White Paper

The Invisible Threat: IPv6 on your network

With an increasing number of operating systems, both for servers and hosts, now being supplied with dual IPv4 and IPv6 stacks, you need to be aware of the fact that you may already have IPv6 protocols running on your network. This paper will explain why you may have IPv6 on your network and why having the right tool can enable network professionals to quickly identify those devices and ensure the integrity of your network.

Table of contents

FLUKE networks

Learn more about IPv6 testing, go to www.flukenetworks.com/ipv6

Why might you already have IPv6 on your network?

The explosive growth of the Internet and the requirement for additional addresses is consuming IPv4 addresses at a significant rate and most sources anticipate that the IPv4 address space will be exhausted in 2010 or 2011. More devices that use IP such as cameras, HVAC controls, alarm systems and sensors, to name just a few, are also contributing to this situation.

Additionally, the extensive use of IPv4 network address translation (NAT) to map multiple private addresses to a single public IPv4 address is becoming more complicated and in some cases may even preclude the use of real time IP communication such as VoIP. Internet backbone routers may experience performance degradation because they need to maintain extensive routing tables that typically exceed 85,000 routes.

Consequently, many operating systems, both client and server and some applications already support dual stack IPv4 and IPv6 architectures and some such as Windows® Vista,® Windows® Server 2008 and Apple® OS X 10.3 have IPv6 enabled by default, and users can easily enable operating systems that are not IPv6 enabled by default.

By default, an IPv6 device has the ability to automatically configure a link local address for each of its' interfaces and by using router discovery can determine the addresses of IPv6 routers, access configuration parameters and global address prefixes. The lack of stateful configuration protocols such as DHCPv6 will not prevent an IPv6 capable device from configuring an IPv6 address for each of its interfaces.

Tunneling mechanisms

So maybe you are thinking "But I am not routing IPv6 traffic in my network so why should I be concerned about IPv6 enabled end-devices?" Well, tunneling takes care of this – it is supported in every operating system and is automatically enabled when the IPv6 stack is installed. Tunneling will enable IPv6 transport over IPv4 connections and vice-versa; it is sometimes encrypted and may be used with anonymous (privacy) addressing not the EUI-64 constructed interface identifier which will allow you to trace it back to the MAC address of the host. (Note: an EUI-64 address is constructed from the device MAC address by adding Hex FF-FE between the first 24 and the last 24 bits of the MAC address).

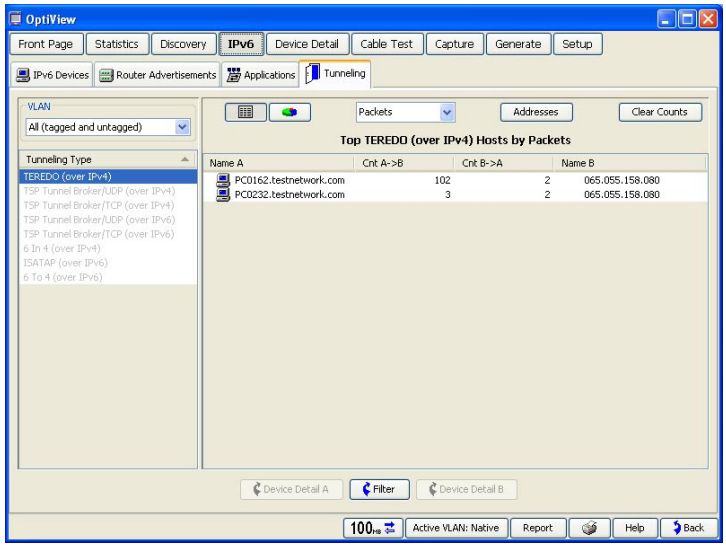

Figure 1 – Tunneling View

Some of the more common tunneling mechanisms are:

- Teredo – Used for connections to the IPv4 Internet. This protocol will make a hole in a Firewall and will allow traversal of Network Address Translators. However, Teredo is more commonly found in home networks rather than enterprise networks.
- TSP Tunnel Broker over TCP, UDP, IPv4 and IPv6. This uses Tunnel Broker in the server or router to traverse NATs
- 6in4 is an Internet transition methodology for migrating from IPv4 to IPv6 and refers to the encapsulation of IPv6 traffic within explicitly-configured IPv4 tunnels. It is also referred to as 'proto-41 static', due to the port number it uses and the fact that endpoints are configured statically. This should not be confused with 6to4 or 6over4 which have similar names but are different. 6in4 encapsulates the entire IPv6 packet directly behind the IPv4 packet header in which the 'protocol' field is set to value 41, which indicates IPv6-in-IPv4.
- Intra-site Automatic Tunnel Addressing Protocol (ISATAP) tunnels provide for a client-to-client tunnel or client-to-router tunnel and requires no manual configuration.
- 6 to 4 – uses a 6to4 relay to connect to an IPv6 network without the need to configure explicit tunnels. This is often hosted by a third party outside of enterprise and uses IPv6 address prefix of 2002::/16; which is enabled by default in Windows.

What are the risks involved with tunneling – if you have a local tunnel within your intranet there is little risk but if you have a local device with a tunnel endpoint outside of your network, it may allow access to the internal network from the Intranet which will probably be unprotected by Firewalls or Intrusion Detection Systems.

Other potential IPv6 vulnerabilities

There are a number of other potential vulnerabilities that you need to be aware of such as rogue router advertisements. This would be non-routers advertising subnet addresses that should not exist on your network that could be caused simply by IPv6 router or host configuration errors or, more importantly, could be an indication of malicious activity. By sending fake router advertisements, an attacker pretends to be a router and cause all other hosts on the subnet to send traffic leaving the subnet to the attacker host resulting in a man-in-the middle attack. The same can be said for DHCPv6 spoofing so it is also important to discover devices offering IPv6 stateful addresses.

Additionally, since IPv4 is more mature than IPv6, operating systems tend to leave more IPv6 ports open, therefore it is important to be able to perform an IPv6 port scan in order to identify those open ports and with IPSec supported as standard in any IPv6 stack, devices can more easily encrypt end-to-end traffic, preventing firewalls detecting the packet content.

The bottom line - attempting to attack a network with malicious traffic is by no means new but having IPv6 enabled devices on your network will potentially allow an attacker (external or internal) to break in by traditional methods and extract data from your network undetected through IPv6.

How a portable analyzer helps

Using a portable tool, network professionals can connect to each subnet, identify IPv6 enabled devices easily, and take action and closing gaps in the network when necessary.

Because ensuring a network runs smoothly is a network engineer's primary duty, security can sometimes be a secondary concern. By using a tool that provides flexibility in addressing both routine maintenance as well as potential IPv6, and other, security vulnerabilities, network engineers can discover potential trouble areas, detect and correct them, all while keeping their network functioning at a high level.

Consequently, every network engineer should have answers to the following:

- Which devices are using IPv6 and who are they communicating with?
- Which IPv6 ports are open posing a potential threat for attacks?
- Which devices are offering stateful DHCPv6 services?
- Are there any "non–routers" advertising IPv6 address prefixes?
- Are there any tunnels open and if so what are the end-points?
- Are there any devices using privacy addresses?
- Are there any devices using end-to-end IPSec encryption that will pass undetected through firewalls?
- Are there any devices scanning IPv6 ports?

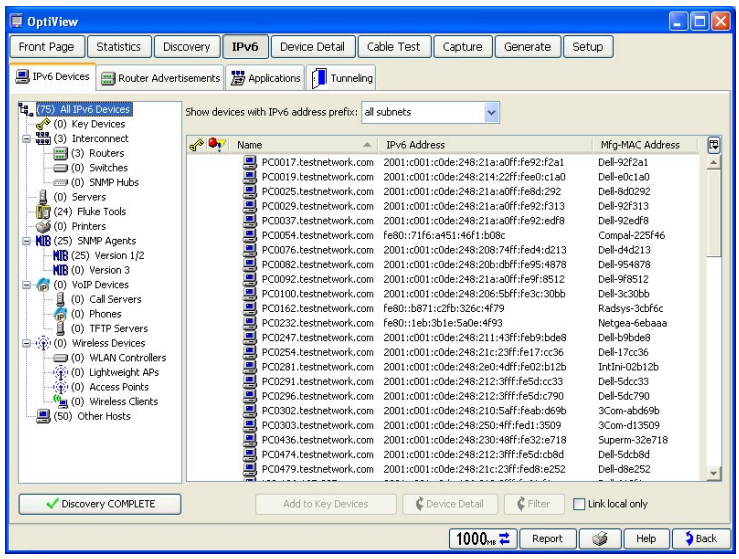

Figure 2 – IPv6 Device Discovery

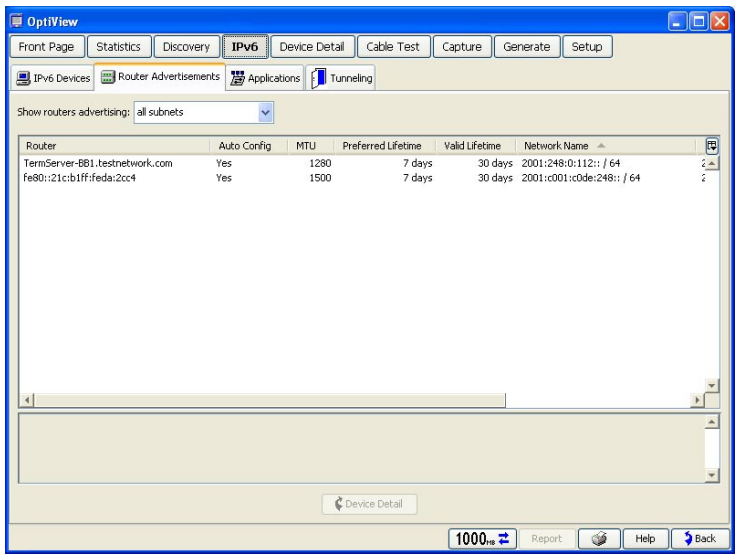

Figure 3 – IPv6 Router Advertisements

Solution: Integrated Portable Analyzer

In order to provide answers to all these questions network professionals require a device that will both passively and actively discover IPv6 devices and services. There are a number of devices available that will provide passive discovery by monitoring IPv6 traffic, capturing IP and MAC addresses but are unable to categorize the devices based on the identified protocols. The OptiView Series III analyzer is the only device that provides active IPv6 discovery by transmitting router solicitation requests in order to identify all IPv6 prefixes for the subnet and by transmitting neighbor solicitations to provide information on other IPv6 devices on the subnet. To obtain additional information, the OptiView provides visibility into router IPv6 Net-to-Media tables (the equivalent of an IPv4 ARP table) to discover link-local addresses off the attached subnet. Additionally, the OptiView Series III is able to access Cisco router prefix tables that provide information on additional subnets.

The OptiView analyzer comes equipped with several key features that allow network professionals to address security problems from the inside:

Free String Match

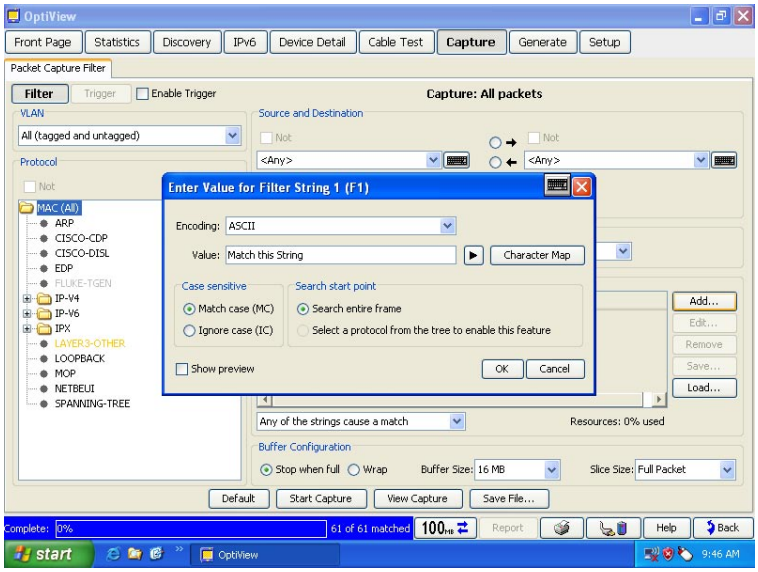

Figure 4 – Free String Match Setup

The OptiView analyzer allows network engineers to use the Free String Match function to match any set of words or phrases – regardless of the position of the packet, payload or header – in real time. An engineer can detect traffic containing certain words or phrases in non-encrypted emails, web pages, file transfers or documents. This allows the engineer to identify improper use of the network as well as detect downloads of restricted documents based on content or file names. The Free String Match feature, and in-depth protocol recognition, also helps engineers identify and track applications that are not allowed on the network, such as streaming media that takes up valuable bandwidth, or P2P traffic that poses a security risk. Up to eight triggers or filters can be defined at any one time, allowing engineers to analyze captures when time allows.

Wireless rogue device identification and location

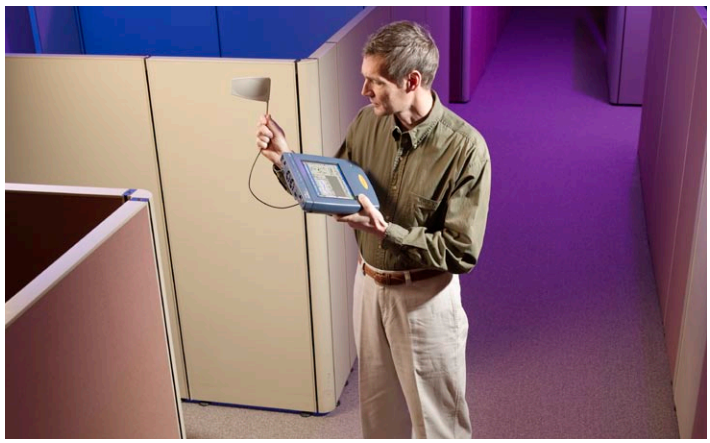

Figure 5 – Rogue Hunting with the OptiView Integrated Network Analyzer

The OptiView analyzer quickly tracks down rogue and unsecured devices, including ad-hoc networks. Audio and visual indicators lead network engineers to the location of the offending device.

User account restrictions and removable hard drive

The OptiView analyzer's user accounts screen lets engineers add and modify analyzer security information for each individual user. This prevents unauthorized use of certain analyzer features for easier compliance with federal regulations, including HIPAA and SOX. Potentially disabled features include: packet capture and decode, traffic generation, remote user interface and analyzer configuration. Network information discovered by the OptiView Series III Integrated Network Analyzer can be stored on the optional removable hard drive, which ensures any sensitive data stored on a network analyzer's hard drive never leaves that environment. The analyzer can be moved from classified environments of different levels and between classified and unclassified systems or private and public networks by simply replacing the hard drive.

Summary

It may be some time before the new internet protocol IPv6 takes over from the current IPv4, but many networks may already be open to attack through mechanisms that have been enabled on devices to support IPv6 traffic.

Network Engineers who do not have the equipment to analyze their networks in order to determine what they have and what's enabled on their networks, in terms of secure IPv6, are not only opening themselves to attack, but may be considered as non-compliant under Sarbanes-Oxley, HIPPA and other regulations, even though these regulations don't require auditors to validate that IPv6 is turned off.

We are not advocating that you disable IPv6 because, face it, at some time in the not too distant future you will need to migrate your network to IPv6 – we just want you too be aware of what is on your network and be able to secure it now, and learn today, what you need to do tomorrow when you deploy IPv6.

The business case for a portable, integrated network analyzer

The OptiView Series III Integrated Network Analyzer helps network professionals manage IT projects, solve network problems and support IT initiatives, resulting in reduced IT costs and improved user satisfaction. It gives you a clear view of your entire enterprise – providing visibility into every piece of hardware, every application, and every connection on your network. No other portable tool offers this much vision and all-in-one capability to help you:

- **Deploy new technologies and applications**
- **Manage and validate infrastructure changes**
- **Solve network and application performance issues**
- **Secure network from internal threats**

It shows you where your network stands today and helps you accurately assess its readiness for the changes you need to make now and in the future. Leverage the power of OptiView to give you vision and control of your network.

IPv6 security threats may be unintentional, but they can no longer be a back burner worry…the risks are simply too great. To address these threats network professionals would benefit from a new tool, one that helps find weak spots in the network and allows them to track down potential vulnerabilities. The OptiView Series III Integrated Network Analyzer adds that additional portable, layer of protection. With this additional protection, network professionals are able to find and address potential problems that could compromise the network – and the business.

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 3381730 H-ENG-N Rev A