

**USG IPv6 Task Force**

**IPv6 Deployment Test Specification**

**Version 0.9**  
**March 8, 2011**

**Stephen Nightingale, NIST**

NIST

<http://www.antd.nist.gov>

# Modification Record

<b>Version</b>	<b>Date</b>	<b>Note</b>
0.1	January 27, 2011	USG IPv6 Deployment Test Specification Draft
0.2	February 1, 2011	DNS, WWW and Mail tests identified and test structure laid out. DNS tests written.
0.3	February 4, 2011	Introduction expanded. WWW tests written.
0.4	February 07, 2011	DNS test overview written. Mail server tests written.
0.5	February 08, 2011	Tests executed on Linux. Procedures updated to include command line format.
0.6	February 10, 2011	Updated to include DOS/Windows commands.
0.7	February 14, 2011	Include DOE edits.
0.8	February 22, 2011	Added hidden fields to tests for processing purposes.
0.9	March 4, 2011	Topology extended to include CPE & PE POP links.

# Acknowledgements

NIST would like to acknowledge the efforts of the following individuals in the development of this test specification.

## **Principle Author:**

Stephen Nightingale      National Institute of Standards and Technology (NIST).

## **Commentators:**

Stu L. Mitchell, Department of the Interior; William (Jay) Huie, Bruce Beckwith, Peter Tseronis, Department of Energy.

## **NIST Disclaimer**

Certain commercial products are identified in this document. This identification does not constitute a recommendation or endorsement from NIST, or that the products are the best available for the task.

# TABLE OF CONTENTS

Modification Record .....	1
Acknowledgements .....	2
TABLE OF CONTENTS .....	3
1. Introduction .....	4
1.1 Scope .....	5
1.2 Abbreviations Used in This Document .....	5
1.3 Topology Requirements .....	5
1.4 Test Equipment Requirements .....	6
2. The Tests .....	8
2.1 DNS record tests .....	8
2.1.0 Test Name: DNSlookup0 .....	9
2.1.1 Test Name: DNSlookup1 .....	10
2.1.2 Test Name: DNSlookup2 .....	11
2.1.3 Test Name: DNSlookup3 .....	12
2.2 Web server tests .....	13
2.2.1 Test Name: WWWlookup1 .....	13
2.2.2 Test Name: WWWlookup2 .....	14
2.2.3 Test Name: WWWlookup3 .....	15
2.2.4 Test Name: WWWlookup4 .....	16
2.3 Mail server tests .....	17
2.3.1 Test Name: MXlookup1 .....	17
2.3.3 Test Name: MXlookup3 .....	19
2.3.4 Test Name: MXlookup4 .....	20
3. References .....	21

# 1. Introduction

The first round of requirements for IPv6 deployment in the Federal Government, as stipulated in the September 28 2010 OMB Memo [OMB2010] calls for “Upgrade public/external facing servers and services to operationally use native IPv6 by FY 2012”. This includes infrastructure such as:

- Web servers,
- Mail servers,
- Domain name servers.

Evaluating the successful enablement of these systems requires a progressive set of tests, with diagnostic capabilities. The kernel of this set can be derived from the operations of the NIST IPv6 Deployment Monitor [deploymentmon]. This deployment monitor is a means to periodically monitor a selected list of externally facing infrastructure components to assess their Internet connectivity over IPv4 and IPv6. This is performed over a list of identified resources, and the results are posted to a NIST website. Such automated monitoring reduces the reporting burden and allows server administrators and federal agencies to focus on the realities of mission production activities.

The set of tasks performed by the deployment monitor represents specific measurable tests and overlaps with the same actions that system administrators would need in discrete deployment testing. These include:

- DNS queries,
- web and mail server reachability,
- ‘Ping’ tests to determine DNS, web and mail server liveness,
- Page retrieval tests to determine web server operation.

These actions can be augmented with “real effects” testing, such as:

- Browser page retrieval, to determine full transfer and rendering, including local browser IPv6 configuration.
- Send and receive mail messages to determine end-to-end message exchange including mail server IPv6 configuration.

The architecture for testing these IPv6 functions requires a Tester and a Node Under Test, linked by an IPv6 connection. The tester side is a command shell, or an application that implements the DNS lookup, ping, web get and mail commands over IPv6, whether tunneled or native. While it is a 2014 goal to generally IPv6-enable Agency internal client side systems, it is necessary for the purpose of addressing the 2012 goals that some internal clients be IPv6-enabled to accomplish the testing. Section 1.3 introduces the topologies needed to achieve this. Section 1.4 lists the detailed test side equipment and service requirements. The tests are enumerated in Section 2.

## **1.1 Scope**

This document identifies and describes tests to determine the IPv6 connectivity of DNS, Web server and Mail server IPv6 connected nodes. It identifies the use of widely available and/or open source tools. It does not describe how to deploy IPv6 for any node.

## **1.2 Abbreviations Used in This Document**

USGv6: The US Government Profile for IPv6 published by NIST.

OMB: Office of Management and Budget.

DNS: Domain Name Server (See RFCs 1034 and 1035).

HTTP: Hypertext Transfer Protocol (See RFC 1945).

SOA: Start of Authority Record – a DNS record.

UDP: User Datagram Protocol (See RFC 768).

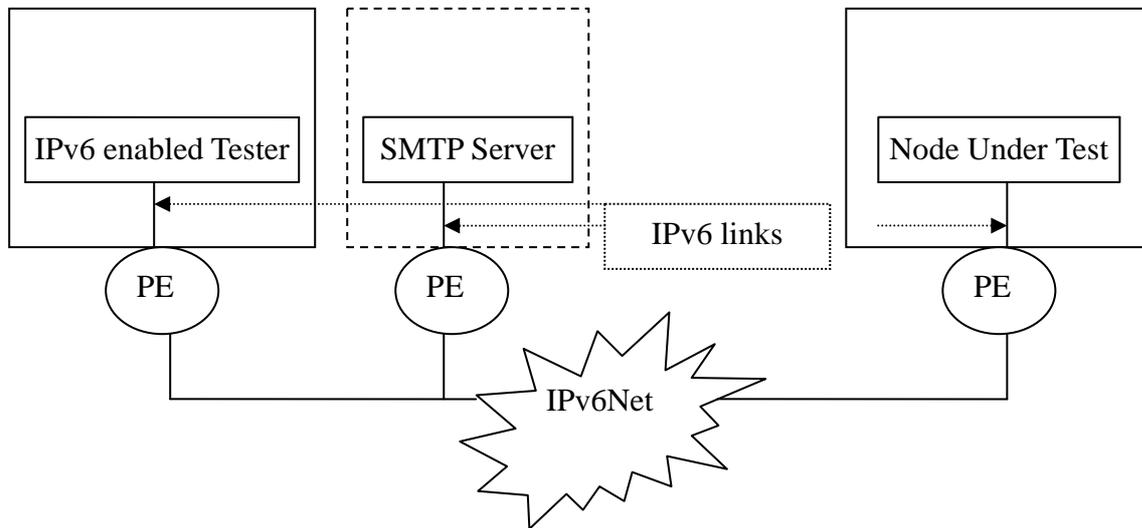
## **1.3 Topology Requirements**

Possible configurations of test architecture for performing IPv6 deployment testing include:

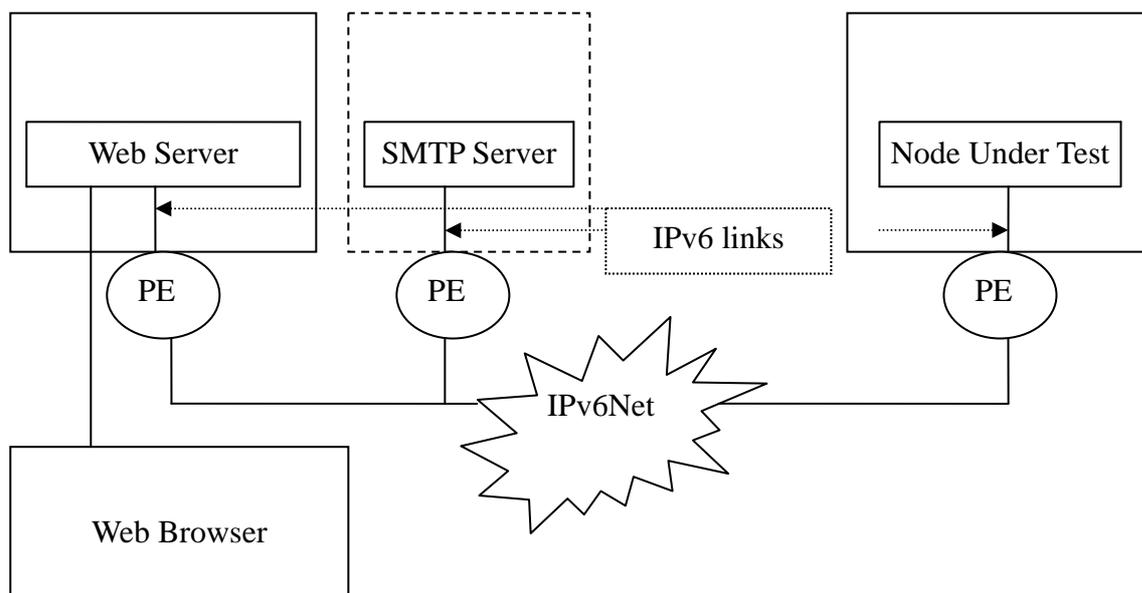
- (a) a Linux or Windows (DOS) command shell,
- (b) a Web application.

Both options are executed using global IPv6 addresses, over a native IPv6 link. Option (a) is depicted in Figure 1, showing the Tester command shell linked through an IPv6 network to the Node Under Test, which may be a DNS server, web server or mail server. In addition to the two endpoints, critical points for Interoperability are the interfaces at the Tester and NUT between “Customer Premises Equipment” (CPE) and “Provider Edge Point of Presence” (PE POP), and these are additional focuses for potential Interoperability failure. Option (b) opens up the possibility of communication between and IPv4 or IPv6-enabled browser, through the

Web application, to the IPv6 service under test. The shell commands may be implemented in a script (Perl, Python, popular scripting language), hosted on a web server. If the server is dual-stack capable, it can be accessed by any browser over IPv4 or IPv6 links, to execute the tests and furnish the results.



**Figure 1: Deployment Testing Configuration**



**Figure 2: Browser-Server driven Deployment Testing Configuration**

## 1.4 Test Equipment Requirements

These are divided into Linux and DOS shell commands:

<b>Service</b>	<b>Purpose</b>	<b>Command</b>
<b>All Nodes</b>	'Ping' an internet node for liveness.	<b>Linux:</b> ping6 -c 4 <a href="http://www.ipv6ready.org">www.ipv6ready.org</a>
		<b>Windows:</b> ping -6 www.ipv6ready.org
<b>All Nodes</b>	Trace the route of a ping packet.	<b>Linux:</b> traceroute <node>
		<b>Windows:</b> tracert <node>
<b>DNS</b>	Query DNS server to ensure AAAA, MX, NS or other records are available.	<b>Linux:</b> dig -6 @ns2.gogo6.com www.kame.net AAAA
		<b>Windows:</b> nslookup -type=AAAA www.kame.net ns2.gogo6.com
<b>Web server</b>	Retrieve a page from a web server.	<b>Linux:</b> wget -6 <a href="http://www.ipv6ready.org">www.ipv6ready.org</a>
		<b>Windows:</b> (not natively installed)
<b>Mail server</b>	Send an email message from the command line and check auto-response.	<b>Linux:</b> sendmail -6 user@address
		<b>Windows:</b> Syntax <tb>

## 2. The Tests

The tests enumerated here include DNS tests in 2.1, Web server tests in 2.2 and Mail server tests in 2.3. These tests are described as discrete procedures without reference to their automatability, or implementation, other than to identify common command line solutions.

### 2.1 DNS record tests

The Domain Name System [RFC1034, RFC1035] is that part of the Internet that serves up addresses when given node names or URLs, and may also perform the reverse service of serving a node name or URL when given an address. An in depth user view and tutorial are given in [cricket]. The set of records includes:

A: for IPv4 records.

AAAA: for IPv6 records.

MX: for mail exchange records.

NS: for name server records.

CNAME: for aliases.

PTR: for reverse records.

SOA: for Start of Authority.

This test specification concentrates on the AAAA, MX, NS and CNAME records. The test progression for testing DNS IPv6 support is to: identify that the target domain name server is live over IPv6, then query it to determine if it serves AAAA records for IPv6 enabled nodes. An additional test is to determine if the server will serve ANY records for a given subdomain, including AAAA, NS and MX, with possible CNAMEs also.

## 2.1.0 Test Name: DNSlookup0

**Objective:** Determine that the domain name server serves AAAA records for the target nodes over an IPv4 link.

**Topology:**

Topology 1. Test system with Linux or DOS shell linked through IPv4 to a DNS server.

**Procedure:**

**Linux:**

- `dig @<DNS server> <DNS node name> AAAA`
- Observe the DNS response at the command line.

**DOS/Windows:**

- `nslookup -type=AAAA <DNS node name> <DNS server>`
- Observe the DNS response at the command line.

**Judgement:**

PASS if the answer includes the domain name, AAAA record and IPv4 address.

FAIL if the answer includes the SOA record only.

**Additional Info:**

Observe UDP request and responses wrapped in IPv4 packets, at Wireshark.

## 2.1.1 Test Name: DNSlookup1

**Objective:** Determine the liveness of the target domain name server using Ping.

**Topology:**

Topology 1. Test system with Linux or DOS shell linked through IPv6 to a DNS server. Optional network traffic ‘sniffer’ such as Wireshark or tcpdump connected to the IPv6 link.

**Procedure:**

**Linux:**

- ping6 -c 4 <DNS nodename>
- Read response at the command line.

**DOS/Windows:**

- ping -6 <DNS nodename>
- Read response at the command line.

**Judgement:**

PASS if one or more ping responses are returned with IPv6 address of the queried server.

INCONCLUSIVE if timeout with no response.

**Additional Info:**

Observe traffic via your sniffer passing an Echo Request, and one or more Echo Responses with IPv6 addresses of the two parties.

## 2.1.2 Test Name: DNSlookup2

**Objective:** Determine that the target domain name server serves AAAA records.

**Topology:**

Topology 1. Test system with Linux or DOS shell linked through IPv6 to a DNS server.  
Optional Wireshark connected to the IPv6 link.

**Procedure:**

**Linux:**

- `dig -6 @<DNS server> <DNS node name> AAAA`
- Observe the DNS response at the command line.

**DOS/Windows:**

- `nslookup -type=AAAA <DNS node name> <DNS server>`
- Observe the DNS response at the command line.

**Judgement:**

PASS if the answer includes the domain name, AAAA and IPv6 address.

FAIL if the answer includes the SOA record only.

**Additional Info:**

Observe UDP request and responses wrapped in IPv6 packets, at Wireshark.

## 2.1.3 Test Name: DNSlookup3

**Objective:** Determine that the target domain name server serves ANY records.

**Topology:**

Topology 1. Test system with Linux or DOS shell linked through IPv6 to a DNS server.  
Optional Wireshark connected to the IPv6 link.

**Procedure:**

**Linux:**

- `dig -6 @<DNS server> <DNS node name> ANY`
- Observe the DNS response at the command line.

**DOS/Windows:**

- `nslookup -type=ANY <DNS node name> <DNS server>`
- Observe the DNS response at the command line.

**Judgement:**

PASS if the answer includes the domain name, AAAA and IPv6 address and additional records.

INCONCLUSIVE if the answer includes the SOA record only.

**Additional Info:**

Observe UDP request and responses wrapped in IPv6 packets, at Wireshark.

## 2.2 Web server tests

The test progression for testing web server IPv6 support involves;

- Getting the AAAA record for the URL from the named DNS server.
- Pinging the web server to determine its liveness.
- Getting the specified web page at the command line, and
- Displaying the web page in an IPv6 enabled browser.

This sequence of tests is enumerated below.

### 2.2.1 Test Name: WWWlookup1

**Objective:** Get a AAAA record for a given URL from the authoritative DNS server for the Web site.

**Topology:**

Topology 1. Test system with Linux or DOS shell linked through IPv6 to a DNS server. Optional Wireshark connected to the IPv6 link.

**Procedure:**

**Linux:**

- `dig -6 @<DNS server> <DNS node name> AAAA`
- Observe the DNS response at the command line.

**DOS/Windows:**

- `nslookup -type=AAAA <DNS node name> <DNS server>`
- Observe the DNS response at the command line.

**Judgement:**

PASS if the answer includes the URL, AAAA and IPv6 address, or a CNAME followed by a different URL plus AAAA and IPv6 address.

FAIL if the answer includes the SOA record only.

**Additional Info:**

Observe UDP request and responses wrapped in IPv6 packets, at Wireshark.

## 2.2.2 Test Name: WWWlookup2

**Objective:** Ping6 the Web server.

**Topology:** Topology 2. Test system with Linux or DOS shell linked through IPv6 to a Web server.

**Procedure:**

**Linux:**

- ping6 -c 4 <URL>
- Read response at the command line.

**DOS/Windows:**

- ping -6 <URL>
- Read response at the command line.

**Judgement:**

PASS if one or more ping responses are returned with IPv6 address of the queried Web server.

INCONCLUSIVE if timeout with no response.

### 2.2.3 Test Name: WWWlookup3

**Objective:** Wget the home page from the command line.

**Topology:**

Topology 2. Test system with Linux or DOS shell linked through IPv6 to a Web server.

**Procedure:**

**Linux:**

- wget -6 <URL>
- Read response at the command line.

**DOS/Windows:**

- <Syntax of wget to be determined>
- Read response at the command line.

**Judgement:**

PASS if a file with the specified html page, or index.html, is saved locally.

INCONCLUSIVE if no response ????

## 2.2.4 Test Name: WWWlookup4

**Objective:** Display the Home Page in an IPv6 enabled browser

**Topology:** Topology 4. IPv6 enabled Web browser linked through IPv6 to a Web server.

**Procedure:**

**Linux and DOS/Windows:**

- Type in a specified URL of a web page at an IPv6 enabled Web server to the Browser.
- View received page.

**Judgement:**

PASS if the page is received and rendered as expected (i.e. identical with the same page received over an IPv4 link).

**Hint:** it is clearer if you choose a Web page that gives an indication of the source address of the initiating browser, i.e. whether IPv6 or IPv4.

## 2.3 Mail server tests

The test progression for testing mail server IPv6 support involves:

- Getting the AAAA record for the mail server from the named DNS server.
- Pinging the mail server to determine its liveness.
- Sending an message to a designated user at the mail server and receiving a configured auto-response.

It is not a part of the mail server test to exercise any emote mail client and its link.

### 2.3.1 Test Name: MXlookup1

**Objective:** Get the MX record for a specified mail server from the specified DNS server.

**Topology:** Topology 1. Tester linked through IPv6 to a DNS server.

**Procedure:**

**Linux:**

- `dig -6 @<DNS server> <mail server name> MX`
- Observe the DNS response at the command line.

**DOS/Windows:**

- `nslookup -type=MX <mail server name> <DNS server>`
- Observe the DNS response at the command line.

**Judgement:**

PASS if the answer includes the node name, MX record and IPv6 address, or a CNAME followed by a different node name with MX record, and IPv6 address.

FAIL if the answer includes the SOA record only.

### 2.3.2 **Test Name:** MXlookup2

**Objective:** Get the AAAA record for the Mail server from the DNS server

**Topology:** Topology 1. Tester linked through IPv6 to a DNS server.

**Procedure:**

**Linux:**

- `dig -6 @<DNS server> <mail server name> AAAA`
- Observe the DNS response at the command line.

**DOS/Windows:**

- `nslookup -type=AAAA <mail server name> <DNS server>`

Observe the DNS response at the command line

**Judgement:**

PASS if the answer includes the URL, AAAA and IPv6 address, or a CNAME followed by a different URL plus AAAA and IPv6 address.

FAIL if the answer includes the SOA record only.

### **2.3.3 Test Name: MXlookup3**

**Objective:** Ping6 the mailserver.

**Topology:** Topology 3. IPv6 enabled tester linked through IPv6 to IPv6 enabled Mail server

**Procedure:**

**Linux:**

- ping6 -c 4 <mail server>
- Read response at the command line.

**DOS/Windows:**

- ping -6 <mail server>
- Read response at the command line.

**Judgement:**

PASS if one or more ping responses are returned with IPv6 address of the queried Mail server.

INCONCLUSIVE if timeout with no response.

## 2.3.4 Test Name: MXlookup4

**Objective:** Send6 to the mail server and view the received message

**Topology:**

Topology 3. Ipv6 enabled tester linked through IPv6 to Ipv6 enabled Mail server and

Topology 5. Locally available Mail client.

**Configuration:**

The Mail server is configured so that messages received for user@mailnode generate an auto-response.

**Procedure:**

**Linux:**

- sendmail -6 <user@mailserver>
- Read response at the mail client.

**DOS/Windows:**

- <sendmail command syntax TBD>
- Read response at the mail client.

**Judgement:**

PASS if the auto-reply is received.

INCONCLUSIVE if no response ????

### 3. References

This test specification refers to documents and websites as shown in the following lists:

<b>Number</b>	<b>Title</b>
[USGv6]	<i>USGv6 Profile</i> , Doug Montgomery, Stephen Nightingale, Sheila Frankel and Mark Carson, NIST SP 500-267, July 2008.
[USGv6Testing]	<i>USGv6 Testing Website</i> , <a href="http://www.antd.nist.gov/usgv6/testing.html">http://www.antd.nist.gov/usgv6/testing.html</a> .
[OMB2010]	<i>IPv6 Deployment in the Federal Government</i> , OMB Memorandum, Vivek Kundra, September 28, 1010.
[Deploymon]	<i>NIST IPv6 Deployment Monitor</i> , <a href="http://usgv6-deploymon.antd.nist.gov">http://usgv6-deploymon.antd.nist.gov</a> , Darrin Santay, NIST December 2010.
[nslookup]	The <i>nslookup</i> DOS shell command, Microsoft Corporation, <a href="http://support.microsoft.com/kb/200525">http://support.microsoft.com/kb/200525</a> .
[dig]	The Linux <i>Domain Information Groper</i> , <a href="http://linux.die.net/man/1/dig">http://linux.die.net/man/1/dig</a> .
[ping]	Linux or DOS, see <a href="http://en.wikipedia.org/wiki/Ping">http://en.wikipedia.org/wiki/Ping</a> .
[traceroute]	Linux (tracert in DOS), see <a href="http://en.wikipedia.org/wiki/Traceroute">http://en.wikipedia.org/wiki/Traceroute</a> .
[Wireshark]	Linux and Windows, see <a href="http://www.wireshark.org/">http://www.wireshark.org/</a> .
[wget6]	<i>Wget for IPv6</i> , see <a href="http://win6.jp/Wget/index.html">http://win6.jp/Wget/index.html</a> .
[cricket]	<i>DNS and BIND 5<sup>th</sup> Edition</i> , Cricket Liu and Paul Albitz, O'Reilly, May 2006.

