

## Exploring IPv6

*Although IPv4 has been* the primary IP addressing scheme used on the Internet and within internal networks for many years, IPv6 is also being used today. The differences are significant, and even technicians who have mastered IPv4 have a lot to learn to master IPv6. This includes the basics of an IPv6 address, its different components, how IPv4 and IPv6 coexist, and how you can assign IPv6 addresses.

- ▶ **Understanding IPv6 addresses**
- ▶ **Exploring the components of an IPv6 address**
- ▶ **Understanding the dual IP stack**
- ▶ **Comparing manual and automatic assignment of IPv6**

### Exploring IPv6 Addresses

IPv4 uses 32 bits and can address about 4 billion addresses. When the Internet was in its infancy, 4 billion addresses seemed like they would last forever—they didn't. The astronomical growth of the Internet resulted in the concern that we may run out of IPv4 addresses, so IPv6 was created.

IPv6 uses 128 bits and can address more than 340 undecillion IP addresses. That's more than 340,000,000,000,000,000,000,000,000,000,000,000,000,000,000 addresses, or more than 340 trillion, trillion, trillion addresses. This will be enough addresses to last quite a while. IPv4 lasted a few decades before needing an upgrade. Perhaps in the year 2040 a newer version of IP will come out to give us some more addresses.

IPv6 is slowly replacing IPv4 on the Internet and on internal networks. In addition to adding more IP addresses, it includes many new capabilities that simply aren't available in IPv4.

You'll easily be able to tell the difference between an IPv4 address and an IPv6 address just by looking at it. IPv6 addresses are displayed as hexadecimal characters instead of the dotted decimal format of IPv4.

▶  
**IPv5 used 64 bits. It was never adopted since designers realized the Internet would quickly run out of IP addresses again if it was adopted.**

The IPv6 address starts with fe80, indicating it is a link-local address. Other types include global and unique local addresses.

As an example, Figure 6.1 shows the IPv4 and IPv6 addresses of a Windows Server 2008 server. The IPv6 address is fe80::184:e9f8:a71b:304:10. The %10 at the end of the IPv6 address is a zone index and identifies the network interface card.

```

Administrator: Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . . : 
    Link-local IPv6 Address . . . . . : fe80::184:e9f8:a71b:304:10
    IPv4 Address. . . . . : 192.168.1.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
  
```

FIGURE 6.1 Viewing IPv4 and IPv6 addresses

## Comparing IPv4 Classes and IPv6 Prefixes

Chapter 5 presented IPv4 classful addresses (Class A, Class B, and Class C). A classful IP address is identified by the first decimal in the IP address. For example, an IP address of 10.80.1.1 has 10 as the first decimal, which is in the Class A range of 1 to 126.

Similarly, an *IPv6 prefix* identifies the type of IPv6 address. As an example, Figure 6.1 showed an IP address starting with fe80, which is a link-local address. You'll see many other prefixes in this chapter that identify specific types of IPv6 addresses.

Prefixes often are accompanied by a prefix notation similar to /3 or /32. This indicates how many bits are in the prefix. For example, 2001 /3 indicates only the first three bits are in the prefix, but 2001:0000 /32 indicates the first 32 bits are in the prefix.

As an introduction, Table 6.1 summarizes the prefixes covered in this chapter.

TABLE 6.1 Common IPv6 prefixes

IPv6 prefix	Description
2 /3	Global unicast addresses. These commonly start with 2001:, but other prefixes starting with 2 are possible.
2001:0000 /32	Teredo tunneling protocol address. This is used for IPv4 and IPv6 compatibility.

(Continues)

The IPv6 prefix notation is similar to CIDR notation in IPv4. It indicates how many bits are a 1 in the subnet mask.

**TABLE 6.1** (Continued)

IPv6 prefix	Description
fe80 /10	Link-local addresses. These are similar to IPv4 APIPA addresses.
fc /7 (fd /8)	Unique local unicast addresses. These are IPv6 addresses assigned in an internal network similar to IPv4 private addresses. The prefix is only 7 bits, which is literally identified as fc in hexadecimal, but the 8th bit is always a 1, so this is always seen as fd in an IPv6 address.
::1	Loopback address. A prefix of 127 zeros followed by a single 1 as the 128th bit is the loopback address. This is similar to the IPv4 loopback address of 127.0.0.1.

## Understanding Hexadecimal

IPv6 addresses are displayed in hexadecimal, so it's important to understand hexadecimal numbers. Chapter 5 introduced binary and compared it to decimal. As a reminder, decimal uses a base of 10 with numbers from 0 through 9, and binary uses a base of 2 with 0 and 1 as the only two values.

Hexadecimal uses a base of 16 with the numbers 0 through 9 followed by *a* through *f*. Each hexadecimal number can be represented using four binary bits. Table 6.2 shows how to count from 0 through F in hexadecimal and includes both the binary and decimal values for each number.

**TABLE 6.2** Hexadecimal values

Hexadecimal number	Binary value				Decimal value
	2 <sup>3</sup>	2 <sup>2</sup>	2 <sup>1</sup>	2 <sup>0</sup>	
0	0	0	0	0	0
1	0	0	0	1	1
2	0	0	1	0	2
3	0	0	1	1	3

Hexadecimal values can be either uppercase or lowercase. For example, f is the same as F. IPv6 addresses are commonly displayed in lowercase.

(Continues)

**TABLE 6.2** (Continued)

Hexadecimal number	Binary value				Decimal value
	2 <sup>3</sup> 8	2 <sup>2</sup> 4	2 <sup>1</sup> 2	2 <sup>0</sup> 1	
4	0	1	0	0	4
5	0	1	0	1	5
6	0	1	1	0	6
7	0	1	1	1	7
8	1	0	0	0	8
9	1	0	0	1	9
a	1	0	1	0	10
b	1	0	1	1	11
c	1	1	0	0	12
d	1	1	0	1	13
e	1	1	1	0	14
f	1	1	1	1	15

## Displaying IPv6 Addresses

When a full IPv6 address is displayed, it will include eight groups of four hexadecimal numbers, separated by colons similar to this:

```
fe80:0000:0000:0000:0184:e9f8:a71b:0304
```

However, you can shorten the IPv6 address using two techniques. First, you can use zero compression to identify a contiguous group of zeros. Zero compression replaces a group of zeros with two colons. Second, you can drop leading zeros in any hexadecimal grouping. Table 6.3 shows the three ways you can display the same IPv6 address.

**TABLE 6.3** Displaying an IPv6 address

Example	Description
fe80:0000:0000:0000:0184:e9f8:a71b:0304	Full IPv6 address
fe80::0184:e9f8:a71b:0304	IPv6 address using zero compression
fe80::184:e9f8:a71b:304	IPv6 address using zero compression and dropping leading zeros

It's important to note that you can use only one set of double colons. In the example (fe80::0184:e9f8:a71b:0304), five groups of hex numbers are displayed. Since an IPv6 address has eight groups of hex numbers, the double colon (::) takes the place of three groups of zeros (0000:0000:0000).

However, if a number had two groups of double colons (for example fe80::0184:e9f8::0304), there would be no way to determine how many groups of zeros each double colon represents. In other words, you can have only one set of double colons in an IPv6 address. Two sets of double colons are not valid in an IPv6 address.

## Comparing IPv6 Transmission Types

Chapter 2 introduced the three methods of transmission for IPv4 as unicast, multicast, and broadcast. As a reminder, these transmissions are as follows:

**Unicast** Traffic sent from one computer to one other computer

**Broadcast** Traffic sent from one computer to all other computers on the same subnet

**Multicast** Traffic sent from one computer to multiple other computers using the IGMP protocol

IPv6 uses three types of transmission known as unicast, multicast, and anycast. These have some similarities to IPv4.

**Unicast** An IPv6 unicast transmission is traffic sent from one computer to one other computer, just as it works in IPv4.

**Multicast** An IPv6 multicast transmission is traffic sent from one computer to multiple other computers, similar to multicast in IPv4. IPv6 provides some improvements in multicasting.

▶  
Anycast is some-  
times called one-to-  
one-of-many.

**Anycast** An IPv6 anycast transmission is traffic sent from one host to one other host from a list of multiple hosts. It is typically used to locate the nearest router or to locate services on the network.

## Understanding the Need for IPv6

The primary driving force of IPv6 was to provide more IP addresses. If only IPv4 addresses were used, experts predicted that the Internet would run out of IPv4 addresses sometime in 2011. Earlier predictions indicated the Internet was on track to run out of addresses during 1990s or 2000s, but steps were taken to extend its lifetime. For example, Network Address Translation (NAT) helped reduce the number of public IP addresses needed.

As mentioned previously, IPv4 uses 32 bits in the IP address. The math shows that 2 raised to the 32nd power ( $2^{32}$ ), or 2 times itself 32 times, equals 4,294,967,296, which is more than 4 billion addresses. However, because of how IPv4 reserved so many different IP address ranges, there are only about 3.7 billion IP addresses available on the Internet. No one wants to see the growth of the Internet stop, and with the 128 bits in an IPv6 address, it has plenty of room for growth.

In addition to providing trillions of trillions more IP addresses, IPv6 also provides several improvements:

**Native Support for IPSec** IPv6 supports Internet Protocol Security (IPSec) without any additions. This allows clients to easily encrypt IPv6 data. IPv4 can use IPSec, but it takes extra effort to make it work.

**More Efficient Routing** IPv6 uses global addresses on the Internet. These are designed for worldwide delivery and reduce the number of routes that Internet routers need to remember. In contrast, many Internet backbone routers maintain routing lists of more than 85,000 IPv4 routes.

**Easy Host Configuration** IPv6 routers can automatically configure internal computers. You can also use Dynamic Host Configuration Protocol version 6 (DHCPv6) servers to provide IPv6 information. However, even if an IPv6 router or DHCPv6 server isn't available, systems can configure themselves with internal IPv6 addresses.

## Understanding Neighbor Discovery

Neighbor Discovery (ND) is an IPv6 protocol that uses Internet Control Message Protocol version 6 (ICMPv6) messages to discover details about the network.

▶  
Chapter 11 explains  
NAT in more depth.

It performs several key functions:

**Discovers Routers** ND identifies routers on the local subnet. These routers can then be queried for IPv6 configuration.

**Discovers Prefixes** The prefix is used in IPv6 similar to how the subnet mask is used in IPv4. ND identifies the prefix used by other hosts on the subnet.

**Discovers Parameters** ND messages tell the computer what IPv6 parameters are being used by other hosts on the subnet.

**Address Autoconfiguration** This determines whether the host can obtain an IP address from a router or a DHCPv6 server. If not, it assigns itself a link-local address, which is similar to IPv4's APIPA addressing.

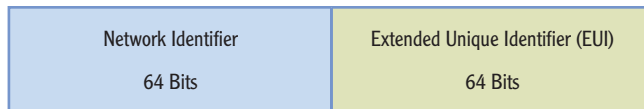
**Detects Duplicate Addresses** This prevents the computer from using an IPv6 link-local address that is already in use.

**Resolves Addresses** ND can resolve a neighbor's IPv6 address to its link-layer address. This is similar to how the Address Resolution Protocol (ARP) resolves IP addresses to MAC addresses in IPv4.

## Exploring the Components of an IPv6 Address

An IPv4 address has a network ID component and a host ID component. Similarly, an IPv6 address has a network identifier and interface identifier components.

Figure 6.2 shows the two basic components of the IPv6 address used on a Windows Server 2008 server. In IPv6, the first 64 bits are typically the network ID, and the last 64 bits are typically the interface identifier, though there are exceptions.



**FIGURE 6.2** The components of an IPv6 address

The interface identifier is similar to the Media Access Control (MAC) address, or physical address used in IPv4. You may remember that the MAC is a group of 48 bits expressed as 12 hexadecimal numbers similar to this: 12:34:56:78:9A:BC.

IPv4-mapped IPv6 addresses and Teredo addresses differ from this basic format, but they still have 128 bits.

EUI-48, EUI-60, and other alternatives are also available. However, Windows Server 2008 uses EUI-64.

The first six hex numbers are the organizational unique identifier (OUI) identifying the manufacturer, and the last six are unique on the network interface card.

In an IPv6 address, the interface identifier (the last 64 bits) is used in place of the MAC address. Windows Server 2008 uses an EUI 64-bit address (EUI-64) defined as part of IPv6. Gigabit network interface cards are configured with EUI-64 addresses. IPv6 uses the 48-bit MAC addresses on older cards and adds 16 extra bits to reach 64 bits.

The interface identifier can also be created using other methods:

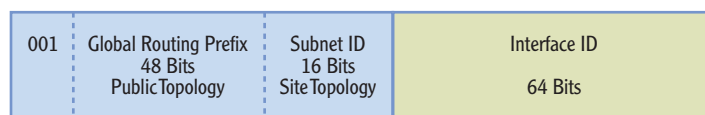
- ▶ A randomly generated temporary identifier
- ▶ A randomly generated permanent identifier
- ▶ A manually assigned identifier

These alternative interface identifiers provide a level of privacy in network communication by hiding the actual identifier of the host.

## Understanding Global Unicast Addresses

*Global unicast addresses* are used on the Internet. You can compare them to IPv4 public IP addresses. However, global unicast addresses are designed for hierarchical routing, which makes them easier to route throughout the Internet.

Figure 6.3 shows the components of a global unicast address. Notice that the first three bits are 001. If the first number of the address is a 2, you know that it is a global unicast address used on the Internet.



001 (2) – First Three Bits 001 (Hex 2) Identify a Global Unicast Address  
Most Global Unicast Addresses Start with 2001:  
Used on the Internet

**FIGURE 6.3** IPv6 global unicast address

The formal definition for global unicast addresses says that only the first three digits are specified as 001, meaning that it could be 0010 (hex 2) or 0011 (hex 3). However, 0011 is reserved and can't be used. In other words, the first number will always be a 2.

Although a wide range of global unicast addresses are possible, the most common one used is 2001. IPv6 global unicast addresses are assigned by the Internet



Assignment Numbers Authority (IANA). They have assigned several banks of IPv6 addresses starting with 2001 (such as 2001:0000, 2001:0200, 2001:0400, and so on). They have also assigned some addresses starting with 2400, 2600, and more, but 2001 remains the most popular.

The first 48 bits of the global unicast address make up the public topology, and the next 16 bits make up the site topology. Addresses in public topology are assigned to Internet service providers (ISPs). ISPs can then use the 16 bits in the site topology to create as many as 65,536 subnets, with each subnet having more than 18 quintillion addresses each.

You can read more about global unicast addresses in the document “IPv6 Global Unicast Address Format” at [www.ietf.org/rfc/rfc3587.txt](http://www.ietf.org/rfc/rfc3587.txt).

◀ You probably know thousands, millions, and billions. What’s next? Trillions, quadrillions, quintillions, sextillions, and more.

## Understanding Link-Local Addresses

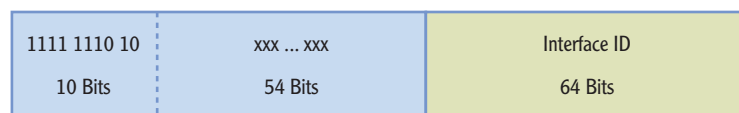
In Chapter 5, you learned about Automatic Private Internet Protocol Addressing (APIPA) addresses. When a DHCP client is unable to reach a DHCP server, it assigns itself an IP address in the 169.254.x.y range.

*Link-local addresses* are similar to APIPA addresses. If a DHCPv6 server or an IPv6 router isn’t available to assign an IPv6 address, an IPv6 client can assign itself a link-local address to communicate with other hosts on the same network. Just as APIPA limits communication to the local subnet, a link-local address limits a client to communication only on the local subnet. This is because link-local addresses are not routable.

However, IPv6 clients can also have another IPv6 address in addition to the link-local address. For public systems, they can also have a global unicast address. For private systems, they can also have a unique local address. The link-local address is used to communicate with local nodes, and the other address is used to communicate with clients past the router.

In contrast, IPv4 uses APIPA as a fallback when a DHCP client doesn’t receive a DHCP address. In IPv4, you’ll have only one address assigned.

Figure 6.4 shows the format of a link-local address. Notice that the first 10 bits are always 1111 1110 10. This equates to fe80 in hexadecimal.



1111 1110 10 (fe80) – fe80/10 Identifies a Link-Local Address  
Similar to APIPA in IPv4

◀ Link-local IPv6 addresses always start with fe80.

**FIGURE 6.4** IPv6 link-local address

Microsoft recommends leaving IPv6 enabled on all systems.

If IPv6 is installed on a system, a link-local address will always be configured. Microsoft systems use the link-local address for Neighbor Discovery processes, and these processes won't work if IPv6 is not enabled on the system.

Autoconfiguration of IPv6 addresses is either stateless or stateful.

**Stateless** The configuration is performed based on router advertisements. The system will start with a self-assigned fe80 address and then go through a process to verify it and learn about the network by communicating with local routers.

**Stateful** The configuration is performed by a DHCPv6 server. The “Using DHCP” section later in this chapter presents the process used by a DHCPv6 client and a DHCPv6 server.

Early documentation specified the use of site-local addresses starting with a prefix of fec0::/10. You may still see this in some documentation; however, the use of site-local addresses has been deprecated and is not recommended.

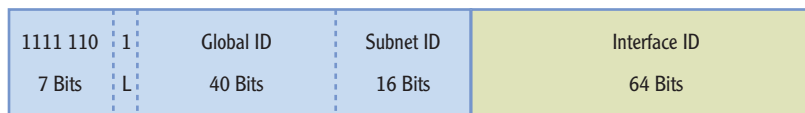
You can read more about unique local addresses in the paper “IPv6 Stateless Address Autoconfiguration” at <http://tools.ietf.org/html/rfc4862>.

## Understanding Unique Local Addresses

*Unique local addresses* are IPv6 addresses used in an internal network. They are similar to IPv4 private IP addresses in that you assign them to computers on your internal network.

Figure 6.5 shows the format of unique local addresses. Unique local addresses are identified by the first seven bits as 1111 110. Additionally, the 8th bit is always a 1.

Unique local IPv6 addresses always start with an IP prefix of fd.



1111 1100 – fd00: Prefix Identifies a Unique Local Address  
Similar to Private IPv4 Addresses  
Used on Internal Networks

**FIGURE 6.5** IPv6 unique local unicast addresses

You can dig into the details of unique local addresses in the paper “Unique Local IPv6 Unicast Addresses” at <http://tools.ietf.org/html/rfc4193>.

## FC OR FD FOR UNIQUE LOCAL ADDRESSES?

Some documentation indicates that a unique local address has the first seven bits to 1111 110, giving it a 7-bit prefix of fc hexadecimal. Other documentation indicates that all unique local IPv6 addresses start with a prefix of fd hexadecimal. Which one is correct? Actually both.

RFC 4193 defines unique local addresses and specifies the eighth bit should be a 1. This “L” bit indicates the address is locally assigned. RFC 4193 states that the value of 0 for the “L” bit may be defined in the future, but for now it’s always a 1.

If only the first seven bits are counted (1111 110), then the eighth bit is implied as a zero. This gives a value of binary value 1111 1100, or fc in hex. However, if the eighth bit is a 1 in the actual IPv6 address, then the first eight bits are 1111 1101, which equates to fd.

In other words, if you see the full IPv6 address, the prefix is fd in hex. If only the first seven bits are represented, the value is fc in hex.

## Understanding the Dual IP Stack

In a perfect world, every computer on the Internet could switch from IPv4 to IPv6 on a specific day. For example, November 9, 2010, could have been designated international IPv6 day, and everyone in the world could have magically switch each computer’s configuration at midnight Greenwich mean time. No one realistically envisions such as a perfect world, though.

Instead, IPv4 and IPv6 must be able to interoperate side by side. IPv6 is currently working on the Internet and will gradually replace IPv4. In the meantime, operating systems and routers support IPv4-mapped IPv6 addresses and Teredo tunneling.

### Using IPv4-Mapped IPv6 Addresses

One way that the IPv4/IPv6 dual IP stack works is by supporting IPv4-mapped IPv6 addresses. Figure 6.6 shows an IPv4-mapped IPv6 address. The first 80 bits are set to 0, the next 16 bits are set to 1, and the last 32 bits hold the IPv4 address.



::ffff:192.168.1.5

**FIGURE 6.6** IPv4-mapped IPv6 address

The IPv4-mapped IPv6 address is expressed with the leading zeros omitted with zero compression (using a double colon, ::), the 16 ones expressed as ffff, and the IPv4 address in traditional dotted decimal format.

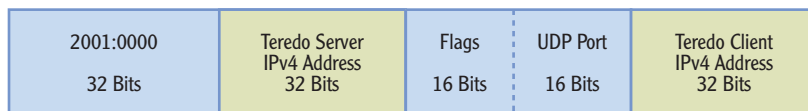
## Understanding IPv4 to IPv6 Tunneling Protocols

Some devices accessible from the Internet aren't yet IPv6 enabled. If only IPv6 was used, data couldn't transit through these devices. *Teredo* is a tunneling protocol that encapsulates IPv6 packets within IPv4 datagrams. This allows the IPv6 packets to transit through these devices.

Teredo is needed for NAT devices that translate private IPv4 addresses to public IPv4 addresses and translate public IPv4 addresses back to private IPv4 addresses. Once IPv6 is fully implemented, Teredo won't be needed anymore.

If Teredo traffic needs to pass through a firewall, the firewall must be configured to allow the Teredo traffic to pass through. By default, a firewall will block traffic using a Teredo tunnel.

Figure 6.7 shows the mapping of a Teredo IPv6 address.



2001:0000/32

**FIGURE 6.7** Teredo IPv6 address

You can tell whether your system is using Teredo by entering **ipconfig /all** at the command prompt. Listing 6.1 shows a partial output from a system that has a Teredo address assigned. Notice the prefix is 2001:0.

**Listing 6.1** Partial result of `ipconfig /all`

```
Tunnel adapter Local Area Connection* 18:
```

Teredo clients have an IPv6 address that starts with 2001:0000/32. This is known as the Teredo prefix.

```

Connection-specific DNS Suffix . . . :
Description . . . . . : Teredo Tunneling
Pseudo-Interface
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . :
2001:0:4137:9e76:4c9:399b:3f57:fe98(Preferred)
Link-local IPv6 Address . . . . . :
fe80::4c9:399b:3f57:fe98%39(Preferred)
Default Gateway . . . . . : ::
NetBIOS over Tcpi. . . . . : Disabled

```

6to4 is another method that used to help the migration between IPv4 and IPv6. It allows IPv6 traffic to be transmitted over an IPv4 network and is popular with routers used in small offices and home offices (SOHOs).

## Comparing Manual and Automatic Assignment of IPv6

Just as you can assign IPv4 addresses manually or via DHCP, you can also assign IPv6 manually or with DHCPv6. Both processes are very similar in IPv4 and IPv6.

### Manually Configuring IPv6

You can use the following steps to manually view or configure the IPv6 information on a Windows Server 2008 server:

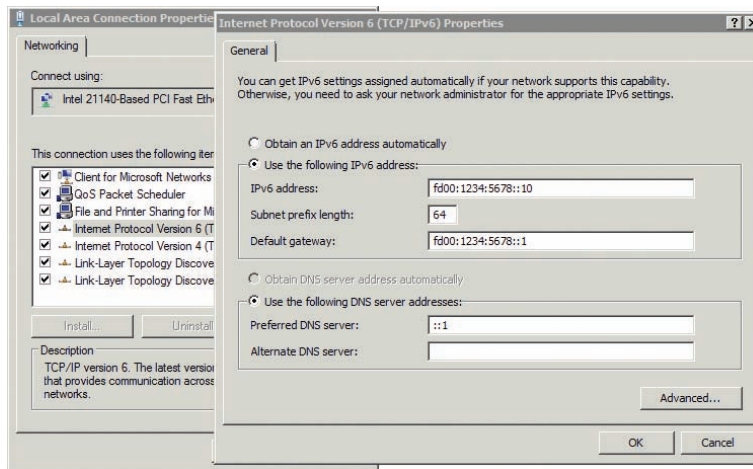
1. Click Start > Control Panel.
2. Type Network in the Control Panel Search box.
3. Select Network And Sharing Center.
4. Click Manage Network Connections in the Tasks pane on the left.
5. Right-click Local Area Connection, and select Properties.
6. Select Internet Protocol Version 6 (TCP/IPv6), and click Properties. Your display will look similar to Figure 6.8.
7. Enter the appropriate IP address, subnet mask, default gateway, and address of a DNS server. In the figure, the server is also the DNS server, so the DNS server is set to the IPv6 loopback address of ::1.

Although these steps work on Windows Server 2008, you can also use them on a Windows 7 system.



You can view the information without changing it. If you are using link-local addresses or a DHCPv6 server, it will be set to Obtain An IP Address Automatically.





**FIGURE 6.8** Viewing the IPv6 configuration of the NIC

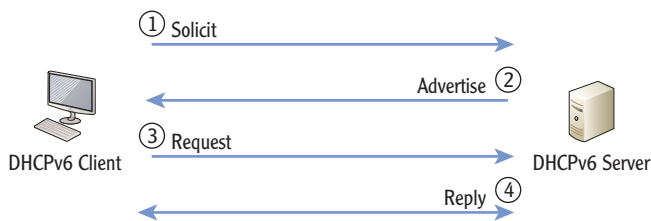
## Using DHCPv6

Just as you can use DHCP to assign TCP/IP information for IPv4 clients, you can also use DHCPv6 to assign TCP/IP information for IPv6 clients. The process is similar. The benefit is that you can assign all the TCP/IP information including the IP addresses of DNS servers, default gateways, and more. The system can configure itself with link-local addresses, but link-local addresses won't provide access outside the subnet since they are not routable and won't include addresses of DNS servers.

Figure 6.9 shows the process of a DHCPv6 client receiving an IPv6 address from a DHCPv6 server.

1. When the DHCPv6 client turns on, it sends a solicit message looking for a DHCPv6 server.
2. The DHCPv6 server answers with an Advertise message. This lets the client know that the server can offer IPv6 configuration information.
3. The DHCPv6 client replies with a Request message formally requesting the IPv6 information.
4. The DHCPv6 server responds with a Reply message. This message includes IPv6 information such as the IPv6 address, the default gateway, and the address of a DNS server.

DHCPv6 servers aren't required on each subnet. If your network includes multiple subnets, you can place DHCPv6 relay agents on each subnet to listen for the DHCPv6 solicit messages and then forward them to the DHCPv6 server. The relay agent then acts as the intermediary, or the proxy, for the four messages going back and forth between the DHCPv6 server and the DHCPv6 client.



**FIGURE 6.9** DHCPv6 process

## THE ESSENTIALS AND BEYOND

In this chapter, you learned about IPv6 addresses. IPv6 is slowly replacing IPv4, and it uses 128 bits instead of the 32 bits used in IPv4. IPv6 addresses are displayed in hexadecimal, and the type of IPv6 address is identified by the prefix. Global unicast addresses start with a prefix of 2 /3. Teredo tunneling protocol addresses (used for IPv4 to IPv6) start with a prefix of 2001:0000 /32. Link-local addresses (automatically assigned) start with fe80 /10. Unique local addresses (private IPv6 addresses) start with fd and are sometimes referenced as fc /7.

### ADDITIONAL EXERCISES

- ▶ Identify whether your computer has an IPv6 address. If so, determine the type of address based on the prefix.
- ▶ Ping the IPv6 loopback address. This is possible only if your computer has an IPv6 address. If your computer doesn't have an IPv6 address, identify the IPv6 loopback address.
- ▶ Use the `ipconfig /all` command to determine whether you have a Teredo address assigned.
- ▶ View the current IPv6 configuration of the network interface card. Document the current settings of the IP address, prefix, default gateway, and DNS server.

To compare your answers to the author's, please visit [www.sybex.com/go/networkingessentials](http://www.sybex.com/go/networkingessentials).

### REVIEW QUESTIONS

1. Which of the following addresses is a valid IPv6 address?
 

<b>A.</b> 192.168.1.256	<b>C.</b> 2001:0000:4137:9e76:3c2b:05ad:3f57:fe98
<b>B.</b> 10.1.25.2	<b>D.</b> 2001:0000:4137:9g76:3c2b:05zd:3x57:gh98

*(Continues)*

**THE ESSENTIALS AND BEYOND** *(Continued)*

2. You need to manually assign an IPv6 address to a client computer for use within a private network. Which one of the following addresses should you use?
  - A. 0000::a123:4567:89ab:cdef
  - B. 2001:0001::fcde:ba98:7654
  - C. 2001:0000: fcde:ba98:7654
  - D. fe80:: a123:4567:89ab:cdef
  - E. fd00:: a123:4567:89ab:cdef
3. Which of the following features is built into IPv6 to provide extra security?
  - A. Teredo tunneling
  - B. Global addresses
  - C. Unique local addresses
  - D. IPSec
4. True or false. An IPv6 address with a prefix of fd is a link-local address.
5. What IPv6 to IPv4 technology uses tunneling to encapsulate an IPv6 packet within an IPv4 packet?
6. You need to assign IPv6 addresses to hosts on a private network. You should use \_\_\_\_\_ addresses.
7. What IPv6 protocol is used to identify routers on the same network?
  - A. Network Discovery
  - B. Teredo
  - C. IGMP
  - D. Anycast
8. IPv4 addresses use public address on the Internet. IPv6 uses \_\_\_\_\_ addresses on the Internet.