

IPv6 Improvements in Windows Vista

By Joseph Davies

Technical Writer, Windows Networking and Device Technologies
Microsoft Corporation



Microsoft

IPv6 is supported in Microsoft® Windows XP and Windows Server™ 2003, but its use among networking services and applications is limited. With Windows Vista™ (in beta testing at the time of the publication of this article), IPv6 support is installed by default and built-in Windows Vista network services and applications are now IPv6-capable. This new level of IPv6 support in Windows Vista has the potential of igniting the networking industry with new applications and connectivity in the same way as the inclusion of a TCP/IP stack in Windows 95 ignited the industry for the applications and services of the Internet.

Note: This article describes features of the February Community Technology Preview beta version of Windows Vista. These features are subject to change and may not be included in the final product due to marketing, technical, or other reasons.

The IPv6 support in Windows Vista has the following features:

Installed, enabled and preferred by default

One of the biggest changes for IPv6 in Windows Vista is that, by default, IPv6 is installed and enabled. Unlike IPv6 in Windows XP and Windows Server 2003, network administrators do not have to deploy and enable IPv6 on Windows Vista desktop computers.

Additionally, Windows Vista by default will prefer the use of IPv6 to IPv4. For example, if a computer running Windows Vista sends a Domain Name System (DNS) name query and the response contains both IPv6 AAAA records and IPv4 A records, the computer running Windows Vista will attempt to communicate using the IPv6 addresses first, subject to the default address selection rules defined in RFC 3484. This behavior causes Windows Vista to use an IPv6 infrastructure when available (either native or based on an IPv6 transition technology), and can provide better connectivity for computers connected to the Internet that are located behind network address translators (NATs).

Windows-wide support for IPv6

With very few exceptions, the networking tools, services and applications in Windows Vista are now IPv6-capable, including key productivity tasks such as Web browsing, Active Directory® directory service domain operations, and file and printer sharing.

New dual IP layer architecture

The implementation of IPv6 in Windows XP and Windows Server 2003 is a dual stack architecture. The separate IPv4 and IPv6 protocol stacks are separate drivers with their own transport (including TCP and UDP) and framing layers. Additionally, the implementation of TCP for the IPv6 protocol stack does not include all of performance enhancements of the IPv4 protocol stack, such as selective acknowledgements, TCP timestamps and window scaling.

The Next Generation TCP/IP stack in Windows Vista is a single stack that supports the dual IP layer architecture, in which both IPv4 and IPv6 share common transport and framing layers. Figure 1 shows the architecture of the Next Generation TCP/IP stack .

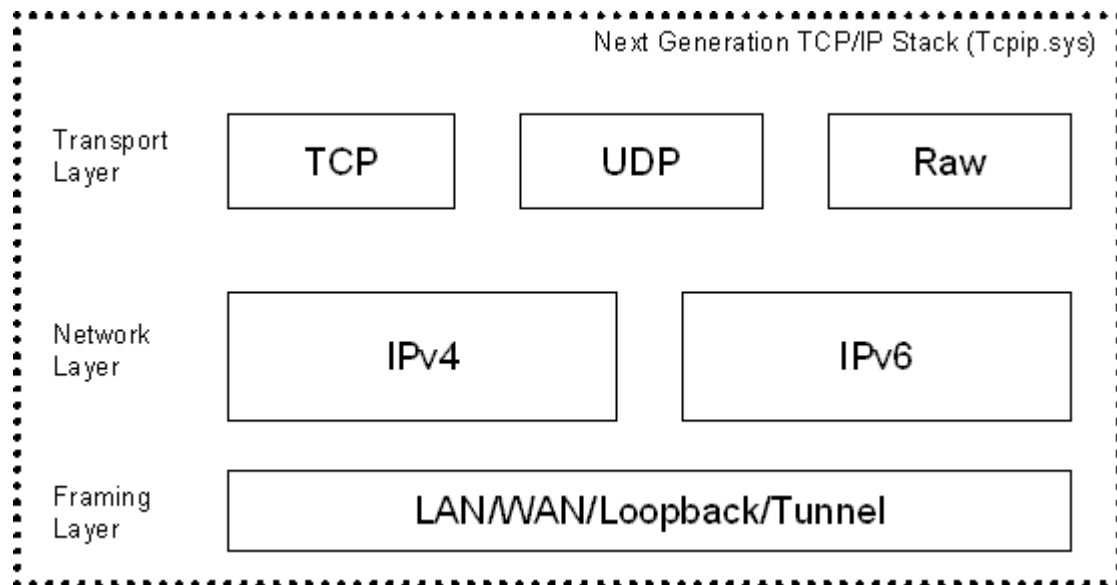


Figure 1 The dual IP layer architecture of the Next Generation TCP/IP stack

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 Windows Vista, 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).

For more information, see [Performance Enhancements in the Next Generation TCP/IP Stack](#).

Full IPsec support

Internet Protocol security (IPsec) support for IPv6 traffic in Windows XP and Windows Server 2003 is limited. For example, there is no support for Internet Key Exchange (IKE) or data encryption, and IPsec security policies, security association, and keys must be manually configured using command-line tools. In Windows Vista, IPsec support for IPv6 traffic is the same as that for IPv4, including support for IKE and data encryption with AES 128/192/256. You can now configure IPsec policies for IPv6 traffic in the same way as IPv4 traffic using Windows graphical user interface (GUI) tools.

Teredo enhancements

Teredo is an IPv6 transition technology supported in Windows XP and Windows Server 2003 that provides IPv6 connectivity for nodes that are located behind NATs. Teredo in Windows Vista is now enabled for Active Directory domain member computers and between Teredo clients 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). This new behavior in Windows Vista allows Teredo to work between a larger set of Internet-connected hosts.

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 now allows you to manually configure IPv6 settings through a set of dialog boxes in the Connections and Adapters folder, similar to how you can manually configure IPv4 settings.

MLDv2

Windows Vista supports Multicast Listener Discovery version 2 (MLDv2), specified in RFC 3810, which allows IPv6 hosts to specify interest in source-specific multicast traffic. An application running on Windows Vista 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

Link-Local Multicast Name Resolution (LLMNR) allows IPv6 hosts on a single subnet without a DNS server to resolve each other's 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 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 3ffe:ffff:100:2a5f::1, a user with a WinINet-based Web browser (such as Internet Explorer) can type `http://[3ffe:ffff: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 2472. 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.

DHCPv6

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

Random Interface IDs for IPv6 Addresses

To prevent address scans of IPv6 addresses based on the known company IDs of network adapter manufacturers, Windows Vista 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 3041. 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.

Using IPv6 in Windows Vista

The support for IPv6 by Windows Vista network applications and services allows the following:

- **IPv6-only operation:** You can completely disable IPv4 and use Windows Vista computers in an IPv6-only networking environment.
- **Active Directory operations:** With a domain controller running Windows Server "Longhorn" (in beta testing at the time of the publication of this article), a computer running Windows Vista can join an Active Directory domain and perform Active Directory domain operations.
- **Broadband IPv6 Internet access:** With support for PPPoE and PPPoE, a computer running Windows Vista can connect directly to a PPPoE-based broadband IPv6 ISP.
- **IPv6 Web browsing:** Internet Explorer in Windows Vista is IPv6-capable, allowing Web browsing of IPv6 Internet resources using either names or IPv6 literal addresses.
- **Peer networking:** The Windows Peer-to-Peer Networking components in Windows Vista use only IPv6 and provide peer applications with easy methods to discover and connect with peers or peer groups.
- **File and printer sharing:** Both the file and printer sharing client and server components of Windows Vista and Windows Server "Longhorn" are IPv6-capable, allowing you to access shared files and send print jobs to shared printers over IPv6.
- **Protected IPv6 communications with IPsec:** IPv6 traffic can be protected with IPsec and IPsec policies can be easily configured and deployed in an Active Directory environment.
- **IPv4 compatibility:** The default configuration of Windows Vista allows for complete interoperability with hosts and networks that are running only IPv4.