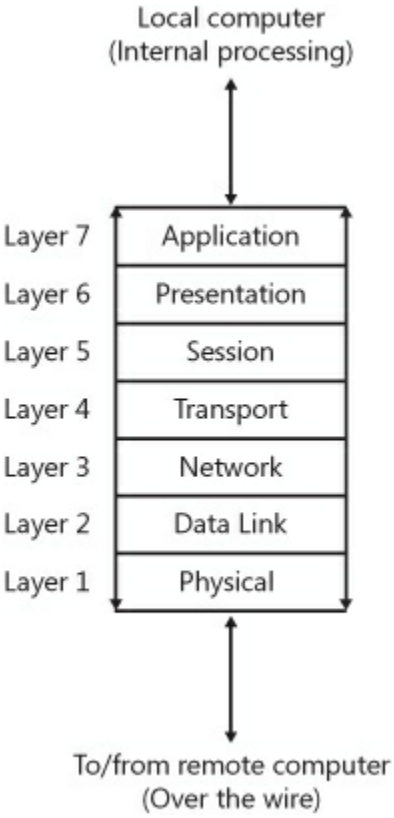
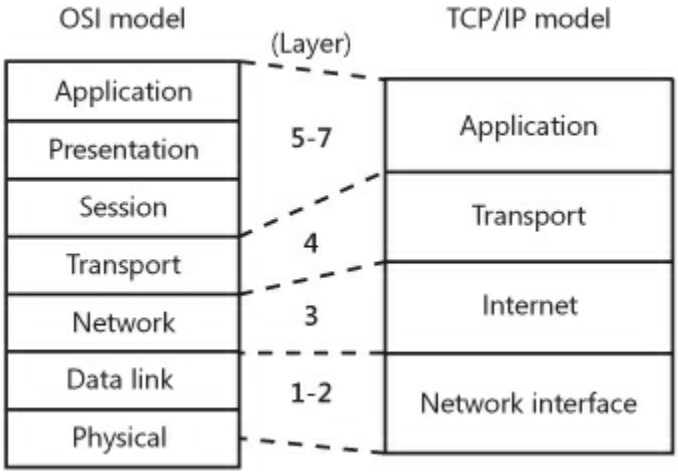
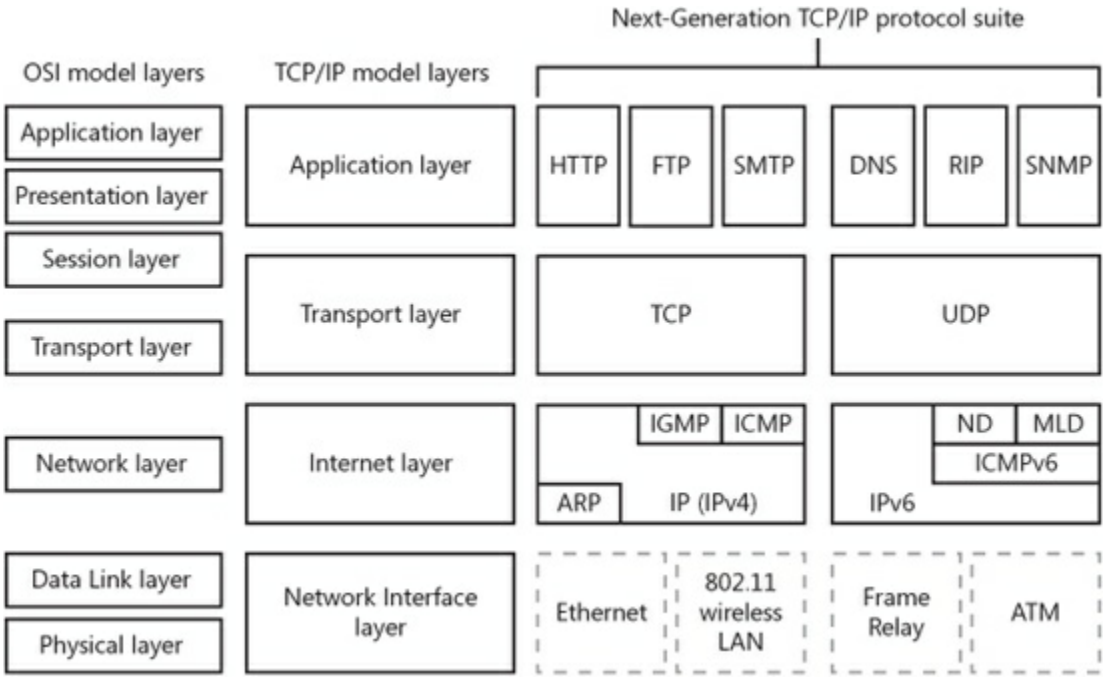


The OSI model of network communications

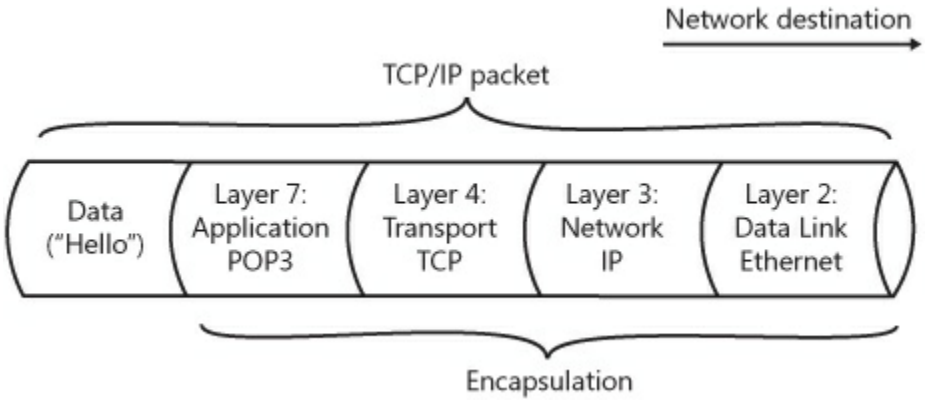


The TCP/IP networking layers are mapped to the OSI model



The Next Generation TCP/IP stack

IPv6 is supported natively in Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2.



An example of a TCP/IP packet

Change Advanced Sharing Settings in Network and Sharing Center relates to the default settings on the local computer for network profiles, such as Home or Work, or Public. For each of these network profiles, you can configure the local computer to enable or disable Network Discovery (a protocol that enables browsing), File And Printer Sharing, Public Folder Sharing, and Media Streaming. However, these settings are mostly relevant for a workgroup environment and are not tested on the 70-642 exam. In a Domain environment, servers will automatically be set to the Domain network profile, and the default features enabled in the Domain network profile should be set for the entire domain by Group Policy.

The See Full Map option in Network and Sharing Center allows you to see the devices on your local LAN and how these devices are connected to each other and to the Internet. This feature is disabled by default in the Domain network profile, but it can be enabled in Group Policy.

Network Map relies on two components:

- The Link Layer Topology Discovery (LLTD) Mapper component queries the network for devices to include in the map.
- The LLTD Responder component responds to the queries from the Mapper I/O.

Although these two components are included only in Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2, you can install an LLTD Responder component on computers running Windows XP so that they will appear on a Network Map on other computers.

ncpa.cpl

The following list describes the three types of network components that can be bound to a connection:

- **Network Clients.** In Windows, network clients are software components, such as Client For Microsoft Networks, that allow the local computer to connect with a particular network operating system. By default, Client For Microsoft Networks is the only network client bound to all local area connections. Client For Microsoft Networks allows Windows client computers to connect to shared resources on other Windows computers.
- **Network Services.** Network services are software components that provide additional features for network connections. File And Printer Sharing For Microsoft Networks and QoS Packet Scheduler are the two network services bound to all local area connections by default. File And Printer Sharing For Microsoft Networks allows the local computer to share folders for network access. QoS Packet Scheduler provides network traffic control, including rate-of-flow and prioritization services.
- **Network Protocols.** Computers can communicate through a connection only by using network protocols bound to that connection. By default, four network protocols are installed and bound to every network connection: IPv4, IPv6, the Link-Layer Topology Discovery (LLTD) Mapper, and the LLTD Responder.

When you configure network bridging, you allow traffic from the wireless, Ethernet, and Token Ring NIC to share the same network space. Hence, a single wireless NIC can be the outbound gateway to disparate networks.

Configuring IPv4 and IPv6 Settings Manually from the Command Prompt

```
netsh interface ipv4 set address "Connection_Name" static Address Subnet_Mask
netsh interface ipv4 set address "local area connection" static 192.168.33.5
255.255.255.0
```

```
netsh interface ipv6 set address "Local Area Connection" 2001:db8:290c:1291::1
```

Note: the default prefix is 64

Understanding Automatic Private IP Addressing

Automatic Private IP Addressing (APIPA) is an automatic addressing feature useful for some ad hoc or temporary networks. Whenever a Windows computer has been configured to obtain an IP address automatically, and when no DHCP server or alternate configuration is available, the computer uses APIPA to assign itself a private IP address in the range of 169.254.0.1 through 169.254.255.254 and a subnet mask of 255.255.0.0.

```
Ipconfig
ipconfig /renew
ipconfig /flushdns
ipconfig /displaydns
ipconfig /registerdns
```

In certain cases, however, a ping attempt takes place over IPv6, such as when you ping a computer by name in a **workgroup environment.**

IMPORTANT: ICMP, FIREWALLS, AND PING

ICMP is blocked by default by Windows Firewall, and it is also blocked by some routers and stand-alone firewalls. Consequently, to use Ping, Tracert, and PathPing successfully, you need to ensure that ICMP is not blocked by the remote host. To enable a firewall exception for ICMP on a computer running Windows Server 2008 R2, use Windows Firewall with Advanced Security console to enable the File and Printer Sharing (Echo Request – ICMPv4-In) firewall rule. To enable a firewall exception for ICMPv6, enable the File and Printer Sharing (Echo Request – ICMPv6-In) firewall rule. You can also enable these firewall rules throughout the domain by using Group Policy.

```
ping
tracert
pathping
arp
        arp –a
        arp –d 192.168.0.254
```

PathPing. PathPing is similar to Tracert except that PathPing is intended to find links that are causing intermittent data loss.

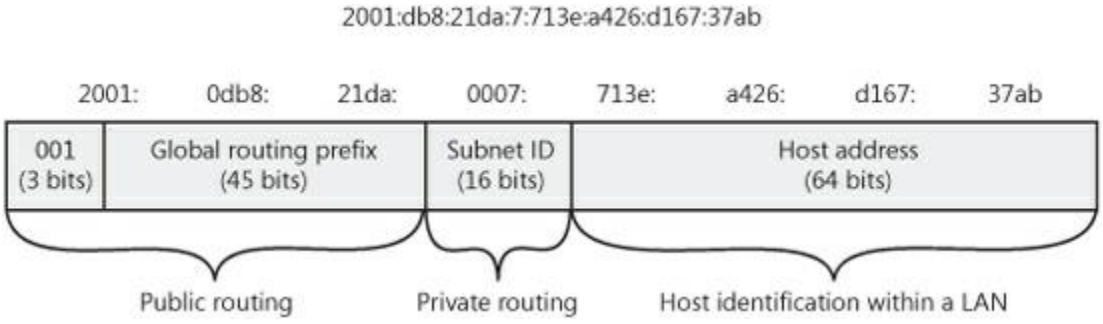
NOTE: IPV6 PREVENTS ARP CACHE POISONING

> To resolve IP-to-MAC address mappings, IPv6 uses a protocol named Neighbor Discovery (ND) instead of the ARP protocol used by IPv4. For this reason, a nice benefit of an all-IPv6 network is that it prevents the possibility of Arp cache poisoning.

Computers can receive IPv6 addresses either from neighboring routers or from DHCPv6 servers. Computers also always assign themselves an address for use on the local subnet only.

Global Addresses

IPv6 global addresses are the equivalent of public addresses in IPv4 and are globally reachable on the IPv6 portion of the Internet. The address prefix currently used for global addresses is 2000::/3, which translates to a first block value between 2000–3FFF in the usual hexadecimal notation.

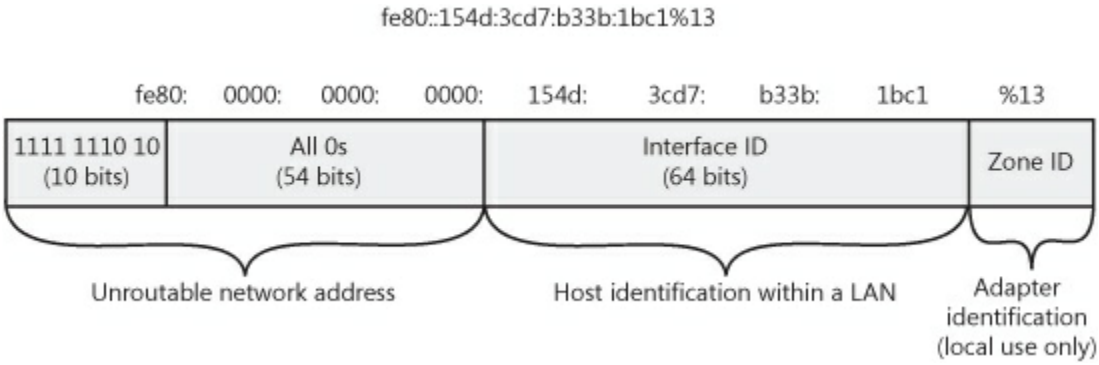


A global IPv6 address

Link-Local Addresses

Link-local addresses are similar to APIPA addresses (169.254.0.0/16) in IPv4 in that they are self-configured, nonroutable addresses used only for communication on the local subnet. However, unlike an APIPA address, a link-local address remains assigned to an interface as a secondary address even after a routable address is obtained for that interface.

Link-local addresses always begin with “fe80”. An example link-local address is **`fe80::154d:3cd7:b33b:1bc1%13`**



A link-local IPv6 address

WHAT ARE THE ZONE IDS AFTER LINK-LOCAL ADDRESSES?

Because all link-local addresses (LLAs) share the same network identifier (fe80::), you cannot determine which interface a link-local address is bound to merely by looking at the address. Therefore, if a computer running Windows has multiple network adapters connected to different network segments, the computer distinguishes the networks by using a numeric zone ID following a percent sign after the IP address, as the following examples illustrate:

- fe80::d84b:8939:7684:a5a4%7
- fe80::462:7ed4:795b:1c9f%8
- fe80::2882:29d5:e7a4:b481%9

The two characters after each address indicate that the preceding networks are connected to the zone IDs 7, 8, and 9, respectively. Although zone IDs can occasionally be used with other types of ac Link-Local Addresses you should always specify the zone ID when connecting to link-local addresses.

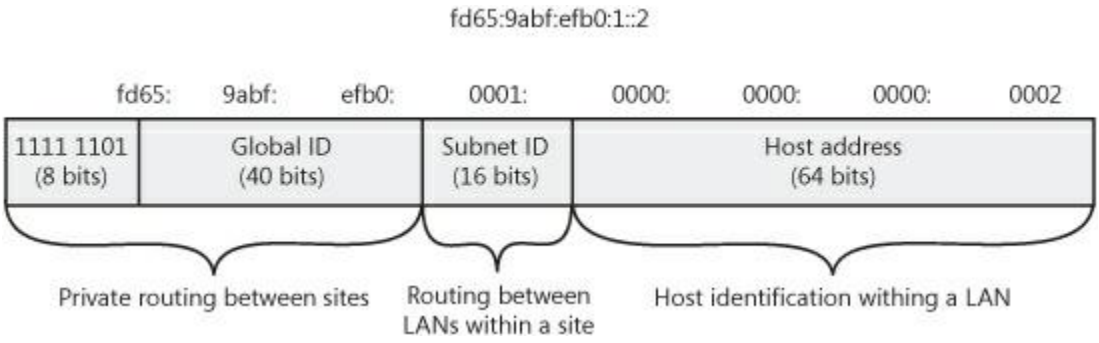
Remember also that zone IDs are relative to the sending host. If you want to ping a neighboring computer's LLA, you have to specify the neighbor's address along with the Zone ID of *your* computer's network adapter that faces the neighbor's computer. For example, in the command `ping fe80::2b0:d0ff:fee9:4143%3`, the address is of the neighboring computer's interface, but the "%3" corresponds to the zone ID of an interface on the local computer.

The zone ID for a link-local address is assigned on the basis of a parameter called the *interface index* for that network interface. You can view a list of interface indexes on a computer by typing `netsh interface ipv6 show interface` at a command prompt.

`netsh interface ipv6 show interface`

Unique Local Addresses

Unique local addresses are the IPv6 equivalent of private addresses in IPv4 (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16). These addresses are routable between subnets on a private network but are not routable on the public Internet. They allow you to create complex internal networks without having public address space assigned. Such addresses begin with "fd". An example of a unique local address used in a large organization is fd00:9abf:efb0:1::2. An example of a unique local address used in a small organization is fd00::2.



A unique local IPv6 address

NOTE: WHAT ARE SITE-LOCAL ADDRESSES?

Site-local addresses in the fec0::/10 address prefix also provide private routing on IPv6 networks, but they have recently been deprecated (officially set on a path toward obsolescence) by RFC 3879.

States of an IPv6 Address

IPv6 hosts typically configure IPv6 addresses by interacting with an IPv6-enabled router and performing IPv6 address autoconfiguration. Addresses are in a *tentative* state for the brief period of time between first assigning the address and verifying that the address is unique. Computers use duplicate address detection to identify other computers that have the same IPv6 address by sending out a Neighbor Solicitation message with the tentative address. If a computer responds, the address is considered

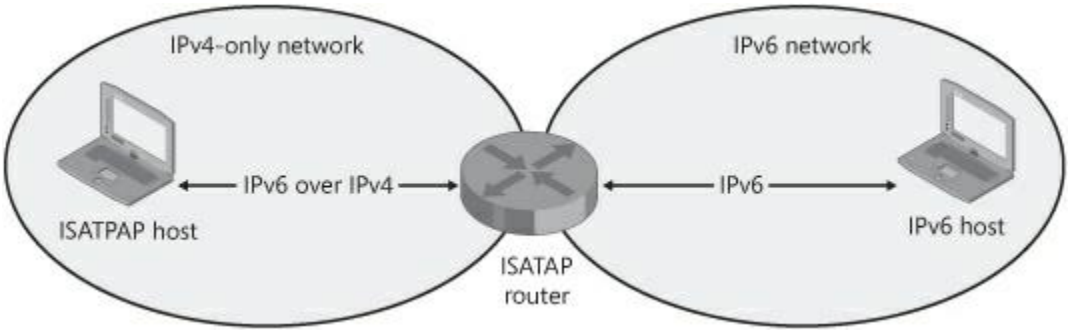
invalid. If no other computer responds, the address is considered unique and valid. A valid address is called preferred within its valid lifetime assigned by the router or autoconfiguration. A valid address is called deprecated when it exceeds its lifetime. Existing communication sessions can still use a deprecated address.

IMPORTANT: LOOPBACK ADDRESSES IN IPV4 AND IPV6

In IPv4, the address 127.0.0.1 is known as the *loopback address* and always refers to the local computer. The loopback address in IPv6 is ::1. On a computer with any IPv4 or IPv6 address, you can ping the loopback address to ensure that TCP/IP is functioning correctly.

Intra-Site Automatic Tunnel Addressing Protocol

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) is a tunneling protocol that allows an IPv6 network to communicate with an IPv4 network through an ISATAP router

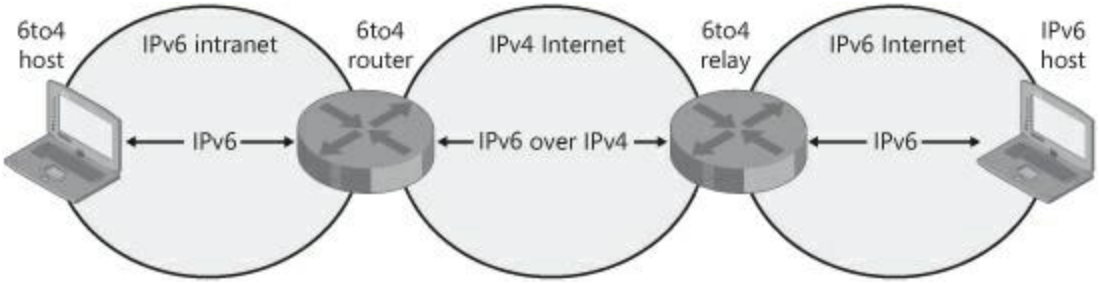


ISATAP routers allow IPv4-only and IPv6-only hosts to communicate with each other.

ISATAP allows IPv4 and IPv6 hosts to communicate by performing a type of address translation between IPv4 and IPv6. In this process, all ISATAP clients receive an address for an ISATAP interface. This address is composed of an IPv4 address encapsulated inside an IPv6 address.

6to4

6to4 is a protocol that tunnels IPv6 traffic over IPv4 traffic through 6to4 routers. 6to4 clients have their router's IPv4 address embedded in their IPv6 address and do not require an IPv4 address. Whereas ISATAP is intended primarily for intranets, 6to4 is intended to be used on the Internet. You can use 6to4 to connect to IPv6 portions of the Internet through a 6to4 relay even if your intranet or your ISP supports only IPv4.

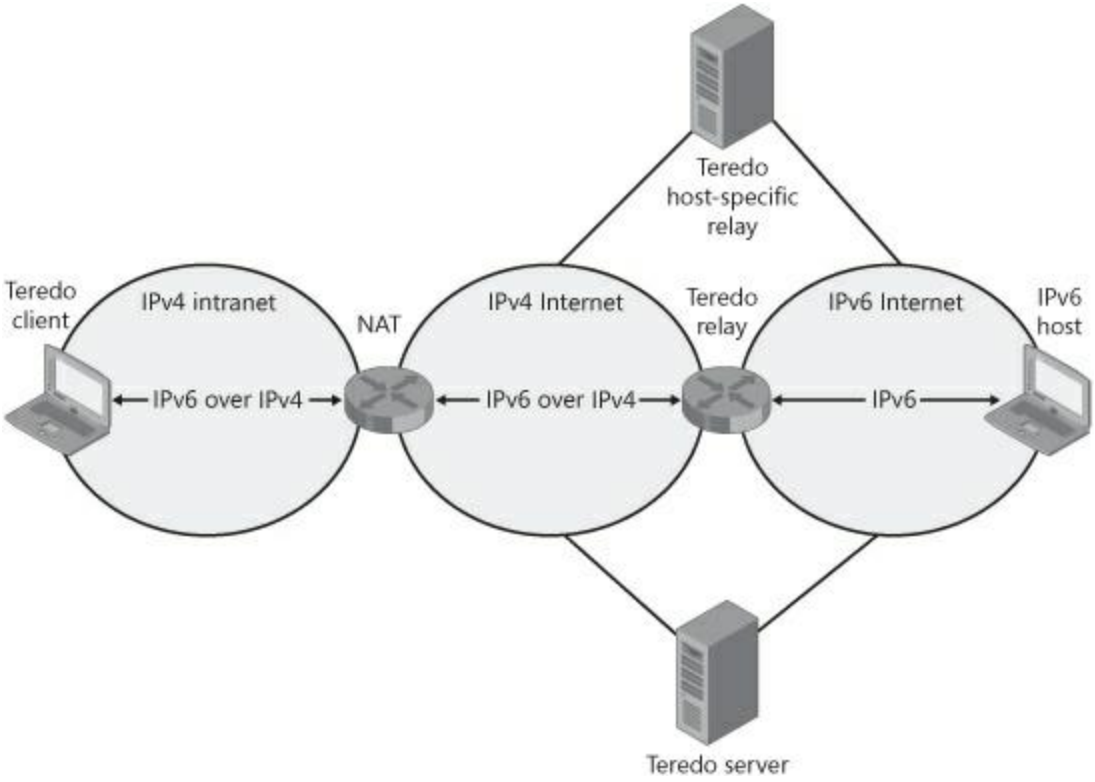


6to4 allows IPv6-only hosts to communicate over the Internet.

Teredo

Teredo is a tunneling protocol that allows clients located behind an IPv4 NAT device to use IPv6 over the Internet. Teredo is used only when no other IPv6 transition technology (such as 6to4) is available.

Teredo relies on an infrastructure, illustrated in Figure 1-54, that includes Teredo clients, Teredo servers, Teredo relays, and Teredo host-specific relays.



Teredo allows hosts located behind IPv4 NAT to use IPv6 over the Internet to communicate with each other or with IPv6-only hosts.

The following list describes each of these Teredo components:

- **Teredo client.** A Teredo client is a computer that is enabled with both IPv6 and IPv4 and that is located behind a router performing IPv4 NAT. The Teredo client creates a Teredo tunneling

interface and configures a routable IPv6 address with the help of a Teredo server. Through this interface, Teredo clients communicate with other Teredo clients or with hosts on the IPv6 Internet (through a Teredo relay).

- **Teredo server.** A Teredo server is a public server connected both to the IPv4 Internet and to the IPv6 Internet. The Teredo server helps perform the address configuration of the Teredo client and facilitates initial communication either between two Teredo clients or between a Teredo client and an IPv6 host.

To facilitate communication among Windows-based Teredo client computers, Microsoft has deployed Teredo servers on the IPv4 Internet.

- **Teredo relay.** A Teredo relay is a Teredo tunnel endpoint. It is an IPv6/IPv4 router that can forward packets between Teredo clients on the IPv4 Internet and IPv6-only hosts.
- **Teredo host-specific relay.** A Teredo host-specific relay is a host that is enabled with both IPv4 and IPv6 and that acts as its own Teredo relay. A Teredo host-specific relay essentially enables a Teredo client that has a global IPv6 address to tunnel through the IPv4 Internet and communicate directly with hosts connected to the IPv6 Internet.

Windows computers include Teredo host-specific relay functionality, which is automatically enabled if the computer has a global address assigned. If the computer does not have a global address, Teredo client functionality is enabled.

IP-HTTPS

IP-HTTPS is a new protocol developed by Microsoft for Windows 7 and Windows Server 2008 R2. It enables hosts located behind a web proxy server or firewall to establish connectivity by tunneling IPv6 packets inside an IPv4-based Hypertext Transfer Protocol Secure (HTTPS) session. HTTPS is used instead of HTTP so that web proxy servers do not attempt to examine the data stream and terminate the connection. IP-HTTPS can be used as the fallback technology for clients when other IPv6 transition technologies are unavailable.