

Lesson

1

Understanding Local Area Networking

Objective Domain Matrix

Skills/Concepts	Objective Domain Description	Objective Domain Number
Examining Local Area Networks, Devices, and Data Transfer	Understand local area networks (LANs)	1.2
	Understand switches	2.1
Identifying Network Topologies and Standards	Understand network topologies and access methods	1.5



Key Terms

broadcast

centralized computing

client/server

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Carrier Sense Multiple Access with Collision Detected (CSMA/CD)

Computer Telephony Integration

CTI-based server

data transfer rate

database server

demilitarized zone (DMZ)

distributive computing

Ethernet

file server

frames

full-duplex

half-duplex

host

hub

IEEE 802.3

IP address

local area network (LAN)

mesh topology

messaging server

multiport repeater

network adapter

network controller

network documentation

network operating systems (NOSs)

network topology

P2P

peer-to-peer

perimeter network

print server

ring topology

RJ-45

serial data transfer

star topology

switch

transceiver

unicast

virtual LAN (VLAN)

web server

Windows 10

wireless access point (WAP)

wireless local area network (WLAN)



Real World Scenario

Lesson 1 Case

Local area networks are used by just about every organization, and today many homes have them as well. This lesson refers to a fictitious company named Proseware, Inc., that wants to implement a new LAN in a brand-new office, which will serve approximately 20 users. The company requires an extremely quick network that can transfer many different types of data. They want the most cost-effective layout without losing speed or efficiency! The network engineer's job responsibilities include selecting the right equipment, making sure it is all compatible, and getting it installed on time. The network engineer should have a thorough understanding of technologies, such as Ethernet and switching, because she will be critical in designing and implementing the network. This lesson covers all of the concepts necessary so you can be confident installing the network that this company desires. As we progress through this book, we will build on this scenario and add lots more networking technologies to the infrastructure.

Examining Local Area Networks, Devices, and Data Transfer

Simply stated, a *network* is two or more computers that exchange data. A *local area network (LAN)* is a group of these computers that are confined to a small geographic area, usually one building. Setting up a LAN requires computers with network adapters, central connecting devices to connect those computers together, and a numbering scheme (such as IP addresses) to differentiate one computer from the next. It can also include servers, some type of protective device such as a firewall, and connections to perimeter networks that are adjacent to the LAN.

Defining the LAN

As mentioned, a LAN requires computers with network adapters, central connecting devices, and some type of medium to tie it altogether, be it cabled or wireless connections. These must be connected together in some way to facilitate the transfer of data. It is important to define how they are connected together, as well as how they actually transmit data.

Certification Ready

What is a local area network (LAN)? Objective 1.2

We mentioned that a network is used to exchange data. But what are the real reasons that an organization will desire (or need) a network? They can be organized into four categories:

Sharing The sharing of files, databases, and media

Communication The methods of communication, such as email, instant messaging, and faxing

Organization The ability to centralize data and make it more accessible and efficient

\$\$\$ The ability for the network to provide cost savings and/or increase productivity

Some would place security in this list of categories, but, unfortunately, as you will find, many networks, devices, and operating systems are insecure when they are fresh out of the box. Just having a network doesn't ensure security. In fact, many steps must be taken to implement a secure network.

To understand local area networks (LANs) better, it helps to write out the structure of the LAN—to *document* it. *Network documentation* is any information that helps describe, define, and otherwise explain how computers are connected in a physical and logical way. For example, the physical connection could be cables, and the logical connection could be the various IP addresses used by the devices on the network.

In the following exercises, you will:

- Examine typical LAN network documentation.
- View the type of network adapter in a computer, inspect the type of connection that the network adapter makes to the network, and view its Properties page.
- Define how information is sent across the LAN.
- Configure IP addresses on hosts.

The ability to document networks is an important skill for network administrators. The documentation phase occurs before networks are built and whenever changes or additions are made to the network. Microsoft Visio is a common tool used for network documentation; Figures 1.1 to 1.3 were developed using Visio.

Examine LAN Network Documentation

To examine LAN network documentation, perform the following steps.

Download

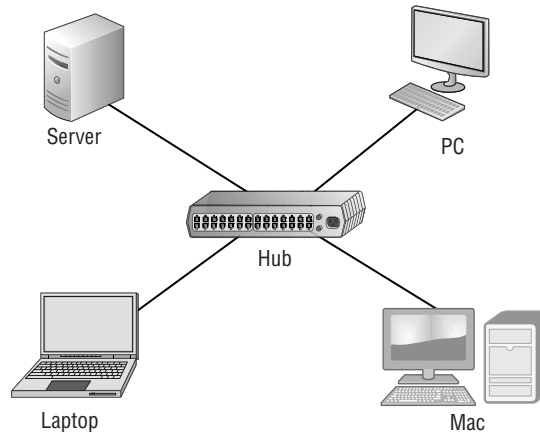
You can download a free trial of Visio from the Microsoft website. A link is provided on the companion website.

Certification Ready

What are the capabilities of hubs as compared to switches? Objective 2.1

1. Examine Figure 1.1, which shows a basic example of a LAN.

FIGURE 1.1 Basic LAN documentation



NOTE

Today, a hub is considered a legacy hardware device that is largely obsolete. Hubs have been replaced by network switches, which are discussed later in this section and can be found in very old installations or specialized applications.

You will notice that in the center of the diagram is a *hub*, also known as a *multiport repeater*. This is the most basic of central connecting devices (CCDs); it connects each of the computers, known as hosts, to each other by way of copper-based cables. When a host needs to send data, it first sends that data to the hub, where it is amplified and *broadcast* to the rest of the network. Broadcasting means that the data is sent out to every host on the network. Of course, only the intended recipient keeps the data; the rest of the hosts discard it. Although this is a bit wasteful, it was the standard for a long time. Today, however, switching technology, which is more efficient, is the standard. You'll learn more about switching technology later in this lesson.

In the figure, several hosts connect to the hub, including:

- A server, used to centralize data and share it with (or *serve* it to) other computers on the network.
- A PC (personal computer) usually acts as a client on the network, most likely getting its information from the server. The PC can also store information locally.
- A Mac (Macintosh) computer, which is another type of client computer; once again, this computer can store information locally, or get it from the server.
- A laptop, which could be a PC or a Mac, is meant for portability. However, it can also store and access data the same way the other computers do.

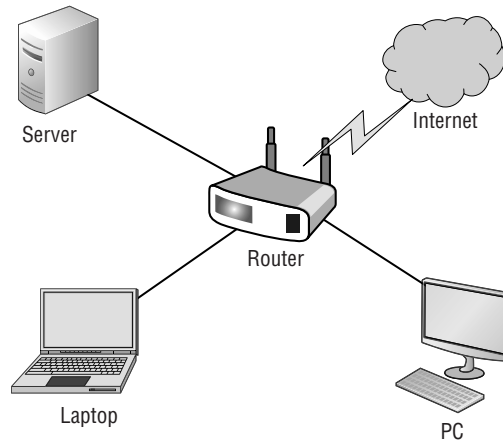
- Examine your own network and record your results. Use Visio, if possible; otherwise, draw out your own network documentation on paper. Whether you are at home or at a school or business, chances are that you are connected to a LAN. Try to identify any hosts on the network (PCs, laptops, servers, etc.). Then, identify the central connecting device that ties everything together. This could be a basic hub, a switch, or a router or multifunction network device.



If you are using Microsoft Visio, utilize the Basic Network Diagram template. This can be accessed in the Network section when starting a new document.

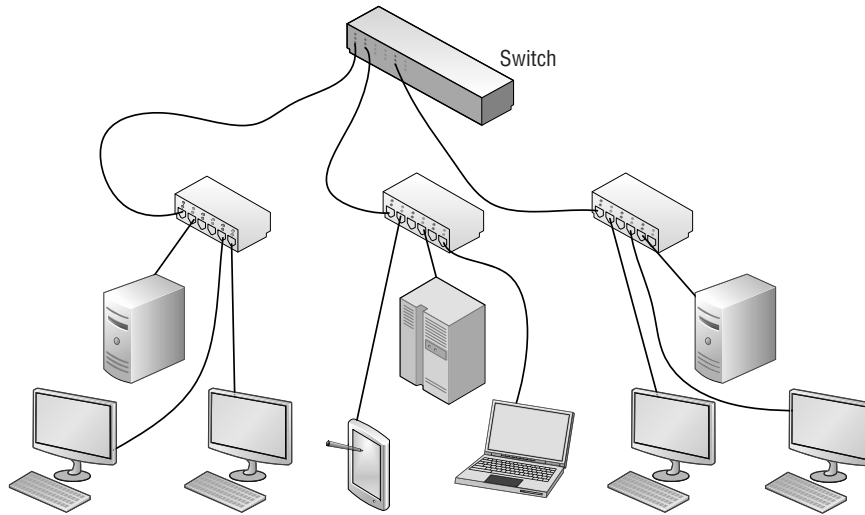
- Examine Figure 1.2. This is an intermediate example of a LAN.

FIGURE 1.2 Intermediate LAN documentation



In Figure 1.2, the hub is replaced with a basic four-port router; these are also referred to as SOHO (Small Office/Home Office) routers. The router acts as a central connecting device, connecting the hosts together, but also has a special communications link to the Internet, allowing the hosts to send and receive data to and from computers on the Internet. That communications link between the router and the Internet is where the LAN ends. So, the PC, laptop, server, and router are part of the LAN. Anything else beyond the router is considered to be outside of the LAN.

- Examine your own LAN again. If possible, identify any routers and connections to the Internet (or other networks). Add these to your written, or Visio, documentation.
- Examine Figure 1.3. This is a slightly more advanced example of a LAN.

FIGURE 1.3 Advanced LAN documentation

In Figure 1.3, more central connecting devices are added. Instead of connecting hundreds of devices to a single central connecting device, you can break up the network in a hierarchical fashion. For example, on the left side of the figure are two PCs and one server connected to a hub. Let's say that these represent 24 computers, and that each other group of computers connected to a hub also represents 24 computers. Instead of connecting all the computers to a single, central connecting device, which might not be able to physically support all of the hosts, the groups of 24 hosts are connected to their own hub. Then, the hubs are all daisy-chained to a *switch* at the top of the figure. The switch will most likely be a powerful (and expensive) device, in order to support all of the computers that ultimately connect to it. You can regard the individual hubs as devices that allow connectivity for single departments in a company, or individual classrooms in a school. The master switch at the top of the hierarchical tree connects everything together; however, it also acts as a single point of failure, which is addressed in Lesson 2. As you can guess, this type of network architecture is the kind we will need to use to accomplish the goals laid out in the scenario at the beginning of this lesson.

The *network adapter*, also known as a network interface card (NIC), is the device that enables the sending and receiving of data to and from your computer. It might be integrated into the motherboard or it might act as a separate device that connects to a PCI slot, or perhaps connects to a PC Card slot or USB port. It connects to the network by way of cable (wired) or by air (wireless). It has its own basic CPU to process transmitted data and a ROM chip to store information about itself. Network adapters also have a software component known as a driver, defining how the card will interact with the operating system; this usually includes a Properties page that can be accessed in the operating system, enabling the user to configure the adapter as he sees fit.

View the Network Adapter

To view the network adapter, perform the following steps.

1. Examine Figure 1.4, which shows a typical network adapter.

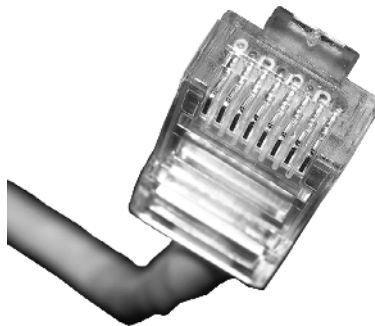
FIGURE 1.4 Photo of a typical network adapter



This particular network adapter is a PCI card, but again, network adapters come in many different forms. However, notice the port on the card. This is known as an *RJ-45* port, and is where the RJ-45 plug at the end of the network cable connects. This is the most common type of network adapter port, allowing the adapter to connect to most of today's wired networks.

2. Look for the network adapter on your computer. If the computer only uses a wireless network adapter, look for an antenna on the card. Laptops have an internal antenna, but you can usually find out if you are connected wirelessly by looking at the wireless LED.
3. Examine Figure 1.5. This is a typical patch cable that connects to an RJ-45 port.

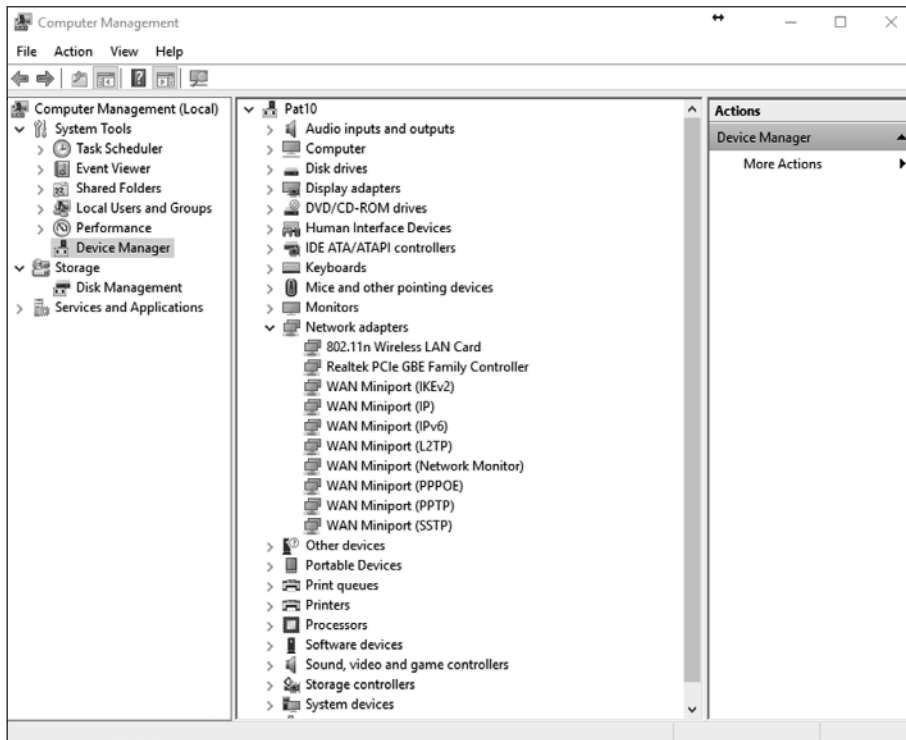
FIGURE 1.5 Photo of a typical patch cable



This type of cable is known as twisted pair. It has an RJ-45 plug on the end, which is molded so it can only connect one way to the RJ-45 port. It also has a tab that locks it in place. The RJ-45 plug is slightly larger than a telephone cable's RJ-11 plug, but looks very similar. Another difference is that the phone plug *usually* has four wires, whereas the RJ-45 plug has eight.

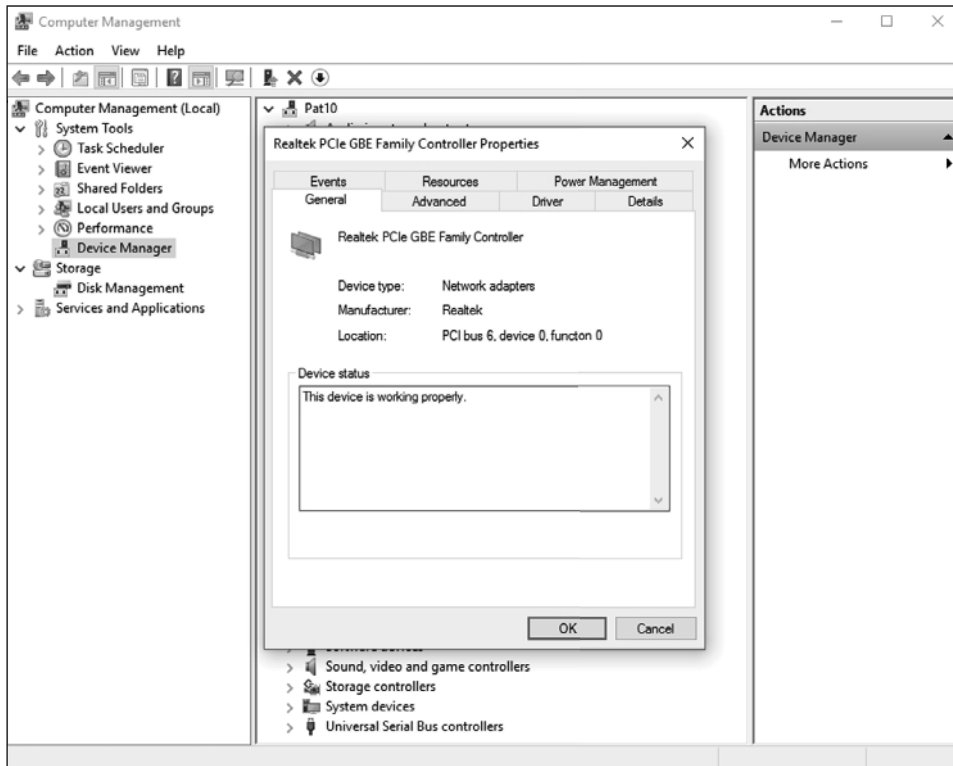
4. Identify the cable that connects your computer to the network. Disconnect the cable (finish any downloads from the Internet if in progress first) and view the connector. If you are connected via a cable, attempt to identify what device is connected to the other end of the cable, such as a hub, switch, or router.
5. Now let's access the operating system and look at the properties of a network adapter. For this example, we are using a Windows 10 client computer with a Realtek PCIe network adapter. However, older versions of Windows have almost identical window and dialog box names, and the navigation to those windows is similar as well.
 - a. Right-click Start and choose Computer Management. Alternatively for Windows 10, and for Windows Server 2016, click Start, type **Computer Management**, and then press Enter.
 - b. Click Device Manager.
 - c. Click the > sign to expand the Network adapters category, as shown in Figure 1.6.

FIGURE 1.6 Device Manager with the Network adapters category expanded



- d. Right-click the network adapter and choose **Properties**. A dialog box similar to the one shown in Figure 1.7 opens.

FIGURE 1.7 Properties dialog box of a Realtec network adapter

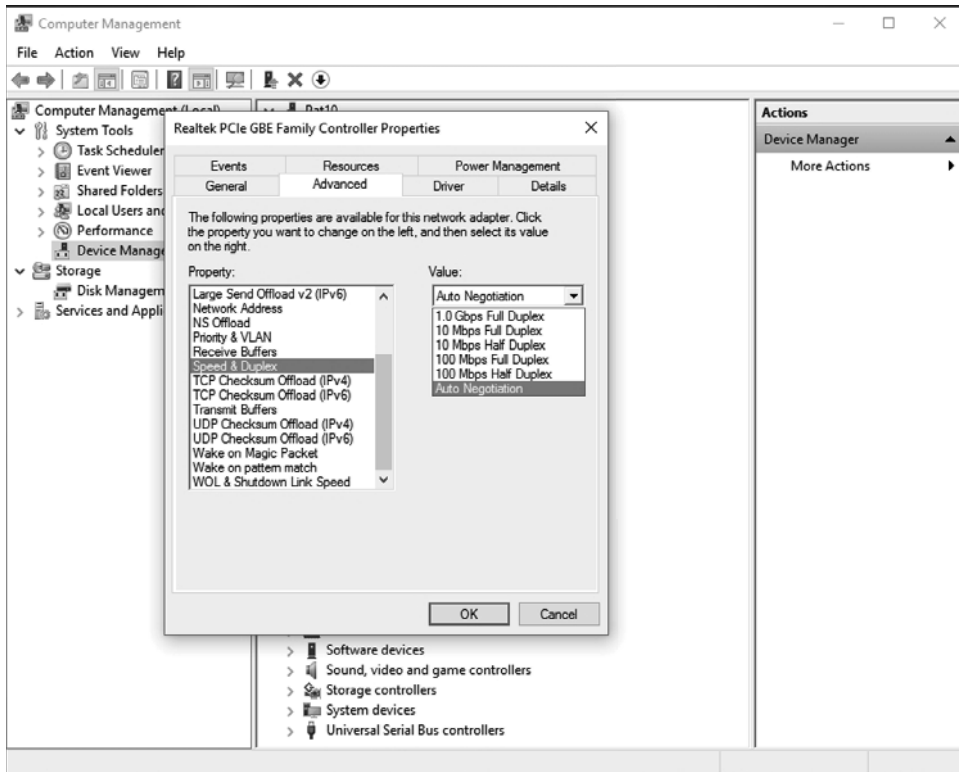


6. Click the **Advanced** tab. If you click the **Speed & Duplex** option, you can then change the value, as shown in Figure 1.8.



NOTE

A network adapter is only as fast as the network it connects to!

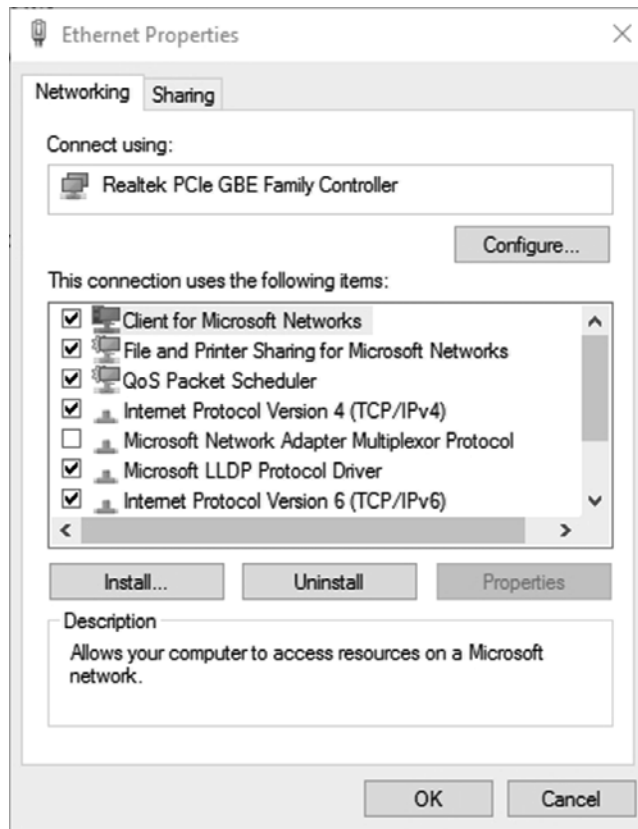
FIGURE 1.8 Link speed of the network adapter

Full-duplex means that the network card can send and receive data *simultaneously*. In the Speed and Duplex drop-down menu, you can select various speeds, including 10 Mbps, 100 Mbps, and 1 Gbps. You can also select *half-duplex*, which means that the network adapter can send and receive data, but not at the same time. Full-duplex is the superior connection, as long as your central connecting device supports it. A full-duplex connection can *transceive* (transmit and receive) twice as much information per second compared with a half-duplex connection. So, to meet the requirements of the original scenario, you would probably want your client computers to connect at 1 Gbps as well as utilize full-duplex negotiations.

You can tell that a card is active because the Link Status field on the physical device shows a green light. You can also open the device Status window (Open Network and Sharing Center, and click the adapter link) to see the current speed of the adapter such as 1 Gbps, its media state, how long it has been up and the current activity.

7. Finally, every network adapter will have a logical name. By default, the network adapter is known as Ethernet, although you can change the name if you so desire. Ethernet will have its own Properties page and a status page. Let's view these now:
 - a. Right-click the Network icon on the far right of the taskbar and choose Open Network And Sharing Center. The Network And Sharing Center window opens.. An alternate way to access the Network and Sharing Center is to right-click Start and choose Control Panel. Then, navigate to Network And Internet > Network And Sharing Center.
 - b. Click the Change Adapter Settings link. The Network Connections window opens. (Navigation to this window is slightly different in other versions of Windows.)
 - c. In this window, right-click the Ethernet icon and choose Properties. The Ethernet Properties dialog box opens, as shown in Figure 1.9.

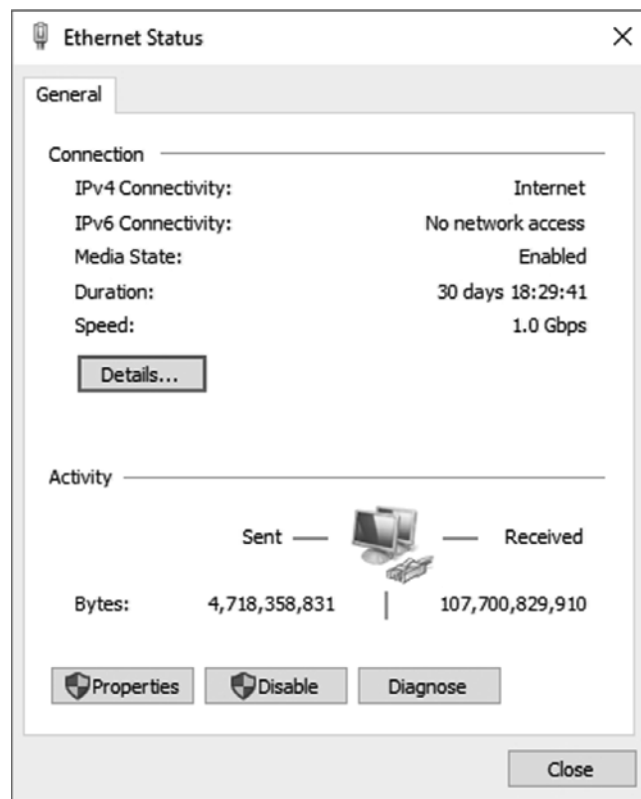
FIGURE 1.9 The Ethernet Properties dialog box



From here, you can configure Internet Protocol (IP), bind new protocols to the network adapter, and so on. You'll access this dialog box frequently during the course of this book.

- d. Click Cancel to close the dialog box. This should return you to the Network Connections window.
- e. Now, double-click the Ethernet icon. The Ethernet Status dialog box opens, as shown in Figure 1.10. This dialog box displays the type of connectivity, speed, and how long the adapter has been connected; it also shows the total bytes sent and received. In addition, from this dialog box, you can access the Properties dialog box and diagnose the network adapter, if necessary.

FIGURE 1.10 The Ethernet Status dialog box



Defining Data Transfer on the LAN

Generally, when data is transferred on the LAN, it is sent in a serial fashion over twisted-pair cabling. *Serial data transfer* means the transfer of one bit at a time—a single bit stream. This is usually the format in which information is sent from one network

adapter to another. Let's discuss this in a little more depth. Suppose one user wants to send a small text file (100 bytes in size) to another user on the network. There are many ways to do this; one way is to map a network drive to the other user's computer and simply copy and paste the text file to the other computer's hard drive. When this is done, a few things happen:

1. First, the text file is packaged by the operating system into what is known as a packet. This packet is slightly larger than the original file. That packet is then sent to the network adapter.
2. Next, the network adapter takes that packet and places it inside of a frame, which is slightly larger than a packet. Usually, this is an Ethernet frame.
3. Now, the frame of information needs to be sent on to the physical media—the cabling. To do this, the network adapter breaks down the frame of information into a serial bit stream to be sent one bit at a time across the cables to the other computer.
4. The receiving computer takes the serial bit stream and re-creates the frame of data. After analyzing the frame and verifying that it is indeed the intended recipient, it strips the frame information so that only the packet remains.
5. The packet is sent to the operating system, and, ultimately, the text file shows up on the computer's hard drive, available to the other user through Windows Explorer. This is a very basic example of data transfer, which is expanded on in Lesson 2.

Usually, local area networks utilize one of several Ethernet standards. *Ethernet* is a set of rules that govern the transmission of data between network adapters and various central connecting devices. All network adapters and central connecting devices must be compatible with Ethernet in order to communicate with each other. A very common type of Ethernet is known as 802.3u or Fast Ethernet that runs at 100 Mbps. Another common one is 802.3ab or Gigabit Ethernet.

In this type of network, when a computer wants to send data, that data is broadcast to every other host on the network by default. The problem with this is that usually there is only one recipient of the data. The rest of the computers simply drop the data packets. This, in turn, wastes network bandwidth. To alleviate this, about 15 years ago, Ethernet switching was developed, and it is used in most networks today. Switching has many advantages, one of which is that the switch only sends unicast traffic. *Unicast* is when information is sent to one host only. This reduces network traffic greatly, and helps with packet loss and duplicates.

We have mentioned network speed a few times already. A more accurate term is *data transfer rate*, otherwise known as bit rate. This is defined as the maximum bits per second (bps) that can be transmitted over the network. As mentioned, it is rated in bits and is signified with a lowercase *b*, for example, 10 Mbps. The lowercase *b* helps to differentiate from data that is stored on a hard drive, which uses an uppercase *B* that stands for bytes, for example 10 MB.

Of course, all this means nothing without an addressing system in place. The most common type of network address is the Internet Protocol address, or IP address.

Configuring Internet Protocol

Internet Protocol, or IP, is the part of TCP/IP that, among other things, governs IP addresses. The *IP address* is the cornerstone of networking. It defines the computer or host you are working on. Today, every computer and many other devices have one. An IP address allows each computer to send and receive information back and forth in an orderly and efficient manner. IP addresses are like your home address. Just like your home address identifies your house number and the street you live on, an IP address identifies your computer number and the network it lives on. A common example of an IP address is 192.168.1.1.

Now, every IP address is broken down into two parts: the network portion, in this case 192.168.1, which is the network your computer is a member of, and the host portion, which is the individual number of your computer, differentiating your computer from any others on the network. In this case, it's .1. How do we know this? The subnet mask tells us.

The subnet mask is a group of four numbers that define what IP network the computer is a member of. All of the 255s in a subnet mask collectively refer to the network portion, while the 0s refer to the host portion. This is illustrated in Table 1.1. This table shows a typical Class C IP address and the default corresponding subnet mask. If you were to configure the IP address of a Windows computer as 192.168.1.1, Windows would automatically default to a subnet mask of 255.255.255.0. If any other computers would like to communicate with yours, they need to be configured with the same network number; however, every computer on the same network needs to have a different host number or an IP conflict might ensue. Of course, as a talented administrator, you'll learn how to avoid IP conflicts—and you'll learn some tips on how to do so in Lessons 4 and 5.

TABLE 1.1 An IP Address and Corresponding Subnet Mask

Type of Address	First Octet	Second Octet	Third Octet	Fourth Octet
IP address	192	168	1	1
Subnet mask	255	255	255	0

IP addresses are actually 32-bit dotted-decimal numbers. If you were to convert an IP address's decimal numbers to binary, you'd have a total of 32 bits. It is considered dotted because each number is separated by a dot. Altogether, they contain four numbers, each of which is a byte or octet. For example, 192 is an octet and its binary equivalent is 11000000, which is 8 bits. 168 is also an octet, its binary equivalent is 10101000, and so on. Adding all four octets together equals 32 bits.

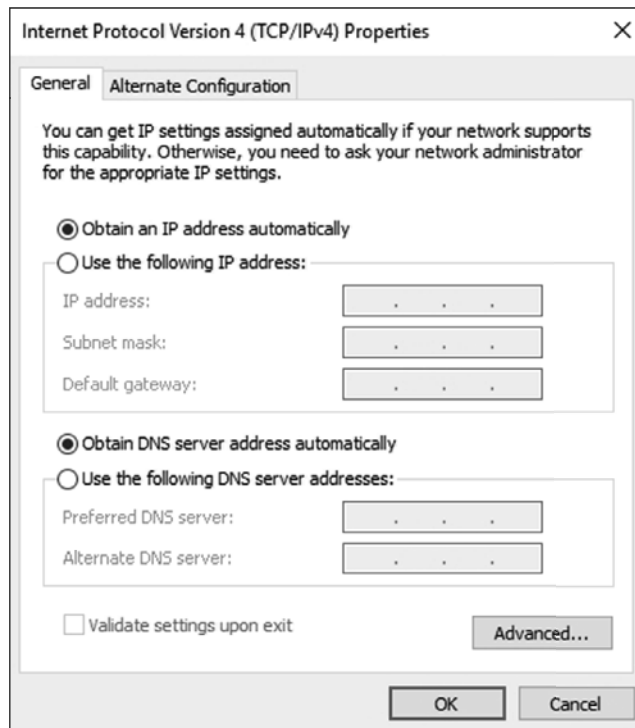
IP addresses are usually applied to your network adapter, but can be applied to other devices, such as switches, routers, and so on. It's the fact that the device or computer has an IP address that makes it a *host*. Let's configure IP on our Windows 10 host now. Remember that other Windows computers will be configured in a very similar way.

Configure IP Addresses

To configure IP addresses, perform the following steps.

1. Access the Ethernet Properties dialog box.
2. Click Internet Protocol Version 4 and then click the Properties button. The Internet Protocol Version 4 Properties dialog box opens. Write down the current settings (if there are any) so that you can return the computer to these settings at the end of the exercise.
3. By default, the Obtain an IP address automatically and Obtain DNS server address automatically radio buttons are enabled, as shown in Figure 1.11. That means that the network adapter will attempt to get all its IP information from a DHCP server or other device like a SOHO (Small Office/Home Office) four-port router. However, we want to configure the adapter statically, so let's continue on!

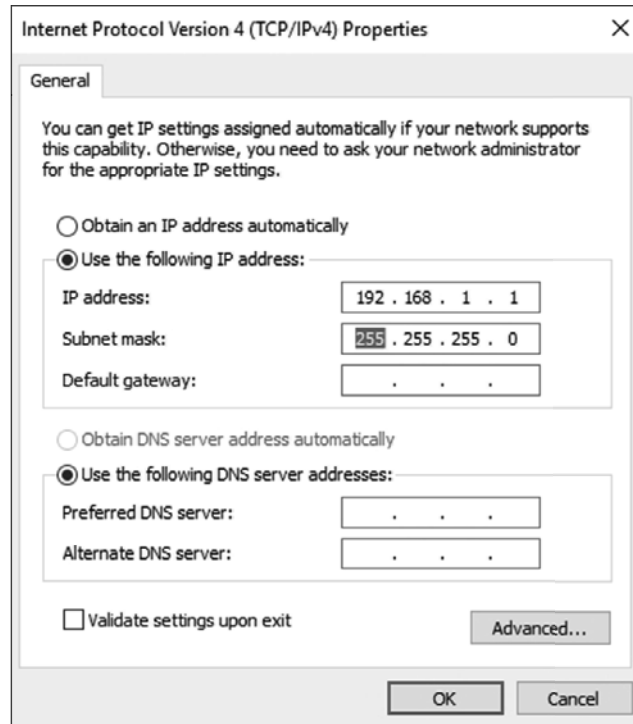
FIGURE 1.11 The Internet Protocol Version 4 Properties dialog box



4. Click the “Use the following IP address” radio button. This enables the other fields so you can type in the IP information. Enter the following:
 - For the IP address, enter **192.168.1.1**.
 - For the Subnet mask, enter **255.255.255.0**.

- Leave the Default gateway and the Preferred DNS server fields blank. The Default gateway is needed if you need to communicate with remote computers. The DNS is needed if you need to perform name resolution (names to IP addresses).
- When you are finished, it should look like Figure 1.12.
- If you have other computers, try configuring their IP addresses as well; the host portion of the IP should ascend once for each computer: .1, .2, .3, and so on.

FIGURE 1.12 The Internet Protocol Version 4 Properties dialog box configured statically

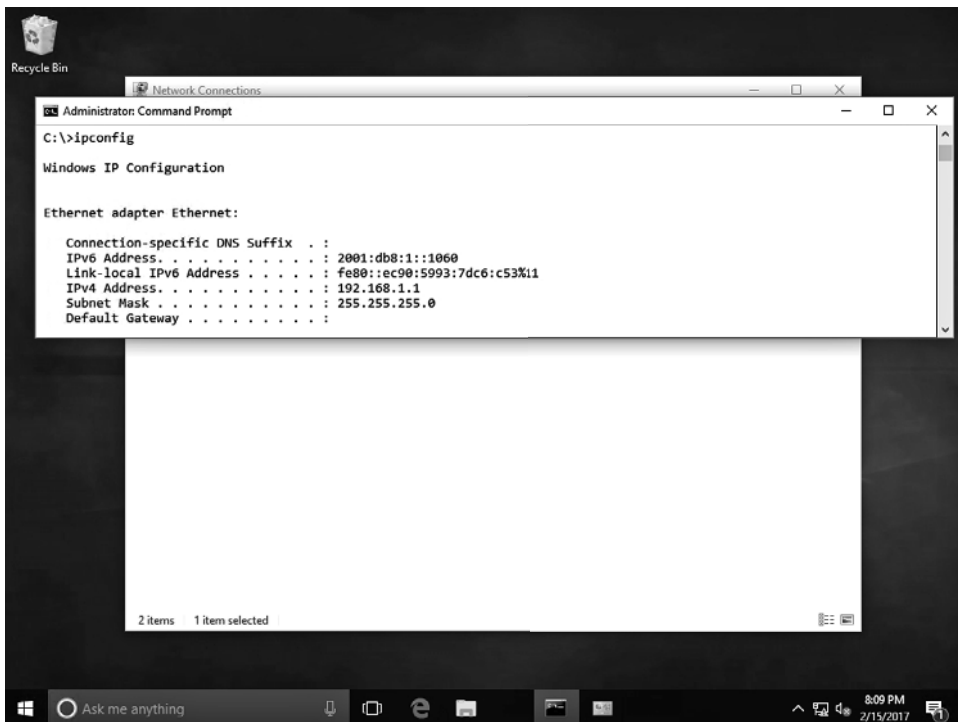


If you are working with others as you complete this exercise, each person should enter a different IP address. For example, the first person should enter 192.168.1.1, the second person should enter 192.168.1.2, and so on. This avoids any possible IP conflicts.

5. Click OK. Then, in the Ethernet Properties dialog box, click OK. This completes and binds the configuration to the network adapter.

6. Test your configuration. We will do this in two ways, first with the `ipconfig` command, and second with the `ping` command:
 - a. Open the Command Prompt window. Do this by pressing the Windows+R keys and typing `cmd` in the Open field. In the Command Prompt window, type `ipconfig`. The results should look similar to Figure 1.13. Notice the IPv4 Address field in the results and the IP address that is listed. It should be the IP address you configured previously. If not, go back and check your Internet Protocol Properties dialog box.

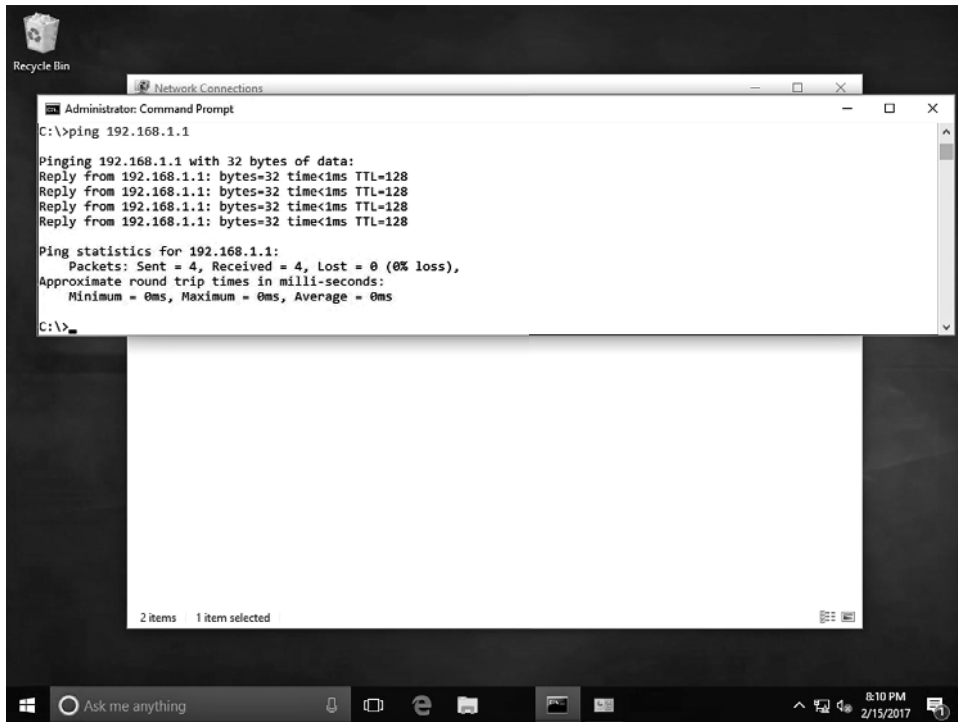
FIGURE 1.13 Ipconfig results in the Command Prompt window



- b. Ping a computer on the same 192.168.1 network. If there are no other computers, ping your own IP address. For example, type the following command:

ping 192.168.1.1

This command sends requests out to the other IP address. If the other computer is running and configured properly, it should reply back. A positive ping would look similar to Figure 1.14, where four replies are received by the pinging computer.

FIGURE 1.14 Ping results in the Command Prompt window

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

If you do not receive replies, but do receive another message, for example, “request timed out,” check the IP configuration again, and check to ensure that the computer you are trying to ping is configured properly. In addition, make sure that the computers are wired to the network.



Always test your network configurations!

You can also ping your own computer by way of the loopback address, also known as the local loopback. Every Windows computer automatically gets this address; it is 127.0.0.1. This is in addition to the logical address that you assigned earlier. Try the command `ping loopback` and check out the results you get. You can also try `ping localhost` and `ping 127.0.0.1`. Regardless, you should get results from 127.0.0.1. When pinging this address, no network traffic is incurred because the network adapter is really just looping the ping back to the OS; it never places any packets on to the network, so this is a solid way to test if TCP/IP is installed correctly to a network adapter, even if you aren’t physically connected to the network!

When you are finished, return your computer back to its regular IP settings. You’ll learn more about the Internet Protocol in Lesson 4.

Identifying Types of LANs

There are several types of local area networks that a computer can connect to. An organization must make a choice as to whether it will have wired connections, wireless connections, or a mix of the two. In addition, it is also possible to have virtual LANs. You should know these types of LANs for the exam.

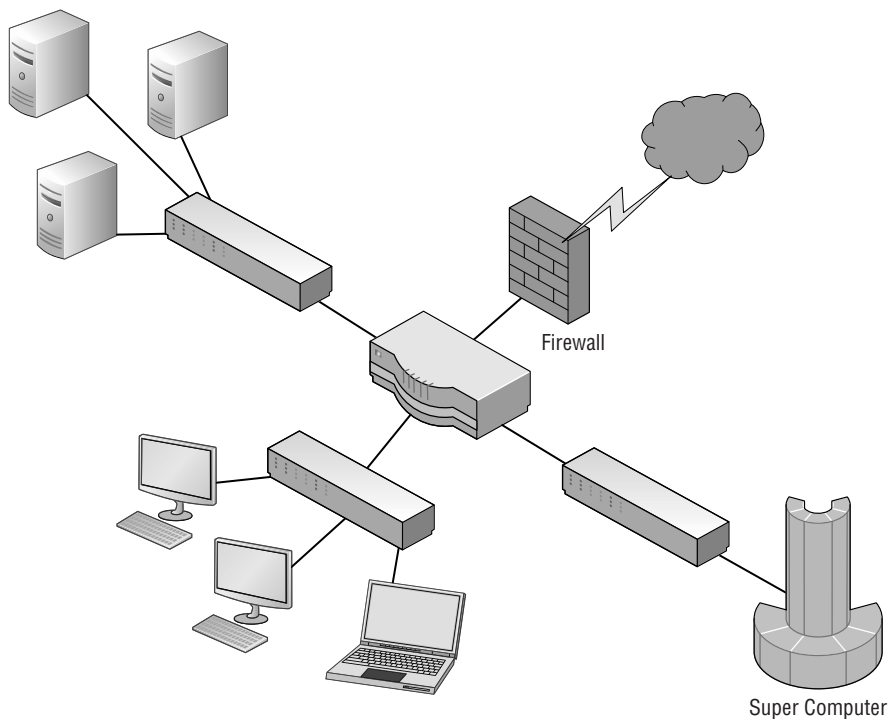
Certification Ready

What is the difference between a wired LAN and a wireless LAN? Objective 1.2

The first and most common type of LAN is the wired LAN. Computers and other devices are wired together by way of copper-based, twisted-pair cables. These cables have RJ-45 plugs on each end, making the actual connection to RJ-45 ports that reside on the computer's network adapter, and on hubs, switches, or routers. (Of course, there will probably be some other cabling equipment in between each of these, but this equipment is covered in more depth in Lesson 3.)

Figure 1.15 gives yet another diagram, but this time it's three LANs connected together by a router. Some new devices appear in this figure: a firewall, which protects the LAN (or LANs) from the Internet, and a supercomputer, which occupies its own little LAN.

FIGURE 1.15 Wired LAN diagram

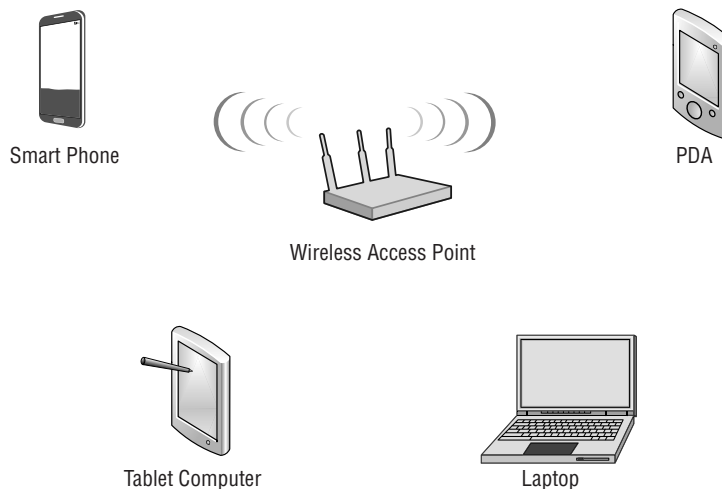


Generally, the connection from the PCs to their switch will be either 100 Mbps or 1 Gbps. Whatever speed you decide to use must be supported by each port of the switch and by each of the computers. In this diagram, they are wired to the switch. To accomplish gigabit network speeds, the cables used would have to be Category 5e or greater (more details on the types of cabling are covered in Lesson 3).

However, the connection from the server farm to the switch in the upper left of the figure and the supercomputer to its switch should be faster than your average PC connection. So, if the PCs on the LAN are connecting at 100 Mbps, the servers might be better off connecting at 1 Gbps; or, if the PCs are connecting at 1 Gbps, the servers would connect at 10 Gbps. High-speed connections should also be made between the three switches and the router. Now we are looking at a more accurate representation of a network setup our fictitious company needs from the original scenario! But just wait, the network documentation is going to get much more detailed. After all, we are only in Lesson 1!

Historically, wired networks are much faster than wireless networks. But now, it is by a much smaller margin due to the fact that wireless networking technology has made giant leaps and bounds over the past decade or so. A *wireless local area network (WLAN)* has many advantages, the most standout of which is the ability to roam. A person with a laptop, handheld computer or PDA, or another like device can work from anywhere. However, because wireless LANs can pose additional security problems, some companies have opted not to use them in their main offices. But with advancements in security, including developments in encryption, wireless is now more popular than ever. Figure 1.16 illustrates some wireless devices.

FIGURE 1.16 Wireless LAN diagram



The *wireless access point (WAP)* acts as the central connecting device for the network. But now, one of the advantages is that the network can consist of more types of devices, including smartphones, PDAs, tablet computers, and laptops. Of course, PCs and laptops equipped with wireless network adapters will be able to connect to this network as well.

Wireless networks and wired networks can coexist. In small networks, a single device can act as a wireless access point, switch, router, and firewall! However, larger networks usually have one or more separate wireless access points that connect in a wired fashion to a network switch. And wireless access points have a limited range. Therefore, you might need to implement multiple WAPs depending on the size of the building and the area you want to cover.

More Info

For more information about wired and wireless networks, refer to Lesson 3.

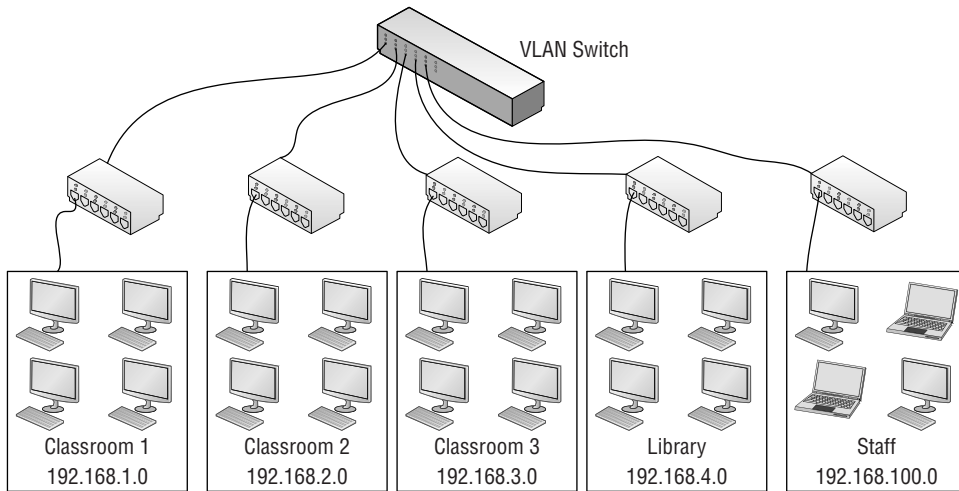
Certification Ready

What is a VLAN? Objective 1.2

There is another type of LAN, the virtual LAN. A *virtual LAN (VLAN)* is a group of hosts with a common set of requirements that communicate as if they were connected together in a normal fashion on one switch, regardless of their physical location.

A VLAN is implemented to segment the network, reduce collisions, organize the network, boost performance, and increase security. Usually, switches control the VLAN. Like subnetting, a VLAN compartmentalizes the network and can isolate traffic. But unlike subnetting, a VLAN can be set up in a physical manner; an example of this is the port-based VLAN, as is shown in Figure 1.17. In this example, each set of computers, such as Classroom 2, has its own VLAN (which is dedicated to the 192.168.2.0 network in this case); however, computers in that VLAN can be located anywhere on the *physical* network. As another example, computers within the VLAN “Staff” could be located in several physical areas in the building, but regardless of where they are located, they are associated with the Staff VLAN because of the physical port they connect to.

There are also logical types of VLANs like the protocol-based VLAN and the MAC address-based VLAN, but by far the most common is the port-based VLAN. The most common standard associated with VLANs is IEEE 802.1Q, which modifies Ethernet frames by “tagging” them with the appropriate VLAN information, based on which VLAN the Ethernet frame should be directed to.

FIGURE 1.17 Example of a VLAN

Getting to Know Perimeter Networks

Perimeter networks are small networks that usually consist of only a few servers, which have some form of access to the Internet. Generally, the term perimeter network is synonymous with DMZ. You should be able to identify a DMZ and its purpose in an organization, as well as know how to implement a basic DMZ.

Certification Ready

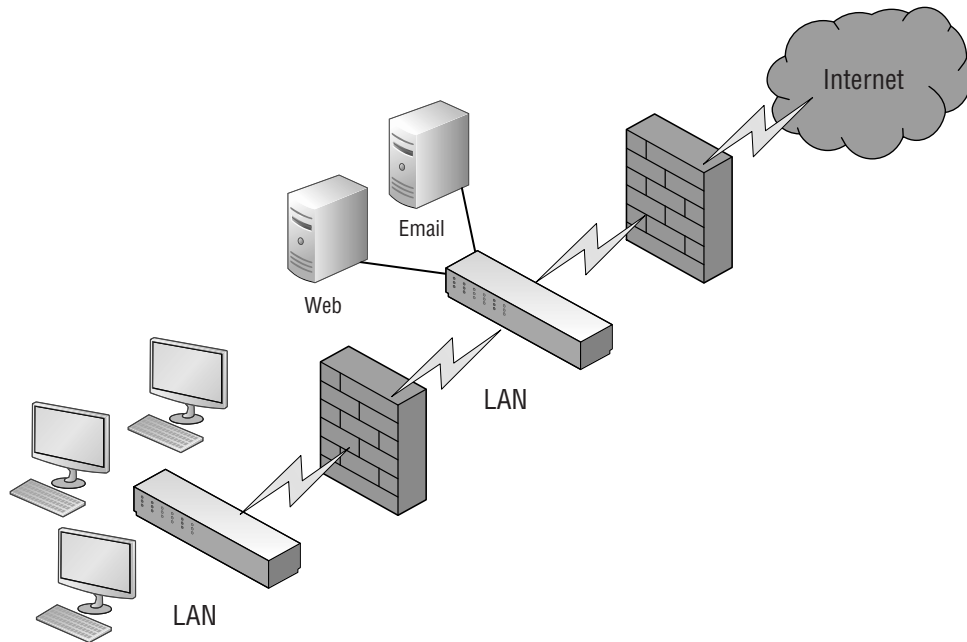
Can you describe the various security zones? Objective 1.2

A *perimeter network* (also known as a *demilitarized zone [DMZ]*) is a small network that is set up separately from a company's private local area network and the Internet. It is called a perimeter network because it is usually on the edge of the LAN, but DMZ has become a much more popular term. The DMZ allows users outside of the company LAN to access specific services located on the DMZ. However, when set up properly, those users are blocked from gaining access to the company LAN. Users on the LAN will quite often connect to the DMZ as well, but without having to worry about outside attackers

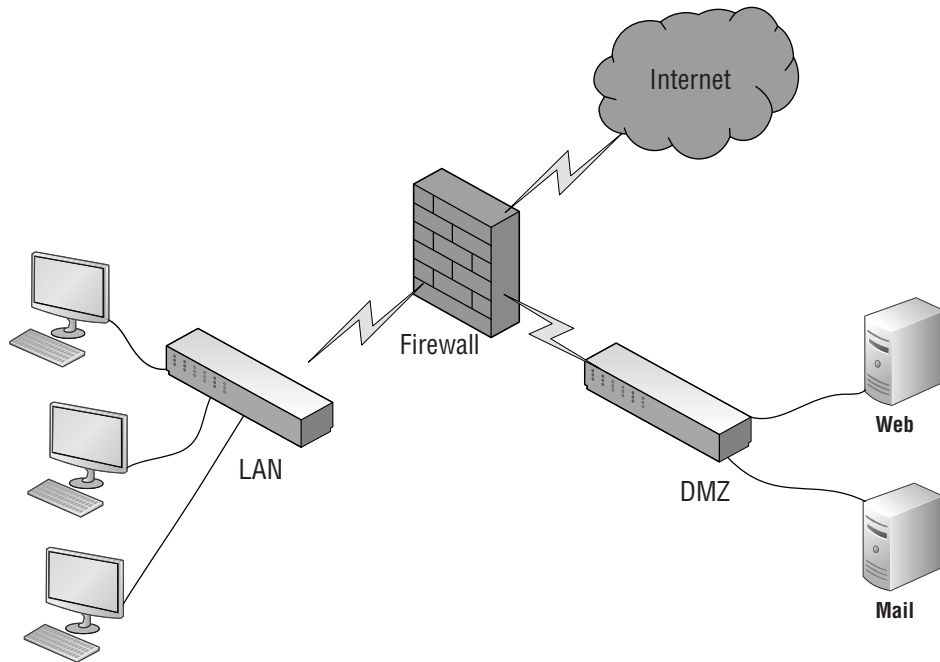
gaining access to their private LAN. The DMZ might house a switch with servers connected to it that offer web, email, and other services. Two common configurations of a DMZ include:

Back-to-Back Configuration This configuration has a DMZ situated in between two firewall devices, which could be black box appliances. An illustration of this is shown in Figure 1.18. In this configuration, an attacker would have to get through two firewalls in order to gain access to the LAN.

FIGURE 1.18 A back-to-back DMZ configuration



3-leg Perimeter Configuration: In this scenario, the DMZ is usually attached to a separate connection of the company firewall. So, the firewall would have three connections: one to the company LAN, one to the DMZ, and one to the Internet, as shown in Figure 1.19. Once again, this could be done with a firewall appliance or server. In this configuration, an attacker would only need to break through one firewall to gain access to the LAN. Although this is a disadvantage, technologies like network intrusion detection/prevention systems can help alleviate most security issues. Also, one firewall means less administration.

FIGURE 1.19 A 3-leg perimeter DMZ configuration

Identifying Network Topologies and Standards

Networks need to be situated in some way to facilitate the transfer of data. Topologies are the physical orientations of computers in a LAN. Access methods are ways that the computer will send data; the most common of these is the client/server-based Ethernet configuration, although there are others. In order to build a LAN, you must first plan out what topology (or topologies) will be used and what type of access method will be implemented. Access methods tend to be not so clear and definite, so let's begin with discussing network topologies.

Identifying Network Topologies

Network topologies define the physical connections of hosts in a computer network. There are several types of physical topologies, including bus, ring, star, mesh, and tree. For the exam, you should know the star, ring, and mesh technologies. We'll throw in the tree topology, known as hierarchical star, for good measure as well because it is considered by many

as an extension of the star topology. We will also identify logical topologies because they are characterized differently than physical topologies.

Certification Ready

Can you describe network topologies and access methods? Objective 1.5

In this exercise, you examine the following *physical* topologies:

- Star
- Mesh
- Ring

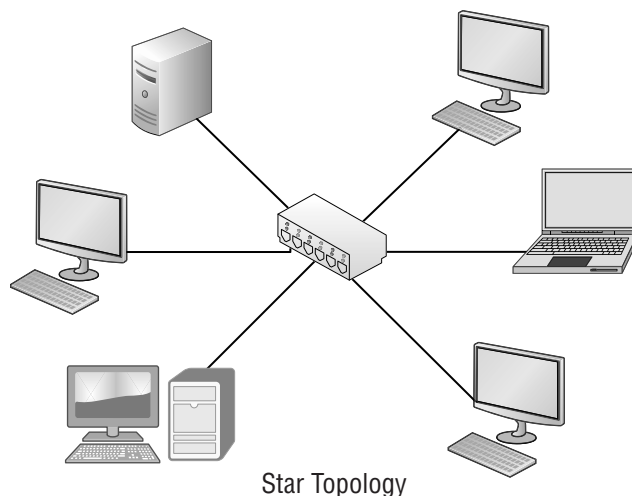
By far, the most common topology is the *star topology*. When a star topology is used, each computer is individually wired to a central connecting device with twisted-pair cabling. The central connecting device could be a hub, a switch, or a SOHO router. This is the type of topology you will usually use when implementing networks.

Identify Topologies

To identify topologies, perform the following steps.

1. Examine Figure 1.20. This illustrates a simple star topology. Notice that it is like Figures 1.1 and 1.2 earlier in this lesson. Indeed, those other figures also illustrate star topologies. Note that the hub in the center of the figure connects each computer by a single cable. This way, if one cable is disconnected, the rest of the network can still function. This is the standard physical topology for an Ethernet network.

FIGURE 1.20 Illustration of a star topology



2. Examine your own computer network. Check to see if it meets the characteristics of the star; namely, is each computer connected to a central connecting device? Are they individually cabled to that device? Add to your network documentation the fact that it is a star if you identify it as such.

In the old days, we had what was known as the bus topology. This is now deprecated. This is a topology for a Local Area Network (LAN) in which all the nodes are connected to a single cable. The cable is called a “backbone.” If that backbone becomes broken, then the entire segment fails. Bus topologies are relatively easy to install and don’t require much cabling compared to the alternatives. However, part of this idea was passed on to the star topology. For example, two individual star networks can be connected (by the central connecting devices) to create a star-bus topology. This is done by daisy-chaining (or stacking) one or more hubs or switches, usually by a special medium dependent interface (MDI) port; this is where the “bus” part of a star-bus topology comes in.

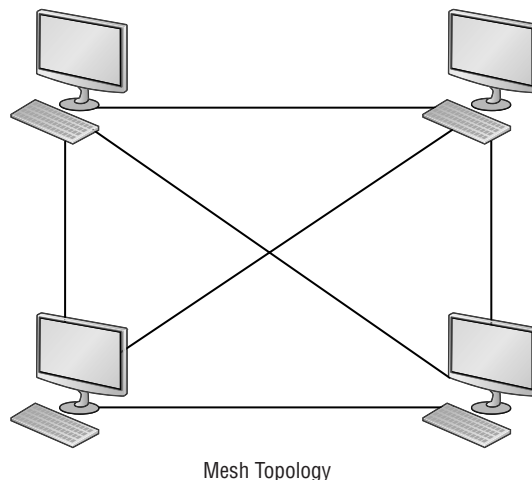
More Information

You will learn more about MDI ports in Lesson 3.

The problem with the star-bus topology is that it is based on the stacking concept. This can pose organizational problems, and is not the best use of bandwidth. A better solution in most scenarios is to use the hierarchical star shown in Figure 1.3 earlier in this lesson.

3. In a *mesh topology*, every computer connects to every other computer; no central connecting device is needed. As you can guess, a true, or “full” mesh, requires a lot of connections, as is illustrated in Figure 1.21. Examine the figure, and calculate how many connections would be needed at each computer to ensure a full mesh configuration.

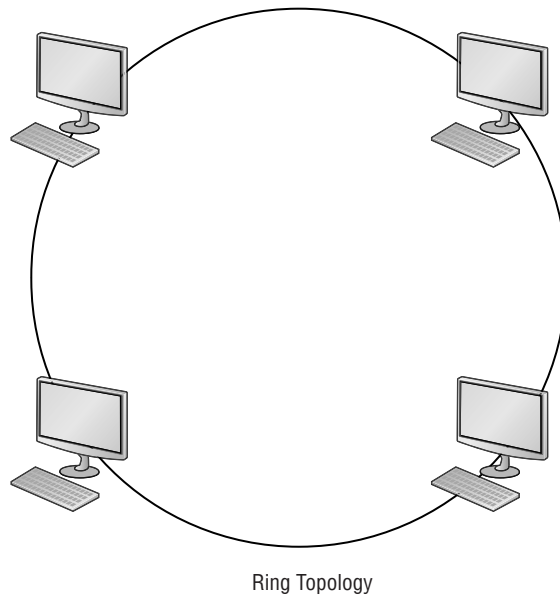
FIGURE 1.21 Illustration of a mesh topology



The number of network connections that each computer will need is the total number of computers minus one. As you can guess, this type of topology is rare, but is necessary in some lab situations and fault-tolerant scenarios (where data needs to be replicated to multiple machines). A lesser version of this topology is the “partial mesh,” where only one or a couple of the computers on the network have a second network connection, for example, if a computer needs to replicate a database to another computer but doesn’t want the connection to be bothered by any other traffic. A computer with two or more network connections is known as a multihomed computer.

4. Lastly, we have the *ring topology*. Examine Figure 1.22, which illustrates how computers are connected in a ring fashion.

FIGURE 1.22 Illustration of a ring topology



In a LAN environment, each computer is connected to the network by way of a closed loop, which was historically done with coaxial cable. When it comes to today’s LANs, the use of coaxial cable has been deprecated; however, when applied to other types of networks like Token Ring, or Fiber Distributed Data Interface (FDDI), it takes on a different meaning—that of a logical topology.

A logical topology describes how the data is actually sent from one computer to the next. Token Ring and FDDI utilize a token-passing system. Instead of computers broadcasting their information to all other computers on an Ethernet network using a star topology, Token Ring and FDDI computers wait to obtain a token. The token is passed from computer to computer, picking up data and dropping it off as needed. Most of these networks have one token, but it is possible to have two in larger networks. The biggest advantage

of Token Ring is that collisions become a nonfactor. A collision is when two computers attempt to send information simultaneously. The result is signal overlap, creating a collision of data, making both pieces of data unrecoverable. In Ethernet networks, data collisions are common due to the whole idea of broadcasting. But in token-based systems, there is only one item flying around the network at high speeds; it has nothing to collide with! Disadvantages include cost and maintenance, plus the fact that Ethernet switching and other Ethernet technologies have done away with a lot of the collisions that were the banes of network engineers until 15 or 20 years ago. Although FDDI networks also utilize ring topology logically as well as physically, they differ from Token Ring networks. A Token Ring network sends data logically in a ring fashion, meaning that a token goes to each computer, one at a time, and continues in cycles. However, the Token Ring computers are physically connected in a star fashion. All computers in a Token Ring network are connected to a central connecting device known as a Multistation Access Unit (MAU or MSAU). You'll learn more about Token Ring in Lesson 2.

Defining Ethernet Standards

Ethernet is far and away the most common type of LAN standard used by today's organizations. It is a scalable technology, but to get the most out of Ethernet, devices, computers, and other hosts should be compatible. This means knowing the various Ethernet standards is very important.

Certification Ready

Can you identify and describe Ethernet standards? Objective 1.5

Ethernet is a group of networking technologies that define how information is sent and received between network adapters, hubs, switches, and other devices. An open standard, Ethernet is the de facto standard and has the largest share of networks in place today, with Token Ring and FDDI filling in the small gaps where Ethernet does not exist. It is standardized by the Institute of Electrical and Electronics Engineers (IEEE) as 802.3. Developed originally by Xerox, it was later championed by DEC, Intel, as well as Xerox. Now, Ethernet products are offered by hundreds of companies, such as D-Link, Linksys, 3Com, HP, and so on.

Computers on Ethernet networks communicate by sending Ethernet *frames*. The frame is a group of bytes packaged by a network adapter for transmission across the network; these frames are created and reside on Layer 2 of the OSI model, which is covered in more depth in the next lesson. By default, computers on Ethernet networks all share a single channel. Because of this, only one computer can transmit at a time. However, newer networks with more advanced switches transcend this limitation of Ethernet, and is covered in more depth in Lesson 2.

IEEE 802.3 defines carrier sense multiple access with collision detection or *Carrier Sense Multiple Access with Collision Detected (CSMA/CD)*. Because computers on a default Ethernet LAN all share the same channel, CSMA/CD governs the way that computers coexist with limited collisions. The basic steps for CSMA/CD are as follows:

1. The network adapter builds and readies a frame for transmission across the network.
2. The network adapter checks if the medium (for example, twisted-pair cable) is idle. If the medium is not idle, it waits for approximately 10 microseconds (10 μ s). This delay is known as the interframe gap.
3. The frame is transmitted across the network.
4. The network adapter checks if any collisions occurred. If so, it moves on to the *collision detected* procedure.
5. The network adapter resets any retransmission counters (if necessary) and ends the transmission of the frame.

If a collision was detected in Step 4, another procedure called the collision detected procedure is employed:

1. The network adapter continues transmission until the minimum packet time is reached (known as a jam signal). This ensures that all receivers have detected the collision.
2. The network adapter increments the retransmission counter.
3. The network adapter checks if the maximum number of transmission attempts was reached. If it was, the network adapter aborts its transmission.
4. The network adapter calculates and waits a random back off period based on the number of collisions detected.
5. Finally, the network adapter starts the original procedure at Step 1 of the CSMA phase of the CSMA/CD process.

If an organization utilizes wireless Ethernet, *Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)* is employed. CSMA/CA is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by transmitting only when the channel is identified as idle. When nodes do transmit, they transmit their packet data in its entirety. CSMA/CA is particularly important for wireless networks, where the collision detection of CSMA/CD is unreliable due to the hidden node problem.

Devices on an Ethernet network must be compatible to a certain extent. If you are using an Ethernet switch, a computer's network adapter must also be of an Ethernet type in order to communicate with it. However, unlike some other networking technologies, different speeds can be negotiated. For example, suppose your switch had a maximum data transfer rate of 100 Mbps, but your network adapter only connected at 10 Mbps. The network adapter would still be able to communicate with the switch, but at the lesser rate. The various speeds of Ethernet and the cable media they use are defined by the various 802.3 standards listed in Table 1.2. Although 802.3 by itself is generally thought of as 10 Mbps, it is further broken up into various subgroups, as shown in the table.

TABLE 1.2 802.3 Ethernet Standards

802.3 Version	Data Transfer Rate	Cable Standard	Cabling Used
802.3	10 Mbps	10BASE5	Thick coaxial
802.3a	10 Mbps	10BASE2	Thin coaxial
802.3i	10 Mbps	10BASE-T	Twisted pair (TP)
802.3j	10 Mbps	10BASE-F	Fiber optic
802.3u	100 Mbps	100BASE-TX (most common) 100BASE-T4 100BASE-FX	TP using two pairs TP using four pairs Fiber optic
802.3ab	1,000 Mbps or 1 Gbps	1000BASE-T	Twisted pair
802.3z	1,000 Mbps or 1 Gbps	1000BASE-X	Fiber optic
802.3ae	10 Gbps	10GBASE-SR, 10GBASE-LR, 10GBASE-ER, and so on...	Fiber optic
802.3an	10 Gbps	10GBASE-T	Twisted pair
802.3ba	40 Gbps and 100 Gbps	40GBASE-T	Twisted pair

All of the 10-Mbps standards listed are a bit slow for today's network applications, but you might find them in some organizations and in other countries outside the United States. Of course, a good network administrator can make even 10-Mbps networks run quickly and efficiently. In fact, an efficient 10-Mbps network can easily outperform a poorly designed 100-Mbps network.

The 10-Gbps standards are much newer as of the writing of this book, and, therefore, are much more expensive. Currently, 1-Gbps connections for clients and 10-Gbps connections for network backbones are common. The most common cabling standards used today are 100BASE-TX and 1000BASE-T. Keep in mind that new standards are constantly being released by the IEEE.

10 Mbps is typically referred to as Ethernet, 100 Mbps is known as Fast Ethernet, and 1 Gbps is known as Gigabit Ethernet.

Identifying the Differences Between Client/Server and Peer-to-Peer

Most of today's networks are distributed. This means that CPU power and applications are not centralized, but instead, every host has a CPU, and every host can run programs that connect to other computers. The most common types of distributed networks are client/server and peer-to-peer. It is important to know the differences between these so you can decide which technology is best for any given customer scenario.

The older type of computing was known as *centralized computing*. This was the case during the days of the mainframe, where there was one supercomputer, and the rest of the devices that connected to the supercomputer were known as terminals (or dumb terminals). They were strictly a keyboard and display with no processing power. Today's computing is known as *distributive computing* and is used for both client/server and peer-to-peer networks. This means that every device or workstation has its own processing power. However, in a way, the idea of centralized computing has made a comeback of sorts. Terminal services and remote sessions to computers are based on the centralized computing model. Also, thin-client computing has been slowly gaining in market share for the past decade or so. Thin-client computers do not have a hard drive. Instead, they store an operating system in RAM, which is loaded up every time the device is turned on. All other applications and data are stored centrally. So, in a way, this is sort of blending some centralized computing in with today's distributive computing.

Defining the Client/Server Model

The *client/server* model is an architecture that distributes applications between servers, such as Windows Server 2016, and client computers, such as Windows 8/8.1 or Windows 10. It also distributes the necessary processing power. It is extremely common in today's LANs, as with most applications that an average user would utilize when connecting to the Internet. For example, when users first come into work, they typically log on to the network. Chances are this is a client/server network. They might be using Windows 10 as the client computer to log on to a Microsoft domain, which is controlled by a Windows server. A simpler example would be a user at home connecting to the Internet. When a user wants to go to a website such as Bing, the user opens a web browser and types `http://www.bing.com/` (or one of many shortcuts). The web browser is the client application. Bing's web server is obviously the "server." It serves the web pages filled with highly functional HTML code. The client computer's web browser decodes the HTML code and fills the web browser display with data for both on-the-job and personal use from the Internet from useful resources, such as Microsoft Outlook. Outlook is the client application; it connects to a mail server, most likely an SMTP server, perhaps run by Microsoft Exchange Server. The examples are endless, but client/server is not the end all when it comes to networking. Sometimes, it is more efficient to not use a server, particularly with a very small number of users.

Here are some examples of usages for servers:

File Server A file server stores files for computers to share. The connection to a file server could be made by browsing, by mapping a network drive, by connecting in the command line, or by connecting with an FTP client. The latter would require special FTP server software to be installed and configured on the file server. By default, Windows Server 2008 and newer can be file servers right out of the box.

Print Server A print server controls printers that can be connected directly to the server or (and more commonly) are connected to the network. The print server can control the starting and stopping of documents, as well as concepts such as spooling, printer pooling, ports, and much more. By default, Windows Server 2008 and newer can also be print servers right out of the box.

Database Server A database server houses a relational database, one that is made up of one or more files. SQL databases fall into this category. They would require special software such as Microsoft SQL Server. Access databases (which are just one file) would not necessarily require a database server; they would usually be stored on a regular file server.

Network Controller A network controller is a server, such as a Microsoft domain controller that oversees user accounts, computer accounts, network time, and the general well-being of the entire domain of computers and users. Windows Server 2016 servers can be domain controllers, but they need to be promoted to that status. By default, a Windows Server operating system is not a controller. Network controller operating systems are also referred to as *network operating systems (NOSs)*.

Messaging Server This server category is enormous. Providing simple services alone would make this a full-time job, but you have to add in fax servers, instant messaging, collaborative, and other types of messaging servers. For a Windows Server to control email, special software known as Exchange Server needs to be loaded in addition to the operating system.

Web Server Web servers are important to share data and give information about a company. Windows servers can be web servers, but Internet Information Services (IIS) must be installed and configured in order to do so.

CTI-based Server CTI is short for *Computer Telephony Integration*. This occurs when a company's telephone system meets the computer system. Special PBXs that used to control phones as a separate entity can now be controlled by servers with powerful software.

Understanding Newer Operating Systems

The client version of Windows is the version that is purchased and installed on personal computers that include desktop computers, laptops, workstations, and tablets. Windows Server operating systems are purchased and installed on stand-alone physical servers, blades, and virtual machines.

Windows XP unified the consumer-oriented Windows 9x series with Windows NT/2000, while introducing a redesigned user interface, including the Start menu, Internet Explorer 6, and Remote Assistance functionality. As a result, Windows XP became one of the most popular client operating systems in history.

Later, Microsoft attempted to replace Windows XP with Windows Vista, which had an updated graphical user interface and improved security. Unfortunately, Windows Vista was not well received, and it failed to overtake Windows XP. To overcome the shortcomings of Windows Vista, Microsoft released Windows 7, which gave increased performance, a more intuitive interface, and fewer User Account Control pop-ups.

The next version of Windows was Windows 8, which was upgraded to support desktop computers, mobile computers, and tablets, while optimized for touch screens. It replaced the Start button and menu with the Start screen, a new platform for developing apps, and the Windows Store. Unfortunately, the new interface made it confusing and difficult to learn. To address some of these problems, Windows released Windows 8.1, which improved the Start screen.

Windows 10 is the newest client operating system. After the failure of Windows 8, Microsoft listened to customer complaints to develop Windows 10. To distance the new version of Windows from Windows 8/8.1, Microsoft skipped Windows 9 and went to Windows 10. Different from previous versions of windows, Windows 10 is released as an “operating system as a service,” which means that it will receive ongoing updates to its features and functionality.

As client operating systems are developed and released, Microsoft also develops and releases server operating systems, as shown in Table 1.3. Until Windows 10, the client operating system and server operating system were introduced together. Although client and server operating systems can provide and request services, server operating systems can provide additional services and can service many more clients simultaneously.

TABLE 1.3 Client and Server Operating Systems

Client Operating Systems	Server Operating Systems	Version Number
Windows 10	Windows Server 2016	10.0
Windows 8.1	Windows Server 2012 R2	6.3
Windows 8	Windows Server 2012	6.2
Windows 7	Windows Server 2008 R2	6.1

Client Operating Systems	Server Operating Systems	Version Number
Windows Vista	Windows Server 2008	6.0
Windows XP	Windows Server 2003/Windows Server 2003 R2	5.1/5.2
Windows 2000 Professional	Windows 2000 Server	5.0
Windows NT 4.0 Workstation	Windows NT 4.0 Server	4.0

Defining the Peer-to-Peer Model

Peer-to-peer networking, first and foremost, means that each computer is treated as an equal. This means that each computer has the equal ability to serve data, and to access data, just like any other computer on the network. Before servers became popular in PC-based computer networks, each PC had and still has the ability to store data. Even after the client/server model became king, peer-to-peer networks still had their place, especially in smaller networks with 10 computers or less. Today, peer computers can serve data; the only difference is that they can only serve it to a small number of computers at the same time.

In these small networks, the cost, administration, and maintenance of a server are too much for a small organization to consider viable. A Microsoft peer-to-peer network might consist of a couple of Windows 7, 8/8.1, and/or Windows 10 computers. These are each client operating systems, and as such are known as peers because there is no controlling server in the network. This usually works well enough for smaller organizations. The beauty of Microsoft client operating systems is that up to 20 PCs can concurrently access an individual peer's shared resources. So, in these environments, one peer usually acts as a sort of pseudoserver, so to speak. But additional resources, such as files, databases, printers, and so on, could be added to any other computer on the network. The main disadvantage of this network model is that there is no centralized user database. User names and passwords are individually stored per computer. To implement a centralized user database, you would need to have a Windows-based server, which would mean that a client/server model would be employed.

Peer-to-peer has taken on a second meaning over the past decade or so. Now, it refers to file sharing networks, and in this case is referred to as *P2P*. Examples of file sharing networks include Napster, Gnutella, and G2, but other technologies also take advantage of P2P file sharing, such as Skype, VoIP, and cloud computing. In a P2P network, hosts are added in an ad hoc manner. They can leave the network at any time without impacting the download of files. Many peers can contribute to the availability of files and resources. A person downloading information from a P2P network might get little bits of information from many different computers; afterwards, the downloading computer might help to share the file as well. Most file sharing peer-to-peer networks use special software to download files, such as BitTorrent. BitTorrent is a protocol as well as a program. The program (and

others like it) is used to download large files from P2P networks. Instead of the files being stored on a single server, the file is distributed among multiple computers (could be a few, could be many). The possible benefits are availability of data and speed (although some torrent transfers will be slow). A computer, its BitTorrent client, and the router you are connected to can all be optimized to increase the speed of torrent downloads. It is estimated that between 20% and 35% of the data transfers on the Internet involve torrents. Another benefit of the BitTorrent client is that you can line up a large number of downloads from one torrent location (or multiple locations), and just let your computer download them while you do other things. A file is seeded (stored) on one or more computers. Then, as clients (peers) download that file (or portions of the file), they are automatically set up to distribute the file (or portions of the file). This way, more and more computers are added to the “swarm,” making the availability of the file much greater. Computers are set up to automatically distribute the file; it’s the default setting, but you can turn off seeding/distribution in your client. You could also block it at your firewall.

Instead of a server hosting the file, a server simply tracks and coordinates the distribution of files. The actual torrent starts with an initial small file (called a torrent file) that you download, which contains information about the files to be downloaded. The reason the whole process is called a torrent is because it usually begins with a small file that starts the download. One of the differences is that when downloading a torrent, there is more than one TCP connection (could be quite a few) to different machines in the P2P network. Contrast this to a single file download from a web server where only one TCP connection is made. This is controlled in a pseudorandom fashion by the tracking server to ensure availability of data. Another difference is that most web servers will put a cap on the number of concurrent downloads you can do, but not so with the torrent client program. The average person uses a BitTorrent client to download movies, MP3s, and other media. Sometimes, these are distributed with the consent of the owner; other times (and quite often), they are illegally seeded and distributed—as well as downloaded! An example of legitimate usage is the *World of Warcraft* game. The owners of the game use the Blizzard BitTorrent to distribute just about everything involved in the game. Newer games for the PS3 and other consoles are doing the same type of thing. D-Link and other network equipment companies are embracing torrent technology as well.

Skill Summary

In this lesson, you learned:

- A network is two or more computers that exchange data. A local area network (LAN) is a group of these computers that are confined to a small geographic area, usually one building.
- The network adapter, also known as a network interface card (NIC), is the device that enables the sending and receiving of data to and from your computer. Today, multiple devices can connect to each other and communicate using a switch.

- Internet Protocol (IP) is the part of TCP/IP that, among other things, governs IP addresses. The IP address is the cornerstone of networking. It defines the computer or host you are working on.
- A wireless local area network (WLAN) has many advantages, the most stand out of which is the ability to roam. A person with a laptop, handheld computer or PDA, or other like device can work from anywhere.
- Network topologies define the physical connections of hosts in a computer network. There are several types of physical topologies, including bus, ring, star, mesh, and tree.
- Today's computing is known as distributive computing and is used for both client/server and peer-to-peer networks. This means that every device or workstation has its own processing power.
- The client/server model is an architecture that distributes applications between servers, such as Windows Server 2016, and client computers, such as Windows 8/8.1 or Windows 10.
- Peer-to-peer networking, first and foremost, means that each computer is treated as an equal. This means each computer has the equal ability to serve data and to access data, just like any other computer on the network. Before servers became popular in PC-based computer networks, each PC had the ability to store data.

Knowledge Assessment

In the following sections, you can find the answers in the Appendix.

Multiple Choice

1. Which of the following regenerates the signal and broadcasts the signal to every computer connected to it?
 - A. Hub
 - B. Switch
 - C. Router
 - D. Firewall
2. Which of the following is *not* a central connecting device?
 - A. Hub
 - B. Switch
 - C. SOHO router
 - D. Windows 10 client
3. When installing a network adapter to a computer so that it can be connected to a network that uses twisted-pair cabling, which type of port must be used by the network adapter?
 - A. RJ-11
 - B. RJ-45
 - C. RG-58
 - D. Fiber optic
4. In Windows 10, which of the following should be used to access the properties of a network adapter?
 - A. Device Manager
 - B. Ping
 - C. Advanced Firewall
 - D. Task Manager
5. When connecting a computer's network adapter to a switch—with the desire for the connection to be able to send and receive data simultaneously—which type of connection is required?
 - A. Half-duplex
 - B. Full-duplex
 - C. Simplex
 - D. 100 Mbps

6. When connecting a computer at a rate of 100,000,000 bits per second, which of the following should be the speed of the network adapter being installed?
 - A. 10 Mbps
 - B. 100 MB/s
 - C. 100 Mbps
 - D. 1,000 Mbps

7. When connecting to a router that has the IP address 192.168.1.100 on a standard, default Class C network using the subnet mask 255.255.255.0, which of the following is a valid IP address for the network adapter?
 - A. 192.168.0.1
 - B. 192.168.1.1
 - C. 192.168.100.1
 - D. 192.168.1.100

8. After installing a network adapter and configuring an IP address and subnet mask, which command can be used to verify that the IP address is configured and listed properly?
 - A. Ping
 - B. Tracert
 - C. CMD
 - D. Ipconfig

9. Which of the following commands enables pinging your own computer to see if it is operational?
 - A. ping localclient
 - B. ping 128.0.0.1
 - C. ping loopback
 - D. ping network adapter

10. Which of the following types of networks should be used to connect a computer to a group of hosts that have been segmented from the regular network?
 - A. LAN
 - B. WLAN
 - C. WAN
 - D. VLAN

Fill in the Blank

1. The manager of IT asks you to connect a perimeter network to the firewall, which will be separate from the LAN. This type of network is known as a _____.
2. A _____ topology can be defined by connecting several hubs to a switch.
3. 802.3u Ethernet networks run at _____ Mbps.
4. A _____ is a program used to download files quickly from a P2P network.
5. The _____ network architecture is physically a star and logically a ring.
6. 802.3ab Ethernet networks run at _____ Mbps.
7. A _____ connection is when data can be sent and received, but not at the same time.
8. A _____ topology can be defined as connecting several computers together in a circle, without the use of a hub or a switch.
9. When several computers are connected in a small geographic area, it is known as a _____.
10. A _____ acts as a central connecting device and allows laptops, PDAs, and handheld computers to communicate with each other.

Business Case Scenarios

In the following section, you can find the answers in the Appendix.

Scenario 1-1: Planning and Documenting a Basic LAN

Proseware, Inc., requires you to implement a 20-computer local area network. Fifteen of these computers will be Windows 10 clients, and five will be Windows Server 2016 computers. They also require a 24-port switch, router, DSL Internet connection, DMZ with web server, and a laptop for the CEO. Create a diagram of the network documentation for this in Microsoft Visio or on paper. Refer to Figures 1-1 through 1-3 for types of devices in the Visio networking stencils.

Scenario 1-2: Selecting the Correct Networking Model

The ABC Company requires a network that can support 50 users. Describe the correct type of networking model to use and explain why.

Scenario 1-3: Selecting Network Adapters for Your LAN Computers

You are consulting for a company that asks you to install five new computers. The network adapter in each computer should be able to communicate at 1,000 Mbps over the preexisting twisted-pair cabling and should be able to send and receive data simultaneously. Which Ethernet standard should you select, and which technology should be utilized?

Scenario 1-4: Configuring the Correct Subnet Mask

A computer is not connecting to certain network devices properly. The IP address information is as follows:

IP address: 192.168.1.210

Subnet mask: 255.254.0.0

Describe how to configure the subnet mask so that the computer can communicate properly with all networking devices and other hosts on the network.

Solutions to Business Case Scenarios

In the following section, you can find the answers in the Appendix.



Real World Scenario

Workplace Ready: Utilizing Full-Duplex Connections

Many network cards have the ability to run in full-duplex mode, but sometimes, it is overlooked. Or, the central connecting device in the network might not have the ability to run in full-duplex, thus reducing the network capability to half-duplex.

When you think about it, that is effectively reducing your network throughput by half. By using full-duplex connections on the central connecting devices, and all of the network adapters, 100 Mbps effectively becomes 200 Mbps, because now the devices can send *and* receive at the same time.

Network devices are usually rated at their half-duplex data transfer rate. So, if you see a network adapter being sold as a 1-Gbps device, look a little further. See if it is full-duplex capable, and if so, you could see a maximum data transfer rate of 2 Gbps.

Remember to set this in the Properties page of the network adapter, which can be found within Device Manager.

For this exercise, access the Internet and locate three different 1-Gbps network adapters that can operate in full-duplex mode. Try manufacturers such as D-Link, Linksys, Intel, and so on. You will need to view the specifications of each device and note the link to those pages as proof of your discovery. Another great source for different equipment is www.pricewatch.com. Access this site to view various networking equipment from different vendors.