was then transferred over FTP to the printer volatile memory and printed successfully 20 out of 20 attempts. Mozilla Firefox was then used to open an HTTP session to the printer for management of the printer via IPv6. This HTTP session was created and maintained a minimum of 20 times with a 100 percent success rate.

Tests for ICMP were performed across the simulated GIG network. A continuous ping test for IPv6 was started and ran for one hour with no loss of packets. Three separate tests of 1,000 ping tests were also performed with 100 percent success. A network tap was used to capture the continuous ping packets and were examined for RFC compliance.

### *Bandwidth Constrained Links*

The printer only provides an Ethernet interface for network connectivity. To verify the ability for traffic to transit Point-to-Point Protocol (PPP) serial links a router was installed with a 1.544M PPP serial link including KIV-7 encryption. Traffic was successfully passed across this link to perform print jobs from a host computer.

### *Transition Mechanisms*

Generic Tunnels are normally created at a router to allow encapsulation of user traffic across the network. In this case, the DUT is a user device with no router capabilities. This device successfully passed traffic across GRE tunnels, but it could not create those tunnels. The DUT is capable of supporting both IPv4 and IPv6 simultaneously or independently. Addresses for IPv4 were successfully obtained using DHCP. Addresses for IPv6 were obtained using IPv6 host autoconfiguration. The printer successfully responded to print requests, FTP, and HTTP on both IPv4 and IPv6 in a dual-stack environment with 100 percent success.

This device is unable to configure tunnels except for IPSec tunnels or support SMTP or Real Time Streaming Protocol file types for printing. FTP is supported for delivery of files to be printed and HTTP is supported for management purposes.

### *Information Assurance*

The printer was configured with test certificates that matched one computer (IPv4 and IPv6) and secure transactions were conducted to allow HTTP and print functions over IPv4. The PKI certificate was downloaded from an existing laptop and copied over to the DUT. This information was sniffed and the packets were examined to try to recover intelligible data. The payload was encrypted and no information was recognizable within the packet. The same type of test was performed on IPv6 using Windows Longhorn. The PKI certificates were downloaded from a server running Longhorn Beta, Build 5384.4.060518-1455, Date 05-22-2006. This test still needs to be run with Linux and Windows XP. A test was not run on Linux due to time constraints. A test was not performed on IPv6 using Windows XP due to the software not supporting an IPv6 address in the windows to create secure connections.

### **Conclusions**

The DUT successfully completed the related IPv6 Performance and Interoperability portions of the GTP. Therefore, the Hewlett Packard Laser Jet 2420d Printer with Jetdirect Card is certified as IPv6 capable.

## **D.19 IPv6 Transitioning: Not Ready for Prime Time**

### **Testing Organization and Publication Date**

U.S. Army Information Systems Engineering Command (USAISEC) Technology Integration Center

December 2005

### **Summary**

The engineers at USAISEC sought to determine the steps necessary to build an IPv6 operational network. The ultimate goal was to transition the USAISEC production network to IPv6. The steps in learning this were documented in detail, while denoting lessons learned and stumbling points so that those who follow can learn from this experience. Many common IPv6 applications and services were assessed and overall performance was evaluated.

### **Test and Evaluation Method**

Experiment

### **Joint Staff IPv6 Operational Criteria Tested** (relevant Level 1 and 2 decomposition items)

**1** (1.5, 1.5.1, 1.5.2)

**2** (2.2, 2.3, 2.2.1, 2.3.1)

**8** (8.1, 8.1.1)

### **Configuration**

The USAISEC network is almost entirely Microsoft Windows-based, as is the replica network. The primary server was comprised of the Active Directory (AD) controller, the primary DNS server, the DHCP server, the File Server, the Printer Server, the streaming media server, and a Web server. The other server is comprised of the secondary DNS and the Live Communications Server (LCS) (the latter of which provides collaborative tools for use across the enterprise). Both servers were loaded with the Windows Server 2003 Enterprise Edition and Service Pack 1. The two Linux servers, loaded with RedHat 9.0, were used to help investigate problems and anomalies in the operation of IPv6 by acting as protocol analyzers and UNIX Web servers.

The clients used myriad configurations. Two UNIX clients were loaded with Fedora Core 4 and Vector 5 Linux. Five clients were loaded with Windows XP Professional with Service Pack 2. Two clients were loaded with Vista Beta 1 Second Release. The Windows machines were joined to the AD domain and loaded with the LCS client software. All machines on the network were built with dual network cards, one using IPv4 exclusively and the other a dual stack IPv4 and IPv6. Thus, connections used for communications were easily monitored and operations of IPv4 and IPv6 could be compared.

## Results

The report shows several areas in which manual intervention by a user or network administrator is required to achieve even basic IPv6 functionality. There were also several areas in which IPv6 lacks the functionality that has come to be expected in IPv4 networks. The results are summarized below:

- Network Communication:
  - On initial boot or connected to the network, the client must first register itself with the authoritative devices on the network. With IPv6 at present, this step is manual and in many cases cannot be accomplished.
- Auto-configuration:
  - DHCPv6 duplicates the functionality of DHCP in IPv4, but it is not yet implemented in any of the Windows operating systems.
- IPv6 Graphical User Interface (GUI) Configuration:
  - With the exception of the Vista beta, Windows operating systems provided an equivalent GUI for IPv6 configuration as they do for IPv4.
- DNS:
  - The DNS built into the Windows Enterprise Server 2003 handles IPv4 and IPv6 addresses, with both forward and reverse lookups.
  - Clients can successfully make DNS queries of IPv4 and IPv6 addresses, as long as the queries are sent via IPv4. By default, the DNS Server does not accept DNS queries over IPv6.
  - The IPv6 capable Ethernet switch blocked DNS query traffic over IPv6 by default, therefore testers had to manually configure this network on the Ethernet switch in order for DNS traffic to pass through. Only then could the Vista client perform DNS lookups.
- Applications:
  - On the Windows XP clients IPv4 was disabled and it was discovered that IPv6 communication disappeared. This is a known flaw in Windows XP and has been corrected in Vista.
  - After disabling IPv4 on the Vista clients after logging into the domain, most network applications could run over pure IPv6.
- Internet Browsers:
  - Internet Explorer can browse Web pages over IPv6, but it will not accept IPv6 Uniform Resource Locators specified by address.
  - A third-party Web browser, Firefox, could browse Web pages over IPv6 using either IPv6 addresses or domain names.

- File Sharing:
  - Windows networking and sharing of drives worked without issue over IPv6.
- Network Devices:
  - The IPv6 capability of most networking devices that were tested meets the current DoD requirement of “IPv6 Capable” but does not satisfy the practical needs of most users wishing to implement IPv6 on an operational DoD network.
- Network Security:
  - The state of the industry in firewalls and IDS appears to be far behind the DoD’s need for network protection.
  - The management interface on one vendor’s machine did not display IPv6 packets that have been screened and did not allow rules to be built using IPv6 criteria. Thus, testers and administrators cannot verify whether the system is properly filtering IPv6 packets.

## **Conclusions**

The IPv6 is not ready for production use at this time. Network administrators considering serving as pilot sites should be prepared for many technical and implementation hurdles. Current Windows operating systems lack many basic features to support IPv6 networking. Many networking hardware devices can support basic IPv6 operation but lack features such as management and security which are vital for operational DoD networks. Corrections should be built into the core of operating systems and into the hardware on network devices. The DoD cannot run its networks on a patchwork of repaired products. Vendors need to address these problems now so that their products can be thoroughly tested before the DoD deployment deadline.

## **Appendix E. DoD IPv6 2003-2005 Test and Evaluation Summary**

To provide a consolidated assessment of current IPv6 T&E within the DoD, this appendix reanalyzes the 39 reports from the FY 2005 submission, using the new methodology in this report. The 39 IPv6 test documents from this reporting period were analyzed at the criterion level using a methodology similar to that discussed in Section 2.2. Each report was analyzed with respect to its applicability to each of the Joint Staff IPv6 operational criteria. Then each report was assessed using quantitative and qualitative factors to determine how well the report demonstrated the applicable criteria. Color status ratings were derived by combining the contributions of the applicable reports for each criterion.

The 2003-2005 Test and Evaluation Matrix (Table E-1) presents all the test reports for this reporting period by Joint Staff IPv6 operational criteria and test method. Ten more reports were applicable to the demonstration of Criteria 1, 2, 3, 4, 7, and 8. However, certain levels of decomposition have not been demonstrated for these criteria and contributed to the red ratings. For example, there was no testing of HAIPE for Criterion 1 and no testing of application transition techniques for Criterion 2. Criteria 5, 6, 9, and 10 had a relatively sparse number of applicable reports.

**Table E-1 2003-2005 Test and Evaluation Matrix**

Joint Staff IPv6 Operational Criteria		Test Methods						Cumulative Status	
		Engineering Analyses	Modeling & Simulation	Experiments	Demonstrations	Pilots	Exercises		Field Tests
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	5	1	7	5		5		⊗
2	Demonstrate end-to-end interoperability in a mixed IPv4 and IPv6 environment	2		11	3		9		⊕
3	Demonstrate equivalent to, or better performance than, IPv4 based networks	2	1	4	1		3		⊕
4	Demonstrate voice, data, and video integration	4		2	1		6		⊕
5	Demonstrate effective operation in low-bandwidth environment	2	1						⊗
6	Demonstrate scalability of IPv6 networks	2			1				⊗
7	Demonstrate support for mobile terminals (voice, data and video)	1	1	1	1		6		⊕
8	Demonstrate transition techniques	3	2	5	2		7		⊗
9	Demonstrate ability to provide network management of networks	1		3	3				⊗
10	Demonstrate tactical deployability and ad hoc networking	1	1	1					⊗
<b>Key:</b>  Criterion has been successfully demonstrated.  Significant progress has been made on this criterion.  Limited progress has been made on this criterion.									