



**Demonstration Plan
to Support
Agency IPv6 Compliance**

**Issued by
Federal CIO Council Architecture and Infrastructure Committee**

Draft version 4.2

Demonstration Plan for Agency IPv6 Certifications	Document No.: TDC	Revision: Draft
	Effective Date:	Page 3 of 19

DOCUMENT HISTORY LOG

Status	Document Revision	Effective Date	Description
Draft	V4	09/19/07	Baseline Release
Draft	V4.1	9/23/07	Incremental Changes to Scripts
Draft	V4.2	10/16/07	Various Changes due to Review

Demonstration Plan to Support Agency IPv6 Compliance	Document No.: TBD	Revision: Draft
	Effective Date:	Page 4 of 19

SIGNATURE PAGE

Approved by:

Approved by:

Approved by:

Demonstration Plan to Support Agency IPv6 Compliance	Document No.: TBD	Revision: Draft
	Effective Date:	Page 5 of 19

TABLE OF CONTENTS

Table of Contents

Table of Contents

1 BACKGROUND6

 1.1 PURPOSE6

 1.2 REQUIREMENTS7

2 DEMONSTRATION CONFIGURATIONS8

 2.1 CORE NETWORK CONNECTIVITY8

 2.2 EXTERNAL NETWORK CONNECTIVITY9

 2.3 CONFIGURATION REQUIREMENTS12

3 IPV6 DEMONSTRATIONS13

 3.1 PREPARATION13

 3.2 DEMONSTRATION ONE – CERTIFICATION OF TRANSPORT ACROSS CORE NETWORK13

 3.2.1 *Demonstration script*14

 3.2.2 *Documentation of Test Results*16

 3.3 DEMONSTRATION TWO – CERTIFICATION OF TRANSPORT FROM CORE NETWORK TO EXTERNAL NETWORK17

 3.3.1 *Demonstration script*18

 3.3.2 *Documentation of Test results*19

Demonstration Plan to Support Agency IPv6 Compliance	Document No.: TBD	Revision: Draft
	Effective Date:	Page 6 of 19

1 Background

1.1 PURPOSE

The purpose of this document is to provide guidance and describe procedures for Agencies to demonstrate IPv6 compliance – to show that IPv6 traffic has been successfully transported (i.e., received, processed, forwarded) through all IPv6 devices in an Agency's operational core backbone network. The guidance in this document is to support the June 2008 requirement for agency core backbone networks to be using IPv6.

This artifact supports the June 2008 deployment testing requirement (as described in the IPv6 Transition Guidance, issued by the Federal CIO Council Architecture and Infrastructure Committee, February 2006) by confirming that an Agency can:

- Transmit IPv6 traffic from the Internet and external peers, through the network backbone (core), to the LAN;
- Transmit IPv6 traffic from the LAN, through the network backbone (core), out to the Internet and external peers;
- Transmit IPv6 traffic from the LAN, through the network backbone (core), to another LAN (or another node on the same LAN).

For these demonstrations, the term “LAN” represents IPv6-configured PCs/Laptops (with associated cabling and switching as needed), directly connected to IPv6 devices (routers, switches) in an Agency's operational core backbone network. The term “Internet and external peers” refers to an external network (a network owned and operated by an organization different from that Agency) chosen for the demonstrations, and which may be from a partner Agency, ISP, or other IPv6 organization.

Connectivity between the Agency's demonstration network and the external peer(s) may be established from either a dedicated circuit, such as a leased line, or via the public Internet.

This connectivity is described further in the following sections: *Demonstration Configurations*; and *Demonstration Two – Transport from Core Network to External Network*.

It must be emphasized that demonstrations of IPv6 compliance must be performed on the Agency's operational core network.

Demonstration Plan to Support Agency IPv6 Compliance	Document No.: TBD	Revision: Draft
	Effective Date:	Page 7 of 19

1.2 REQUIREMENTS

In order to demonstrate IPv6 compliance, the Agency should perform the following:

- Identify its operational core backbone network, based on the following definition provided by the IPv6 Working Group:

“For the purposes of the IPv6 transition, the core network (a.k.a. backbone network) is the set of network transport devices (routers, switches) that provide the highest level of traffic aggregation in the network, and thus at the highest level of hierarchy in the network.”

As part of identifying its operational core backbone network, Agencies must specify device types, number of devices, and topology (connectivity between devices) that constitute its operational core backbone network.

- Configure IPv6 on all IP devices (e.g., routers, switches) in the Agency's operational core backbone network.
 - Identify which external network(s) will be used for the demonstrations, and how the Agency's IPv6 operational core backbone network will connect to that external network(s). An external network is a network owned and operated by an organization different from that Agency, and may be from a partner Agency or ISP.
 - Develop a diagram of their operational core backbone network, clearly depicting IPv6 addressing, internal network connectivity and topology, and external network connectivity.
-

Demonstration Plan to Support Agency IPv6 Compliance	Document No.: TBD	Revision: Draft
	Effective Date:	Page 8 of 19

2 Demonstration Configurations

2.1 CORE NETWORK CONNECTIVITY

In order to perform the demonstrations, PCs/Laptops that can generate and terminate the IPv6 traffic flows associated with each demonstration are required. These PCs/Laptops are to be configured with IPv6 and have the utilities needed to generate, terminate, and capture IPv6 traffic flow information.

Figure 1 illustrates a configuration where the PCs/Laptops are directly connected to IPv6 devices in the Agency's operational IPv6 core backbone network.

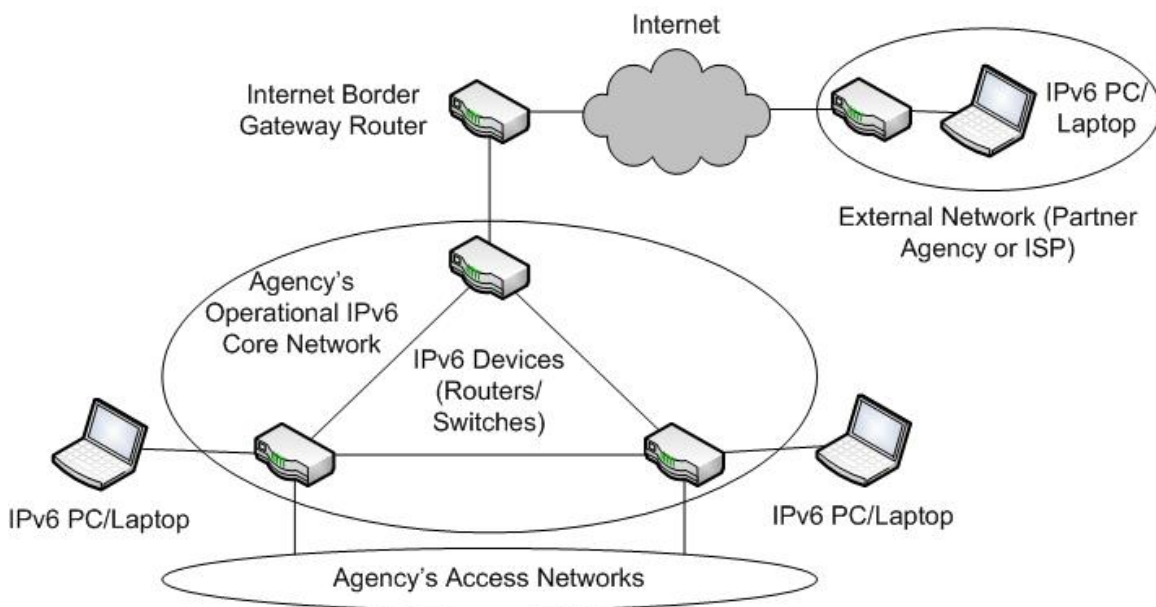


Figure 1. IPv6 PCs/Laptops directly connected to Agency's operational core backbone network

This figure depicts an Agency operational core backbone network consisting of three interconnected IPv6 devices. This IPv6 core backbone network is connected to the Agency's access networks, as well as to an external network.

This demonstration configuration is straightforward, in that the IPv6 PCs/Laptops are directly connected to the Agency's operational core backbone network, and do not connect through any intermediate networks.

Demonstration Plan to Support Agency IPv6 Compliance	Document No.: TBD	Revision: Draft
	Effective Date:	Page 9 of 19

Figure 2 illustrates an alternate demonstration configuration, in which the IPv6 PCs/Laptops are connected to the Agency's operational IPv6 core backbone network via the Agency's operational access networks.

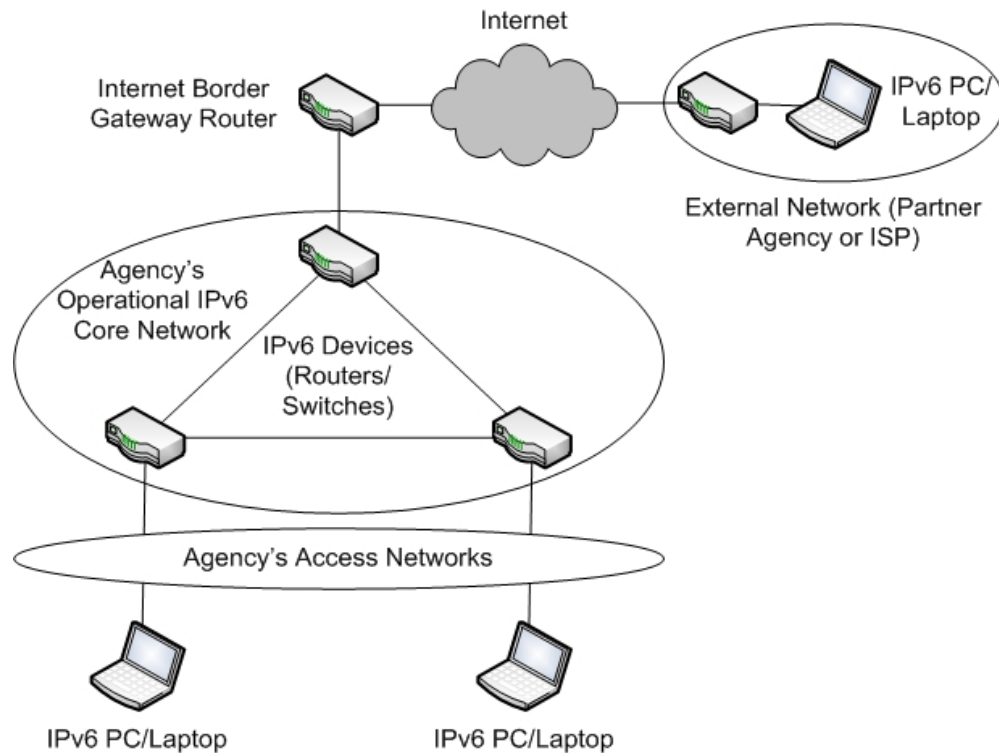


Figure 2. IPv6 PCs/Laptops connected via Agency's access networks

IPv6 connectivity must be established from the operational core backbone network, through the operational access networks, to the IPv6 PCs/Laptops. This is achieved via IPv6 tunnels or by deploying IPv6 dual-stack within the operational access networks.

While the **Figure 2** configuration is a bit more complex than that shown in **Figure 1**, it more accurately represents an operational IPv6 deployment.

An Agency's configuration decision will depend on technical, operational, and fiscal resources.

Demonstration Plan to Support Agency IPv6 Compliance	Document No.: TBD	Revision: Draft
	Effective Date:	Page 10 of 19

2.2 EXTERNAL NETWORK CONNECTIVITY

For each demonstration configuration, the demonstration network is shown connected to an external network. This connection may be through that Agency's access to the Internet, or, if security concerns preclude use of the public Internet, a dedicated connection between the demonstration network and the external network may be considered.

If an Agency's Internet Service Provider (ISP) is IPv6-enabled and can offer IPv6 services to the Agency as an external network, the ISP can serve as an external network

Figure 3 shows an Agency's operational IPv6 core backbone network connected to the Internet via an IPv6-enabled Internet border gateway router.

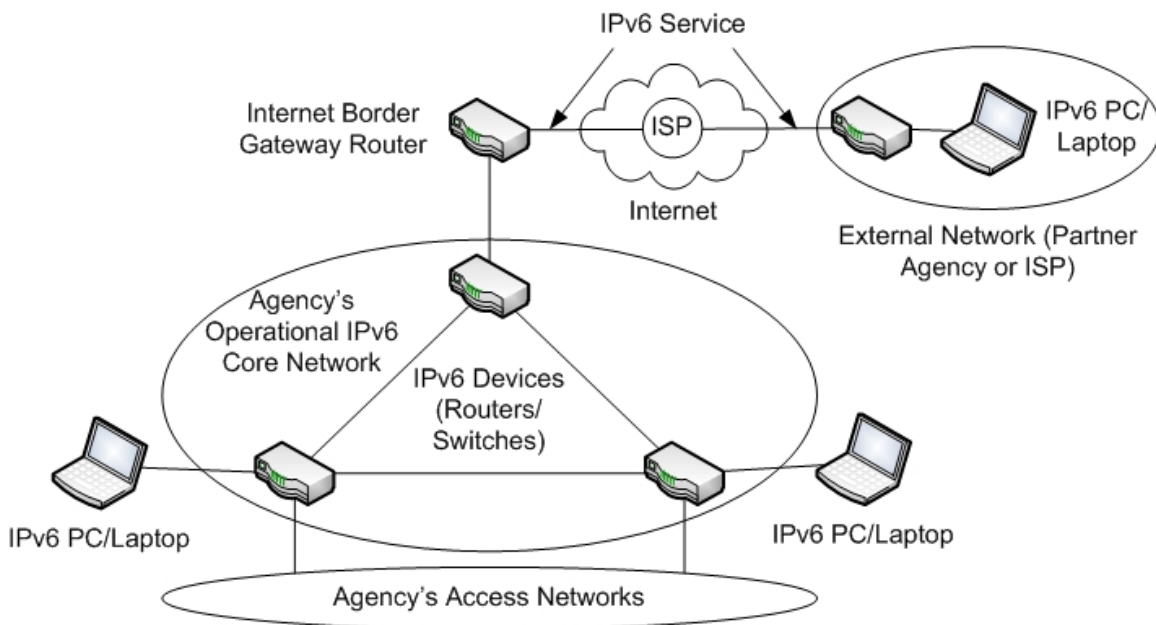


Figure 3. IPv6 Connectivity between Agency and External ISP Network

The Agency's ISP provides IPv6 connectivity between the Agency and external network and thus, IPv6 is enabled in the external network to the IPv6 PC/Laptop used for the demonstration.

If, however, an Agency's ISP is not IPv6 enabled or does not offer IPv6 Internet services, a static IPv6 over IPv4 tunnel can be used between the Agency Internet border gateway router and the corresponding Internet border gateway router within the external network.

An example of an IPv6 over IPv4 tunnel is shown in **Figure 4**.

Demonstration Plan to Support Agency IPv6 Compliance	Document No.: TBD	Revision: Draft
	Effective Date:	Page 11 of 19

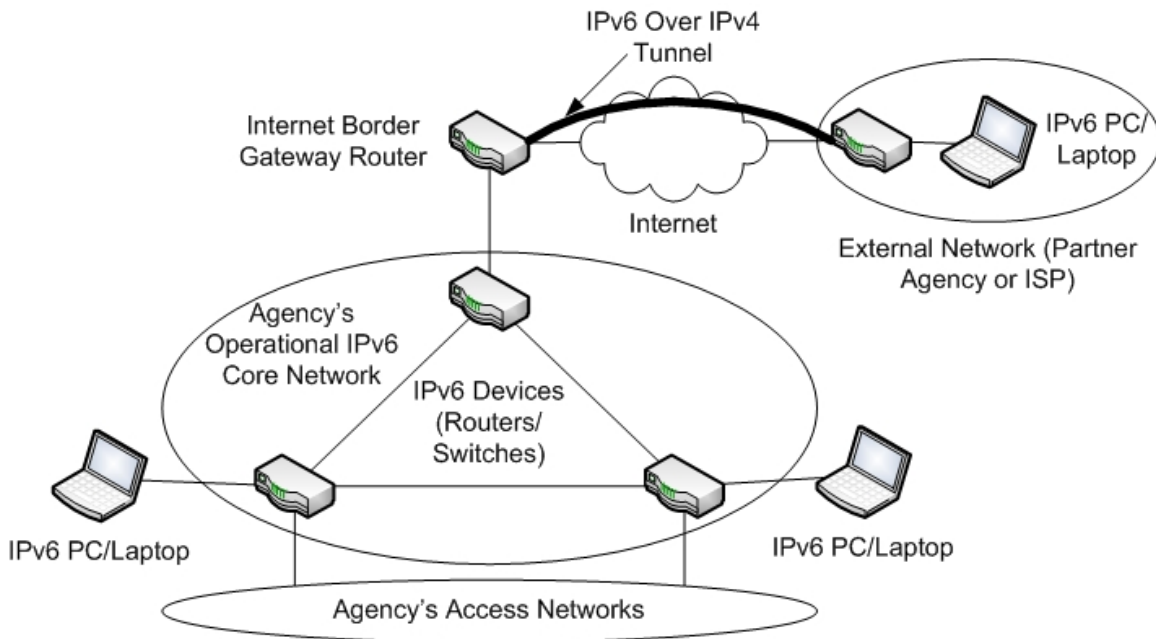


Figure 4. IPv6 Connectivity between Agency and External Network via an IPv6 over IPv4 Tunnel

Figure 5 depicts a dedicated connection, consisting of a circuit from an ISP, e.g., a T-1, connecting the Agency's IPv6 core backbone network to an external partner's IPv6 device.

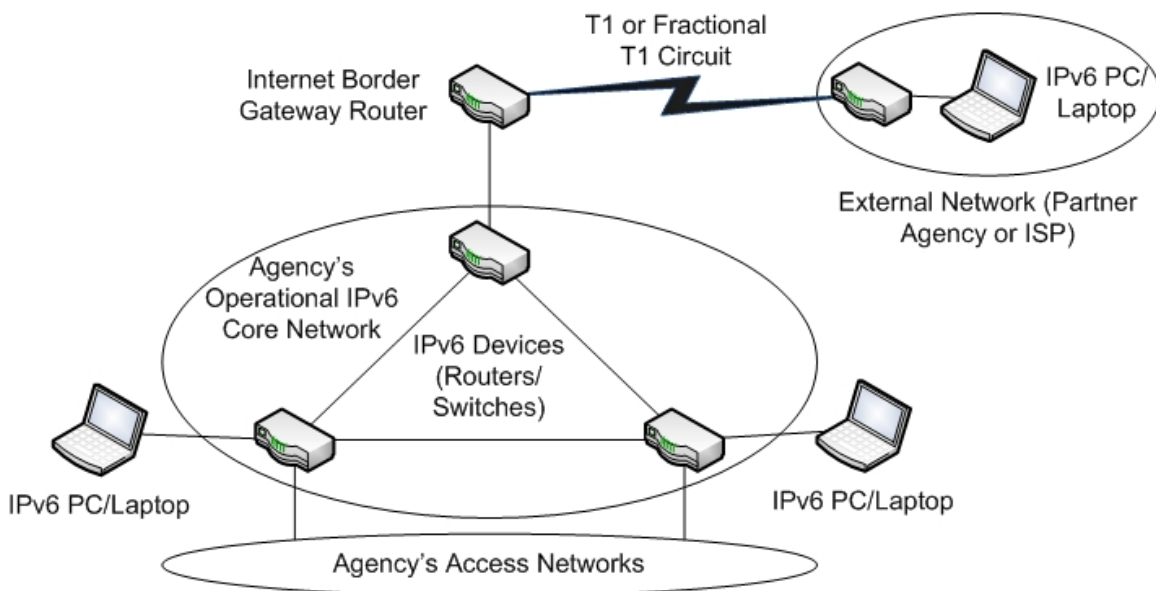


Figure 5. IPv6 connectivity between the agency and external network via a dedicated circuit

Demonstration Plan to Support Agency IPv6 Compliance	Document No.: TBD	Revision: Draft
	Effective Date:	Page 12 of 19

2.3 CONFIGURATION REQUIREMENTS

The following components are required for the demonstration configurations:

- Two demonstration PCs/Laptops (Source and Destination), running an IPv6-capable operating system (e.g., Vista, Solaris, Linux, or HP)
- Ping (or a multi-hop ping) for IPv6 must be available on the PCs/Laptops
- Traceroute for IPv6 must be available on the PCs/Laptops
- Associated cabling/hardware
- Ability to capture screen shots from demonstration PCs/Laptops
- Diagram of IPv6 operational core backbone network, illustrating IPv6 addressing, network connectivity and topology, and external network connectivity

For IPv6 connectivity between Agency and external networks (depending on configuration choice):

- IPv6 router on external network
- IPv6 PC/Laptop on external network

And one of the following:

- IPv6 service from an ISP, or
 - IPv6 over IPv4 Tunnel established between Internet border gateway router in the Agency's demonstration network and the router in the external network, or
 - Dedicated circuit between Agency's operational IPv6 core backbone network and the external network
-

Demonstration Plan to Support Agency IPv6 Compliance	Document No.: TBD	Revision: Draft
	Effective Date:	Page 13 of 19

3 IPv6 Demonstrations

3.1 PREPARATION

To prepare for the IPv6 demonstrations, the Agency should:

- Provide source and destination PCs/Laptops, configured and enabled with IPv6, and validate that the ping, traceroute, and screen capture utilities are available
- Connect source and demonstration PCs/Laptops to IPv6 devices on the Agency's operational core backbone network or (depending on configuration choice) Agency's access networks, and at the external network
- Enable IPv6 on all IP devices on the Agency's operational core backbone network, the Internet border gateway router, the Agency's access networks (if required in configuration), and at the external network
- Enable IPv6 connectivity between Agency and external networks, using either IPv6 Internet service, IPv6 over IPv4 tunneling, or a dedicated circuit

3.2 DEMONSTRATION ONE – CERTIFICATION OF TRANSPORT ACROSS CORE NETWORK

The following demonstrations support the requirement to:

- Transmit IPv6 traffic from the LAN, through the network backbone (core), to another LAN (or another node on the same LAN).

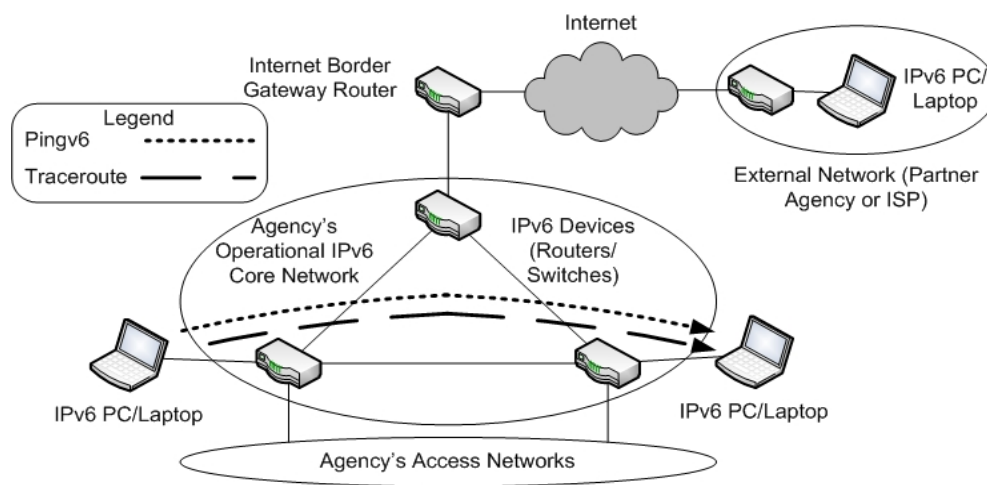


Figure 6. IPv6 Demonstration across Agency's Operational Core Network Using *Pingv6* and *Traceroute*

Demonstration Plan to Support Agency IPv6 Compliance	Document No.: TBD	Revision: Draft
	Effective Date:	Page 14 of 19

An equivalent demonstration can be provided with IPv6 PCs/Laptops connected to the Agency's access networks, using the configuration shown in **Figure 2**.

Since Demonstration One is only across the Agency's operational IPv6 core network, external network connectivity is not needed. The external network is depicted for completeness only.

For all demonstrations, source and destination PCs/Laptops must not be connected to the same IPv6 device, unless the Agency's operational core backbone network consists of only one IP (and thus only one IPv6) device.

Since the demonstrations are to illustrate IPv6 transport across the Agency's operational IPv6 core backbone network, connecting both PCs/Laptops to the same IPv6 device cannot represent transport across the core. This can only be achieved when the PCs/Laptops are connected to different IPv6 devices within the core backbone network.

The Agency's operational IPv6 core backbone network and IPv6 PCs/Laptops must be ready for the demonstration by verifying the items in the Section 3.1 – Preparation.

3.2.1 DEMONSTRATION SCRIPT

The demonstration scripts within this document provide examples using Microsoft Vista. *This is done for illustrative purposes only, and does not indicate any preference for Microsoft Vista.* Other operating systems, such as Solaris, Linux, or HP, provide equivalent or similar functionality as that described below.

Part 1 – Verify IPv6 Configuration Information

1. Verify IPv6 configuration (interfaces, addressing, routing) on each of the demonstration PCs/Laptops. For example, using Vista:

ipconfig /all

netsh interface ipv6 show addresses

2. Use screen capture utility to record PC/Laptop IPv6 configuration information. For example, using Vista:

accessories/snipping tool

Part 2 – Demonstrate IPv6 Connectivity

3. Run the utility *ping* in IPv6 mode between the source and destination demonstration PCs/Laptops. For example, using Vista:

ping -6 <destination PC/Laptop IPv6 address>

Stop *ping* after a minimum of ten *pings*.

Success Criterion: A minimum of ten consecutive successful IPv6 *pings* between source and destination PCs/Laptops.

Demonstration Plan to Support Agency IPv6 Compliance	Document No.: TBD	Revision: Draft
	Effective Date:	Page 15 of 19

4. Use screen capture utility to record *ping* results. For example, using Vista:
accessories/snipping tool

Part 3 – Demonstrate IPv6 Transport Across Core

5. Run the utility *tracert* in IPv6 mode between the source and destination demonstration PCs/Laptops. For example, using Vista:

tracert -d -R -6 <destination PC/Laptop IPv6 address>

Notes: -d is used to not resolve destination address to hostname; -R is used to trace round-trip path. An option to *tracert* is to use the utility *pathping*:

pathping -d -6 <destination PC/Laptop IPv6 address>

6. Use screen capture utility to record *tracert* and/or *pathping* results. For example, using Vista:

accessories/snipping tool

Success Criterion: Successful *tracert* and/or *pathping* between source and destination PCs/Laptops.

Part 4 – Demonstrate Completeness

In order to show that IPv6 traffic has successfully transported via all IPv6 devices in the Agency's operational core backbone network, demonstration PCs/Laptops may need to be moved and connected to other IPv6 devices in that Agency's operational core network.

For example, in **Figure 6** only two out of the three IPv6 devices in the Agency's operational core backbone network are utilized given the placement of source and destination PCs/Laptops and subsequent IPv6 traffic flows.

In order to demonstrate the third IPv6 device, one of the PCs/Laptops is moved and connected to the third IPv6 device and Parts 2 and 3 of the Demonstration Script are run on the new configuration:

7. As necessary, in order to demonstrate IPv6 transport across all IPv6 devices in the Agency's operational core backbone network, move and reconnect demonstration PCs/Laptops. Where these PCs/Laptops are moved depends on the size and topology of the Agency's operational core network.
8. Run the steps in Part 2 of this Demonstration Script.
9. Run the steps in Part 3 of this Demonstration Script.

Success Criteria: The success criteria from Parts 2 and 3 of this test script also apply to Part 4.

Demonstration Plan to Support Agency IPv6 Compliance	Document No.: TBD	Revision: Draft
	Effective Date:	Page 16 of 19

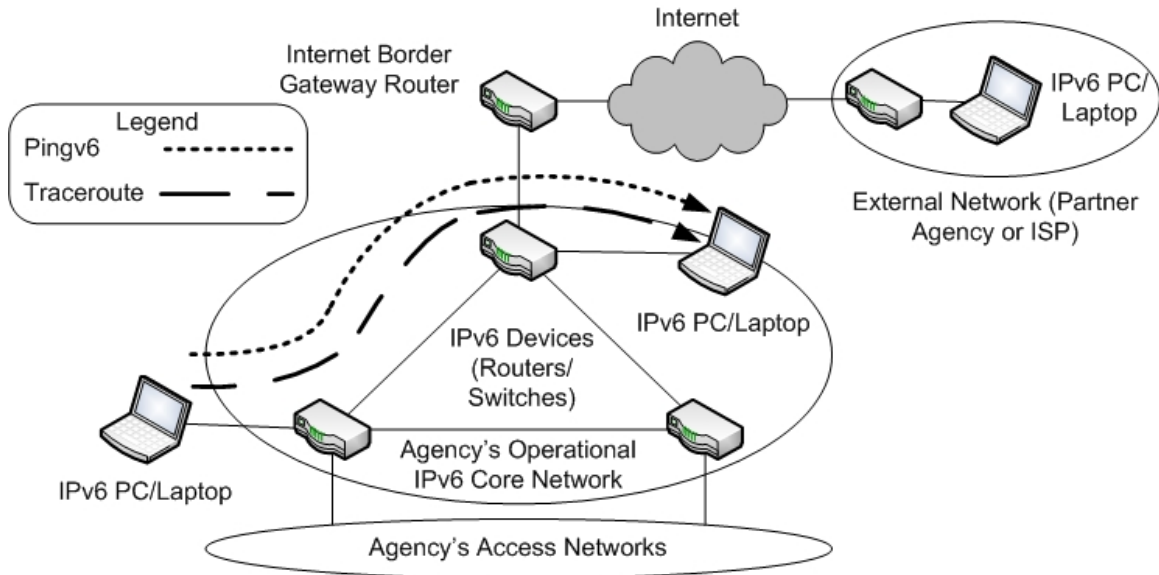


Figure 7. Demonstrating completeness – running *pingv6* and *traceroute* across IPv6 devices

3.2.2 DOCUMENTATION OF TEST RESULTS

Upon successful completion of Demonstration One, the Agency should generate electronic copies of the following documentation:

- Diagram of the IPv6 operational core network, clearly showing IPv6 addressing, network connectivity and topology.
- IPv6 configuration information from Part 1.
- Results of IPv6 connectivity demonstrations for all IPv6 devices in the Agency's operational core network (Parts 2 and 4).
- Results of IPv6 transport demonstrations for all IPv6 devices in the Agency's operational core network (Parts 3 and 4).

Demonstration Plan to Support Agency IPv6 Compliance	Document No.: TBD	Revision: Draft
	Effective Date:	Page 17 of 19

3.3 DEMONSTRATION TWO – CERTIFICATION OF TRANSPORT FROM CORE NETWORK TO EXTERNAL NETWORK

The following demonstration will satisfy M-05-22 to:

- Transmit IPv6 traffic from the Internet and external peers, through the network backbone (core), to the LAN.
- Transmit IPv6 traffic from the LAN, through the network backbone (core), out to the Internet and external peers.

An example configuration is shown in **Figure 8**.

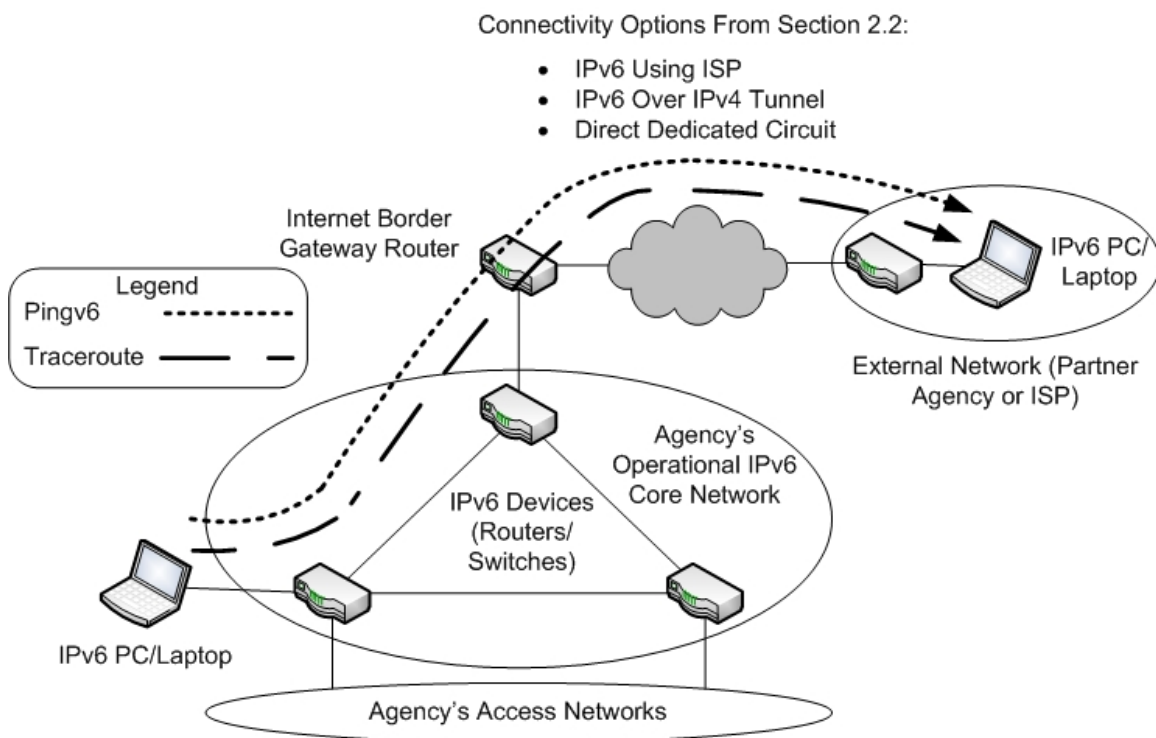


Figure 8. IPv6 demonstration between Agency and external networks using *pingv6* and *traceroute*

Note that **Figure 8** shows the three IPv6 connectivity options described in Section 2.2: IPv6 Internet service via an ISP; IPv6 over IPv4 tunneling; or a dedicated circuit.

As with Demonstration One, source and destination PCs/Laptops must not be connected to the same IPv6 device, unless the Agency's operational core backbone network consists of only one IP (and thus only one IPv6) device.

Demonstration Plan to Support Agency IPv6 Compliance	Document No.: TBD	Revision: Draft
	Effective Date:	Page 18 of 19

The Agency's operational IPv6 core backbone network and IPv6 PCs/Laptops must be ready for the demonstration by verifying the items in the Section 3.1 – Preparation.

3.3.1 DEMONSTRATION SCRIPT

All of the demonstration scripts in this document provide examples using Microsoft Vista. *This is done for illustrative purposes only, and does not indicate any preference for Microsoft Vista.* Other operating systems, such as Solaris, Linux, or HP, provide equivalent or similar functionality as that described below.

Part 1 – Verify IPv6 Configuration Information

1. Verify IPv6 configuration (interfaces, addressing, routing) on each of the demonstration PCs/Laptops. For example, using Vista:

ipconfig /all

netsh interface ipv6 show addresses

2. Use screen capture utility to record PC/Laptop IPv6 configuration information. For example, using Vista:

accessories/snipping tool

Part 2 – Demonstrate IPv6 Connectivity Between Agency and External Networks

3. Run the utility *ping* in IPv6 mode between the source and destination demonstration PCs/Laptops. For example, using Vista:

ping -6 <destination PC/Laptop IPv6 address>

Stop *ping* after a minimum of ten *pings*.

Success Criterion: A minimum of ten consecutive successful IPv6 *pings* between source and destination PCs/Laptops.

4. Use screen capture utility to record *ping* results. For example, using Vista:

accessories/snipping tool

Part 3 – Demonstrate IPv6 Transport between Agency and External Networks

5. Run the utility *tracert* in IPv6 mode between the source and destination demonstration PCs/Laptops. For example, using Vista:

tracert -d -R -6 <destination PC/Laptop IPv6 address>

Notes: -d is used to not resolve destination address to hostname; -R is used to trace round-trip path. An option to *tracert* is to use the utility *pathping*:

pathping -d -6 <destination PC/Laptop IPv6 address>

Demonstration Plan to Support Agency IPv6 Compliance	Document No.: TBD	Revision: Draft
	Effective Date:	Page 19 of 19

6. Use screen capture utility to record *tracert* and/or *pathping* results. For example, using Vista:

accessories/snipping tool

Success Criterion: Successful *tracert* and/or *pathping* between source and destination PCs/Laptops.

3.3.2 DOCUMENTATION OF TEST RESULTS

Upon successful completion of Demonstration Two, the Agency should generate electronic copies of the following documentation:

- Diagram of the IPv6 operational core network, clearly showing IPv6 addressing, network connectivity and topology, and connectivity to the external network.
- IPv6 configuration information from Part 1.
- Results of IPv6 connectivity demonstration between the Agency's operational core network and the external network (Part 2).
- Results of IPv6 transport demonstration between the Agency's operational core network and the external network (Part 3).

The documentation listed in sections 3.2.2 and 3.3.2 respectively (demonstrating compliance in support of the June 2008 requirement that agency core backbone networks use IPv6) should be made available to OMB upon request.
