8

CHAPTER

IPV6

Chapter Outline

Objectives

- Develop an understanding of the fundamentals of IPv6
- Define the structure of IPv6
- Understand the IPv6 addressing and its prefix
- Be able to represent the IPv6 with correct notation
- Be able to configure basic IPv6 on computers
- Be able to configure basic IPv6 on routers
- Recognize the IPv6 stateless autoconfiguration settings
- Be able to provide basic IPv6 troubleshooting

Key Terms

IPv6
IPng
datagram
IPsec
stateless address autoconfiguration (SLAAC)
full IPv6 address
double-colon notation
network prefix
prefix length
interface identifier
unicast address
global unicast address
multicast address
anycast address
6to4 prefix
FP
TLA ID (0x2002)
V4ADDR
SLA ID
Interface ID
IPv6 stateless autoconfiguration
link-local address
FE80::/64
Neighbor Solicitation
Duplicate Address Detection (DAD)
Privacy Extensions for Stateless Address Autoconfiguration
MLD (Multicast Listener Discovery)
ipv6 unicast-routing
ipv6 enable
show ipv6 interface
ipv6 address *ipv6 interface address*
eui-64
ND protocol
RA messages
router solicitation messages
2001:DB8::/32 Prefix
RIPng
rip_tag
OSPFv3
ping6
traceroute6/tracert6

INTRODUCTION

This chapter looks at IPv6, the IP addressing system that has been developed to replace IPv4. IP version 4 (IPv4) is the current TCP/IP addressing technique being used on the Internet. The address space for IPv4 is running out, even though there is a theoretical limit of approximately 4.3 billion unique IPv4 addresses. However, not all the IPv4 addresses can be used, because there are IPv4 address blocks reserved for special purposes, such as multicast, unspecified future use, local identification, loopback, and private use. These special purpose reserved addresses account for around 600 million unique addresses.

Address space for IPv4 is quickly running out due to the rapid growth of the Internet and the development of new Internet-compatible mobile technologies. Examples of this include the IP addressable telephone, wireless personal digital assistants (PDAs), cell phones, game consoles, and home-networking systems. There have been many predictions of when the IPv4 address pool will be exhausted. The answer to this question is not clear. Techniques such as Network Address Translation/Port Address Translation (NAT/PAT), Dynamic Host Control Protocol (DHCP), and Classless Inter-Domain Routing (CIDR) have been implemented to prolong the life of IPv4. These techniques reuse the existing IPv4 address space and handle the address space allocation more efficiently.

IPv6
IP version 6.

IPng
Next generation IP.

A solution to the limited number of available IPv4 addresses is to migrate to IPv6. IP version 6 (**IPv6**) is the solution proposed by the Internet Engineering Task Force (IETF) for expanding the possible number of IP addresses to accommodate the growing users on the Internet. IPv6, introduced in 1999, is also called **IPng**.

This chapter provides a comparison of IPv6 and IPv4 in Section 8-1. The structure of the IPv6 address is examined in Section 8-2. Concepts such as the network prefix and the prefix length are examined. IPv6 network settings are examined in Section 8-3. Steps for configuring IPv6 in both the Windows and Mac OS X environments are examined. The steps for configuring a router to run IPv6 are examined in section 8-4. This chapter concludes with a look at troubleshooting the IPv6 connection in Section 8-5.

8-1 COMPARISON OF IPV6 AND IPV4

IPv4 and IPv6 are not compatible technologies, and they cannot communicate directly with each other. So, before migrating to an IPv6 environment, the network devices and network equipment need to be IPv6 compatible or enabled. Most likely new network hardware and software will have to be acquired to make the network IPv6 ready. A good migration plan has to be developed to prepare for IPv6. The investment of time, money, and training is required for a successful adoption of IPv6.

The size of the IPv6 address is increased to 128 bits, which is four times larger than the 32-bit address space IPv4 is using. This significantly increases the number of available IP addresses. By doing this, the theoretical number of unique addresses increases from 4.3x109 (IPv4) to 3.4x1038 in IPv6. This is a staggering number considering the world population is 7x109 people.

Increasing the number of bits for the address also results in changing the IP header size. The IPv4 **datagram** is shown in Figure 8-1. A datagram is a self-contained entity that carries sufficient information to be routed from source to destination without relying on previous data exchanges between the source and destination computers or the transporting network.

Datagram
A self-contained entity that carries sufficient information to be routed from source to destination without relying on previous data exchanges between the source and destination computers or the transporting network.

The IPv4 header size is comprised of the information detailed in Figure 8-1. A total of 64 bits are used to define the source and destination IP addresses. Note that both the source and destination addresses are 32 bits in length. The combination of the two gives 64 bits. The total length of the IPv4 header is 160 bits; therefore, this means 160 – 64 = 96 bits are used to make up the remaining fields.

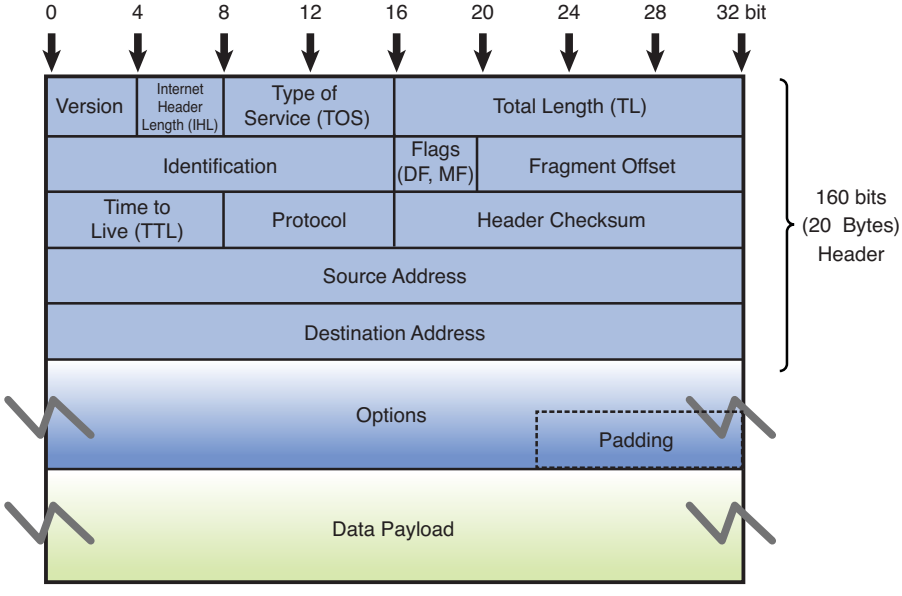

FIGURE 8-1 The IPv4 Datagram (160 bits-96 bits for header fields)

Figure 8-2 shows the IPv6 datagram. The IPv6 header size is 320 bits; however, 256 bits are used to define the source and destination IPv6 addresses. This means that 64 bits are used to define the remaining field as compared to 96 bits for IPv4.

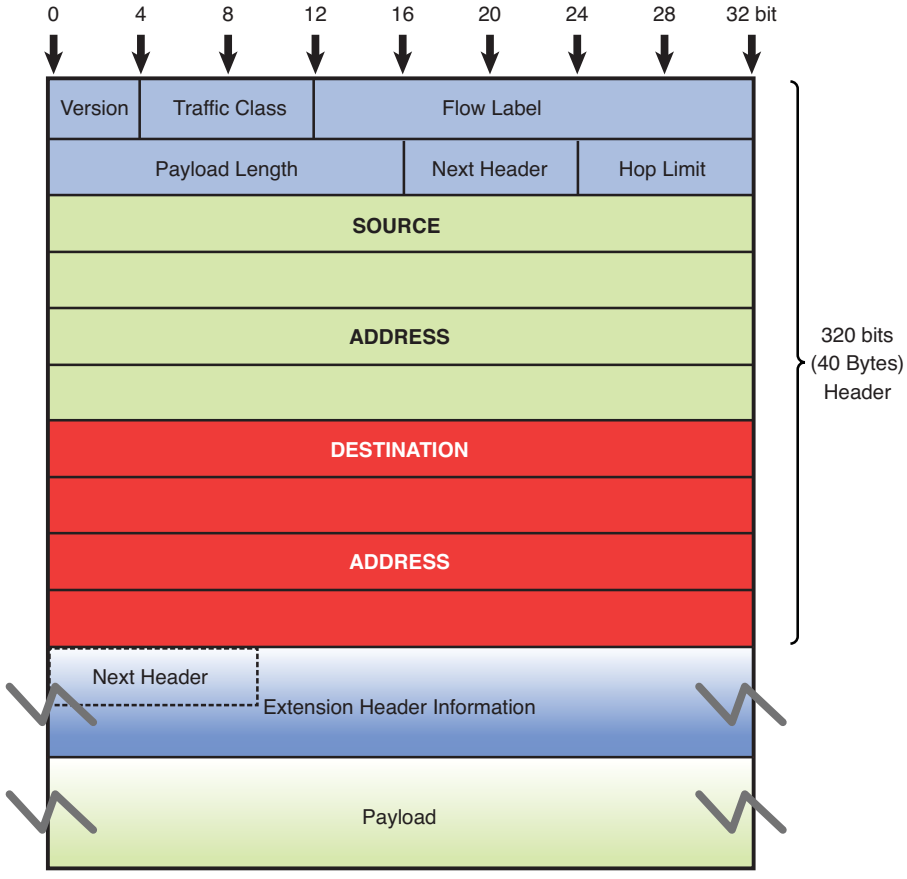

FIGURE 8-2 The IPv6 Datagram (320 bits-64 bits for header fileds)

The IPv6 header has been simplified resulting in less header fields than in IPv4. This is designed to make packet processing more efficient by routers and other network equipments. One noticeably missing header field in IPv6 is the checksum field. This means there is no checksum calculation done by the routers in the path. This increases the routing performance and efficiency. The error detection is now done at the link layer and transport layer. In IPv4, the TCP transport layer is required to check the integrity of the packet by doing a checksum calculation. The same cannot be said for the UDP transport layer because the checksum is optional. Now, the checksums are required for both transport layers in IPv6.

IPsec
The IETF standard for securing the IP communications between the network nodes by authenticating and encrypting the session.

One new feature that is built in with IPv6 is the IP security (IPsec). **IPsec** is the IETF standard for securing the IP communications between the network nodes by authenticating and encrypting the session. When using IPv4, a secure network IP communication link generally has to be initiated to provide security similar to an IPSec application. In IPv6, every node is enabled with the IPSec feature. This makes creating end-to-end IPSec sessions much easier to establish. In addition, IPSec feature is a part of the extension headers. In IPv6, there is a mandatory IPv6 main header and then there could be an extension header or extension headers. All

options and special purposed fields can be provisioned into extension headers when needed. IPSec is one of the special options. This is how IPv6 simplifies its header fields.

Another giant step forward taken by IPv6 is the elimination of the broadcast. Broadcasts can cause many problems in computer networks. When a broadcast happens, every computer on the network is interrupted, even if only two computers are involved. The worst case situation is a broadcast storm. When this happens, the performance on a network is severely degraded, and it can bring down an entire network. IPv6 does not use broadcasts. It uses multicasts instead. A multicast is used in the core of many functions in IPv6. The multicast addresses are allocated from the multicast block. Any address starting with "1111 1111" in binary or "FF" in colon hexadecimal notation is an IPv6 multicast address. The concept of colon hexadecimal notation is discussed in Section 8-2. Even though there is no such thing as broadcast, there is a multicast address to the all-host multicast group.

Stateless address autoconfiguration (SLAAC) is another important feature of IPv6. This feature allows for a server-less basic network configuration of the IPv6 computers. With IPv4, a computer generally obtains its network settings from a DHCP server. With IPv6, a computer can automatically configure its network settings without a DHCP server by sending a solicitation message to its IPv6 router. The router then sends back its advertisement message, which contains the prefix information that the computer can use to create its own IPv6 address. This feature significantly helps simplify the deployment of the IPv6 devices, especially in the transient environments such as airports, train stations, stadiums, hotspots, and so on.

Stateless Address Autoconfiguration (SLAAC)
Allows a server-less basic network configuration of the IPv6 computers.

8-2 IPV6 ADDRESSING

It was previously mentioned that IPv6 uses a 128-bit address technique, as compared to IPv4's 32-bit address structure. There is also a difference in the way the IP addresses are listed. IPv6 numbers are written in hexadecimal rather than dotted decimal, as with IPv4. For example, the following is an IPv6 address represented with 32 hexadecimal digits Note: 32 hex digits with 4 bits/hex digit = 128 bits):

6789:ABCD:1234:EF98:7654:321F:EDCB:AF21

This is classified as a **full IPv6 address**. The *full* means that all 32 hexadecimal positions contain a value other than 0.

Full IPv6 Address
All 32 hexadecimal positions contain a value other than 0.

Why doesn't IPv6 use the "dotted decimal" format of IPv4? The answer is it would take many decimal numbers to represent the IPv6 address. Each decimal number takes at least seven binary bits in ASCII (American Standard Code for Information Interchange) code. For example, the decimal equivalent of the first eight hexadecimal characters in the previous full IPv6 address is

6789:ABCD = 103.137.171.205

The completed decimal equivalent number for the full IPv6 address is

103.137.171.205.18.52.239.152.118.84.50.31.237.203.175.33

The equivalent decimal number is 42 characters in length. In fact, the decimal equivalent number could be 48 decimal numbers long.

In terms of bits, one 4 hex bit group requires 4 x 4 = 16 bits. Assuming that 8 bits are used to represent the decimal numbers, it will take 12 x 8 = 72 bits to express one hex bit group in a decimal format. There is a significant bit savings obtained by expressing the IPv6 address in a hexadecimal format.

Double-Colon Notation
A technique used by IPv6 to remove 0s from the address.

IPv6 uses seven colons (:) as separators to group the 32 hex characters into 8 groups of four. Some IPv6 numbers will have a 0 within the address. In this case, IPv6 allows the number to be compressed to make it easier to write the number. The technique for doing this is called **double-colon notation**. For example, assume that an IPv6 number is as follows:

6789:0000:0000:EF98:7654:321F:EDCB:AF21

Consecutive 0s can be dropped and a double-colon notation can be used as shown:

6789::EF98:7654:321F:EDCB:AF21

Recovering the compressed number in double-colon notation simply requires that all numbers left of the double notation be entered beginning with the leftmost slot of the IPv6 address. Next, start with the numbers to the right of the double colon.

Begin with the rightmost slot of the IPv6 address slots and enter the numbers from right to left until the double colon is reached. Zeros are entered into any empty slots:

6789 :0 :0 :EF98 :7654 :321F :EDCB :AF21

IPv4 numbers can be written in the new IPv6 form by writing the IPv4 number in hexadecimal and placing the number to the right of a double colon. Example 8-1 demonstrates how a dotted-decimal IP number can be converted to IPv6 hexadecimal.

Example 8-1 Convert the IPv4 address of 192.168.5.20 to an IPv6 hexadecimal address

Solution:

First convert each dotted-decimal number to hexadecimal.

Decimal	Hex
192	C0
168	A8
5	05
20	14

(Hint: Use a calculator or a lookup table to convert the decimal numbers to hexadecimal.) The IPv6 address will have many leading 0s; therefore, the IPv6 hex address can be written in double-colon notation as

:: C0A8:0514.

IPv4 addresses can also be written in IPv6 form by writing the IPv4 number in dotted-decimal format, as shown. Note that the number is preceded by 24 hexadecimal 0s:

0000: 0000: 0000: 0000: 0000: 0000:192.168.5.20

This number can be reduced as follows:

::192.168.5.20

Similar to IPv4 classless addresses, IPv6 addresses are fundamentally divided into a network portion followed by a host portion. The network portion is called the **network prefix** and the number of bits used is the **prefix length**. The prefix is represented with a slash followed by the prefix length. This is the same notation used to designate the CIDR in IPv4. For example, the IPv6 address of 2001:DB8:FEED:BEEF::12 has a 64-bits network prefix. It then can be represented as 2001:DB8:FEED:BEEF::12/64. However, the concept of a CIDR is not relevant in IPv6, because there is enough IP address space for everyone. So, in IPv6, the host portion of the address or what is called the **interface identifier** is always 64-bits in length. This automatically leaves 64 bits as the network prefix. In a typical IPv6 customer site, a network of /48 is usually allocated by IANA. This provides the site with 65,536 subnets, which is more than sufficient. This means that when a site is assigned a /48, the site is capable of having up to 65536 subnets and each subnet is capable of hosting more than 1.8×10^{19} IPv6 addresses.

There are three types of IPv6 addresses: unicast, multicast, and anycast. The **unicast** IPv6 address is used to identify a single network interface address and data packets are sent directly to the computer with the specified IPv6 address. There are several types of unicast addresses, including link-local addresses, **global unicast addresses**, and unique local addresses. Link-local addresses are designed to be used for and are limited to communications on the local link. Every IPv6 interface will have one link-local address.

Per RFC 4291, "IP Version6 Addressing Architecture," the network prefix of link-local addresses, is defined as FE80::/10. Unique local unicast addresses are addresses for local use only, and they are similar to the private IP addresses used in IPv4. Unique local unicast addresses use the prefix of FD00::/8 and were designed to replace site-local addresses, which are being deprecated.

Global unicast addresses are equivalent to the public ip addresses in IPv4. They have unlimited scope, and they are routable on the Internet. IANA is responsible for allocating the IPv6 global unicast address space. Currently, the range of allocated IPv6 addresses starts from prefix 2000::/3.

Network Prefix
The network portion of the IPv6 address.

Prefix Length
Number of bits used to make up the network prefix.

Interface Identifier
The host portion of the IPv6 address.

Unicast Address
Used to identify a single network interface address, and data packets are sent directly to the computer with the specified IPv6 address.

Global Unicast Addresses
These are equivalent to the public IP addresses in IPv4.

Multicast Address
Data packets sent to a multicast address are sent to the entire group of networking devices such as a group of routers running the same routing protocol.

Anycast Address
Obtained from a list of addresses.

IPv6 **multicast addresses** are defined for a group of networking devices. Data packets sent to a multicast address are sent to the entire group of networking devices such as a group of routers running the same routing protocol. Multicast addresses all start with the prefix FF00::/8. The next group of characters in the IPv6 multicast address (the second octet) are called the scope. The scope bits are used to identify which ISP should carry the data traffic.

The **anycast** IPv6 **addresses** might seem like a new type of address, but the concept was not new. Anycast addresses can be thought of as a cross between unicast and multicast addresses. While the unicast traffic sends information to one address and the multicast traffic sends information to every address in the group, the anycast traffic sends information to any one address of the group. The trick is which address of the group to send information to. The most logical and efficient answer is the nearest or the closet address. Similar to multicast where the nodes will join the multicast group, the anycast nodes share the same anycast address. The data will be sent to a node within the anycast group. This node is the nearest to the sender.

Actually, the anycast concept is used in the IPv4 environment today with the root DNS servers. There are 13 DNS root servers in the world, but the DNS query is only sent to one of those servers.

IPv6 addressing is being used in a limited number of network sites (e.g., the federal government); however, the Internet is still running IPv4 and will be for some time. But, there are transition strategies in place to help with the IPv4 to IPv6 transition.

6to4 Prefix
A technique that enables IPv6 hosts to communicate over the IPv4 Internet.

One possible transition to IPv6 is called the **6to4 Prefix**, which is essentially a technique that enables IPv6 sites to communicate over the IPv4 Internet. This requires the use of a 6to4 enabled router, which means that 6to4 tunneling has been enabled. This also requires the use of a 6to4 Relay router that forwards 6to4 data traffic to other 6to4 routers on the Internet.

Figure 8-3 illustrates the structure of the 6to4 prefix for hosts. The 32 bits of the IPv4 address fit into the first 48 bits of the IPv6 address.

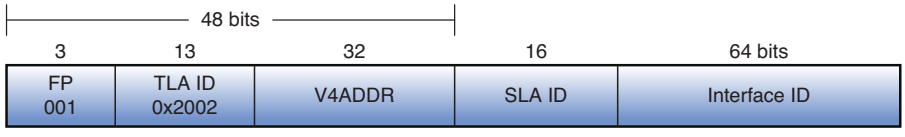

FIGURE 8-3 The 6to4 prefix format

Note the following shown in Figure 8-3:

- **FP** is the Format Prefix, which is made up of the higher order bits. The **001** indicates that this is a global unicast address. The current list of the IPv6 address allocation can be viewed at www.iana.org/assignments/ipv6-unicast-address-assignments. Currently, IANA allocates 2000::/3 as an IPv6 global pool. 2000 can be written in binary as **001**0 0000 0000 0000. 001 is the 3 highest order bits, which correspond to the FP.
- **TLA ID (0x2002)** are the top-level identifiers that are issued to local Internet registries. These IDs are administered by IANA (**http://www.iana.org/**). The

TLA is used to identify the highest level in the routing hierarchy. The TLA ID is 13 bits long.

- **V4ADDR** is the IPv4 address of the 6to4 endpoint and is 32 bits long.
- **SLA ID** is the Site Level Aggregation Identifier that is used by individual organizations to identify subnets within their site. The SLA ID is 16 bits long.
- **Interface ID** is the Link Level Host Identifier and is used to indicate an interface on a specific subnet. The interface ID is equivalent to the host IP address in IPv4.

The 6to4 prefix format enables IPv6 domains to communicate with each other even if they don't have an IPv6 ISP. Additionally, IPv6 can be used within the intranet, but access to the Internet is still available. The 6to4 provides unicast IPv6 connectivity between IPv6 host and via the IPv4 Internet.

8-3 IPV6 NETWORK SETTINGS

Almost all the modern computer operating systems being used today are IPv6 capable. On most operating systems, the IPv6 configuration settings can be found at the same location where the TCP/IP settings for IPv4 reside. This is provided in the Local Area Connections Properties window for both Windows XP and Windows 7. The Local Area Connections Properties window for Windows XP is provided in Figure 8-4. The Local Area Connections Properties window for Windows 7 is provided in Figure 8-5.

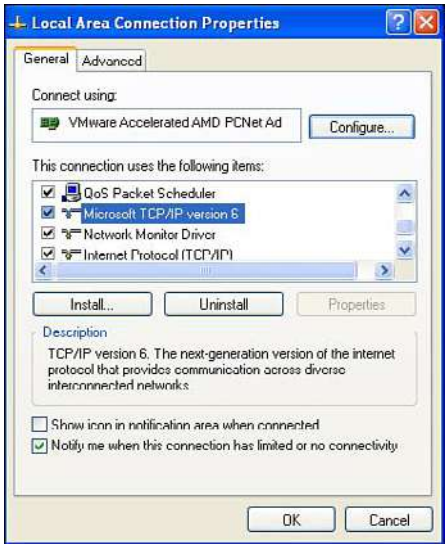

FIGURE 8-4 The Local Area Connections Properties window for Windows XP

There is an option available to obtain the IPv6 configuration automatically as well as an option for manual configuration. This option is available in the Internet Pro-

tocol Version 6 (TCP/IPv6) Properties window, as shown in Figure 8-6. This same feature is available with IPv4. However, Windows XP is one of the exceptions where there is no manual configuration mode for assigning the IPv6 address. The majority of the operating systems enable IPv6 with the automatic configuration mode by default. The following is a summary of the configuration options provided in the TCP/IPv6 Properties window:

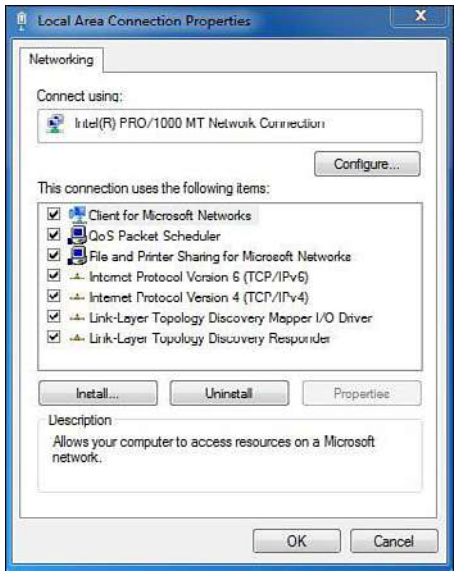

FIGURE 8-5 The Local Area Connections Properties window for Windows 7

- **Obtain an IPv6 address automatically**: In this option, the IPv6 address is automatically configured for this network connection.
- **Use the following IPv6 address**: Specifies the IPv6 address and default gateway are manually configured:
  - **IPv6 address**: This space is used to type in an IPv6 unicast address.
  - **Subnet prefix length**: This space is used to specify the subnet prefix length for the IPv6 address. For unicast addresses, the default value is 64.
  - **Default gateway**: This space is used to enter the IPv6 address for the default gateway.
- **Obtain DNS server address automatically**: This selection indicates the IPv6 addresses for the DNS servers are automatically configured.
- **Use the following DNS server addresses:** This space is used to specify IPv6 addresses of the preferred and alternate DNS servers for this network connection:
  - **Preferred DNS server**: This space is used to input the IPv6 unicast address for the preferred DNS server.
  - **Alternate DNS server**: This space is used to enter the IPv6 unicast address of the alternate DNS server.

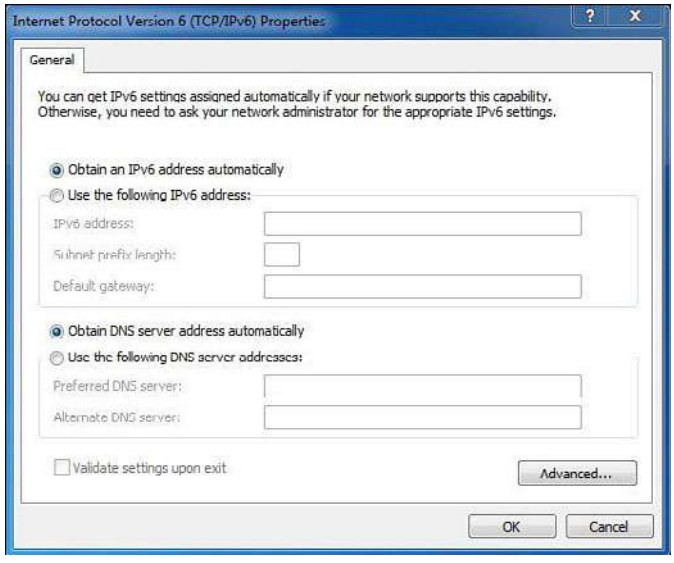

FIGURE 8-6 Internet Protocol Version 6 (TCP/IPv6) Properties window for Windows 7

IPv6 configuration settings are also available for the Mac OS X operating system in the TCP/IP window, as shown in Figure 8-7. The user has the option to configure the IPv6 address automatically or manually. The option for automatically configuring the IPv6 address is selected in Figure 8-7.

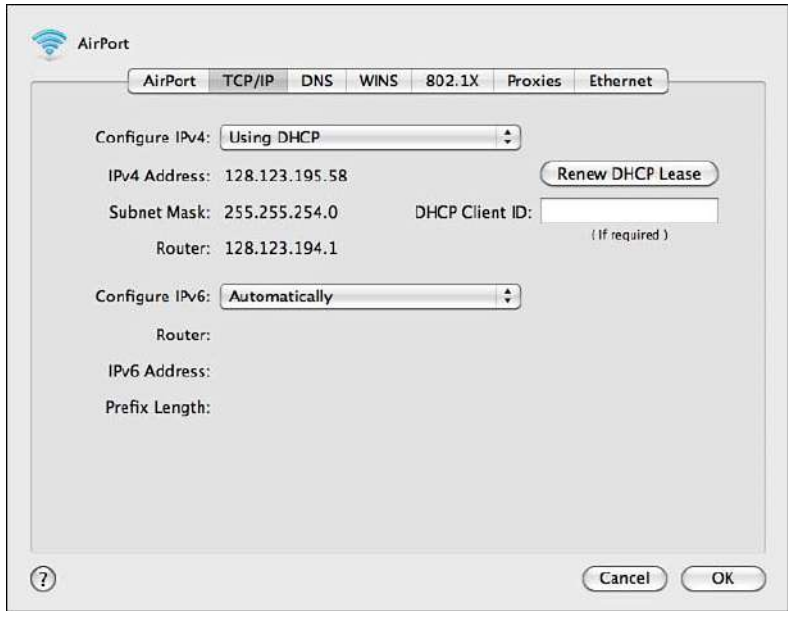

FIGURE 8-7 Mac OS X IPv6 configuration

IPv6 Stateless Autoconfiguration
Enables IPv6-enabled devices that are attached to the IPv6 network to connect to the network without requiring support of an IPv6 DHCP server.

Link-Local Address
Indicates the IP address was self-configured.

In typical places, such as homes and businesses, IPv6 is not yet enabled on the network environment. So, what would happen to all the machines with IPv6 enabled in the automatic configuration mode? The answer is what is called the **IPv6 stateless autoconfiguration**. This feature enables IPv6-enabled devices that are attached to the IPv6 network to connect to the network without requiring support of an IPv6 DHCP server.

This means that, even though an IPv6 DHCP server and an IPv6 enabled router are not involved, any IPv6 machine can self-configure its own **link-local address**. The term link-local address indicates the IP address is self-configured. This means that any IPv6 host should be able to communicate with other IPv6 hosts on its local link or network. The interface identifier of the link-local address is derived by transforming the 48 bits of the EUI-48 MAC address to 64 bits for EUI-64. This EUI-48 to EUI-64 transform algorithm is also used to derive the interface identifier for the global unicast address. Example 8-2 demonstrates how to convert an EUI-48 MAC address of 000C291CF2F7 to a modified EUI-64 format.

Example 8-2

1. Expanding the 48-bit MAC address to a 64-bit format by inserting "FFFE" in the middle of the 48 bits.

   000C29 **FFFE** 1CF2F7.

2. Change the seventh bit starting with the leftmost bit of the address from 0 to 1. This seventh bit is referred to as the U/L bit or universal/local bit. 000C29 is 0000 00**0**0 0000 1100 0010 1001 in binary format. When its seventh bit is changed to 1, it becomes 0000 00**1**0 0000 1100 0010 1001, which is 0**2**0C29 in hexadecimal number.

3. The result is a modified EUI-64 address format of 020C29FFFE1CF2F7.

FE80::/64
The prefix for a link-local addresses.

Neighbor Solicitation
Purpose of this solicitation is to discover the link-layer address of another IPv6 node or to confirm a previously determined link-layer address.

Duplicate Address Detection (DAD)
Process of detecting another machine with the same IPv6 address.

To complete the autoconfiguration IPv6 address, the subnet prefix of **FE80::/64** is then prepended to the interface identifier resulting in a 128-bit link-local address. To ensure that there is no duplicate address on the same link, the machine sends a **Neighbor Solicitation** message out on the link. The purpose of this solicitation is to discover the link-layer address of another IPv6 node or to confirm a previously determined link-layer address. If there is no response to the message, it assumes that the address is unique and therefore assigns the link-local address to its interface. The process of detecting another machine with the same IPv6 address is called **Duplicate Address Detection (DAD)**. Figures 8-8, 8-9, and 8-10 show the local-link addresses from different operating systems. Look for the FE80:: prefix in each figure.

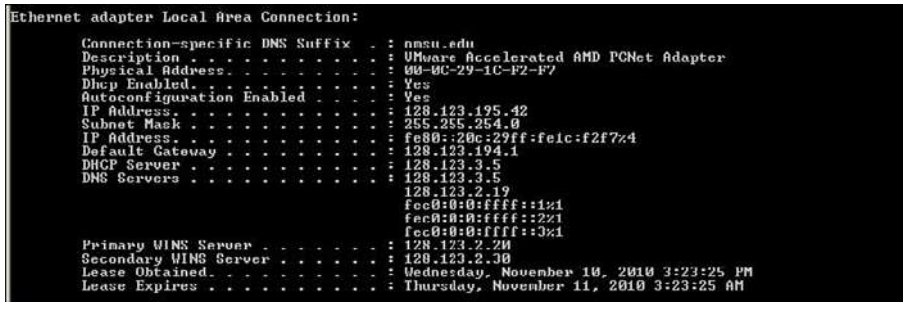

FIGURE 8-8 Windows XP—**ipconfig** result with a link-local address

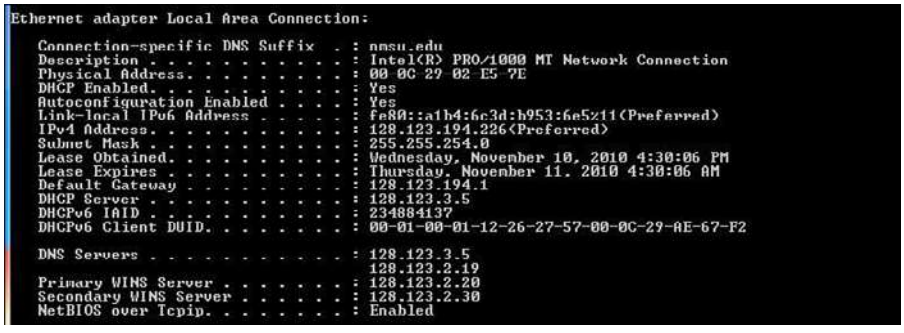

FIGURE 8-9 Windows 7—**ipconfig** result with a link-local address

FIGURE 8-10 Mac OS X—**ifconfig** result with a link-local address

Privacy Extensions for Stateless Address Autoconfiguration
Allows the generation of a random identifier with a limited lifetime.

The derivation of the IPv6 interface identifier from the MAC address generates some concerns regarding privacy issues. The concern is that the MAC address can be tracked throughout the Internet. A MAC address always attaches to the device v, and the interface identifier does not change no matter where it is physically located. The danger of this is that the movement or location of the device can be traced using the MAC address. To remedy these concerns, the IETF created RFC 4941 "**Privacy Extensions for Stateless Address Autoconfiguration** in IPv6." This RFC allows the generation of a random identifier with a limited lifetime to replace the machine's MAC address. An address like this will be difficult to trace because it regularly changes. Figure 8-9 shows the link-local address of a Windows 7 machine, which has been randomly generated. Therefore, this IPv6 address does not appear to be anything resembling its MAC address. The link-local address shown in Figure 8-9 is

fe80::a1b4:6c3d:b953:6e5%11

where %11 is the interface index or scope ID designated by Windows 7. IPv6 enables a socket application to specify an interface to use for sending data by specifying an interface index. It is possible for a computer to have more than one network interface card (NIC) and as a result to have multiple link-local addresses. Additionally, each link-local address can have a different scope. The purpose of the scope ID is to indicate which address it is used for.

The MAC or physical address is 000C2902E57E.

8-4 CONFIGURING A ROUTER FOR IPV6

Multicast Listener Discovery (MLD)
Enables the switches to listen to MLD packets to determine how to efficiently forward multicast packets to specific listeners on specific ports.

ipv6 unicast-routing
This command activates the IPv6 forwarding mechanism on the routers.

Not every piece of networking equipment is IPv6-capable, and this must be verified before implementing IPv6. IPv6-capable equipment can operate in the IPv4 and IPv6 environment. IPv6 relies heavily on multicast messages for enabling a lot of functions; therefore, the network switches must be able to support IPv6 multicast functions as well. In IPv4, IGMP (Internet Group Management Protocol) is used for determining which computers should join a multicast group. However, IGMP is no longer used in IPv6. For multicast group management, IPv6 uses **Multicast Listener Discovery (MLD)** instead. Similar to IGMP in IPv6, MLD snooping enables the switches to listen to MLD packets to determine how to efficiently forward multicast packets to specific listeners on specific ports.

Today, most routers are IPv6-capable. Those that are not might just require a software upgrade. On Cisco routers, IPv6 is not enabled automatically. To enable IPv6 unicast packet forwarding on Cisco routers, the global command **ipv6 unicast-routing** is entered. The following is the sequence of commands required to enable IPv6 unicast-routing:

```
Router# conf t
Router(config)#
Router(config)# ipv6 unicast-routing
```

ipv6 enable
Enables IPv6 on a specific interface.

The **ipv6 unicast-routing** command only activates the IPv6 forwarding mechanism on the routers. However, IPv6 is still not yet enabled on a specific interface. To enable IPv6 on a specific interface, you must enter the **ipv6 enable** command. The following example shows how to enable IPv6 on a gigabitethernet 3/1 interface. This step requires that the interface must first be selected. In this case, the command **int Gig3/1** is entered from the (config)# prompt. The prompt changes to (config-if)# and the command **ipv6 enable** is entered:

```
int Gig3/1
Router(config)# int Gig3/1
Router(config-if)# ipv6 enable
```

For Cisco routers, enabling IPv6 on the interface automatically configures the link-local address for that interface. The link-local address can only communicate with the IPv6 devices on the same network link.

The command **show running-config** is used to verify the IPv6 configuration. The use of this command is next demonstrated and a portion of the running configuration for interface GigabitEthernet 3/1 is provided:

```
Router#show running-config
.
.
!
interface GigabitEthernet3/1
 no ip address
 ipv6 enable
!
```

Also, the command **show ipv6 interface** can be used to show the state of the IPv6 configuration on the interface. This command shows the IPv6 of the interface. In the following example, it shows that IPv6 is enabled on the interface gigabitEtheret3/1. It shows the interface has a link-local address, but not the global address. Along with that the IPv6 network discovery protocol information is shown:

show ipv6 interface
Used to show the state of the IPv6 configuration on the interface.

```
Router#show ipv6 interface gigabitEthernet 3/1
GigabitEthernet3/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::217:DFFF:FEF5:1000
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FFF5:1000
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Output features: HW Shortcut Installation
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

The IPv6 global address can be configured on the interface by using the command **ipv6 address** *ipv6 interface address* issued from the (config-if)# prompt. There are two ways to program the IPv6 interface address. One is to specify the entire 128-bit IPv6 address followed by the prefix length. Another way is to specify a 64-bit prefix and to use the **eui-64** option. Using the option **eui-64** allows the router to choose its own host identifier (right most 64-bits) from the EUI-64 (Extended Universal Identifier-64) of the interface. The following example uses the IPv6 address of 2001:DB88:FEED:BEEF::1 on the router interface. This has a 64-bit network prefix of 2001:DB88:FEED:BEEF.

ipv6 address *ipv6 interface address*
The command used to configure the IPv6 address on an interface.

eui-64
Allows the router to choose its own host identifier.

```
Router(config)# int Gig3/1
Router(config-if)# ipv6 address 2001:DB88:FEED:BEEF::1/64
```

Next, the command **show ipv6 interface gigabitEthernet 3/1** is used to display the configuration of the Gig3/1 interface. This time the command shows that the interface gigabitEthernet 3/1 now has an IPv6 global address assigned to it, which is 2001:DB8:FEED:BEEF::1:

```
Router#show ipv6 interface gigabitEthernet 3/1
GigabitEthernet3/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::217:DFFF:FEF5:1000
  Global unicast address(es):
  2001:DB8:FEED:BEEF::1, subnet is 2001:DB8:FEED:BEEF::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FFF5:1000
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Output features: HW Shortcut Installation
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

ND Protocol
Network Discovery Protocol. ICMPv6 messages of the type Router Advertisement (RA).

RA Messages
Router advertisement. This is a response to a link-local router solicitation message.

Router Solicitation Messages
These messages are sent to ask routers to send an immediate RA message on the local link so the host can receive the autoconfiguration information.

Now that IPv6 is enabled on the router, the router can begin to participate in the IPv6 functions. The router plays a key role in the stateless autoconfiguration of an IPv6 network. An IPv6 router uses the **neighbor discovery (ND)** protocol to periodically advertise information messages on the links to which they are connected. These are ICMPv6 messages of the type Router Advertisement (RA). One parameter of the router advertisements is the IPv6 network prefix for the link that can be used for host autoconfiguration. Upon receiving **RA messages**, an unconfigured host can build its global unicast address by prepending the advertised network prefix to its generated unique identifier just like in the link-local address case.

Another way for a host to autoconfigure itself is by sending **router solicitation messages** to the connected routers. These messages are sent to ask routers to send an immediate RA message on the local link, so the host can receive the autoconfiguration information without having to wait for the next schedule RA. Note: The time interval between RA messages is configurable. By default, router advertisements are sent every 200 seconds in Cisco routers.

As a result, the global unicast address of every machine on this network is the combination of the network prefix of 2001:DB8:FEED:BEEF and the self-generated interface identifier for that machine. Both Figure 8-11 and Figure 8-12 show two IPv6 addresses with the 2001:DB8:FEED:BEEF prefix. There are two IPv6 addresses. One is a global unicast address and another is a random generated identifier as part of the

privacy identifier. This was discussed earlier in this section (see Privacy Extensions for Stateless Autoconfiguration). Microsoft calls this random identifier IPv6 a "temporary IPv6 address." This is shown to be a temporary address in Windows 7.

```
        IP Address. . . . . . . . . . . . : 2001:db8:feed:beef:460:45ab:3d6e:56e3
        IP Address. . . . . . . . . . . . : 2001:db8:feed:beef:20c:29ff:fe1c:f2f7
        IP Address. . . . . . . . . . . . : fe80::20c:29ff:fe1c:f2f7%4
        Default Gateway . . . . . . . . . : 128.123.7.1
                                            fe80::217:dfff:fef5:1000%4
```

FIGURE 8-11 Windows XP—**ipconfig** result with an IPv6 global unicast address

```
IPv6 Address . . . . . . . . . . : 2001:db8:feed:beefa1b4:6c3d:b953: 6e5 (Preferred)
Temporary IPv6 Address. . . . . . : 2001:db8:feed:beef:44ab:2c4d:f3d0:6674 (Preferred)
Link-local IPv6 Address . . . . . :fe80:a1b4:3c3d:b953:6e5%11 (Preferred)
IPv4 Address . . . . . . . . . . : 128.123.7.207 (Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained . . . . . . . . . . : Friday, November 12, 2012 4:49:33 PM
Lease Expires . . . . . . . . . . : Saturday, November 13, 2012 4:49:33 AM
Default Gateway . . . . . . . . . : fe80::217:dffffef5:1000%11
```

FIGURE 8-12 Windows 7—**ipconfig** result with an IPv6 global unicast address

In Windows XP, both of these are presented as IP addresses. Of course, we can tell that one is a modified EUI-64 format, and the other one is randomly generated. An IPv6 address with ff:fe in the middle indicates the EUI-48 to EUI-64 transform. On Mac OS X, no random identifier is used. The global unicast address is the product of the modified EUI-64 format, as shown in Figure 8-13.

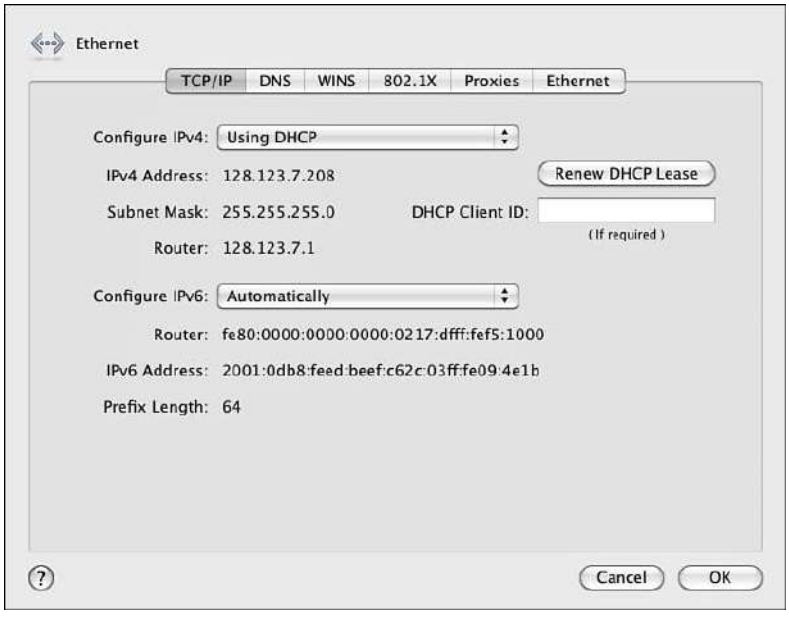

FIGURE 8-13 Mac OS X—**ipconfig** result with an IPv6 global unicast address

2001:DB8::/32 Prefix
This IPv6 address prefix is reserved for documentation. This is recommended by RFC3849 to reduce the likelihood of conflict and confusion when using IPv6 addresses in examples, books, documentation, or even in test environments.

Throughout this chapter, the IPv6 prefix used is **2001:DB8::/32**. This is a special range designated by the IANA to be used for any testing or documentation. This IPv6 prefix cannot be used nor can it be routed on the Internet.

With the global unicast address, the machine is now reachable from anywhere on the IPv6 network. However, it is a daunting task to remember the IPv6 global unicast address. It is not practical to use the long 128-bits address. This required a DNS server that can translate a host name to an IPv6 address. The DNS record for IPv6 is called AAAA (Quad A) record.

8-5 IPV6 ROUTING

When interconnecting IPv6 networks together, a routing protocol is required. IPv6 supports static, RIP, OSPF, EIGRP, and IS-IS routing. Most of these protocols had to be revised to be able to deal with IPv6 addresses. However, the routing protocols for IPv6 work the same way as they do with IPv4. In fact, they still maintain the same routing principles. The following material demonstrates how to configure IPv6 routing for static, RIP, OSPF, EIGRP, and ISIS.

IPv6: Static

Configuring a static route for IPv6 is almost the same as it is in IPv4. In IPv4, one can specify the next hop IP address or/and the exit interface. In IPv6, there is an extra feature. The next hop IP address in IPv6 can either be the link local address or the global address. The following examples show how to configure an IPv6 static route using these three different methods:

```
Router# conf t
Router(config)# ipv6 route 2001:0db8:BEEF::/32 FA1/0
Router(config)# ipv6 route 2001:0db8:BEEF::/32 FA1/0 fe80::2
Router(config)# ipv6 route 2001:0db8:BEEF::/32 2001:0db8:FEED::1
```

The first static route shows the route to the network 2001:0db8:BEEF::/32 is configured via interface FastEthernet1/0. The second static route gives an option of the link-local next hop address, which is specified with the fe80 prefix. The third static entry shows a route to the network that points to the global IPv6 address of 2001:0db8:FEED::1.

IPv6: RIP

RIPng
Routing Information Protocol next generation, which is required to support IPv6 routing.

RIP routing using IPv6 requires the use of a RIP version called Routing Information Protocol next generation or **RIPng**. The basic features of RIPng are the same as RIPv2. For example, this is still a distance vector protocol, there is a maximum hop limitation; however, RIPng is updated to use IPv6 for transport. Also, RIPng uses the IPv6 multicast address of FF02::9 for all RIP updates.

Configuring RIPng on Cisco routers is simple. The biggest difference between configuring RIPv2 and RIPng on Cisco routers is now RIPng must be configured on a per network link or per-interface basis rather than per-network basis as in RIPv2.

The following examples demonstrate how to enable RIPng and how to configure RIPng on a Cisco router interface:

```
Router# conf t
Router(config)#
Router(config)# ipv6  router rip RIP100
Router(config)#
Router(config)# int Gig3/1
Router(config-if)# ipv6 rip RIP100 enable
```

The command **ipv6 router rip** *rip_tag* is used to enable RIPng on Cisco routers. The *rip_tag* is a tag to identify the RIP process. The RIPng is enabled on the Gigabit interface 3/1 with the command **ipv6 rip** *rip_tag* **enable**. The same command will be used to enable other RIP interfaces. This is different than configuring RIPv2 where the network statement needs to be issued for every RIP network.

rip_tag
Used to identify the RIP process.

IPv6: OSPF

The current OSPF version used in IPv4 is OSPFv2. Most of OSPF information relies heavily on the IP number (for example the router ID <area ID> and the link-state ID). To support IPv6, the OSPF routing protocol has been significantly revamped. The new OSPF version for IPv6 is **OSPFv3**. The basic foundation of OSPF still remains intact—for example, OSPFv3 is still a link state routing protocol. However, OSPFv3 uses the IPv6 link-local multicast addresses of FF02::5 for all OSPF routers and FF02::6 for OSPF designated routers.

OSPFv3
The OSPF version that supports IPv6.

OSPFv3 is now enabled on a per-link basis, not on a per-network basis on Cisco routers. This is similar to the changes in RIPng. OSPFv3 indentifies which networks are attached to the link and propagates them into the OSPF area. The following example demonstrates how to enable OSPFv3 and how to configure OSPFv3 on a Cisco router interface:

```
Router# conf t
Router(config)#
Router(config)# ipv6  router ospf 99
Router(config)#
Router(config)# int Gig3/1
Router(config-if)# ipv6 ospf 99 area 0.0.0.0
```

The command **ipv6 router ospf** *process_id* is used to enable OSPFv3 on Cisco routers. OSPFv3 is enabled on the Gigabit interface 3/1 with the command **ipv6 ospf** *process_id* ***area*** *area_id.* The same command is used to enable other OSPF interfaces. The router in this example is configured to be area 0 which is the backbone (area 0.0.0.0).

IPv6: EIGRP

EIGRP is inherently a multiprotocol routing protocol. It was designed to support non-IP protocols, such as IPX and Appletalk, and it supports the IP protocols IPv4 and now IPv6. IPv6 EIGRP uses the IPv6 link-local multicast addresses of FF02::A for all EIGRP Hello packets and updates.

IPv6 EIGRP is now configured over a network link, so there is no need to configure a network statement as in IPv4 EIGRP. The following example demonstrates how to enable IPv6 EIGRP and how to configure it on a Cisco router interface:

```
Router# conf t
Router(config)#
Router(config)# ipv6  router eigrp 999
Router(config-rtr)# no shut
Router(config)# int Gig3/1
Router(config-if)# ipv6 eigrp 999
```

The command **ipv6 router eigrp** *as_number* is used to enable EIGRP on Cisco routers. The IPv6 EIGRP protocol is created in a shutdown mode by default. The **no shutdown** is issued to ensure that the protocol is enabled. Next, the IPv6 EIGRP is enabled on the Gigabit interface 3/1 with the command **ipv6 eigrp** *as_number.* The network link is now part of the EIGRP routing network.

IPv6: IS-IS

As mentioned in Chapter 3, IS-IS is designed to work on the same network layer just like IP. Therefore, it does not require an IP protocol for it to function. Later, IS-IS was adapted to work with IP. Because of its IP independence, IS-IS is much easier than most protocols to incorporate with IPv6. Only a few adjustments to IS-IS have been made to better support IPv6.

Configuring IPv6 IS-IS is very similar to the method used in IPv4. In IPv6, IS-IS is always enabled on a per network link basis. This is the same for the IPv4 configuration. The same global command (**clns routing**) is used to enable the IS-IS routing protocol. The same NET address is used in the IPv6 configuration as in the IPv4 configuration. The only big difference is the use of keyword **ipv6** when enabling the IPv6 IS-IS interface. The following example demonstrates how to enable IPv6 IS-IS and how to configure it on an interface of a Cisco router:

```
Router# conf t
Router(config)# clns routing
Router(config)# router isis
Router(config-rtr)# net 49.0001.c202.00e8.0202.00
Router(config)#
Router(config)# int Gig3/1
Router(config-if)# ipv6 router isis
```

The command **clns routing** is used to enable the connectionless network service. The command **router isis** will allow the IS-IS protocol to be configured. The **net** *NET Address* assigns the NET address to IS-IS. Then, the IPv6 IS-IS is enabled on the Gigabit interface 3/1 with the command **ipv6 router isis**.

This section demonstrated the steps for configuring IPv6 routing for static, RIP, OSPF, EIGRP, and IS-IS. As was demonstrated, the steps are similar to configuring routing for IPv4; however, there are some distinct differences required to enable an IPv6 interface.

8-6 TROUBLESHOOTING IPV6 CONNECTION

One big question that needs to be answered before troubleshooting IPv6 connectivity is: Does the network environment support IPv6? If the answer is yes, the same network troubleshooting techniques and approaches still apply on IPv6 as on IPv4. Remember what has changed is only the network layer on the OSI model. Other layers are still intact and stay the same. You will still need to troubleshoot the physical connections to make sure the physical layer is working properly. The data link layer still needs to be inspected to see if the packets are being forwarded, MAC addresses are still being seen, and hosts are still in the correct VLANs.

The commands such as **ipconfig** in Windows and **ifconfig** for Linux or Mac OS X can be used to view the TCP/IP configuration information of a host. This is always a good start in network troubleshooting. First, you have to see what is configured and whether it is configured correctly before you can move on to the next step. The examples of these commands are shown throughout this chapter.

Many basic network tools that are available in IPv4 are available in IPv6 as well. Ping is one of the most commonly used tools to test the connectivity between two hosts. Ping is implemented using ICMP echo and Echo reply for a very simple hello network test. In IPv6, the ICMP version 6 is being used instead; therefore the tool has changed slightly to accommodate the change in the ICMP protocol fields. The command **ping6** can be used to explicitly specify the IPv6 address, even though most operating systems have modified the **ping** command to understand both the IPv4 and IPv6 addresses. An issue of using the **ping** command in IPv6 is the lengthy address and the time required for entering the destination address. For example, the following is an example. The first part shows the IPv6 address that is assigned to the router's R1 interface.

ping6
Command used to explicitly specify the IPv6 address.

```
R2(config-if)# ipv6 address 2001:C16C:0000:0001:0000:0000:0000:0001/64
```

The IPv6 address can be simplified using double colon notation, as shown:

```
R2# ping ipv6 2001:C16C:0:1::1
```

The IPv6 address is still complicated even with the reduced address length. A solution to this is to assign a hostname to the specified IPv6 address. In this case, the hostname R1-WAN will be assigned to the specified IPv6 address using the command **ipv6 host R1-WAN 2001:C16C:0:1::1/64**, as shown:

```
R2(config)# ipv6 host R1-WAN 2001:C16C:0:1::1
```

Now, the **ping** command, using the newly assigned hostnames for R1 and R2, can be used. An example is provided:

```
R2(config)# ipv6 host R1-WAN 2001:C16C:0:1::1
R2# ping R1-WAN
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:C16C:0:1::1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
R2#
```

traceroute6
The router tool that enables the user to see the routing information between the two hosts.

tracert6
The Windows tool that enables the user to see the routing information between the two hosts.

Another useful network tool is **traceroute** or **tracert** in Windows world. This tool enables the user to see the routing information between the two hosts. The IPv6 version of this tool is **traceroute6** or **tracert6** in Windows. Like **ping**, the IPv6 version of traceroute has to understand the ICMP version 6 messages as well. The structure for the **traceroute6** command is shown. The Host name and web addresses assume the DNS entries have been made:

```
traceroute6 <destination address, Host name, or web address>
```

For example, the following could be entered to run a traceroute:

```
traceroute6 2001:C16C:0:2::2
traceroute6 www.6bone.net
traceroute6 R1-WAN
```

When will the Internet switch to IPv6? The answer is not clear, but the networking community recognizes that something must be done to address the limited availability of current IP address space. Manufacturers have already incorporated IPv6 capabilities in their routers and operating systems. What about IPv4? The bottom line is that the switch to IPv6 will not come without providing some way for IPv4 networks to still function. Additionally, techniques such as NAT have made it possible for intranets to use the private address space and still be able to connect to the Internet. This has significantly reduced the number of IPv4 addresses required for each network and have delayed the need to immediately switch to IPv6.

SUMMARY

This chapter presented an overview of the fundamentals of the IP version 6. IPv6 is proposed to replace IPv4 to carry the data traffic over the Internet. The student should understand the following:

- The basic differences between IPv6 and IPv4
- The basic structure of a 128-bit IPv6 hexadecimal address
- The addresses that IPv6 uses
- How to setup IPv6 on the computers
- The purpose of link-local addresses
- How to setup IPv6 on the routers

QUESTIONS AND PROBLEMS

Section 8-1

1. What is the size of the IPv6 address?
2. What is a datagram?
3. How many bits are used to define the IPv4 source and destination address?
4. How many bits are used to define the IPv6 source and destination address?
5. Why is IPv6 faster than IPv4 for transferring packets?
6. At what layer is error detection performed in IPv6?
7. What is IPsec?
8. How is IPsec enabled with IPv6?
9. How are broadcasts handled in IPv6?
10. Why is DHCP not required in IPv6?

Section 8-2

11. How many bits are in an IPv6 address?
12. IPv6 numbers are written in what format?
13. Express the following IPv6 numbers using double-colon notation:
    a. 5355:4821:0000:0000:0000:1234:5678:FEDC
    b. 0000:0000:0000:1234:5678:FEDC:BA98:7654
    c. 1234:5678:ABCD:EF12:0000:0000:1122:3344
14. Express the IPv4 IP address 192.168.12.5 in IPv6 form using dotted decimal.
15. Recover the following IPv6 address from the following double-colon notation:

    1234:5678::AFBC

16. Define the structure of the 6to4 prefix.
17. What is the purpose of the 6to4 relay router?
18. What does it mean to have a full IPv6 address?
19. What is the network prefix for the following IPv6 address and how big is the network prefix?

    2001:1234:ABCD:5678::10/64
20. What is the length of the interface identifier in IPv6?
21. These types of addresses started with FF00::/8:
    a. Anycast
    b. Multicast
    c. Global unicast
    d. Link-local
    e. None of these answers are correct
22. This address is only deliverable to the nearest node.
    a. Anycast
    b. Multicast
    c. Global unicast
    d. Link-local
    e. None of these answers are correct
23. The range of these addresses starts with 2000::/3.
    a. Anycast
    b. Multicast
    c. Global unicast
    d. Link-local
    e. None of these answers are correct
24. The network prefix for this address is FE80::/10.
    a. Anycast
    b. Multicast
    c. Global unicast
    d. Link-local
    e. None of these answers are correct

25. The IPv6 addresses are equivalent to public addresses in IPv4.
    a. Anycast
    b. Multicast
    c. Global unicast
    d. Link-local
    e. None of these answers are correct
26. This type of address can be thought of as a cross between unicast and multicast addresses.
    a. Anycast
    b. Multicast
    c. Global unicast
    d. Link-local
    e. None of these answers are correct
27. Every IPv6 interface will have at least one of these addresses.
    a. Anycast
    b. Multicast
    c. Global unicast
    d. Link-local
    e. None of these answers are correct
28. These types of IPv6 addresses can be thought of as private addresses in IPv4.
    a. Anycast
    b. Multicast
    c. Global unicast
    d. Link-local
    e. None of these answers are correct
29. The 001 of this address indicates it is what type of address?
    a. Anycast
    b. Multicast
    c. Global unicast
    d. Link-local
    e. None of these answers are correct

30. These types of IDs are administered by IANA.
    a. FP ID
    b. SLA ID
    c. TLA ID
    d. Interface ID
    e. None of these answers are correct
31. This type of ID is used to indicate an interface on a specific subnet.
    a. FP ID
    b. SLA ID
    c. TLA ID
    d. Interface ID
    e. None of these answers are correct
32. This ID is used to identify subnet within the site.
    a. FP ID
    b. SLA ID
    c. TLA ID
    d. Interface ID
    e. None of these answers are correct

Section 8-3

33. This type of operating system has no manual configuration mode for assigning the IPv6 address.
34. In regard to subnet address length in IPv6, the default value for unicast addresses is
    a. 32
    b. 64
    c. 128
    d. None of these answers are correct
35. All the machines in a network are running IPv6 enabled in the automatic configuration mode. What mode is this, and what does this mean?
36. Which of the following types of IPv6 address is self-configured?
    a. Anycast
    b. Multicast
    c. Global unicast
    d. Link-local
    e. None of these answers are correct

37. How many DNS root servers are there in the world?

38. Why does a computer issue a neighbor solicitation message?

    a. To discover the unicast address of another IPv6 node

    b. To discover the anycast address of another IPv6 node

    c. To discover the link-layer address of another IPv6 node

    d. To discover the global unicast address of another IPv6 node

39. The process of detecting another machine with the same IPv6 address is called which of the following?

    a. Duplicate Address Detection

    b. Redundant Address Detection

    c. Stateless Address Detection

    d. Global Address Detection

40. What is the benefit of the "Privacy Extensions for Stateless Address Autoconfiguration in IPv6?"

Section 8-4

41. For multicast group management, IPv6 uses which of the following?

    a. Unicast Listener Discovery

    b. Stateless Listener Discovery

    c. Unicast Listener Discovery

    d. Multicast Listener Discovery

42. What global command is used to enable IPv6 unicast packet forwarding on Cisco routers?

43. To enable IPv6 on an interface, which of the following commands must be entered?

    a. **ipv6 enable**

    b. **ipv6 configure**

    c. **ipv6 interface**

    d. **ipv6 routing**

44. The following information is displayed after entering the **show running-config** command:

```
!
interface GigabitEthernet1/1
 no ip address
 ipv6 enable
```

This information verifies which of the following? (Select all that apply.)

a. IPv4 is configured.

b. Interface ge1/1 is configured.

c. IPv6 is enabled.

d. Interface status is ip.

45. The **show ipv6 interface gigabitEthernet 3/1** command is entered on a router. The address GigabitEthernet3/1 FE80::217:DFFF:FEF5:1000 is listed. What type of address is this?

46. The command **ipv6 address 2001:DC21:2244:3311::1/64** is entered on a router. What is the network prefix of this address and what is its length? What is the command doing?

47. What is the EUI option?

48. What is the purpose of the network discovery protocol in IPv6?

49. What is the purpose of the router solicitation message in IPv6?

Section 8-5

50. What is the following command showing?

```
Router(config)# ipv6 route 2001:0db8:ABCD::/32 FA0/0
```

51. List the command to create a static route for 2001:0db8:1234::/32 that points to the global network 2001:0db8:ABCD::1.

52. Create a static route for 2001:0db8:1234::/32 off the FA0/0 interface that gives the link-local next hop address, which is specified with the fe80::1 prefix.

53. What is RIPng and what is it used for?

54. What is the multicast address for RIPng?

55. List the command that is used to enable RIPng on Cisco routers.

56. What is the purpose of the rip tag?

57. What version of OSPF is used with IPv6?

58. What are the IPv6 link-local multicast addresses for routers and the link-local addresses for designated routers?

59. What command is used to configure OSPF routing for IPv6, using a process ID of 50?

60. What does the following command do?

```
Router(config-if)# ipv6 ospf 50 area 0.0.0.0
```

61. What is the IPv6 link-local multicast addresses for EIGRP? What is the link-local address used for in IPv6?

62. What is the command for enabling EIGRP for IPv6 with a specified AS of 100?

63. List the configuration for enabling ISIS for IPv6. List the router prompts and all commands required for enabling IS-IS on the Gig1/1 interface. Use a net address of 49.0002.b123.a456.0012.00.

Section 8-6

64. What command is used to view the /TCP/IP setting in Windows?

65. What command is used to view the /TCP/IP setting in Linux?

66. What is the purpose of the **ping6** command?

67. What is the purpose of the **traceroute6** or **tracert6** command in IPv6?

68. List three things that should be answered before troubleshooting IPv6 connectivity?

Critical Thinking

69. Your boss read about IPv6 and wants to know if the network you oversee is ready for the transition. Prepare a response based on the networking and computer operating systems used in your facility.

70. The **show ipv6 interface** command is issued to examine a router's R1 interface. The interface has been configured with an IPv6 address. Where is the MAC address of the interface found?

```
R1# sh ipv6 interface
Serial0/0/0 is up, line protocol is up
IPv6 is enabled, link-local address is
FE80::213:19FF:FE7B:1101/64
No Virtual link-local address(es):
Global unicast address(es):
2001:C16C:0:1::1, subnet is 2001:C16C:0:1::/64
Joined group address(es):
FF02::1
FF02::2
FF02::0001:FF00:0001
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
Hosts use stateless autoconfig for addresses.
```

71. What is the purpose of the command **ipv6 address 2001:C16C:0:2:213:19FF :FE7B:1101/64 eui-64**?

72. Answer the following for the given IPv6 address: 2001:C15C:0000:0001:0000 :0000:0000:0001/64

    a. Write this address using double colon notation

    b. Identify the network prefixs