OptiView® Series III Network Analyzers IPv6 Analysis Option

Whether or not your organization is considering deployment of IPv6, at some time in the future, because IPv4 is running out of addresses, Internet backbone router tables are becoming too large and better support is required for real-time delivery of data through QoS, organizations will inevitably need to migrate from IPv4 to IPv6. However, there are other issues to consider today, such as:

- *Do you have any IPv6 hosts on your network?*
- *Many operating systems are already shipping with IPv6 enabled by default and network staff may be unaware that these IPv6 enabled hosts are even on their network.*
- *Are your firewalls and Intrusion Detection Systems IPv6 aware?*
- *Tunneling mechanisms such as Teredo, ISATAP and 6 to 4 that allow IPv6 traffic to be transported over IPv4 can potentially compromise your network security since they are sometimes able to circumvent firewalls*

And if you are deploying IPv6 you need a network analyzer to show you where your network stands today and accurately assess the impact of the IPv6 deployment.

Fluke Networks has extended the powerful, award winning capabilities of the OptiView® Series III Network Analyzers to include IPv6 to help you:

- *Validate IPv6 deployment*
- *Manage infrastructure changes and resolve IPv6 configuration issues*
- *Solve IPv6 performance problems*
- *Assess IPv6 network vulnerabilities*

Advanced active discovery techniques identify IPv6 networks and devices in seconds.

The analyzer monitors traffic and actively queries hosts to provide a complete IPv6 network and device inventory including routers, switches, wireless access points, DHCP6 servers, hosts, and servers. It enables you to identify and document multi- and single-homed devices that have dual IPv4 and IPv6 addresses or only have either an IPv4 or IPv6 address enabling you to locate IPv4 only devices which will be unable to operate in pure IPv6 networks.

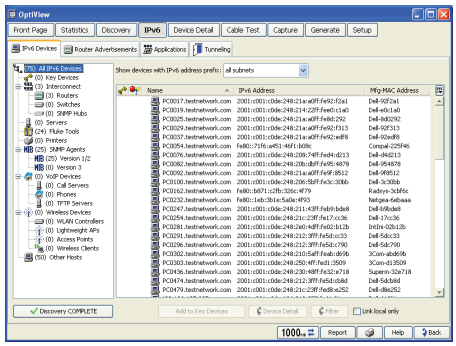

Figure 1: *IPv6 Device Discovery*

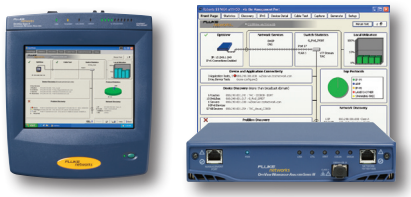

Figure 2: *OptiView Network Analyzers – Portable and Rack Models*

Identify Tunneling hosts

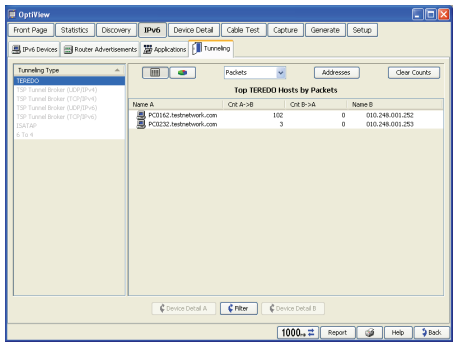

Figure 3: *Tunneling*

The OptiView identifies devices that are using IPv6 to/from IPv4 tunneling since unauthorized tunneling could represent a security risk.

The analyzer is capable of discovering the following tunneling types:

- Intra-site Automatic Tunnel Addressing Protocol (ISATAP) tunnels Client to client tunnel or client to router; which requires no manual configuration.
- Teredo, used for connections to the IPv4 Internet. This protocol will make a hole in a Firewall and allows Network Address Translation traversal.
- TSP Tunnel Broker over TCP, UDP, IPv4 and IPv6 which uses a Tunnel Broker in servers or routers to traverse NATs
- 6 to 4 – uses a 6-to-4 relay to connect to IPv6 network, often a third party outside of enterprise; uses IPv6 address of 2002::/16; and is enabled by default in Windows.

Verify Router configurations

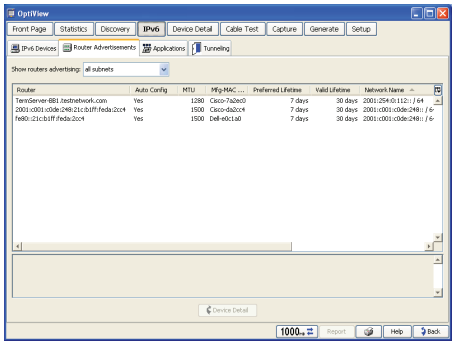

Figure 4: *IPv6 Router Ads*

IPv6 nodes can assign a domain name via IPv6 Router Advertisements (RA) "based domain name auto configuration." This process allows a node to create its own domain name using "locally available" and "advertised by routers" information and it is important for IT staff to ensure that router advertisements are identical by subnet and identify Router advertisements from non-routers which will impact connectivity and may indicate a Denial of Service attack. Information displayed by the analyzer includes:

- Router name that displays all IPv6 discovered routers with a Type field of 134.
- Auto Configure that determines whether the router is configured to stateless which uses a router prefix and an interface ID, or stateful which uses DHCP to auto configure.
- Maximum Transmission Unit (MTU), which is the packet size limit for a physical network. If data is too large for the network MTU setting, it must be fragmented, and then reassembled at the destination device. This is important since in IPv6, the sending host, not the router, can only perform fragmentation.
- Preferred Lifetime is the length of time the prefix generated by a "stateless" auto configuration remains preferred.
- Valid Lifetime is the length of time the prefix remains valid for On Link Determination. The valid lifetime is always greater than the preferred lifetime.
- Network Name is the prefix name.

Additionally, for Cisco routers, you are able to review the IPv6 Router Prefix table and the IPv6 net-to-media table (this replaces the IPv4 ARP table)

Verify IPv6 Application connectivity

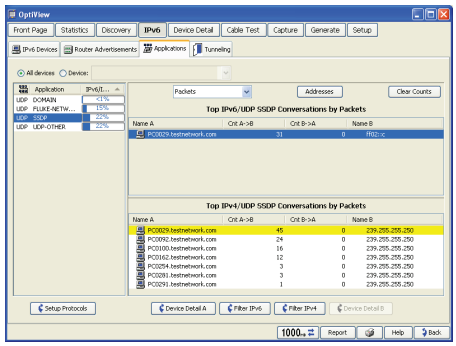

Figure 5: *Applications*

The analyzer compares applications that use both IPv6 and IPv4 and therefore may not work in a pure IPv6 network. The optional Application Troubleshooting Expert OPVS3-ATE) allows you to verify IPv6 connectivity, ensure that application ports can be opened and report the response time. Identify which end-points and servers are unable to reach their destination over IPv6 and indicate the cause that may include:

- No route to destination
- Administratively prohibited
- Beyond scope of source address
- Address unreachable
- Port unreachable
- Source address failed ingress/egress policy
- Reject route to destination

Packet Capture and Decode

Perform Gigabit line-rate packet capture and filtering to troubleshoot problems where packet level analysis is required and perform advanced troubleshooting with complete IPv6 post-capture analysis when deploying IPv6. Sophisticated capture filters allow collection of more relevant data and limit the amount of traffic to analyze by filtering on individual addresses or conversation, address range for IPV4, IPv6, IP subnet and protocols.

The capture process may be started or stopped through a user defined trigger event – capture the traffic before, after or around an event occurrence without being present. This ensures you capture the event the first time and avoids initiating random traffic captures that may not contain anything of interest.

For more information about IPv6, visit **www.flukenetworks.com/IPv6**

NETWORKSUPERVISION

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to **www.flukenetworks.com/contact**.

Printed in U.S.A. 9/2008 3369494 D-ENG-N Rev A