

# Changes to IPv6 in Windows Vista and Windows Server 2008

Joseph Davies

Both Microsoft Windows Vista and Windows Server 2008 include the Next Generation TCP/IP stack, a redesigned TCP/IP protocol stack with an integrated version of both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). For more information, see Next Generation TCP/IP Stack in Windows Vista and Windows Server 2008, the September 2005 The Cable Guy article.

This article describes the new features for IPv6 and the Teredo IPv6 transition technology in the Next Generation TCP/IP stack.

## Changes to IPv6

IPv6 is the long-term replacement for IPv4, the current and widely used Internet layer of the TCP/IP protocol suite that was designed in the late 1970s. IPv6 provides the following benefits for TCP/IP-based networking connectivity:

- Large address space The 128-bit address space for IPv6 provides ample room to provide every device on the present and foreseeable future Internet with a globally reachable address.
- Efficient routing With a streamlined IPv6 header and addressing that supports hierarchical routing infrastructures, IPv6 routers on the Internet can forward IPv6 traffic faster than their IPv4 counterparts.
- Ease of configuration IPv6 hosts can configure themselves by either interacting with a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server or by interacting with their local router and using stateless address autoconfiguration.
- Enhanced security The IPv6 standards solve some of the security issues of IPv4 by providing better protection against address and port scanning attacks and by requiring that all IPv6 implementations support Internet Protocol security (IPsec) for cryptographic protection of IPv6 traffic.

The changes to IPv6 in Windows Vista and Windows Server 2008 are the following:

- Dual IP layer architecture
- Installed and enabled by default
- GUI-based configuration
- Full Support for IPsec
- MLDv2
- LLMNR
- Literal IPv6 addresses in URLs
- IPv6 over PPP
- DHCPv6
- Random interface IDs

## Dual IP Layer Architecture

The implementation of IPv6 in Windows XP and Windows Server 2003 is a dual stack architecture, which has separate protocol components for IPv4 and IPv6 that are installed through the Network Connections folder. The separate IPv4 and IPv6 protocol components had their own Transport layer that included Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) and framing layer.

# Changes to IPv6 in Windows Vista and Windows Server 2008

Joseph Davies

The Next Generation TCP/IP stack is a single protocol component installed through the Network Connections folder that supports the dual IP layer architecture, in which both IPv4 and IPv6 share common Transport and Framing layers.

Because there is a single implementation of TCP, TCP traffic over IPv6 can take advantage of all the performance features of the Next Generation TCP/IP stack. These features include all of the performance enhancements of the IPv4 protocol stack of Windows XP and Windows Server 2003 and additional enhancements new to the Next Generation TCP/IP stack, such as Receive Window Auto Tuning and Compound TCP which can dramatically improve performance on high-latency/high-delay connections and better support for TCP traffic in high-loss environments (such as wireless LAN networks).

## Installed and Enabled by Default

In Windows Vista and Windows Server 2008, IPv6 is installed and enabled by default as the Internet Protocol version 6 (TCP/IPv6) component from the properties of a connection in the Connections and Adapters folder. In Windows Vista and Windows Server 2008, many operating system components now support IPv6.

When both IPv4 and IPv6 are enabled, the Next Generation TCP/IP stack prefers the use of IPv6. For example, if a Domain Name System (DNS) Name Query Response message contains a list of both IPv6 and IPv4 addresses, the Next Generation TCP/IP stack will attempt to communicate over IPv6 first, subject to the address selection rules that are defined in RFC 3484. For more information, see Source and Destination Address Selection for IPv6, the February 2006 The Cable Guy article.

The preference of IPv6 over IPv4 offers IPv6-enabled applications better network connectivity because IPv6 connections can use IPv6 transition technologies such as Teredo, which allow peer or server applications to operate behind network address translators (NATs) without requiring NAT configuration or application modification.

Enabling IPv6 by default and preferring of IPv6 traffic does not impair IPv4 connectivity. For example, on networks without IPv6 records in the DNS infrastructure, communications using IPv6 addresses are not attempted unless the user or application specifies the destination IPv6 address.

To take advantage of IPv6 connectivity, networking applications must be updated to use Windows Sockets functions that are not specific to IPv4 or IPv6. For more information, see the IPv6 Guide for Windows Sockets Applications.

Note: Due to misconfigured DNS servers on the Internet, computers that use both IPv4 and IPv6 might not be able to resolve names and connect to Internet resources. This rare problem occurs when a misconfigured DNS server receives a request to resolve a name to one or more IPv6 addresses (a request for AAAA records). If the DNS server does not support IPv6, the name query fails. The querying node then sends a request to resolve the name to a set of IPv4 addresses (a request for A records). The misconfigured DNS server drops the subsequent DNS query for IPv4 addresses and the entire name resolution attempt fails, resulting in impaired network connectivity for the requesting node. If you are experiencing this problem, ask your Internet service provider to reconfigure their DNS server to accept the subsequent DNS query for A records after failing the DNS query for AAAA records. Alternately, you can temporarily disable IPv6 on the requesting computer. This issue exists on the DNS servers and is common to all computers that use both IPv4 and IPv6.

# Changes to IPv6 in Windows Vista and Windows Server 2008

Joseph Davies

## GUI-based Configuration

In Windows XP and Windows Server 2003, you must manually configure IPv6 configuration settings with netsh interface ipv6 commands at a Windows command prompt. Windows Vista and Windows Server 2008 now allow you to also manually configure IPv6 settings through the properties of the Internet Protocol version 6 (TCP/IPv6) component in the Connections and Adapters folder, similar to how you can manually configure IPv4 settings.

## Full Support for IPsec

Internet Protocol security (IPsec) support for IPv6 traffic in Windows XP and Windows Server 2003 is limited. There is no support for Internet Key Exchange (IKE) or data encryption. IPsec security policies, security associations and keys are configured through text files and activated through a command line tool, IPsec6.exe.

In Windows Vista and Windows Server 2008, IPsec support for IPv6 traffic is the same as that for IPv4, including support for IKE and data encryption with AES 128/192/256. The IP Security Policies snap-in now supports the configuration of IPsec policies for IPv6 traffic in the same way as IPv4 traffic using either the IP Security Policies snap-in or the new Windows Firewall with Advanced Security snap-in.

## MLDv2

Windows Vista and Windows Server 2008 supports Multicast Listener Discovery version 2 (MLDv2), specified in RFC 3810, which allows IPv6 hosts to register interest in source-specific multicast traffic with their local multicast routers. A host running on Windows Vista or Windows Server 2008 can register interest in receiving IPv6 multicast traffic from only specific source addresses (an include list) or from any source except specific source addresses (an exclude list).

## LLMNR

Windows Vista and Windows Server 2008 support Link-Local Multicast Name Resolution (LLMNR), which allows IPv6 hosts on a single subnet without a DNS server to resolve each other names. This capability is useful for single-subnet home networks and ad hoc wireless networks. Rather than unicasting a DNS query to a DNS server, LLMNR nodes send their DNS queries to a multicast address on which all the LLMNR-capable nodes of the subnet are listening. The owner of the queried name sends a response. IPv4 nodes can also use LLMNR to perform local subnet name resolution with having to rely on NetBIOS over TCP/IP broadcasts.

## Literal IPv6 Addresses in URLs

The WinINet API in Windows Vista and Windows Server 2008 now supports RFC 2732 and the use of IPv6 literal addresses in URLs. For example, to connect to the Web server at the IPv6 address 2001:db8:100:2a5f::1, a user with a WinINet-based Web browser (such as Internet Explorer) can type `http://[2001:db8:100:2a5f::1]` as the URL. Although typical users might not use IPv6 literal addresses, the ability to specify the IPv6 address in the URL is valuable to application developers, software testers, and network troubleshooters.

## IPv6 over PPP

The built-in remote access client now supports IPv6 over the Point-to-Point Protocol (PPP) (PPPoE), as defined in RFC 5072. Native IPv6 traffic can now be sent over PPP-based connections. For example, PPPoE support allows you to connect with an IPv6-based Internet service provider (ISP) through dial-up or PPP over Ethernet (PPPoE)-based connections that might be used for broadband Internet access.

# Changes to IPv6 in Windows Vista and Windows Server 2008

Joseph Davies

## DHCPv6

The DHCP Client service in Windows Vista and Windows Server 2008 supports Dynamic Host Configuration Protocol for IPv6 (DHCPv6) defined in RFCs 3315 and 3736. A computer running Windows Vista or Windows Server 2008 can perform both stateful and stateless DHCPv6 configuration on a native IPv6 network. The DHCP Server service in Windows Server 2008 also supports DHCPv6.

## Random Interface IDs

To prevent address scans of IPv6 addresses based on the known company IDs of network adapter manufacturers, Windows Vista and Windows Server 2008 by default generates random interface IDs for non-temporary autoconfigured IPv6 addresses, including public and link-local addresses. A public IPv6 address is a global address that is registered in DNS and is typically used by server applications for incoming connections, such as a Web server.

Note that this new behavior is different than that for temporary IPv6 addresses, as described in RFC 4941. Temporary addresses also use randomly derived interface IDs. However, they are not registered in DNS and are typically used by client applications when initiating communication, such as a Web browser.

## Changes to Teredo

Teredo is an IPv6 transition technology that allows IPv6/IPv4 nodes that are separated by one or more NATs to communicate end-to-end with global IPv6 addresses. NATs are commonly used on the Internet to preserve the public IPv4 address space by translating the addresses and port numbers of traffic to and from private network hosts that use private IPv4 addresses.

Although NATs extend the life of the public IPv4 address space, this functionality comes at the cost of violating the original design principle of the Internet that all nodes should communicate with a unique global address. Because of the reuse of private addresses and the translation between private and public addresses that occur at the NAT, servers and peers that are located on private networks behind NATs cannot communicate without either manually configuring the NAT or modifying application protocols.

Although IPv4 traffic for servers and peers that are behind a NAT might have problems traversing a NAT, Teredo-based IPv6 traffic can traverse a NAT without having to configure the NAT or modify application protocols. Teredo IPv6 addresses are global addresses, unique to the entire Internet. Teredo restores global addressing and end-to-end connectivity for IPv6 traffic for an environment that does not support global addressing and end-to-end connectivity for IPv4 traffic.

Teredo was first released with the Advanced Networking Pack for Windows XP with Service Pack 1 and is included with Windows XP Service Pack 2 and later and Windows Server 2003 Service Pack 1 and later. Teredo is provided with Windows Vista (enabled by default) and Windows Server 2008 (disabled by default). Applications that are already IPv6-enabled require no additional modification. Teredo is just one of the ways in which the Next Generation TCP/IP stack can send and receive IPv6 traffic.

Teredo in Windows Vista and Windows Server 2008 supports the following:

# Changes to IPv6 in Windows Vista and Windows Server 2008

Joseph Davies

- Teredo is now enabled for domain member computers. Teredo for Windows XP and Windows Server 2003 automatically disabled itself if the computer was a member of a domain. A domain member computer is more likely to be attached to a network that has deployed either native IPv6 connectivity or Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), an IPv6 transition technology. However, domain member computers can also benefit from Teredo-based IPv6 connectivity.
- Teredo can now work if there is one Teredo client behind one or more symmetric NATs. A symmetric NAT maps the same internal (private) address and port number to different external (public) addresses and ports, depending on the external destination address (for outbound traffic). Teredo for Windows XP and Windows Server 2003 disables itself if it detects that it is behind a symmetric NAT. This new behavior allows Teredo to work between a larger set of Internet-connected hosts.

**Note:** Teredo traffic is IPv6 packets that have been encapsulated as IPv4-based UDP messages. A Teredo client cannot initialize or communicate with other Teredo clients if an edge firewall drops all outbound UDP traffic.

## Security with IPv6 and Teredo

Having IPv6 and Teredo enabled by default does not make your computer more vulnerable to attack by malicious users or programs because of the following:

- Windows Firewall, included with and enabled by default for both Windows Vista and Windows Server 2008, is a stateful host-based firewall for both IPv4 and IPv6 traffic. All of the protections against unwanted, unsolicited, incoming traffic apply to both IPv4 and IPv6 traffic.
- Windows Firewall allows exceptions for wanted, unsolicited, incoming traffic based on TCP or UDP ports or by specifying a program name and apply to an individual computer. Windows Firewall-based exceptions are much more specific than exceptions configured on typical NATs.
- The Windows Filtering Platform is a new architecture in Windows Vista and Windows Server 2008 that allows third-party software developers access to the TCP/IP packet processing path, wherein outgoing and incoming packets can be examined or changed before allowing them to be processed further. By tapping into the TCP/IP processing path, ISVs can create firewalls, antivirus software, diagnostic software, and other types of applications and services. The Windows Filtering Platform is designed for both IPv4 and IPv6 traffic. Third-party host-based firewall products that use the Windows Filtering Platform will typically support both IPv4 and IPv6 traffic.

Computers running Windows Vista have IPv6, Teredo, and Windows Firewall enabled by default, and are protected from unwanted, unsolicited, incoming IPv6 traffic.