CHAPTER 21

Comparing IPv4 and IPv6

One of the primary ways computers are identified in a TCP/IP network is with an IP address. As an A+ technician, you are very likely to come across the different types of IP addresses, and you might even need to troubleshoot some problems related to IP addressing. In this chapter, you'll learn about some of the basics both for IPv4 and for IPv6 addresses.

Exam 220-801 objectives in this chapter:

- 2.3 Explain properties and characteristics of TCP/IP.
  - IP class
    - Class A
    - Class B
    - Class C
  - IPv4 vs. IPv6
  - Public vs. private vs. APIPA
  - Static vs. dynamic
  - DHCP
  - Subnet mask
  - Gateway
- 2.4 Explain common TCP and UDP ports, protocols, and their purpose.
  - Protocols
    - DHCP
- 2.6 Install, configure, and deploy a SOHO wireless/wired router using appropriate settings.
  - NAT

Exam 220-802 objectives in this chapter:

- 1.6 Setup and configure Windows networking on a client/desktop.
  - Configuring an alternative IP address in Windows
    - IP addressing
    - Subnet mask
    - DNS
    - Gateway
  - Network card properties
    - Half duplex/full duplex/auto
    - Speed
    - Wake-on-LAN
    - PoE
    - QoS

REAL WORLD **FIRST PRINTERS AND IP ADDRESSES**

My printer recently died, so I needed a new one. We have several computers in our house, so I wanted to make sure that everyone could use the printer. The solution was to purchase a network printer.

Setting up the new printer was relatively painless. I followed the quick-start directions to put it together, connected to my network, and used Windows 7 to locate and connect to it. This all went without a hitch, and I really didn't need to know anything about networking to get this network printer up and running.

But then we lost power for a short time, and suddenly no one could print. Did the printer go bad? Did I need to take it back and get another one? Or was there another problem?

I found that the problem was that the printer was assigned a new IP address after power came back on. I needed to take some steps to fix the immediate problem and prevent it from happening again. Taking these steps was a lot easier than exchanging the printer or calling in an A+ technician like you to come and fix it. Thankfully, I had the knowledge to fix it, and after you finish this chapter, you'll be prepared to help users who have the same common problem.

Examining IPv4 Addresses

Internet Protocol version 4 (IPv4) addresses have been around since the 1980s, and they are the most common IP addresses in use. You might also see IPv6 addresses (discussed later in this chapter), but you can count on seeing IPv4 addresses. With that in mind, you'll need to know some basics about IPv4 addresses.

NOTE **IP ADDRESS**

It's common to see "IP address" when referring to an IPv4 address. Unless the IP address is displayed showing that it is obviously an IPv6 address, you can assume that IP address refers to an IPv4 address.

Dotted Decimal Format

IPv4 addresses are created with 32 bits. However, it's not easy for us to read a string of 32 ones and zeros, so IPv4 addresses are commonly displayed in dotted decimal format. Each IP address has four decimal numbers separated by three dots, like this: 192.168.1.5.

Each decimal can be represented with eight bits (also called an octet). Four octets (or four sets of eight) add up to 32 bits. For example, the IP address of 192.168.1.5 can be represented as follows:

```
1100 0000 . 1010 1000 . 0000 0001 . 0000 0101
```

Most of us would rather work with decimal numbers, but it's worthwhile knowing that the IP address is composed of 32 bits with four octets of eight bits.

If all bits are a one in any octet (1111 1111), the value is 255. This is important to remember because an IPv4 address cannot have any decimals greater than 255. For example, the following IP address is not valid: 192.168.*256*.2 because the third decimal is 256. The decimal number of 256 can be displayed in binary as 1 0000 0000, but an octet in an IPv4 address has only eight bits.

EXAM TIP

Any IPv4 address with a number greater than 255 is not valid. IPv4 addresses can include only numbers between 0 and 255.

Two Parts of an IP Address

It is not apparent at first, but an IPv4 address has two parts. The first part is the network identifier, or network ID, and the second part is the host identifier, or host ID.

The network ID identifies the network, and all systems on the same network have the same network ID. Additionally, all systems on the same network have different host identifiers.

The Subnet Mask and the Network ID

IP addresses are matched with a subnet mask to identify the network ID and the host ID. Subnet masks are displayed in dotted decimal format similar to an IP address. The three most common subnet masks are as follows:

- 255.0.0.0
- 255.255.0.0
- 255.255.255.0

When the subnet mask is 255, that portion of the IP address is the network ID. When the subnet mask is 0, that portion of the IP address is the host ID.

> ***NOTE*** **SUBNET MASKS**
>
> **As you continue in your IT career, you'll learn that the subnet mask can include numbers other than 255 or 0. However, for the A+ exam, you'll see subnet masks with the numbers of 255 or 0. This makes it much simpler to identify the network ID.**

Consider Table 21-1, which shows an IP address of 192.168.1.5 and a subnet mask of 255.255.255.0.

TABLE 21-1 Identifying a Network ID

	First octet	Second octet	Third octet	Fourth octet
192.168.1.5	192	168	1	5
255.255.255.0	255	255	255	0
Network ID	192	168	1	0

In the first octet, the subnet mask is 255, so 192 is part of the network ID. The subnet mask is 255 in the second and third octets also, so 168 and 1 are also part of the network ID. However, the subnet mask is 0 in the last octet, so that portion of the network ID is 0.

Put together, you can see that the network ID is 192.168.1.0.

Host ID

The host ID is whatever is left over. Consider 192.168.1.5 with a subnet mask of 255.255.255.0. The network ID is 192.168.1.0, and the host ID is 5. The most important part of this is remembering that each system has different host IDs. More specifically, no two systems can have the same IP address. Because the network IDs must be the same, the host IDs must be unique on the network.

Consider what would happen if you and your neighbor both had the same mail address. How would the postal service know how to get the correct mail to you? Similarly, if two systems have the same IP address, TCP/IP is going to have problems getting the data to the correct system.

NOTE **IP CONFLICTS AND 0.0.0.0**

When two systems have the same IP address, it results in an IP address conflict. Usually, one system will recognize the conflict and assign itself an IP address of 0.0.0.0 and will be unable to communicate on the network. In some cases, both systems will be unable to communicate on the network.

Network ID Challenge

Table 21-2 shows a list of IP address and subnet mask combinations. Test yourself and see whether you can determine the network ID for each.

TABLE 21-2 Determine the Network ID

	First octet	Second octet	Third octet	Fourth octet
192.168.7.15	192	168	7	15
255.255.255.0	255	255	255	0
Network ID	?	?	?	?
172.16.4.3	172	16	4	3
255.255.0.0	255	255	0	0
Network ID	?	?	?	?
10.5.3.5	10	5	3	5
255.0.0.0	255	0	0	0
Network ID	?	?	?	?

In the first combination (192.168.7.15, 255.255.255.0), the subnet mask is 255 for the first three octets. Only the first three numbers in the IP address are in the network ID. Therefore, the network ID is 192.168.7.0

In the second combination (172.16.4.3, 255.255.0.0), the subnet mask is 255 in the first two octets. Only 172 and 16 are in the network ID, so it is 172.16.0.0.

The last combination (10.5.3.5, 255.0.0.0) has a 255 in only the first octet. The network ID is 10.0.0.0.

A network ID is always displayed with trailing zeros. That is, it is not accurate to show the network ID as 192.168.7, 172.16, or 10. The trailing zeros must be included so that you have four decimal numbers as 192.168.7.0 or 172.16.0.0, or 10.0.0.0.

EXAM TIP

You should be able to look at an IP address and subnet mask and easily determine the network ID. You'll see only one of the following subnet masks on the A+ exam: 255.255.255.0, 255.255.0.0, or 255.0.0.0.

Network IDs in a Network

The following two important points about the network ID and the host ID are worth repeating:

- All computers within a network must have the same network identifier.
- All computers within a network must have unique host identifiers.

For example, consider Figure 21-1. It shows two networks, labeled as Network 1 and Network 2, separated by a router. Each of the computers on Network 1 must have the same network ID. However, one of them is incorrect. Can you see which one?

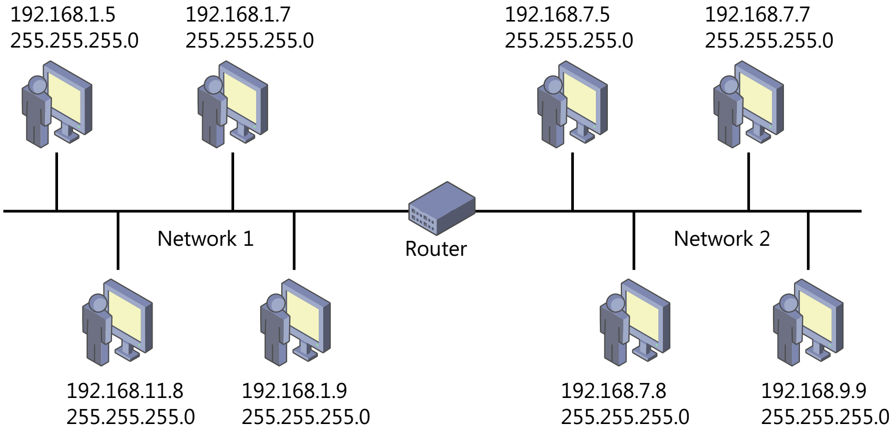


FIGURE 21-1 Two networks connected with a router.

EXAM TIP

The ability to identify an incorrect IP address on a computer is very valuable when troubleshooting and for answering some questions on the A+ exam.

Similarly, each of the computers on Network 2 must have the same network ID. However, one of these is also configured incorrectly. Can you see which one?

Most of the computers on Network 1 have a network ID of 192.168.1.0. However, the one on the bottom left has an IP address of 192.168.11.8, giving it a network ID of 192.168.11.0. This computer will be unable to communicate with any other system on the network.

The network ID on Network 2 for three of the computers is 192.168.7.0. However, the computer on the bottom right has a network ID of 192.168.9.0. This computer will be unable to communicate with other computers.

✓ Quick Check

1. What is wrong with the following IPv4 address: 192.257.2.5, 255.255.0.0?
2. What is the network ID of 192.168.24.6 with a subnet mask of 255.255.255.0?

Quick Check Answers

1. IPv4 addresses can't have numbers greater than 255 (such as 257).
2. 192.168.24.0.

Classful IP Addresses

A classful IP address has a predefined subnet mask based on the first number in the IP address. That is, just by looking at the IP address, you can identify the subnet mask. When you know the subnet mask, you should also be able to identify the network ID.

Table 21-3 shows the three classful IP addresses covered on the A+ exam. The first number of a Class A address is in the range of 1 to 126. An IP address of 10.1.2.3 has 10 as the first number. The number 10 is in the range of 1 to 126, so this is a Class A address and it has a subnet mask of 255.0.0.0. Further, the network ID is 10.0.0.0.

TABLE 21-3 Classful IP Addresses

Class	First octet range	Example	Subnet Mask
A	1 to 126	10.1.2.3	255.0.0.0
B	128 to 191	172.16.5.4	255.255.0.0
C	192 to 223	192.168.1.2	255.255.255.0

EXAM TIP

You should be able to easily identify the class of an IP address when you see it. For example, what class is 172.16.34.45? What is its subnet mask? What class is 192.168.7.3, and what is its subnet mask? 172.16.34.45 is a Class B address because the first number is 172 (in the range of 128 to 191), and the subnet mask is 255.255.0.0. 192.1687.7.3 is a Class C address because the first number is 192 (in the range of 192 to 223) and the subnet mask is 255.255.255.0.

Networks, Subnets, and LANs

It's important to recognize the difference between a network and a local area network (LAN). A network includes all the computers connected together with the same network ID. A LAN includes two or more networks connected together in the same location. These networks are separated by one or more routers.

Subnetting is beyond the scope of the A+ exam, but in short, it divides classful IP networks into smaller subnetworks, or subnets. Each subnet has the same network ID, and each subnet is separated by one or more routers. A LAN includes two or more subnets, two or more networks, or a combination of subnets and networks.

You might hear many technicians refer to networks generically as subnets. It's common, but it isn't entirely accurate. Technically, a network is a subnet only if the classful IP address has been divided.

Loopback Addresses

You might notice a range of numbers missing between Class A and Class B addresses. The entire range of 127.0.0.0 through 127.255.255.255 is reserved for testing. However, there's really only one address used in this range for testing. It's called the *loopback address,* and the address is 127.0.0.1.

For example, you can use the following command from the command prompt to ping the loopback address:

```
Ping 127.0.0.1
```

You should see a response similar to this:

```
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

EXAM TIP

You can also use the command ping localhost because systems resolve the name localhost to the IP address of 127.0.0.1. If the response is "Request timed out," it indicates a problem with TCP/IP on the local computer. As an A+ technician, you should make this one of the first things you check if you suspect a networking problem.

Ping sends four packets to the loopback address, and four replies are returned. This verifies that TCP/IP is installed and working correctly on the system. It doesn't check connectivity with other systems or verify that the hardware is working, but it does verify the TCP/IP protocols, also called the TCP/IP stack. It will succeed even if the network interface card (NIC) is disabled or unplugged from the network.

CIDR Notation

Another way that the IP address and subnet mask can be expressed is with Classless Inter-Domain Routing (CIDR) notation. CIDR notation identifies the number of bits that are one in the subnet mask, using /n. In this case, the n is the number of bits that are a one.

For example, consider a subnet mask of 255.255.255.0. The first octet is 255, representing eight ones (1111 1111). Similarly, the second octet is another eight ones, and the third octet is another eight ones. Therefore, the first 24 bits of the subnet mask are all ones. In this case, you can use /24 to represent the subnet mask.

Table 21-4 shows a few examples of CIDR notation.

TABLE 21-4 Expressing IP Addresses with CIDR Notation

IP Address	Subnet Mask	CIDR Notation
10.1.2.3	255.0.0.0	10.1.2.3 /8
172.16.1.2	255.255.0.0	172.16.1.2 /16
192.168.1.5	255.255.255.0	192.168.1.5 /24

There is no difference in the actual IP address or subnet mask when CIDR notation is used; it's just displayed differently. For example, the following two combinations represent the same IP address and subnet mask:

- 192.168.1.5, 255.255.255.0
- 192.168.1.5 /24

Unicast, Broadcast, and Multicast Addressing

IPv4 uses three primary types of addressing when sending traffic. The types are unicast, broadcast, and multicast.

- **Unicast** is one-to-one traffic. That is, the data is sent from one system to one other system.
- **Broadcast** is one-to-all traffic. One system sends the data to all other systems on the network. However, this is certainly not to all other systems in the world. Routers block broadcast traffic so that a broadcast is sent only to all the computers with the same network ID. A broadcast address is 255.255.255.255.

- **Multicast** is one-to-many traffic. A system can send data to multiple other systems. Multicast addresses are in the range of 224.0.0.1 through 255.255.255.254.

Only broadcast traffic stops at routers. Unicast and multicast traffic is routed to the correct destination through one or more routers.

✓ **Quick Check**

1. **What class is the following IP address: 10.192.168.5?**
2. **How can you check the TCP/IP stack?**

Quick Check Answers

1. Class A.
2. Ping the loopback address of 127.0.0.1.

TCP/IP Addressing in a Network

To communicate with other systems on the same network, every system in a network must have an IP address. Systems also need to have other information to communicate with systems in other networks.

You might remember that networks are separated by one or more routers. Each system needs to know the IP address of at least one adapter on a router so that it can reach other networks.

Default Gateway

A *gateway* is a path out of a network, and the default gateway identifies the default path out of a network. For example, if an internal system is trying to connect to the Internet, it goes through the default gateway. The default gateway is an interface on a router, and it has an IP address.

Figure 21-2 shows a network diagram with two default gateways identified in two different networks. Systems in Network 1 go through the default gateway with an address of 192.168.1.1. Systems in Network 2 go through the default gateway with an address of 192.168.7.1.

When a system transfers traffic from one computer to another, it first identifies the network ID of both systems. If the network IDs are the same, it knows that the computers are on the same network. If the networks IDS are different, it knows it needs to go through the default gateway.

While some people call the default gateway the router, you can see in Figure 21-2 that this isn't entirely accurate. It's like calling a car door a car. You use the door to get out of the car, but the door isn't the car. Similarly, you use the default gateway to get out of a network through the router, but the default gateway isn't the router.

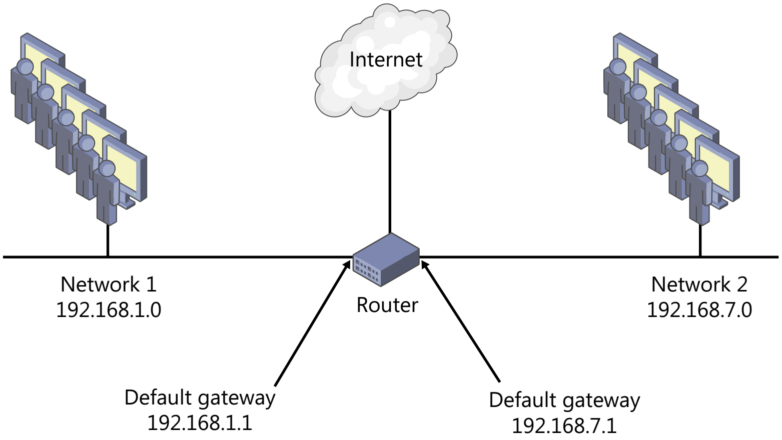


FIGURE 21-2 Default gateways for different networks.

Note that the default gateways for the networks are not the same. That is, each network has only one default path out of the network and only one default gateway.

It is very common to assign a default gateway with the first IP address in the network. It's not required, but it is common. For example, Network 1 has a range of IP addresses of 192.168.1.1 through 192.168.1.254, so you'll often see the default gateway assigned the address of 192.168.1.1.

EXAM TIP

The default gateway must have the same network ID as other systems in the network. If it has a different network ID, systems won't be able to communicate with it, and it won't be able to reach any systems outside of the network.

Public vs. Private IPs

Systems on internal networks use private IP addresses, and systems on the Internet use public IP addresses. Private IP addresses are formally defined in Request for Comments (RFC) 1918 as any address in one of the following ranges:

- 10.0.0.0–10.255.255.255 (Class A)
- 172.16.0.0–172.31.255.255 (Class B)
- 192.168.0.0–192.168.255.255 (Class C)

These are the only addresses you'll see on any internal network. Additionally, routers on the Internet will not route any traffic using these IP addresses as either a source or destination IP address.

EXAM TIP

You should be able to identify an address as public or private. If you see a computer in an internal network with a public IP address assigned, you'll know that it is not configured correctly.

NAT

Network Address Translation (NAT) is a protocol that translates private IP addresses to public and public IP addresses back to private. It is installed on a system such as a router or firewall located between the Internet and a private network.

Internal networks have private IP addresses and public networks have public IP addresses. However, computers on an internal network still need to be able to communicate on public computers on the Internet. NAT helps this process. It also helps hide internal computers from attackers on the Internet.

In smaller networks, a router with NAT would have one public IP address. In many larger networks, devices running NAT use multiple public IP addresses.

Figure 21-3 shows an internal network that accesses the Internet through a router with NAT. The internal network has private IP addresses, and NAT translates them to a public IP address when a user connects. For example, a user in a private network can access Bing.com on the Internet by using Internet Explorer. NAT translates the IP addresses so that the user in the private network can access the public website.

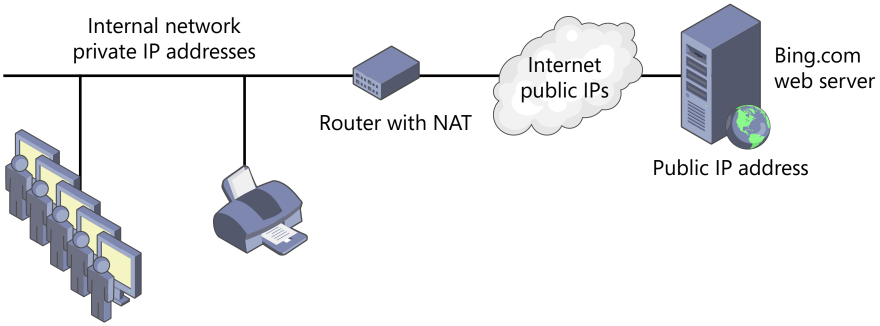


FIGURE 21-3 NAT translates private and public IP addresses.

✔ Quick Check

1. **What identifies the default path out of a network for a system?**
2. **Is 198.162.5.1 a private address?**

Quick Check Answers

1. The default gateway.
2. No. However, 192.168.5.1 (not 198.162.5.1) is a private address.

Static vs. Dynamic IP Addresses

Each computer on a network must have an IP address assigned. Most computers will receive the IP address dynamically or automatically, but you can also manually assign a static IP address.

Using DHCP for Dynamic IP Addresses

Dynamic Host Configuration Protocol (DHCP) is used to dynamically assign IP addresses and other TCP/IP configuration information to systems. A DHCP client is any system configured to receive TCP/IP information from a system running DHCP.

Large organizations use a DHCP server, but small offices and home offices (SOHOs) often have a wireless router that includes DHCP. When a DHCP client turns on, it sends a DHCP query, and if DHCP is running on the network, DHCP will provide TCP/IP configuration to the client.

DHCP commonly provides an IP address, subnet mask, and the default gateway. In many cases, DHCP will also provide the system with the address of a DNS server and a WINS server.

MORE INFO **CHAPTER 20, "UNDERSTANDING PROTOCOLS," AND CHAPTER 23, "EXPLORING WIRELESS NETWORKING"**

DNS and WINS are discussed in Chapter 20. As a reminder, DNS resolves host names to IP addresses and WINS resolves NetBIOS names to IP addresses. Chapter 23 covers wireless networks, including wireless routers.

APIPA Addresses

If a system can't reach a DHCP server, it will often assign itself an Automatic Private IP Address (APIPA). An APIPA address always starts with 169.254 and has a subnet mask of 255.255.0.0. The address can be anything in the range of 169.254.0.1 to 169.254.255.254.

Recalling the discussion earlier in this chapter about the network ID, do you know the network ID of the following address: 169.254.3.7 255.255.0.0? The network ID is always 169.254.0.0. Because of this, computers with APIPA addresses can communicate with each other without a DHCP server and without any manual configuration.

However, APIPA does not assign a default gateway, the address of a DNS server, or any other TCP/IP information. It assigns only the IP address and a subnet mask.

Chapter 24, "Connecting and Troubleshooting a Network," covers command-line tools such as ipconfig that you can use to identify a computer's assigned IP address. If you see an address starting with 169.254, you know that it is an APIPA address.

EXAM TIP

APIPA addresses are assigned if a DHCP client does not receive a response from DHCP. They always start with 169.254 and have a subnet mask of 255.255.0.0. They never assign a default gateway, address of a DNS server, or any other information. If you see an APIPA address, it's a clear indication of a DHCP-related problem. Troubleshooting steps would include identifying why the client can't reach DHCP and why DHCP is not responding.

Reserving IP Addresses

You can also use DHCP to reserve a specific IP address to a client. You do so by mapping the media access control (MAC) address of the DHCP client to a specific IP address. When the DHCP client turns on and requests an IP address, the DHCP server recognizes the client and gives it a specific IP address.

The Real World sidebar at the beginning of this chapter gives a perfect example. I recently purchased a network printer that ran as a DHCP client. When it first turned on, DHCP running on my wireless router assigned it an IP address of 192.168.1.114. I then configured other systems in my home network to use this printer with an IP address of 192.168.1.114.

At some point, we had a power outage. When the printer turned back on, DHCP assigned it an IP address of 192.168.1.123. At this point, none of my systems could print to the printer because they were trying to reach it with the IP address of 192.168.1.114.

After I realized the problem, I could have resolved it in one of two ways:

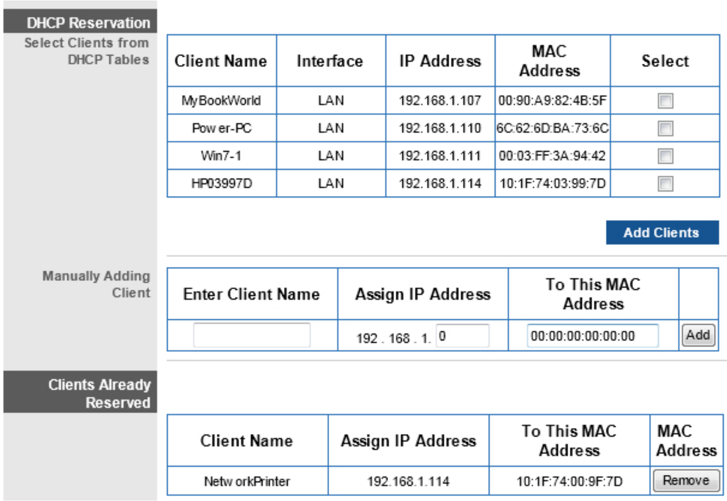
- Manually assign the IP address of 192.168.1.114
- Reserve the address of 192.168.1.114 to this printer

I chose to reserve the address. Figure 21-4 shows the DHCP reservation table from my wireless router. The table at the top shows all the clients currently assigned IP addresses from DHCP. The bottom table shows how I reserved the printer's MAC address (10:1F:74:00:9F:7D) to the IP address of 192.168.1.114.

Every time the printer turns on, it sends a DHCP query, and the wireless router assigns it an address of 192.168.1.114.

NOTE Ipconfig /all and MAC address

You can determine the MAC address of a system by entering ipconfig /all at a command prompt. The MAC address is listed as the physical address.



DHCP Reservation

Select Clients from DHCP Tables

Client Name	Interface	IP Address	MAC Address	Select
MyBookWorld	LAN	192.168.1.107	00:90:A9:82:4B:5F	□
Pow er-PC	LAN	192.168.1.110	6C:62:6D:BA:73:6C	□
Win7-1	LAN	192.168.1.111	00:03:FF:3A:94:42	□
HP03997D	LAN	192.168.1.114	10:1F:74:03:99:7D	□

Manually Adding Client

Enter Client Name	Assign IP Address	To This MAC Address	
	192 . 168 . 1. 0	00:00:00:00:00:00	Add

Clients Already Reserved

Client Name	Assign IP Address	To This MAC Address	MAC Address
Netw orkPrinter	192.168.1.114	10:1F:74:00:9F:7D	Remove

FIGURE 21-4 Reserving an IP address based on the MAC address.

Manually Assigning Static IP Addresses

Occasionally, you'll want to manually assign an IP address. In this case, you must type in all of the information needed by the system. You can assign static IP addresses for a server in a small office home office (SOHO) or a network printer. You won't need to do so very often, but you can also assign static IP addresses to client or desktop systems.

EXAM TIP

It's common either to manually assign an IP address for a network printer or to use a DHCP reservation to ensure that it always has the same IP address.

The process is different depending on what device you're configuring the IP address. Network printers usually have a menu-driven interface on the front panel that you can use. Operating systems allow you to configure the properties of the network interface card.

Accessing the NIC in Windows

Configuring the NIC is the same in Windows 7, Windows Vista, and Windows XP. However, the path to the NIC is a little bit different in these systems. You can use the following steps to access the NIC on each operating system.

Windows 7:

1. Click Start and type **Network and Sharing Center** in the Search Programs And Files text box.
2. Select Network And Sharing Center. Alternatively, you can open the Control Panel and select the Network And Sharing Center from the Network And Internet category.

3. On the left-pane menu, click Change Adapter Settings. You'll now see a list of available NICs on the system.

Windows Vista:

1. Click Start and type **Network and Sharing Center** in the Start Search text box.
2. Select Network And Sharing Center. Alternatively, you can open the Control Panel and select the Network And Sharing Center from the Network And Internet category.
3. On the left-pane menu, click Manage Network Connections. You'll now see a list of available NICs on the system.

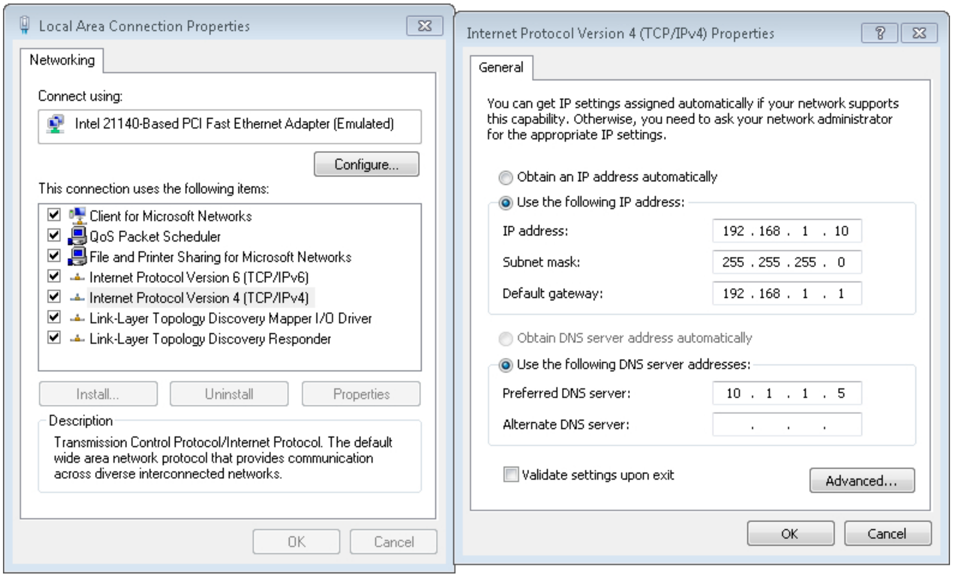
Windows XP:

1. Click Start and select Control Panel.
2. If you're using Category View, select Network And Internet Connections and then Network Connections. If you're using Classic View, select Network Connections. You'll now see a list of available NICs on the system.

Assigning Static or Dynamic Addresses in Windows

After you've accessed the NIC, you use the following steps to manipulate the properties. These steps are for a Windows 7 computer, but they are the same on other Windows systems.

1. Right-click the network interface card (NIC) adapter and select Properties. The adapter is commonly named Local Area Connection.
2. Select Internet Protocol Version 4 (TCP/IPv4) and click Properties.
3. With the General tab selected, you can select Obtain An IP Address Automatically. With this selected, the computer will receive all of the TCP/IP configuration information from DHCP.
4. If you want to manually assign an IP address, select Use The Following IP Address.
5. Enter a valid IP address, subnet mask, and default gateway for your network. If your network has a DNS server, you can also enter its IP address here. Your display will resemble the following graphic.



Local Area Connection Properties

Networking

Connect using:

Intel 21140-Based PCI Fast Ethernet Adapter (Emulated)

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Install... Uninstall Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 10 . 1 . 1 . 5

Alternate DNS server: . . .

□ Validate settings upon exit

Advanced...

OK Cancel

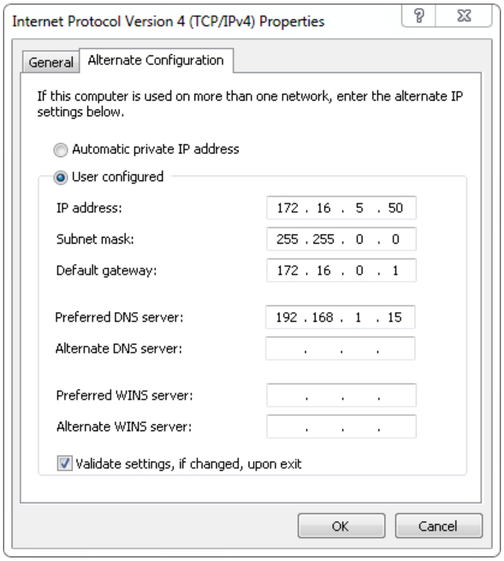
6. Click OK twice, and you're done.

Assigning Alternate IP Addresses in Windows

Mobile users sometimes need to have both a dynamic and a static IP address. For example, imagine Lori has a laptop that she uses at work and when she travels to customer locations. While at work, her computer is configured to obtain an IP address dynamically from DHCP. However, when she visits Lucerne Publishing, she needs a statically assigned IP address to access the Internet through their network. You could train Lori how to do this and have her manually make these changes, but there's an easier way: by configuring an alternate IP address.

If you followed the previous steps to assign an IP address in Windows, you might have noticed a subtle change when you selected Obtain An IP Address Automatically. Specifically, an additional tab named Alternate Configuration appears. This tab *disappears* when you select Use The Following IP Address.

Select this tab and you can configure the alternate configuration settings. Figure 21-5 shows this property page configured with an alternate IP address, subnet mask, default gateway, and DNS server. Normally, Automatic Private IP Address is selected.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

If this computer is used on more than one network, enter the alternate IP settings below.

○ Automatic private IP address

● User configured

IP address: 172 . 16 . 5 . 50

Subnet mask: 255 . 255 . 0 . 0

Default gateway: 172 . 16 . 0 . 1

Preferred DNS server: 192 . 168 . 1 . 15

Alternate DNS server: . . .

Preferred WINS server: . . .

Alternate WINS server: . . .

☑ Validate settings, if changed, upon exit

FIGURE 21-5 Assigning alternate configuration settings.

When Lori is at work, her computer receives the TCP/IP settings from DHCP. Lucerne Publishing doesn't have a DHCP server, so when she goes there, her computer never receives a DHCP response. Instead, it will assign itself the TCP/IP configuration settings from the Alternate Configuration tab.

EXAM TIP

By default, the Alternate Configuration is set to Automatic private IP address. Therefore, if a system doesn't receive a response from DHCP, it will assign itself an APIPA address.

Manipulating NIC Properties

Beyond the TCP/IP settings, the NIC has several other properties that you might need to manipulate. Chapter 19, "Exploring Cables and Connectivity," discusses this in the context of comparing half-duplex, full-duplex, and auto settings. A NIC is normally set to automatically configure the speed and duplex setting based on the connection, and you can use the steps in Chapter 19 to verify or modify the settings.

As a reminder, you can access these properties by right-clicking the NIC and selecting Properties. From the Properties page, click the Configure button and then click the Advanced tab. These properties are not standardized, so they usually have different names on different NICs.

Some of the other settings you can manipulate include the following:

- **Wake-On-LAN (WOL)**. This might be listed as WOL, Wake On Magic Packet, Wake On Pattern Match, Shutdown Wake-On-LAN, or something similar. A WOL packet (also called a magic packet) is a specially formatted packet that can cause a computer to turn on even if it is sleeping, hibernating, or completely turned off. Administrators use this to send updates to systems during non-business hours. This setting needs to be enabled on the NIC and in BIOS.

NOTE **SLEEP AND HIBERNATE**

Sleep is a low-power state, but the computer can wake up rather quickly. Hibernate copies the contents of RAM onto the disk as a file and turns the system off. When the system is turned back on, it copies the data from the disk back to RAM, returning the system to the same state it was in when it was turned off.

- **QoS (Quality of Service)**. This may be named QoS, Quality Of Service, Flow Control, or something similar. Some networks use QoS techniques to control the traffic by assigning different priorities to different types of traffic. For example, an administrator might want to cap the amount of streaming video that is allowed on a network and use QoS techniques to give streaming video traffic a very low priority. QoS is enabled on the NIC and configured on multiple devices throughout the network.
- **PoE (Power over Ethernet)**. Some NICs on mobile devices can be powered by voltages sent over an Ethernet cable. This is useful in devices located in remote areas where power isn't readily accessible. You need only to plug in a twisted-pair Ethernet cable into the RJ-45 port, and it powers the device. It isn't used for a desktop computer, but it is used from some wireless access points, IP phones, and IP cameras and can be configured on them.

✓ **Quick Check**

1. **A system has an IP address of 169.254.5.6. What does this indicate?**
2. **What are the two ways IP addresses can be assigned?**

Quick Check Answers

1. **It's an APIPA address, and the system is not receiving a response from DHCP.**
2. **Manually and with DHCP.**

Examining IPv6 Addresses

An IPv6 address uses 128 bits instead of the 32 bits used by an IPv4 address. IPv6 addresses are typically displayed as eight groups of four hexadecimal characters. For example, the following is a valid IP address:

FC00:0000:0000:0076:0000:042A:B95F:77F5

You might remember from Chapter 1 that a hexadecimal number uses the characters 0–9 and A–F. Each hexadecimal number can be represented with four bits. For example, 8 is 1001 and F is 1111.

Why We Need IPv6

While IPv4 lasted quite a while, the Internet officially ran out of IPv4 addresses. The Internet Assigned Numbers Authority (IANA), which assigns IP addresses, issued the last batch of IPv4 addresses on February 3, 2011. Without IPv6, the Internet would need to stop growing.

IPv4 supports about 3.7 billion IP addresses on the Internet, using a 32-bit address space. In contrast, IPv6 uses 128 bits, so it can support more IP addresses. Specifically, IPv6 supports over 340 undecillion IP addresses. If you're like me, you probably don't use *undecillion* in everyday language. Here's where it comes in: million, billion, trillion, quadrillion, quintillion, sextillion, septillion, octillion, nonillion, decillion, undecillion.

This will be enough for everyone to have as many IP addresses for their own use as they need. Computers, printers, TVs, gaming devices, mobile phones, tablets, and more can all have their own IP address with IPv6, and you're not likely to run out.

With 340 undecillion IPv6 addresses, that works out to more than 3.7 billion IP addresses for every person on the planet. Therefore, everyone can have more addresses than are available with IPv4 on the entire Internet today. Actually, it's more: it works out to about 50 thousand trillion trillion IPv6 addresses per person. I just find it a little easier to comprehend numbers in the billions.

You might be wondering about IPv5. It was designed to use 64 bits for an IP address, but the designers realized that 64 bits wouldn't give them enough IP addresses. It never made it past the draft stages, and IPv6 was adopted to replace IPv4 instead.

Omitting IPv6 Leading Zeros

Each group of hexadecimal numbers in an IPv6 address includes four characters. However, if this number has leading zeros, you can omit them. This works the same in decimal. If I asked you to write down the number seven, you would write 7. You wouldn't typically write 007.

Similarly, the following IPv6 address can be written by omitting leading zeros in each of the groups:

- FC00:0000:0000:0076:0000:042A:B95F:77F5
- FC00:0:0:76:0:42A:B95F:77F5

Table 21-5 shows this with the hexadecimal groups labeled. You can see that leading zeros are omitted in the second, third, fourth, fifth, and sixth groups. An important point to make here is that we still have eight groups of hexadecimal numbers.

TABLE 21-5 Omitting Leading Zeros in an IPv6 Address

1st	2nd	3rd	4th	5th	6th	7th	8th
FC00	0000	0000	0076	0000	042A	B95F	77F5
FC00	0	0	76	0	42A	B95F	77F5

It's also important to point out that you can't omit trailing zeros. In the first group, FC00 cannot be shortened to just FC. Of course, this works the same in decimal. If I owed you 20 dollars, you wouldn't be very happy if I just gave you two dollars, saying that I decided to omit a zero.

IPv6 Zero Compression

IPv6 addresses often have a long string of zeros within them. You can include them, but you can also use a double colon (::) to indicate a string of zeros. Anyone that reads the address with the double colon knows to replace it with a string of zeros.

For example, the following two addresses are the same:

FC00:0000:0000:0076:0000:042A:B95F:77F5

FC00::76:0:42A:B95F:77F5

The second IPv6 address shows only six groups of hexadecimal numbers. Because you know that a full IPv6 has eight groups of numbers, you know that the double colon represents two groups of zeros.

An important rule is that you can compress only one string of zeros with a double colon. For example, the following is not valid:

FC00:0000:0000:0076:0000:042A:B95F:77F5

FC00::76::42A:B95F:77F5

You can see two strings of zeros in the original IPv6 address. Without seeing the original IPv6 address, you won't know how many zeros to assign to each double colon. It could be either of the following:

FC00:**0000:0000**:0076:0000:042A:B95F:77F5

FC00:0000:0076:**0000:0000**:042A:B95F:77F5

EXAM TIP

Valid IPv6 addresses include only hexadecimal numbers (0–9 and A–F). An IPv6 address can be expressed as eight groups of hexadecimal numbers separated by colons, or fewer groups with a single double colon. You can use only a single double colon in an IPv6 address.

IPv6 Prefixes

IPv6 addresses use prefixes to identify the network identifier. This is similar to how an IPv4 address uses an IP address and subnet mask to identify the network. However, IPv6 does not use a subnet mask. Instead, IPv6 uses prefix length notation. This is similar to CIDR notation used with IPv4 addresses.

For example, you might see an address like the following:

2001:0DB8:1234::5678:9ABC:DEF0:/48

The /48 prefix notation indicates that the first 48 bits are in the prefix. Similarly, the /64 in the following IPv6 address indicates that the first 64 bits are in the prefix:

2001:0DB8:1234::5678:9ABC:DEF0:/64

Peaceful Coexistence with IPv4

The IPv6 designers recognized that it wasn't feasible to require everyone in the world to switch over at the same time. Could you imagine someone picking an arbitrary date, such as February 3, 2011, and telling everyone in the world that they needed to switch over on that day? Some would be left behind with no Internet access.

Instead, they designed IPv6 so that it can interoperate with IP4. They can both operate on a network at the same time without any problems.

You'll find that most networks that are running IPv6 today are also running IPv4. At some point in the future, IPv4 will be phased out, but that's unlikely to happen anytime soon.

IPv6 Loopback Address

IPv6 has a loopback address similar to IPv4. As a reminder, you can ping the loopback address to verify that the TCP/IP stack is functioning properly. In this case, you can verify that the IPv6 portion of TCP/IP is functioning properly.

The IPv6 loopback IP address is ::1. This is using zero compression, indicating that it's a string of zeros with only a single one at the end. You can use the following command to test it from the command prompt:

```
Ping ::1
```

If successful, you should see the following results:

```
Pinging ::1 with 32 bytes of data:
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Ping statistics for ::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

✓ **Quick Check**

1. **What is wrong with the following IPv6 address: 2001:DB00:34:5678::DEG0:/48?**
2. **What is wrong with the following IPv6 address: 2001::B80:12:5678::DA30:/64?**

Quick Check Answers

1. **It has an invalid hexadecimal number (G in DEG0).**
2. **It has two sets of double colons, but only one set is allowed.**

Chapter Summary

- IPv4 addresses use 32 bits and are expressed in dotted decimal format like this: 192.168.1.5.
- The subnet mask is used to identify the network ID portion of an IP address. All computers on a network must have the same network ID.
- Classful IP addresses are identified by the first number in the IP address.
  - Class A: 1 to 126 as in 10.1.2.3,
    Subnet mask: 255.0.0.0
  - Class B: 128 to 191 as in 172.16.1.2
    Subnet mask: 255.255.0.0
  - Class C: 192 to 223 as in 192.168.1.2
    Subnet mask: 255.255.255.0
- The IPv4 loopback address is 127.0.0.1. Pinging this address verifies that the TCP/IP stack is functioning.
- The default gateway identifies the default path out of a network to other networks. It is the IP address of the router's NIC that is connected to the network. It is typically the first IP address on the network.
- Only private IP addresses should be used in a private network. Private IP address ranges are:
  - 10.0.0.0–10.255.255.255
  - 172.16.0.0–172.31.255.255
  - 192.168.0.0–192.168.255.255
- DHCP assigns TCP/IP configuration information to DHCP clients. This includes an IP address, subnet mask, default gateway, address of DNS, address of WINS, and more. A DHCP client receives DHCP information when it turns on.
- If a DHCP client doesn't receive a response from DHCP, it assigns itself an IP address starting with 169.254. This address is known as an APIPA address.

- An alternate address can be used with DHCP for a computer used in different locations. If DHCP doesn't respond, the alternate IP address will be used.
- IPv6 addresses use 128 bits and are expressed as eight groups of hexadecimal numbers separated by colons. Valid hexadecimal numbers are only 0–9 and A–F.
- Zero compression replaces zeros in IPv6 with two colons. You can use only one set of double colons in an IPv6 address.
- IPv4 and IPv6 are compatible with each other and can run on the same network without problems.
- The IPv6 loopback address is ::1.

Chapter Review

Use the following questions to test your knowledge of the information in this chapter. The answers to these questions, and the explanations of why each answer choice is correct or incorrect, are located in the "Answers" section at the end of this chapter.

1. Which of the following is a Class C IPv4 address?

   A. 10.1.2.3

   B. 127.0.0.1

   C. 172.16.5.4

   D. 192.168.1.21

2. Which of the following would be appropriate to assign to a client in a private network?

   A. 10.1.1.1

   B. 198.162.6.1

   C. 173.16.2.3

   D. 127.0.0.1

3. A system has an IP address and subnet mask combination such as the following:

   192.168.1.5

   255.255.255.0

   Which of the following would be a valid IP address for the default gateway?

   A. 255.255.255.255

   B. 192.168.1.1

   C. 192.168.15.1

   D. 192.168.1.0

4. A system is unable to access any network resources. You check the IP address and see that it includes the following information:

   IP address: 169.254.34.78

   Subnet mask: 255.255.0.0

   Default gateway: blank

   What is the most likely problem?

   A. DHCP

   B. IP address is wrong

   C. Subnet mask is wrong

   D. Default gateway is down

5. Which of the following would most often have manually assigned IP addresses?

   A. Windows 7–based computers in a SOHO

   B. Windows 7–based computers in a large domain

   C. Servers and network printers

   D. Servers and USB attached printers

6. Which of the following is a valid IPv6 address?

   A. FC00:0:0:76:0:0:042A:B95F:77F5

   B. FC00::0157:03CE::A47:52AF

   C. FC00:76::4234:BF:F5

   D. FC00:0000:1200:2076:0000:42A4:C95G:F523

7. Which of the following is the loopback address for IPv6?

   A. 127.0.0.1

   B. ::1

   C. 192.168.1.1

   D. 255.255.255.255

Answers

1. **Correct Answer:** D
   - **A. Incorrect:** 10.1.2.3 is a Class A address, in the range of 1 to 126.
   - **B. Incorrect:** 127.0.0.1 is the IPv4 loopback address.
   - **C. Incorrect:** 172.16.5.4 is a Class B address in the range of 128 to 191.
   - **D. Correct:** The first number in a Class C address is in the range of 192 to 223, and 192 is in this range.
2. **Correct Answer:** A
   - **A. Correct:** Only valid private IP addresses should be assigned to computers in a private network. A private IP address should be in one of the following ranges: 10.0.0.0–10.255.255.255, 172.16.0.0–172.31.255.255, 192.168.0.0–192.168.255.255.
   - **B. Incorrect:** An IPv4 address starting with 198 is public.
   - **C. Incorrect:** An IPv4 address starting with 173 is public.
   - **D. Incorrect:** This is the IPv4 loopback address.
3. **Correct Answer:** B
   - **A. Incorrect:** This is a broadcast address and should not be assigned to the default gateway.
   - **B. Correct:** The default gateway must have the same network ID as other clients on the network. In this case, the network ID of the system is 192.168.1.0. If the default gateway is 192.168.1.1, it also has a network ID of 192.168.1.0.
   - **C. Incorrect:** An IP address of 192.168.15.1 gives the default gateway a network ID of 192.168.15.0, which is different from the system's network ID.
   - **D. Incorrect:** 192.168.1.0 is the network ID and should not be assigned to a client.
4. **Correct Answer:** A
   - **A. Correct:** An address starting with 169.254 is an Automatic Private IP Address (APIPA). A DHCP client will assign itself an APIPA address if it doesn't receive a response from DHCP.
   - **B. Incorrect:** The IP address is correct as an APIPA address.
   - **C. Incorrect:** The subnet mask is correct for APIPA.
   - **D. Incorrect:** APIPA doesn't assign a default gateway.

5. **Correct Answer:** C
    - **A. Incorrect:** Windows 7–based computers normally receive IP addresses automatically from DHCP.
    - **B. Incorrect:** Windows 7–based computers normally receive IP addresses automatically from DHCP.
    - **C. Correct:** Servers and network printers often have manually assigned IP addresses.
    - **D. Incorrect:** A USB-attached printer does not use an IP address.
6. **Correct Answer:** C
    - **A. Incorrect:** An IPv6 address has eight groups of hexadecimal numbers separated by seven colons, but this has nine groups separated by eight colons.
    - **B. Incorrect:** An IPv6 can use one set of double colons for zero compression, but not two.
    - **C. Correct:** This is a valid IPv6 address using zero compression and omitting leading zeros. The full IPv6 address is FC00:0076:0000:0000:0000:4234:00BF:00F5.
    - **D. Incorrect:** IPv6 addresses use hexadecimal numbers (0–9 and A–F). G is not a valid hexadecimal number.
7. **Correct Answer:** B
    - **A. Incorrect:** 127.0.0.1 is the IPv4 loopback address.
    - **B. Correct:** The IPv6 loopback address is ::1.
    - **C. Incorrect:** 192.168.1.1 is a valid IPv4 address but not the loopback address.
    - **D. Incorrect:** 255.255.255.255 is the broadcast address.