

Support for IPv6 in Windows Server 2008 R2 and Windows 7

Joseph Davies

With Windows Server 2008 R2 and Windows 7 (now in beta testing), Microsoft continues its platform-wide support for IPv6 with a protocol stack that supports industry standards and built-in applications and services. As with Windows Vista and Windows Server 2008, IPv6 in Windows Server 2008 R2 and Windows 7 is installed and enabled by default.

In this column, we'll take a look at the features in Windows 7 and Windows Server 2008 R2 that take advantage of IPv6. In doing so, we'll see how IPv6 can be leveraged to create new and innovative productivity and connectivity solutions.

HomeGroup

HomeGroup in Windows 7 is a new way for computers on home networks to associate with each other and to let family members share documents, pictures, music, videos, and printers. HomeGroup relies on IPv6 connectivity and the Windows Peer-to-Peer Networking Platform on computers running Windows 7 on a single-subnet home network.

The Argument against Disabling IPv6

It is unfortunate that some organizations disable IPv6 on their computers running Windows Vista or Windows Server 2008, where it is installed and enabled by default. Many disable IPv6 based on the assumption that they are not running any applications or services that use it. Others might disable it because of a misperception that having both IPv4 and IPv6 enabled effectively doubles their DNS and Web traffic. This is not true.

From Microsoft's perspective, IPv6 is a mandatory part of the Windows operating system and it is enabled and included in standard Windows service and application testing during the operating system development process. Because Windows was designed specifically with IPv6 present, Microsoft does not perform any testing to determine the effects of disabling IPv6. If IPv6 is disabled on Windows Vista, Windows Server 2008, or later versions, some components will not function. Moreover, applications that you might not think are using IPv6—such as Remote Assistance, HomeGroup, DirectAccess, and Windows Mail—could be.

Therefore, Microsoft recommends that you leave IPv6 enabled, even if you do not have an IPv6-enabled network, either native or tunneled. By leaving IPv6 enabled, you do not disable IPv6-only applications and services (for example, HomeGroup in Windows 7 and DirectAccess in Windows 7 and Windows Server 2008 R2 are IPv6-only) and your hosts can take advantage of IPv6-enhanced connectivity.

DirectAccess

DirectAccess is a key feature in Windows 7 and Windows Server 2008 R2 that provides remote DirectAccess clients with bidirectional access to intranet resources by using an IPsec-protected connection to a DirectAccess server. DirectAccess leverages end-to-end global IPv6 addressing and connectivity to transparently connect remote computers to an intranet as if they were connected with an Ethernet cable.

DirectAccess clients running Windows 7 or Windows Server 2008 R2 automatically create a protected and tunneled IPv6 connection to a DirectAccess server running Windows Server 2008 R2 whenever a client determines it is on the Internet.

IP-HTTPS

6to4 and Teredo are two transition technologies that allow an IPv6 host to tunnel IPv6 traffic across the IPv4 Internet. However, Web proxy servers and some firewalls might block this encapsulated IPv6

Support for IPv6 in Windows Server 2008 R2 and Windows 7

Joseph Davies

traffic. IP-HTTPS is a new protocol for Windows 7 and Windows Server 2008 R2 that allows hosts to establish connectivity through a Web proxy or firewall by tunneling IPv6 packets inside an IPv4-based secure HTTPS session.

IP-HTTPS is used only when the client cannot connect to the server using any of the other standard IPv6 connectivity protocols—native IPv6, Teredo, or 6to4. You can configure IP-HTTPS behavior with Netsh.exe command-line tool commands in the netsh interface httpstunnel context or with the new IP-HTTPS State Group Policy setting described later in this article.

Teredo Server and Relay

Windows Server 2008 R2 includes support for Teredo server and relay functionality. Previous versions of Windows included support only for a Teredo client and a Teredo host-specific relay. To understand what this means, let's step back and review some background on Teredo.

Teredo is an IPv6 transition technology defined in RFC 4380 that provides unicast IPv6 connectivity across the IPv4 Internet for hosts separated from the Internet by a Network Address Translation (NAT) device that does not support 6to4 or native IPv6 addressing. Figure 1 shows the components of a Teredo infrastructure.

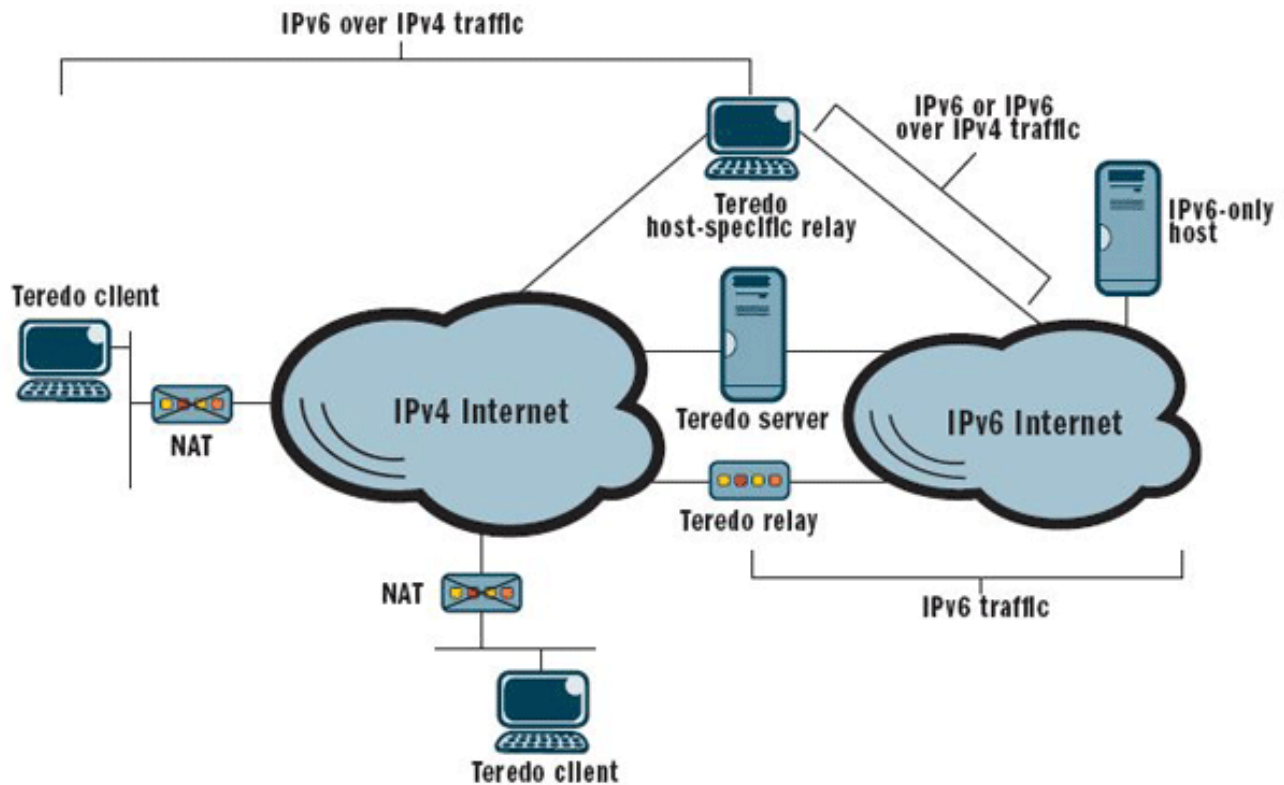


Figure 1 Components of a Teredo Infrastructure

A Teredo client tunnels IPv6 packets to either other Teredo clients or to nodes on an IPv6 network, such as the IPv6 Internet, through a Teredo relay or Teredo host-specific relay. A Teredo client communicates with a Teredo server to configure a Teredo-based IPv6 address or to help initiate communication with other Teredo clients or hosts on the IPv6 Internet.

Support for IPv6 in Windows Server 2008 R2 and Windows 7

Joseph Davies

A Teredo relay is a router that forwards packets between Teredo clients on the IPv4 Internet and IPv6 hosts. A Teredo host-specific relay is an IPv6/IPv4 node that has an interface and connectivity to both the IPv4 Internet and the IPv6 Internet and can communicate directly with Teredo clients over the IPv4 Internet, without the need for an intermediate Teredo relay.

Prior to Windows Server 2008 R2, Microsoft deployed Teredo servers and relays on the Internet that Windows-based Teredo clients use by default, and left it to ISPs to deploy additional Teredo servers and relays for their customers.

Configuring a Teredo Server

The DirectAccess Setup wizard automatically configures Teredo server functionality on the DirectAccess server and configures DirectAccess clients to use that DirectAccess server as a Teredo server. To manually configure a computer running Windows Server 2008 R2 as a Teredo server, connect the computer to the IPv4 Internet and configure two consecutive, public, static IPv4 addresses on the Internet interface. For example, configure the Internet interface with the IPv4 addresses 131.107.41.171 and 131.107.41.172. Then, at a command prompt, run the netsh interface teredo set state server FirstIPAddress command.

By default, Windows-based Teredo clients resolve the name `teredo.ipv6.microsoft.com` to determine the IPv4 address of the Microsoft Teredo server on the Internet. If you deploy your own Teredo server, you must configure your client computers with either the first IPv4 address of your Teredo server or a DNS name that resolves to that same IPv4 address. You can use the netsh interface `teredo set state server=NameOrFirstIPv4Address` command to configure your hosts with your Teredo server. Alternatively, for computers running Windows 7 and Windows Server 2008 R2, you can use the Teredo Server Name Group Policy setting described in this article.

Configuring a Teredo Relay

Teredo host-specific relay functionality is enabled by default, but the host is acting as an endpoint, rather than a router. In contrast, a Teredo relay forwards IPv6 packets between interfaces corresponding to the IPv4 Internet and an IPv6 network, which could be an intranet or the IPv6 Internet.

To enable relay functionality, you need to enable forwarding on the Teredo interface and the interfaces that connect to your IPv6 network. Examples of such interfaces are an Ethernet interface for a native IPv6 intranet or your Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) interface if you are using ISATAP for IPv6 connectivity on your intranet. Use the netsh interface `ipv6 set interface interface=InterfaceNameOrIndex forwarding=enabled` command to enable forwarding on the appropriate interfaces.

Group Policy Settings for Transition Technologies

You can centrally configure settings for IP-HTTPS, Teredo, 6to4, and ISATAP through Group Policy for computers running Windows 7 or Windows Server 2008 R2. In previous versions of Windows, you had to configure the equivalent settings through Netsh.exe commands.

You'll find these settings in the Group Policy Management Editor snap-in at:

[Computer Configuration](#) | [Policies](#) | [Administrative Templates](#) | [Network](#) | [TCP/IP Settings](#) | [IPv6 Transition Technologies](#).

Figure 2 shows the new Group Policy settings.

**Support for IPv6 in Windows Server 2008 R2 and
Windows 7**
Joseph Davies

Figure 2: IPv6 Transition Technologies Group Policy Settings

Setting name	Description	Netsh.exe command equivalent
6to4 Relay Name	Allows you to specify a 6to4 relay name for a 6to4 host. A 6to4 relay is used as a default gateway for IPv6 network traffic sent by the 6to4 host.	netsh interface 6to4 set relay name=
6to4 Relay Name Resolution Interval	Allows you to specify the interval at which the 6to4 relay name is resolved.	netsh interface 6to4 set relay interval=
6to4 State	Allows you to configure the state of the 6to4 client.	netsh interface 6to4 set state=
IP-HTTPS State	Allows you to configure the state of the IP-HTTPS client.	netsh interface httpstunnel set interface state=
ISATAP Router Name	Allows you to specify a router name or IPv4 address for an ISATAP router.	netsh interface ipv6 isatap set router name=
ISATAP State	Allows you to configure the state of the ISATAP host.	netsh interface ipv6 isatap set state=
Teredo Client Port	Allows you to specify the UDP port the Teredo client will use to send packets.	netsh interface teredo set state clientport=
Teredo Default Qualified	Allows you to set Teredo to be ready to communicate. By default, Teredo enters a dormant state when not in use. The qualification process brings it out of a dormant state.	N/A
Teredo Refresh Rate	Allows you to configure the rate at which Teredo clients refresh the NAT translation table.	netsh interface teredo set state refreshinterval=
Teredo Server Name	Allows you to specify the name of the Teredo server.	netsh interface teredo set state servername=
Teredo State	Allows you to specify the state of the Teredo service.	netsh interface teredo set state type=

The DirectAccess Setup wizard uses these Group Policy settings to configure DirectAccess clients with the DirectAccess server as the Teredo server and the ISATAP router. You can also use them independently of DirectAccess to deploy ISATAP on your intranet or to centrally configure 6to4, Teredo, and IP-HTTPS settings for your hosts.