United States

# Department of Veterans Affairs


## VA Approach and Test Plan for IPv6

Version 3.0
February 2008

Prepared by:
VA IPv6 Workgroup

# 1 OBJECTIVE

The Department of Veterans Affairs (VA) is committed to the successful deployment of Internet Protocol version 6 (IPv6) across the VA Information Technology (IT) infrastructure. Over the next 12 to 15 months, the primary effort will be to focus on the requirements and deadlines of the IPv6 mandate identified by Office of Management and Budget (OMB) Memorandum 05-22. The requirements for June 2008, as set forth by OMB, include the following:

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

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

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

# 2 SUMMARY

The VA intends to accomplish the IPv6 transition and meet the OMB requirements by March 2008, mitigating risk to the VA IT enterprise by using a controlled approach, defining a subset of VA-managed IPv6–enabled backbone devices, and taking advantage of any business case opportunities.

# 3 APPROACH

The following approach is planned to achieve success in meeting the requirements of the OMB IPv6 by the deadline of June 2008. This approach does not address the longer term testing and deployment of IPv6 across the VA IT enterprise beyond June 2008.

VA intends to test IPv6-enabled components from a representative sample of each of the various affected equipment configurations that exist across the VA IT enterprise. The remaining VA network hardware and software will be made “IPv6 ready” only to the extent of ensuring that all other applicable equipment is capable of being set up and configured to the tested profiles (e.g. with sufficient memory, correct IOS, etc.). In other words, the implementation will be based on requirements for IPv6 rather than installing and activating IPv6 on all 1500+ routers across the entire enterprise, precluding current testing and/or pilot(s) with IPv6.

a. The scope of initial IPv6 testing will be defined by establishing categories of devices that are involved in the One-VA WAN backbone and Internet gateway infrastructure (such as LAN/WAN routers, switches, firewalls, IPS, and etc.) as appropriate for testing.

b. Within each category, the number of different equipment configurations that exist across the One-VA WAN backbone and Internet gateway infrastructure (by manufacturer, model, IOS, etc.) will be identified.

c. Each configuration identified in (b) above will be mirrored in the IPv6 lab environment and tested to ensure that each configuration in each category is capable and compatible, from an IPv6 perspective. The setup/configuration for each configuration and category will be documented for use as a template at other sites for testing and future deployment purposes.

d. Selected sites that are representative of each of the configurations and categories will be identified and tested according to the OMB criteria (see *Section 1 - Objective*). This testing will be done across the One-VA WAN backbone and Internet gateway infrastructure when the appropriate security analyses has been completed and the requisite security components have been put into place.

e. Upon successful completion of the OMB test set at all of the test locations, it will be concluded that all other instances of the same tested configurations and categories of devices located elsewhere within the One-VA WAN backbone and Internet gateway infrastructure will pass similar tests.

f. When the OMB-mandated testing is complete, IPv6 capabilities introduced into the VA enterprise will remain enabled on the One-VA WAN backbone and Internet gateway infrastructure to facilitate continued technology and business case assessments. Continuation or removal of IPv6 capabilities will be contingent on a complete assessment of potential risks and measures available to mitigate those risks.

g. Testing results will be documented (see *Section 4 - IPv6 Test Case Templates* for examples) and provided to the VA CIO and OMB along with rationale and test procedures.

# 4 CONFIGURATION REQUIREMENTS

The following components are required for the demonstration configurations:

a. Two demonstration PCs (Source and Destination), running an IPv6-capable operating system (e.g., Vista, Solaris, Linux, or HP)

b. One Linux or Windows based IPv6 Web Server containing sample web content

c. Ping (or a multi-hop ping) for IPv6 must be available on the PCs and server

d. Traceroute/tracert for IPv6 must be available on the PCs and server used for testing

e. Associated cabling/hardware

f. Ability to capture screen shots from demonstration PCs

g. 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):

a. IPv6 router on external network

b. IPv6 PC/Laptop on external network

c. External IPv6 enabled web server, such as http://www6.research.earthlink.net/

And one of the following:

a. IPv6 service from an ISP or other provider, or

b. IPv6 over IPv4 Tunnel established between Internet border gateway router in the Agency's demonstration network and the router in the external network

# 5 IPv6 TEST CASE TEMPLATES

## *5.1 Test Case 1 – Inbound*

| ***INBOUND*** ***"Transmit IPv6 traffic from the Internet and external peers through the network backbone to the LAN"*** | **External Location #1** **Name:** Cisco RTP **Traffic Direction:** Source **Site Type:** IPv6 Enabled Business Partner | **External Location #2** **Name:** IRS **Traffic Direction:** Source **Site Type:** IPv6 Enabled Federal Partner |
|---|---|---|
| **VA Site #1** **Name:** ECSIP DMZ **Traffic Direction:** Destination **Site Type:** VA Internet DMZ | **Test:** #1, #2 **Test Results:** | **Test:** #1, #2 **Test Results:** |

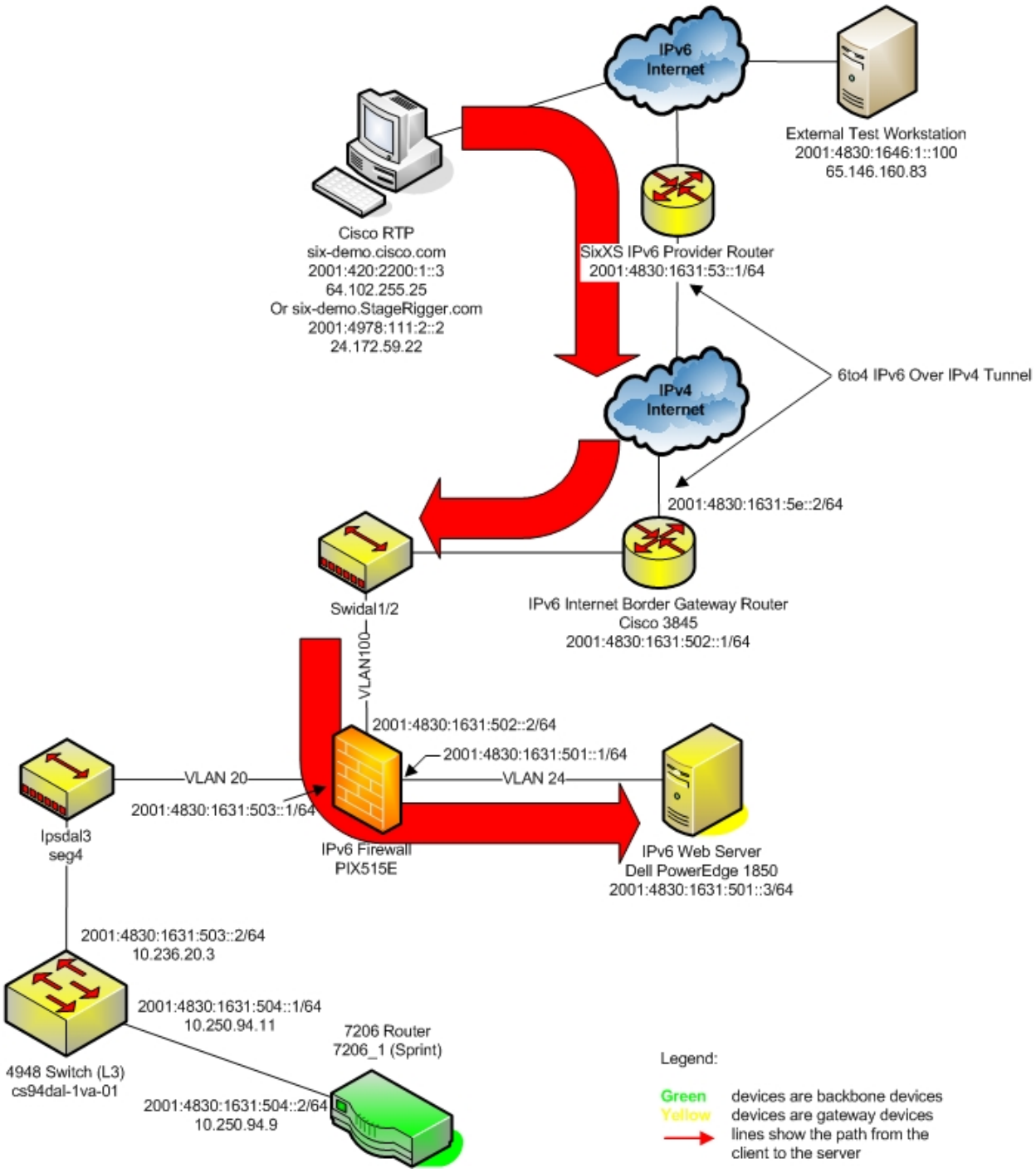
**Proposed Tests**

1. An external IPv6 client will access a test Web page served from an internal IPv6 Web server in the VA's DMZ. The Web Server should be dual stacked and reachable via both IPv4 and IPv6.
2. An external IPv4 client will access a test Web page served from the same Web server in the VA's DMZ using IPv4. The Web Server should be dual stacked and reachable via both IPv4 and IPv6.
3. If permitted, run the PING, pathping, and the traceroute utility to the internal IPv6 web server's address from the client configured with a native IPv6 stack. Use "ping -6 <destination web server's IPv6 address>", "pathping -6 <destination web server's IPv6 address>" and "tracert –d –R -6 <destination web server's IPv6 address>" to validate the results.

**Success Criteria**

1. The Web page hosted on the IPv4 Web server is accessible via an IPv4 configured client.
2. The Web page hosted on the same IPv6 enabled Web server is accessible via an IPv6 configured client. The local test site verifies that the client's IP address is a valid IPv6 address from the Partner.
3. If not blocked by the agency's security policy, ping, pingpath and traceroute/tracert should work and provide evidence of remote layer 3 reachability.

## Test Scenario 1



### *Test Case 2 - Outbound*

| ***OUTBOUND*** ***"Transmit IPv6 traffic from the LAN through the network backbone out to the Internet and external peers"*** | **External Location #1** **Name:** Cisco RTP **Traffic Direction:** Destination **Site Type:** IPv6 Web Site | **External Location #2** **Name:** IRS **Traffic Direction:** Destination **Site Type:** IPv6 External Federal Partner |
|---|---|---|
| **VA Site #1** **Name:** Little Rock, AK **Traffic Direction:** Source **Site Type:** VAMC | **Test:** #1 **Test Results:** | **Test:** #1 **Test Results:** |
| **VA Site #2** **Name:** Falling Waters, WV **Traffic Direction:** Source **Site Type:** NSOC/Data Center | Test: **#1** **Test Results:** | **Test:** #1 **Test Results:** |

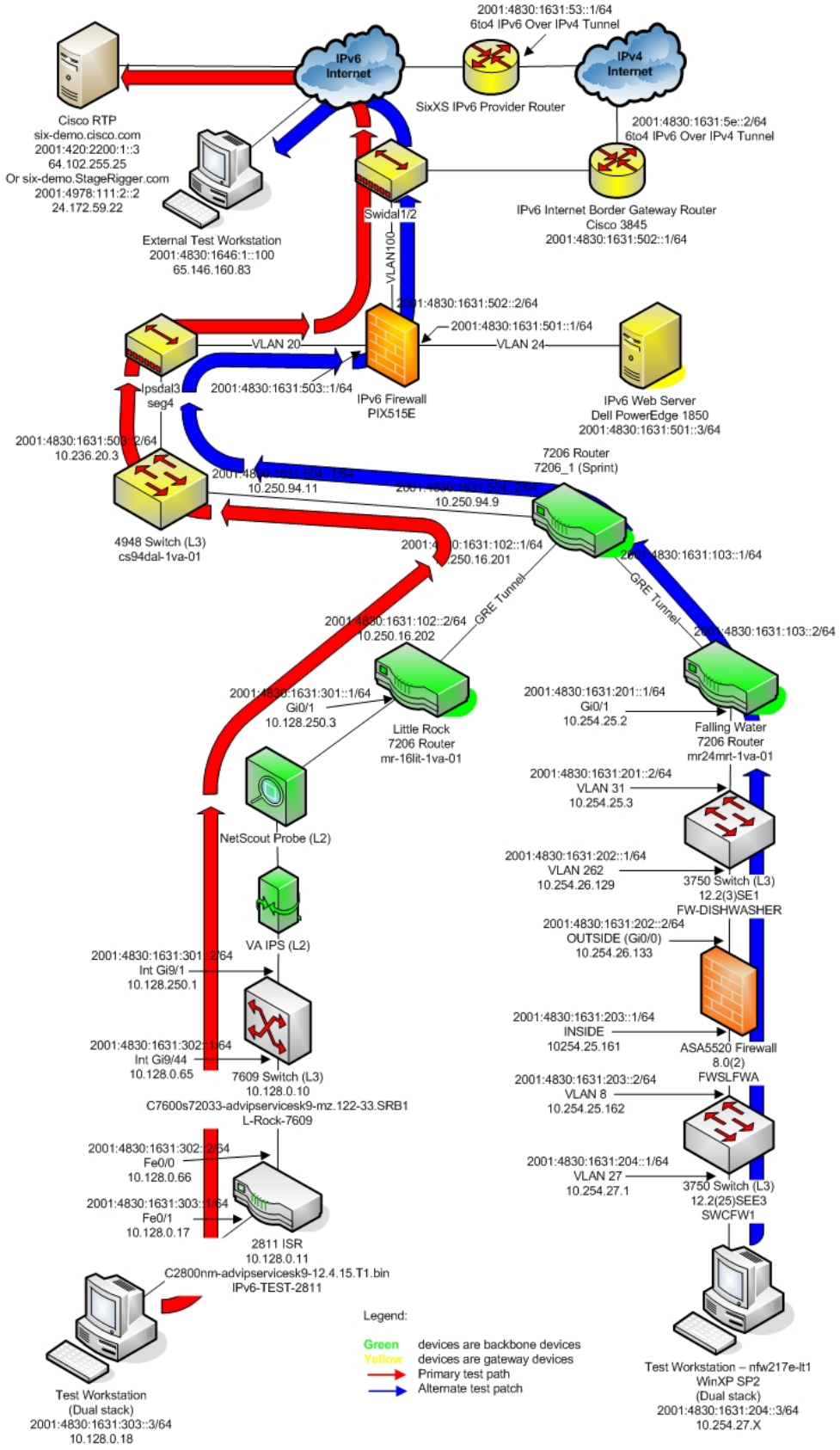
**Proposed Tests**

1. Access an external Web page using a client enabled with dual stack, IPv4 and IPv6.
2. If permitted, run the PING, pathping, and the traceroute utility to the internal IPv6 web server's address from the client configured with a native IPv6 stack. Use "ping -6 <destination web server's IPv6 address>", "pathping -6 <destination web server's IPv6 address>" and "tracert –d –R -6 <destination web server's IPv6 address>" to validate the results.

**Success Criteria**

1. The test Web site/page displays correctly.
2. The remote test Web site verifies that the client's IP address is an IPv6 address from the VA's assigned IPv6 address block.
3. If not blocked by the agency's security policy, ping, pingpath and traceroute/tracert should work and provide evidence of remote layer 3 reachability.

## Test Scenario 2



### *Test Case 3 - Internal*

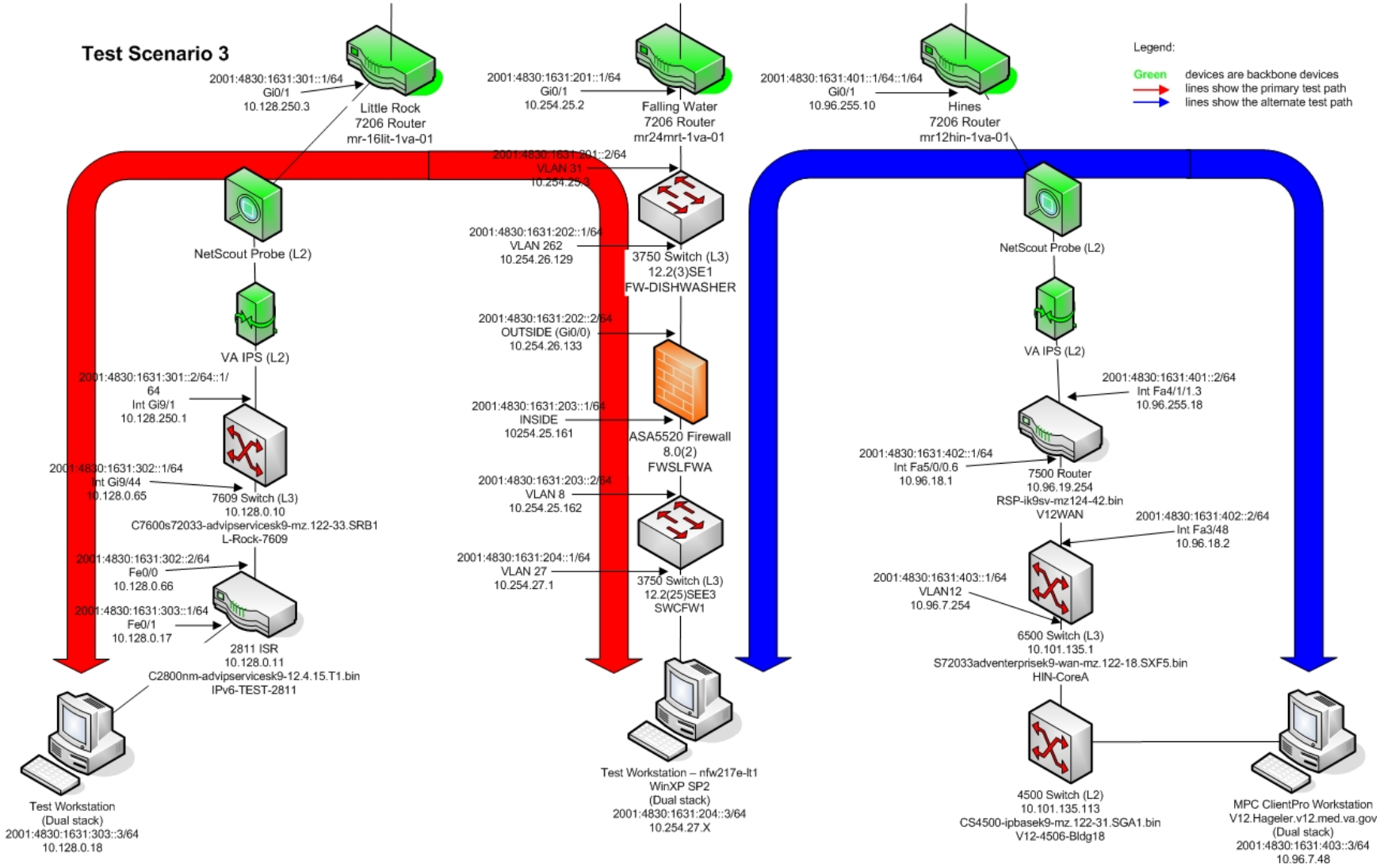
| ***INTERNAL*** ***"Transmit IPv6 traffic from the LAN through the network backbone to another LAN or another node on the same LAN"*** | **VA Site #1** **Name:** Falling Waters, WV **Traffic Direction:** Destination **Site Type:** NSOC/Data Center | **VA Site #2** **Name:** Little Rock, AK **Traffic Direction:** Destination **Site Type:** VAMC | **VA Site #3** **Name:** Hines, IL **Traffic Direction:** Destination **Site Type:** VAMC |
|---|---|---|---|
| **VA Site #1** **Name:** Falling Waters, WV **Traffic Direction:** Source **Site Type:** NSOC/Data Center | **N/A** | **Test:** #1, #2 **Test Results:** | **Test**: #1, #2 **Test Results:** |
| **VA Site #2** **Name:** Little Rock, AK **Traffic Direction:** Source **Site Type:** VAMC | **Test:** #1, #2 **Test Results:** | **N/A** | **Test:** #1, #2 **Test Results:** |
| **VA Site #3** **Name:** Hines, IL **Traffic Direction:** Source **Site Type:** VAMC | **Test:** #1, #2 **Test Results:** | **Test:** #1, #2 **Test Results:** | **N/A** |

**Proposed Tests**

1. Run PING, pathping and traceroute to an IPv6 client using a native IPv6 stack. "ping -6 <destination PC's IPv6 address>" and "tracert –d –R -6 <destination PC's IPv6 address>"
2. Using an Xlight FTP server and client, transfer data between the two using a native IPv6 stack.

**Success Criteria**

1. If not blocked by the agency's security policy, ping, pingpath and traceroute/tracert should work and provide evidence of remote layer 3 reachability.
2. File transfer completes successfully.
3. The test file transfer is within 20% of an equivalent IPv4 FTP transfer.


Test Scenario 3
Legend:
Green devices are backbone devices
lines show the primary test path
lines show the alternate test path
2001:4830:1631:301::1/64
Gi0/1
10.128.250.3
Little Rock
7206 Router
mr-16lit-1va-01
2001:4830:1631:201::1/64
Gi0/1
10.254.25.2
Falling Water
7206 Router
mr24mrt-1va-01
2001:4830:1631:401::1/64::1/64
Gi0/1
10.96.255.10
Hines
7206 Router
mr12hin-1va-01
2001:4830:1631:201::2/64
VLAN 31
10.254.25.3
NetScout Probe (L2)
2001:4830:1631:202::1/64
VLAN 262
10.254.26.129
3750 Switch (L3)
12.2(3)SE1
FW-DISHWASHER
2001:4830:1631:202::2/64
OUTSIDE (Gi0/0)
10.254.26.133
VA IPS (L2)
2001:4830:1631:301::2/64::1/64
Int Gi9/1
10.128.250.1
2001:4830:1631:203::1/64
INSIDE
10254.25.161
ASA5520 Firewall
8.0(2)
FWSLFWA
2001:4830:1631:302::1/64
Int Gi9/44
10.128.0.65
7609 Switch (L3)
10.128.0.10
C7600s72033-advipservicesk9-mz.122-33.SRB1
L-Rock-7609
2001:4830:1631:203::2/64
VLAN 8
10.254.25.162
2001:4830:1631:204::1/64
VLAN 27
10.254.27.1
3750 Switch (L3)
12.2(25)SEE3
SWCFW1
2001:4830:1631:302::2/64
Fe0/0
10.128.0.66
2001:4830:1631:303::1/64
Fe0/1
10.128.0.17
2811 ISR
10.128.0.11
C2800nm-advipservicesk9-12.4.15.T1.bin
IPv6-TEST-2811
Test Workstation
(Dual stack)
2001:4830:1631:303::3/64
10.128.0.18
Test Workstation – nfw217e-lt1
WinXP SP2
(Dual stack)
2001:4830:1631:204::3/64
10.254.27.X
NetScout Probe (L2)
VA IPS (L2)
2001:4830:1631:401::2/64
Int Fa4/1/1.3
10.96.255.18
2001:4830:1631:402::1/64
Int Fa5/0/0.6
10.96.18.1
7500 Router
10.96.19.254
RSP-ik9sv-mz124-42.bin
V12WAN
2001:4830:1631:402::2/64
Int Fa3/48
10.96.18.2
2001:4830:1631:403::1/64
VLAN12
10.96.7.254
6500 Switch (L3)
10.101.135.1
S72033adventerprisek9-wan-mz.122-18.SXF5.bin
HIN-CoreA
4500 Switch (L2)
10.101.135.113
CS4500-ipbasek9-mz.122-31.SGA1.bin
V12-4506-Bldg18
MPC ClientPro Workstation
V12.Hageler.v12.med.va.gov
(Dual stack)
2001:4830:1631:403::3/64
10.96.7.48

**DOCUMENTATION OF TEST RESULTS**

Upon successful completion of Tests 1, 2 & 3, the Agency will generate the following to prove compliance:

- Document baseline of IPv4 and IPv6 if client and server are dual stacked
- Take screenshots of ping -6/pathping -6 successes
- Take screenshots of traceroute/tracert results
- Take screenshots of IPv6 address configuration with the netsh, ipconfig, or ifconfig commands
- Take screenshots of test web pages accessed
- Take screenshots of successful file transfer with Xlight FTP server/client software