1 Basic Network Concepts

CERTIFICATION OBJECTIVES

Knowing how computers communicate in a network environment is essential to passing the Network+ certification exam and to being a good network professional who can troubleshoot networking issues. This chapter introduces you to the basics of what makes a network tick, and covers basic topics and terminology that will set the foundation for the rest of your studies.

We will look at the various topologies, network operating systems, and common terminology used in day-to-day discussions between IT professionals. In this chapter, you will learn the purpose of a network, the different types of networks, network topologies, cables, and connectors, and you will learn about network architectures. You will finish the chapter by learning about some of the most popular network operating systems.

CERTIFICATION OBJECTIVE 1.01

Identifying Characteristics of a Network

More and more people are building home and small office networks now as a result of the low cost of networking devices such as hubs and home routers. As a Network+ Certified Professional, you will need to ensure that you can support these small, medium, and large networks, so you will start by learning some basic terms.

A network is a group of systems that are connected to allow sharing of resources—such as files or printers—or sharing of services—such as an Internet connection. There are two aspects of setting up a network: the hardware used to connect the systems together and the software installed on the computers to allow them to communicate. This chapter is designed to give you an understanding of the hardware used to build a network, and later chapters discuss the software needed. The network hardware is made up of two basic components: the entities that want to share the information or resources, such as servers and workstations, and the medium that enables the entities to communicate, which is a cable or a wireless medium.

Servers, Workstations, and Hosts

A typical network involves having users sit at workstations, running such applications as word processors or spreadsheet programs. The workstation also is

known as a client, which is just a basic computer running a client operating system such as Windows XP or Linux. These users typically store their files on a central server so that they can share the files with other users on the network. The server is a special computer that contains more disk space and memory than are found on client workstations. The server has special software installed that allows it to function as a server. This special software can provide file and print services (to allow sharing of files and printers), provide web pages to clients, or provide e-mail functionality to the company.

The term *host* refers to any computer or device that is connected to a network and sends or receives information on that network. A host can be a server, a workstation, a printer with its own network card, or a device such as a router. We can summarize by saying that any system or device that is connected to the network is known as a host.

WANs, LANs, and MANs

Some other terms that you will hear often are LAN, WAN, and MAN. A *local area network (LAN)* typically is confined to a single building, such as an office building, your home network, or a college campus. A *wide area network (WAN)* spans multiple geographic locations and is typically made up of multiple LANs. For example, I have a company with an office in Halifax, Nova Scotia (that's a city in Canada next door to the penguins) that has 100 computers all connected together. This would be considered a LAN. Now if we expand the company and create an office in Toronto, the network in Toronto also would be considered a LAN. If we want to allow the two offices to share information with one another, we would connect the two LANs together, creating a WAN.

The term *metropolitan area network (MAN)* is not used often anymore; it refers to a network that exists within a single city or metropolitan area. If we had two different buildings within a city that were connected together, it would be considered a MAN.

Types of Networks

Organizations of different sizes, structures, and budgets need different types of networks. A local newspaper company has needs for its network that would be different from the needs of a multinational company. Networks can be divided into one of two categories: peer-to-peer or server-based networks.

Peer-to-Peer Network

A *peer-to-peer* network has no dedicated servers; instead, a number of workstations are connected together for the purpose of sharing information or devices. When there is no dedicated server, all workstations are considered equal; any one of them can participate as the client or the server. Peer-to-peer networks are designed to satisfy the networking needs of home networks or of small companies that do not want to spend a lot of money on a dedicated server but still want to have the capability to share information or devices. For example, a small accounting firm with three employees that needs to access customer data from any of the three systems or print to one printer from any of the three systems may not want to spend a lot of money on a dedicated server. A small peer-to-peer network will allow these three computers to share the printer and the customer information with one another (see Figure 1-1). The extra cost of a server was not incurred because the existing client systems were networked together to create the peer-to-peer network.

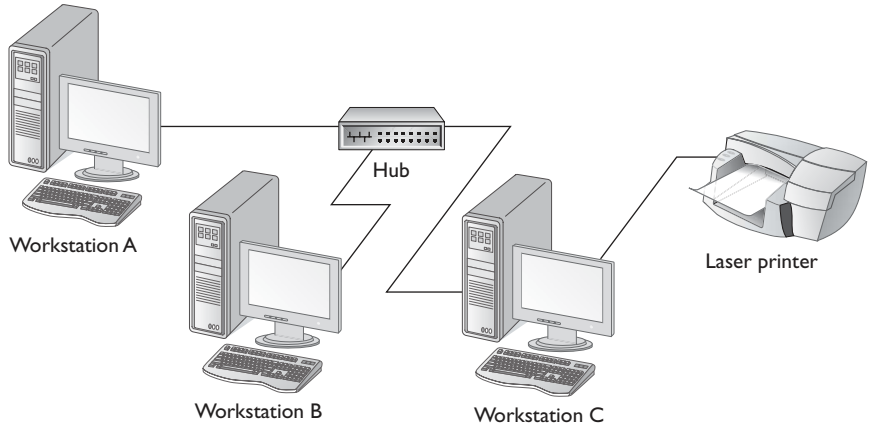
on the job

The Microsoft term for a peer-to-peer network is a workgroup. Be aware that peer-to-peer networks typically consist of fewer than 10 systems.

Most of the modern operating systems such as Windows XP and Windows Vista already have built-in peer-to-peer networking capabilities, which is why building a peer-to-peer network would be a "cheap" network solution. The disadvantage of a peer-to-peer network is the lack of centralized administration—with peer-to-peer networks, you need to build user accounts and configure security on each system.

FIGURE 1-1

A peer-to-peer network



It is important to note that peer-to-peer networks are designed for fewer than 10 systems, and with Microsoft client operating systems such as Windows XP Professional, only 10 concurrent network connections to those clients are allowed. This means that if you have 15 or 20 employees, you eventually will need to implement a server-based network.

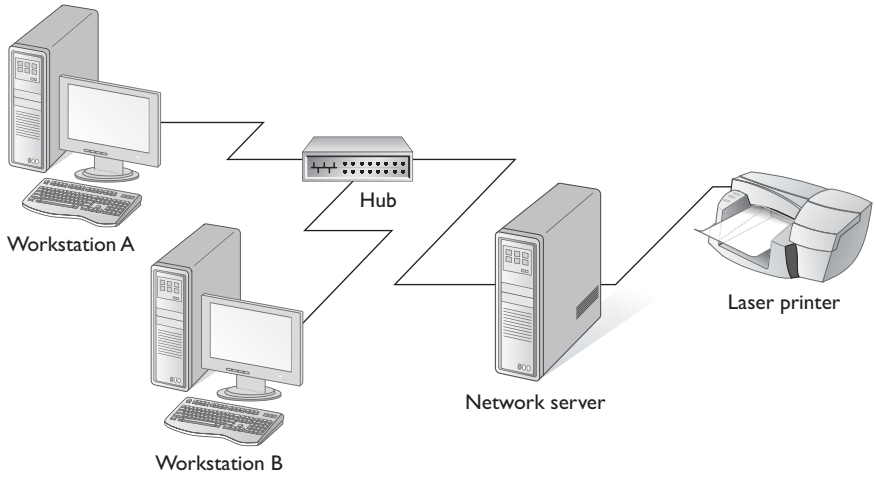
Server-Based Networks

A big disadvantage of peer-to-peer networking is that you can't do your day-to-day administration in a single place. With peer-to-peer networking, user accounts typically are created on all the systems, and data files are stored throughout all the systems. This leads to a more complicated environment and makes your job harder as a network administrator. Usually after four or five systems have been networked, the need for a dedicated server to store all of the user accounts and data files becomes apparent—this is a server-based network (see Figure 1-2).

The advantage of a server-based network is that the data files that will be used by all of the users are stored on the one server. This will help you by giving you a central point to set up permissions on the data files, and it will give you a central point from which to back up all of the data in case data loss should occur. With a server-based network, the network server stores a list of users who may use network resources and usually holds the resources as well.

FIGURE 1-2

A server-based network



The server in a server-based network may provide a number of different services. The services it will offer to the network usually are decided by the server's role. There are a number of different roles that a server could play on a network:

- File and print servers
- Application servers
- Web servers
- Directory servers

File and print servers control and share printers and files among clients on the network. File and print servers were the original reason to have a network; a large number of users needed access to the same files, so the files were placed on a server, and all clients were connected to the server when they needed to work with the files. File servers often have the following characteristics:

- Large amounts of memory
- Fast hard disks
- Multiple CPUs
- Fast I/O buses
- High-capacity tape drives
- Fast network adapters
- Redundant power supplies
- Hot-swappable hard disks and power supplies

File and print servers also check the access control list (ACL) of each resource before allowing a user to access a file or use a printer. If the user or a group to which the user belongs is not listed in the ACL, the user is not allowed to use the resource, and an "access denied" message appears on the user's screen.

Application servers are servers that run some form of special program on the server. A good example of an application server is a server that runs the company's e-mail server. The e-mail server software is special software that can be run on a server operating system. Another example of software that would run on an application server is a database server product such as Microsoft SQL Server. A database server

is a server that holds the company's core business data and typically gives this data to custom applications that run on the workstations. These are some applications that you might find on an application server:

- Microsoft SQL Server
- Oracle
- Microsoft Exchange Server
- IBM Lotus Domino

Web servers are servers that run the Hypertext Transfer Protocol (HTTP) and are designed to publish information on the Internet or the corporate intranet. Web servers are popular in today's businesses because they host web applications (web sites) for the organization. These web applications could be designed for internal use, or they could be used to publish information to the rest of the world on the Internet. Examples of web server software are Microsoft's Internet Information Services that runs on Windows or Apache web server software that runs on UNIX/Linux, Novell NetWare, and Windows.

Directory servers hold a list of the user accounts that are allowed to log on to the network. This list of user accounts is stored in a database (known as the directory database) and can store information about these user accounts such as address, city, phone number, and fax number. A directory service is designed to be a central database that can be used to store everything about such objects as users and printers.

In a server-based network environment, the centralized administration comes from the fact that the directory server stores all user accounts in its directory database. When a user sits at a client machine to log on to the network, the logon request is sent to this directory server. If the username and password exist in the directory database, the client is allowed to access network resources.

It is important to note that a server can have numerous roles at the same time. A server can be a file and print server, as well as an application server, or it can be a file, print, and directory server all at the same time. Because a single server can perform multiple roles, a company will not need to purchase an additional server every time a new product (or feature) is implemented on the network, and this fact reduces the cost of a server-based network.

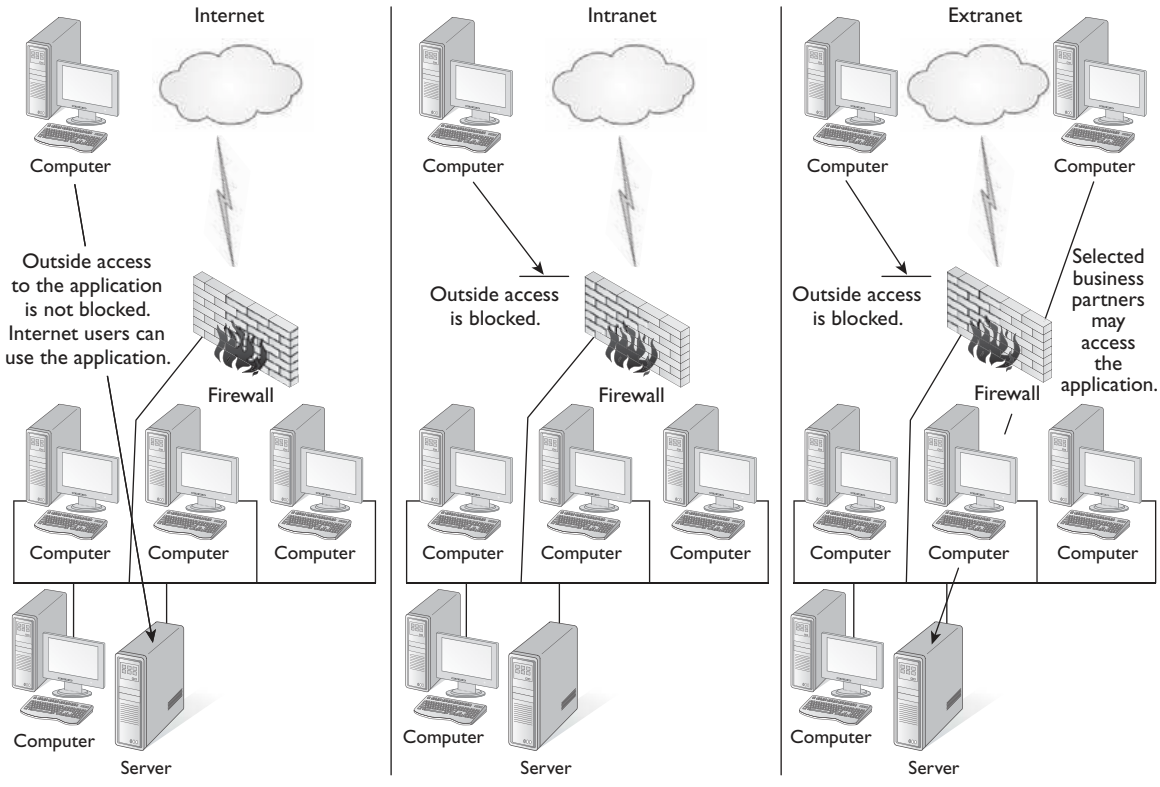
Internet, Intranet, and Extranet

Internet, intranet, and extranet are three terms that describe "Internet-type" applications that are used by an organization, but how do you know if a web application is part of your intranet or part of the Internet?

- **Internet** If you wish to expose information to everyone in the world, then you would build an Internet-type application. An Internet-type application uses Internet protocols such as HTTP, FTP, or SMTP and is available to persons anywhere on the Internet. We use the Internet and web applications as ways to extend who the application can reach. For example, I no longer need to go to the bank to transfer funds. Because the bank has built a web site on the Internet, I can do that from the comfort of my own home.
- **Intranet** An application is considered to be on the company's intranet if it is using Internet-type protocols such as HTTP or FTP but the application is available only within the company. The information on a company's intranet would not be accessible to persons on the Internet because it is not for public use. For example, a few years ago I was sitting with my banking officer going over my account and noticed that the bank had moved all of its customer account information to a web site and that the banking officer was using a web browser to retrieve my account details. Although the application was being used by a web browser, it was still an "internal" application meant only for banking officers.
- **Extranet** From time to time, an application that has been built for the company's intranet and used by internal employees will need to be extended to select business partners or customers. If you extend your intranet out to select business partners or customers, you have created an extranet. An extranet cannot be used by anyone else external to the company except for those selected individuals. Figure 1-3 displays the basic configurations of Internet, intranet, and extranet.

This section has introduced you to some terms such as peer-to-peer versus server-based networking, Internet, intranet, and extranet; now let's look at how the network is laid out with the different network topologies!

FIGURE 1-3 Visualizing the difference between Internet, intranet, and extranet



CERTIFICATION OBJECTIVE 1.02

Identifying Network Topologies

This section will introduce you to a number of different network topologies, but this topic is a lead-in to a bigger topic introduced later in the chapter: network architecture. A network architecture is made up of a topology, a cable type, and an access method. Before we can discuss network architectures, we need to specify what the different types of topologies, cables, and access methods are.

A network topology is the physical layout of computers, cables, and other components on a network. There are a number of different network topologies, and a network may be built using multiple topologies. The different types of network layouts are

- Bus topology
- Star topology
- Mesh topology
- Ring topology
- Hybrid topology
- Wireless topology

Bus Topologies

A bus topology uses one cable as a main trunk to connect all of the systems together (shown in Figure 1-4). A bus topology is very easy to set up and requires no additional hardware such as a hub. The cable is also called a trunk, a backbone, or a segment.

With a bus topology, when a computer sends out a signal, the signal travels the cable length in both directions from the sending computer. When the signal reaches the end of the cable length, it bounces back and returns in the direction it came from. This is known as signal bounce. Signal bounce is a problem, because if another signal is sent on the cable length at the same time, the two signals will collide and be destroyed and then must be retransmitted. For this reason, at each end of the cable there is a terminator. The terminator is designed to absorb the signal when the signal reaches the end, preventing signal bounce. If there is no termination, the entire network fails because of signal bounce, which also means that if there is ever a break in the cable, you will have unterminated ends and the entire network will go down, as shown in Figure 1-5.

FIGURE 1-4

With a bus topology, all system, are connected to one linear cable.

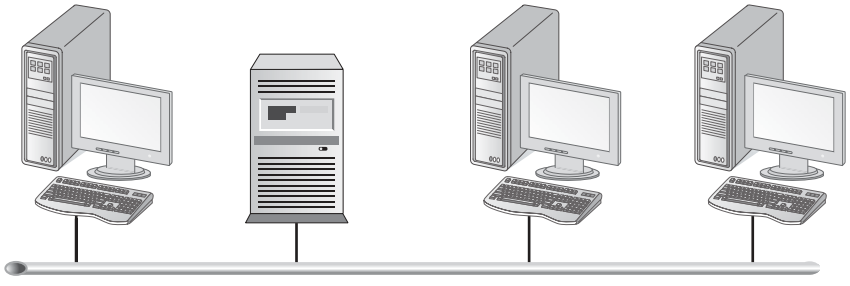
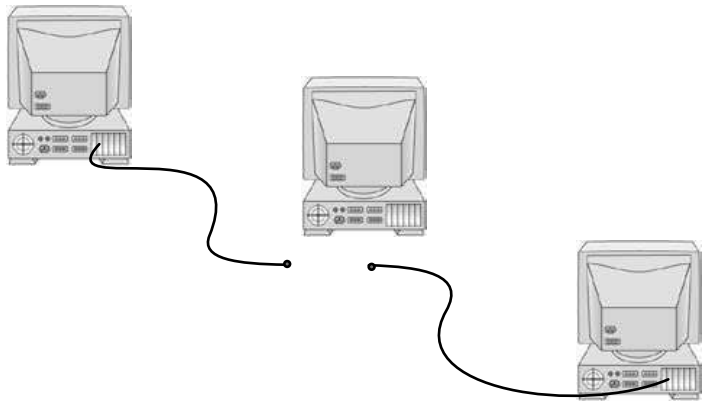
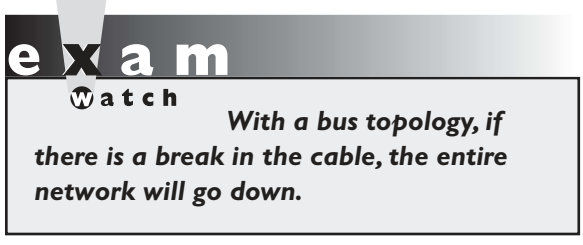


FIGURE 1-5

A break in the cable with the bus topology causes the entire network to fail.





With a bus topology, if there is a break in the cable, the entire network will go down.

A bus is a passive topology, which means that the workstations on the bus are not responsible for regenerating the signal as it passes by them. Since the workstations do not play an active role, the workstations are not a requirement of a functioning bus, which means that if a workstation fails, the bus does not fail. But if there is an unterminated end in the bus, the entire network will fail.

Advantages of a Bus Topology

One advantage of a bus topology is cost. A bus topology uses less cable than a star topology or a mesh topology, and you do not need to purchase any additional devices such as hubs. Another advantage of a bus topology is the ease of installation. With a bus topology, you simply connect the workstation to the cable segment or backbone. You need only the amount of cable to connect the workstation to the backbone. The most economical choice for a network topology is a bus topology, because it is easy to work with and a minimal amount of additional devices are required. Most importantly, if a computer fails, the network stays functional.

Disadvantages of a Bus Topology

The main disadvantage of a bus topology is the difficulty of troubleshooting it. When the network goes down, it is usually due to a break in the cable segment. With a large network, this problem can be tough to isolate.

Scalability is an important consideration in the dynamic world of networking. Being able to make changes easily within the size and layout of your network can be important in future productivity or downtime. The bus topology is not very scalable.

Star Topologies

In a star topology, all computers are connected through one central device known as a hub or a switch, as illustrated in Figure 1-6. Each workstation has a cable that goes from the network card to the hub device. One of the major benefits of a star topology is that a break in the cable causes only the workstation that is connected to the cable to go down, not the entire network, as with a bus topology. Star topologies are very popular topologies in today's networking environments.

Advantages of a Star Topology

One advantage of a star topology is scalability and ease of adding another system to the network. If you need to add another workstation to the network with a star topology, you simply connect that system to an unused port on the hub. Another benefit is the fact that if there is a break in the cable it affects only the system that is connected to that cable. Figure 1-7 shows a hub with a few ports available.

Centralizing network components can make an administrator's life much easier in the long run. Centralized management and monitoring of network traffic can be vital to network success. With a star configuration, it is also easy to add or change configurations because all of the connections come to a central point.

exam Watch

With a star topology, if there is a break in the cable, only the system connected to that cable is affected.

FIGURE 1-6

Computers connected in a star topology are all connected to a central hub or switch.

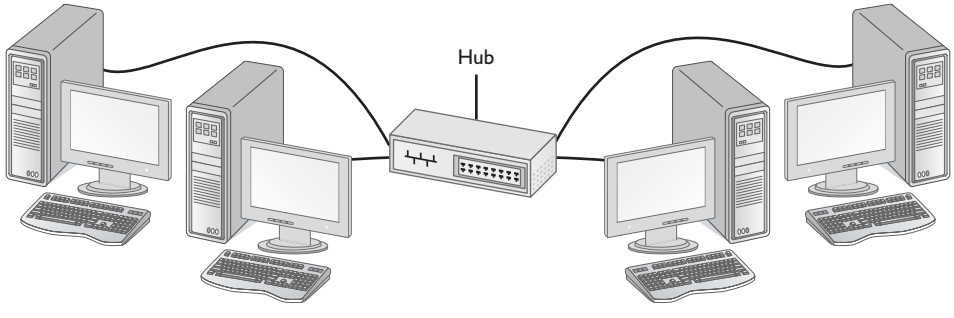


FIGURE 1-7

A five-port hub with four available ports

Disadvantages of a Star Topology

On the flip side, if the hub fails in a star topology, the entire network comes down, so we still have a central point of failure. But this is a much easier problem to troubleshoot than trying to find a cable break with a bus topology.

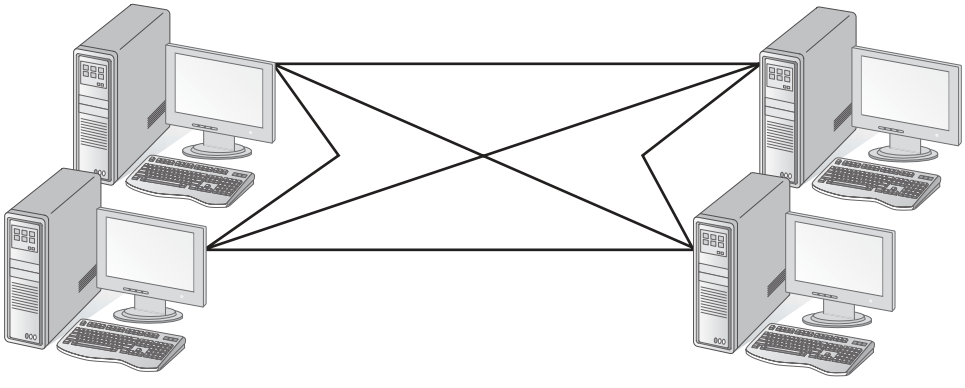
Another disadvantage of a star topology is cost. To connect each workstation to the network, you will need to ensure that there is a hub with an available port, and you will need to ensure you have a cable to go from the workstation to the hub. Today, the cost is increasingly less of a disadvantage because of the low prices of devices such as hubs and switches.

Mesh Topologies

A mesh topology is not very common in computer networking today, but you must understand the concept for the exam. In a mesh topology, every workstation has a connection to every other component of the network, as illustrated in Figure 1-8.

FIGURE 1-8

Computers in a mesh topology are all connected to every other computer on the network.



Advantages of a Mesh Topology

The biggest advantage of a mesh topology is fault tolerance, meaning that, if there is a break in a cable segment, traffic can be rerouted through a different pathway because there are multiple pathways to send data from one system to another. This fault tolerance means that it is almost impossible for the network to go down due to a cable fault.

Disadvantages of a Mesh Topology

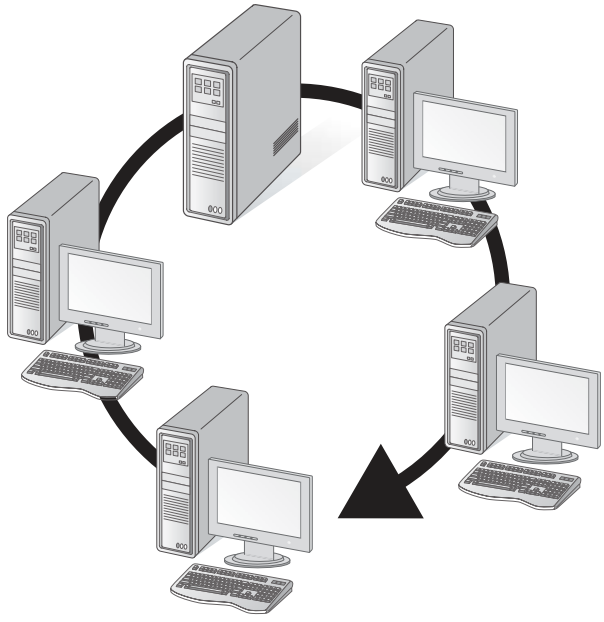
A disadvantage of a mesh topology is the cost of the additional cabling and network interfaces to create the multiple pathways between each system. A mesh topology is very hard to administer and manage because of the numerous connections.

Ring Topologies

In a ring topology, all computers are connected via a cable that loops in a ring or circle. As shown in Figure 1-9, a ring topology is a circle that has no start and no end. Because there are no ends, terminators are not necessary in a ring topology. Signals travel in one direction on a ring while they are passed from one computer to the next, with each computer regenerating the signal so that it may travel the distance required.

FIGURE 1-9

A ring topology



Advantages of a Ring Topology

A major advantage of a ring topology is that signal degeneration is low because each workstation is responsible for regenerating or boosting the signal. With the other topologies, as the signal travels the wire, it gets weaker and weaker as a result of outside interference: eventually, it becomes unreadable if the destination system is too far away. Because each workstation in a ring topology regenerates the signal, the signal is stronger when it reaches its destination and seldom needs to be retransmitted.

Disadvantages of a Ring Topology

The biggest problem with ring topologies is that if one computer fails or the cable link is broken, the entire network could go down. With newer technology, however, this isn't always the case. The concept of a ring topology today is that the ring will not be broken when a system is disconnected; only that system is dropped from the ring.

Isolating a problem can be difficult in some ring configurations. (With newer technologies, a workstation or server will put out a beacon if it notices a break in the ring.) Another disadvantage is that if you make a cabling change to the network or move a workstation, the brief disconnection can interrupt or bring down the entire network.

Hybrid Topologies

It is important to note that it is typical for networks to implement a mixture of topologies to form a hybrid topology. For example, a very popular hybrid topology is a star-bus topology, in which a number of star topologies are connected by a central bus, as shown in Figure 1-10. This is a popular topology because the bus will connect hubs that are spread over distance.

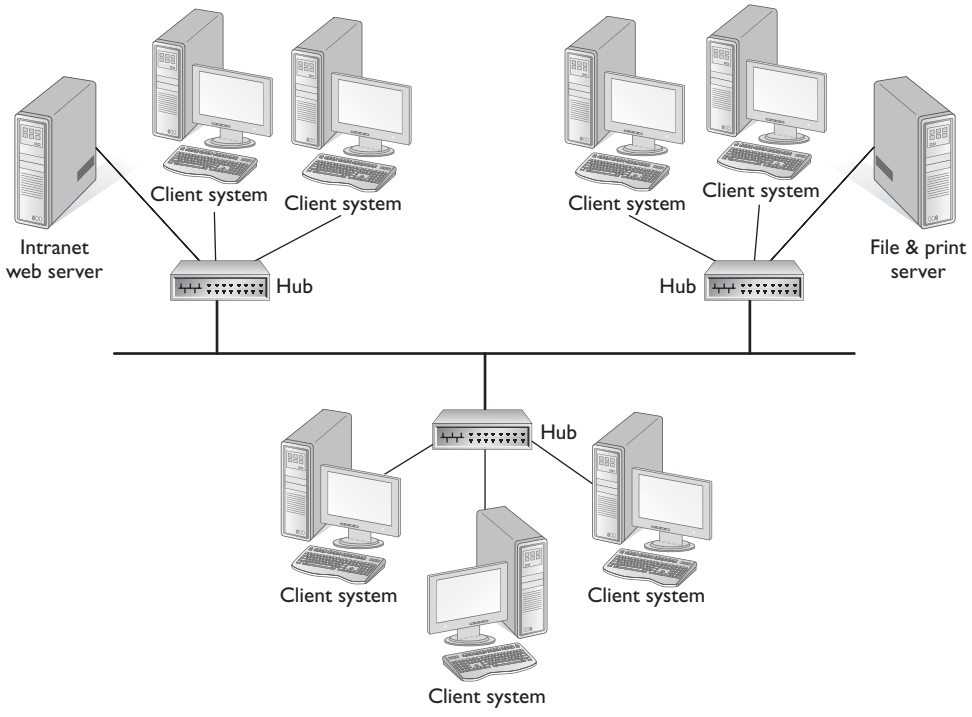
Another very popular hybrid topology is the star-ring topology. The star-ring topology is popular because it looks like a star but acts as a ring. For example, there is a network architecture known as Token Ring (more on this later, in the section "Network Architectures") that uses a central "hub" type device, but the internal wiring makes a ring. Physically it looks like a star, but logically it acts as a ring topology.

Wireless Topologies

A wireless topology is one in which few cables are used to connect systems. The network is made up of transmitters that broadcast the packets using radio

FIGURE 1-10

A star-bus hybrid topology

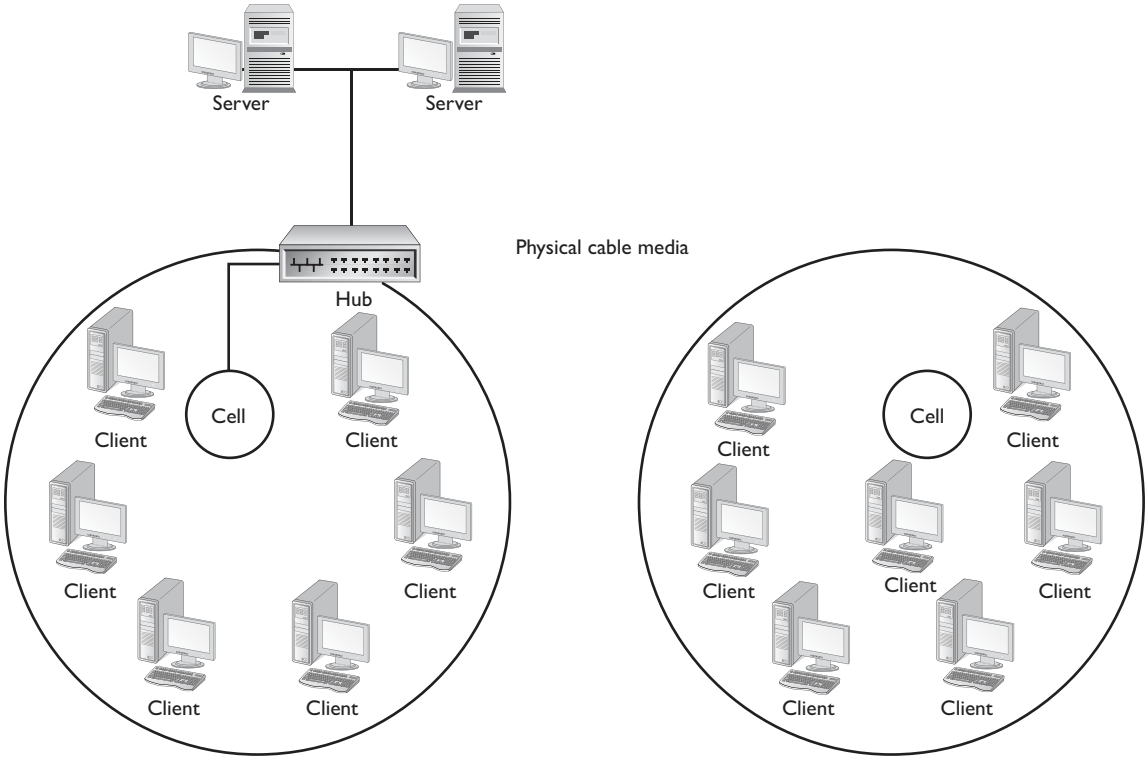


frequencies. The network contains special transmitters called *cells*, or *wireless access points*, which extend a radio sphere in the shape of a bubble around the transmitter. This bubble can extend to multiple rooms and possibly floors in a building. The PCs and network devices have a special transmitter-receiver, which allows them to receive broadcasts and transmit requested data back to the access point. The access point is connected to the physical network by a cable, which allows it, and any wireless clients, to communicate with systems on the wired network. A wireless network topology is shown in Figure 1-11.

Notice in Figure 1-11 that the wireless cells, or access points, are connected to the network by connecting into the hub or switch that has a connection to the rest of the wired network. Also notice that the clients do not have cables connecting them to the network. These are wireless clients, and they will get access to the network through the wireless cell (or access point).

Another option for wireless networks is the use of a radio antenna on or near the building, which allows one cell to cover the building and the surrounding area. This approach is best in a campus-type arrangement, where many buildings that need to be included in the cell are in a close geographical area. This setup does not easily

FIGURE 1-11 A wireless network topology



allow you to connect the buildings by a backbone and physical cables and then to each building containing the required cells for all its PCs and devices.

Wireless networks also can consist of infrared communications, similar to a remote-control TV, but this type of communication is slow and requires a direct line of sight—as well as close proximity—for the communication to work. Infrared mainly is used only between two systems. Infrared is not used often as a complete networking solution and should not be considered even as an option for a whole network; it is useful between laptops or a laptop and a printer.

Advantages of a Wireless Topology

The nice thing about wireless networks is the lack of cabling. The wireless network requires only base backbone segments to connect the wireless cells to the wired network if there is one. Once these are set up, the PC and network devices also need

the special transmitter-receiver network interface cards to allow the PCs and devices to communicate with the cell and then through the cell to the servers.

Troubleshooting failed devices and cells is very easy and makes failed components easy to find and replace.

Disadvantages of a Wireless Topology

Disadvantages of wireless networks include a greater chance of signal interference, blockage, and interception. Other devices and machinery that emit radio frequencies or "noise" can cause interference and static, which can disrupt the bubble of communication around the cell. Another source of noise is lightning during storms. This noise is the same static you hear when lightning strikes while you are speaking on a phone.

Blockage can occur in structures that are made of thick stone or metal, which do not allow radio frequencies to pass through easily. This drawback usually can be overcome somewhat by changing the frequency used by the devices to a higher frequency. You can determine early if this is going to be a problem in your building by trying to use a radio inside the building to pick up some radio stations. If the radio will not pick them up, the building material is too thick to allow radio frequencies to pass through the walls. This problem can be overcome by installing a cell in each room where a PC or network device will be placed.

Another major disadvantage with wireless is signal interception. Signal interception means unwanted third parties could intercept wireless communications without physically being on the premises; they would simply have to be within the signal range. One of the key steps to securing wireless communication is to limit who can connect to the network and to encrypt the traffic in transit. You will learn about wireless security in Chapter 7.

exam Watch

For the Network+ exam you need to be able to visually recognize the different network topologies from a network diagram.

Point-to-Point and Point-to-Multipoint

There are two popular layouts for topologies: they are either point-to-point or point-to-multipoint. A *point-to-point* topology—also known as host to host—is one system connected directly to another system. In the past these systems would connect directly through the serial ports with a null modem cable, but these days, you could connect them using a crossover cable or a wireless connection.

A *point-to-multipoint* topology uses a central device that connects all the devices together. This topology is popular with wireless. With point-to-multipoint, when the central device sends data, it is received by all devices connected to the central device. But if one of the devices that are connected sends data, then it is received by only the destination system.

Segments and Backbones

With the various topologies you've looked at, you have seen the words segment and backbone mentioned a couple of times. A network segment is a cable length (or multiple cable lengths) that is uninterrupted by network connectivity devices, such as bridges and routers. It is typical that a single network may be broken into multiple network segments through the use of a bridge or router to cut down on network traffic, as shown in Figure 1-12.

In Figure 1-12, notice that there are three network segments named Segment A, Segment B, and Segment C. Also notice that each network segment could have a number of clients and servers all connected through a number of hubs that are then connected to a backbone. This is just one possible solution involving network segments.

FIGURE 1-12 A single network broken into multiple network segments

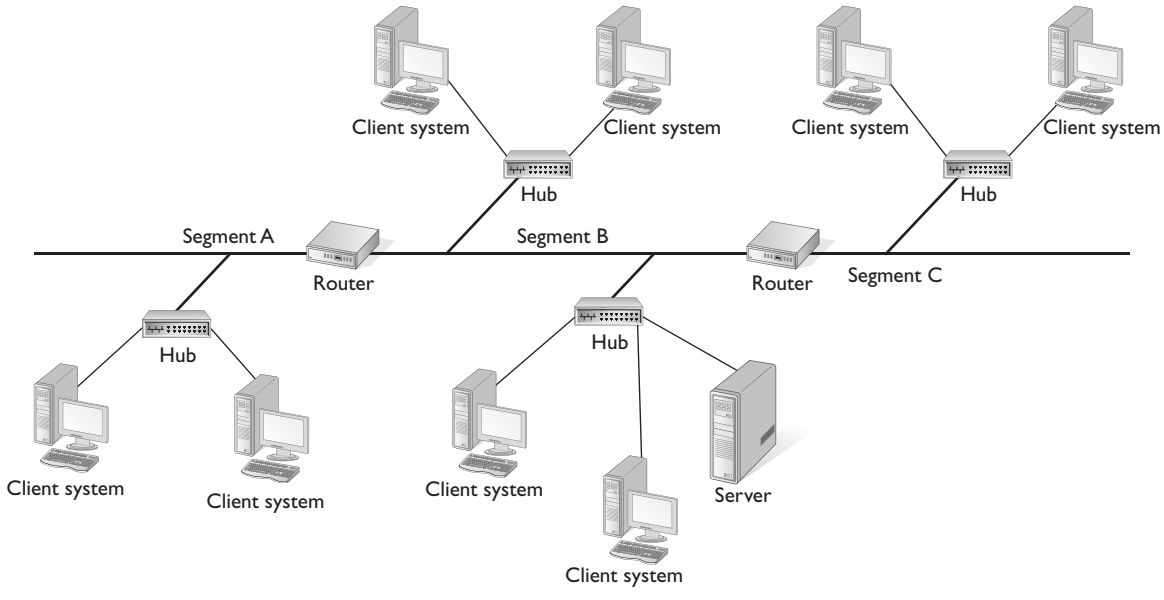
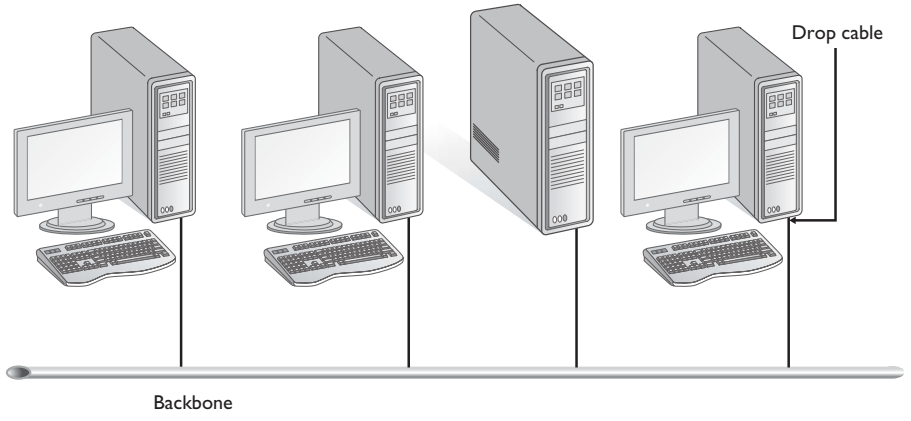


FIGURE 1-13

A network backbone with drop cables connecting the computers



You also saw the word backbone mentioned a few times. A backbone is the main cable segment or trunk in the network. In a bus network, you might see a main cable trunk that has smaller cables connecting the workstations. These smaller cables, known as *drop cables*, connect the workstations to the backbone. Figure 1-13 shows a backbone with drop cables.

Another example of a backbone is a satellite linking geographically dispersed local area networks (LANs), making a wide area network (WAN). Such a backbone is an example of a wireless communications network, whereas the previous examples all used cable as the medium.

CERTIFICATION OBJECTIVE 1.03

Network Media and Connectors

Now that you have learned that networks are built using a topology of bus, star, or ring, let's take a look at how the systems will be connected in the topology that you choose. Cabling is the medium for the transmission of data between hosts on the LANs. LANs can be connected together using a variety of cable types, such as unshielded twisted-pair, coax, or fiber. Each cable type has its own advantages and disadvantages, which you will examine in this section.

There are three primary types of cable media that can be used to connect systems to a network—coaxial cable, twisted-pair cable, and fiber-optic cable. Transmission

rates that can be supported on each of these physical media are measured in millions of bits per second, or megabits per second (Mbps).

Coaxial Cable

Coaxial, or coax, cable looks like the cable used to bring the cable TV signal to your television. One strand (a solid-core copper wire) runs down the middle of the cable. Around that strand is a layer of insulation, and covering that insulation is braided wire and metal foil, which shields against electromagnetic interference. A final layer of insulation covers the braided wire. Because of the layers of insulation, coaxial cable is more resistant to outside interference than other cabling, such as unshielded twisted-pair (UTP) cable. Figure 1-14 shows a coaxial cable with the copper core and the layers of insulation.

exam Watch

Both thinnet and thicknet have a transfer rate of 10 Mbps.

There are two types of coax cabling: thinnet and thicknet. The two differ in thickness and maximum cable distance that the signal can travel. Let's take a look at thinnet and thicknet:

- **Thinnet** This refers to RG-58 cabling, which is a flexible coaxial cable about ¼-inch thick. Thinnet is used for short-distance communication and is flexible enough to facilitate routing between workstations. Thinnet connects directly to a workstation's network adapter card using a British naval connector (BNC) and uses the network adapter card's internal transceiver. The maximum length of thinnet is 185 meters. Figure 1-15 displays thinnet coaxial cabling and the BNC connector on the end.
- **Thicknet** This coaxial cable, also known as RG-8, gets its name by being a thicker cable than thinnet. Thicknet cable is about ½-inch thick and can support data transfer over longer distances than thinnet. Thicknet has a maximum cable length of 500 meters and usually is used as a backbone to connect several smaller thinnet-based networks. Due to the thickness of ½ inch, this cable is harder to work with than thinnet cable. A transceiver often is connected directly to the thicknet cable using a connector known as a vampire tap. Connection from the transceiver to the network adapter card is made using a drop cable to connect to the adapter unit interface (AUI) port connector. Table 1-1 summarizes the characteristics of thicknet and thinnet.

FIGURE 1-14

A coaxial cable

FIGURE 1-15

Thinnet coaxial cable with a BNC connector

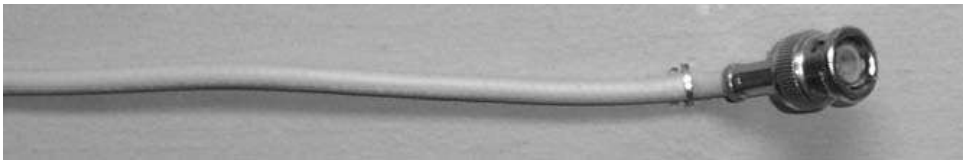


TABLE 1-1

Thinnet Versus Thicknet

Coax Type	Cable Grade	Thickness	Maximum Distance	Transfer Rate	Connector Used to Connect NIC to Cable Type
Thinnet	RG-58	0.25 in	185 m	10 Mbps	BNC
Thicknet	RG-8	0.5 in	500 m	10 Mbps	AUI

Twisted-Pair Cable

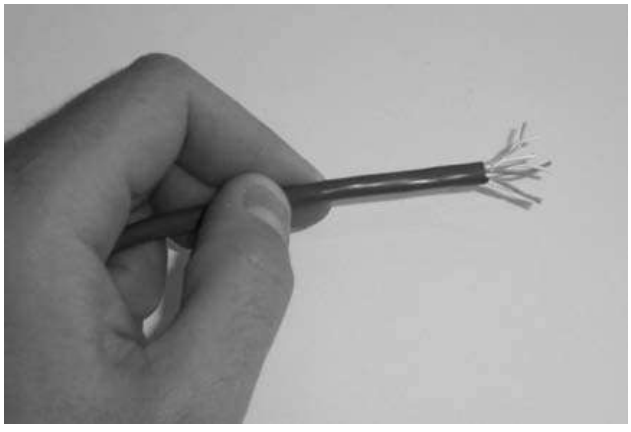
Coaxial cable is not as popular today as it was a few years ago; today the popularity contest has been dominated by twisted-pair cabling. Twisted-pair cabling gets its name by having four pairs of wires that are twisted to help reduce crosstalk or interference from outside electrical devices. (Crosstalk is interference from adjacent wires.) Figure 1-16 shows a twisted-pair cable. Just as there are two forms of coaxial cable, there are two forms of twisted-pair cabling—unshielded twisted-pair (UTP) and shielded twisted-pair (STP).

exam Watch

For the exam know that the RG-59 and RG-6 cable grades are used with home video devices such as TVs and VCRs. RG-59 is used for short distances, while RG-6 is a more expensive coax used for longer distances.

FIGURE 1-16

Unshielded twisted-pair (UTP) cable



Unshielded Twisted-Pair (UTP) Cable

Unshielded twisted-pair (UTP) cables are familiar to you if you have worked with telephone cable. The typical twisted-pair cable for network use contains four pairs of wires. Each member of the pair of wires contained in the cable is twisted around the other. The twists in the wires help shield against electromagnetic interference. The maximum distance of UTP is 100 meters.

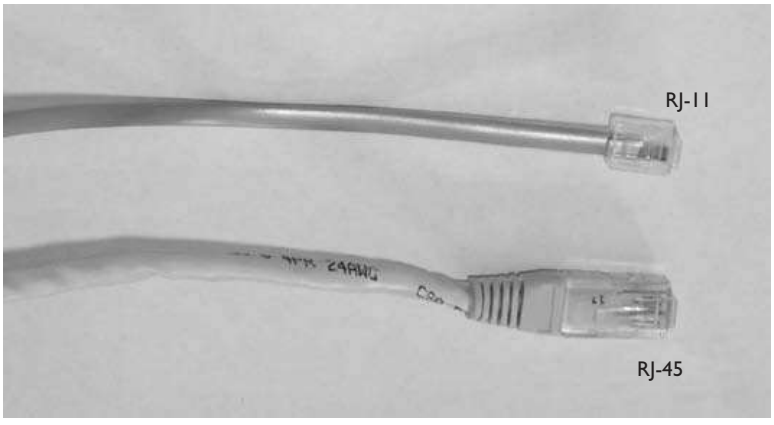
UTP cable uses small plastic connectors designated as registered jack 45, or most often referred to as RJ-45. RJ-45 is similar to the phone connectors, except that instead of four wires, as found in the home system, the network RJ-45 connector contains eight contacts, one for each wire in a UTP cable. The bottom cable in Figure 1-17 is an RJ-45 connector.

It can be easy to confuse the RJ-45 connector with the RJ-11 connector. The RJ-11 connector is a telephone connector and is shown in Figure 1-17 (the cable on the top). In an RJ-11 connector, there are four contacts; hence there are four wires found in the telephone cable. With RJ-45 and RJ-11, you will need a special crimping tool when creating the cables to make contact between the pins in the connector and the wires inside the cable.

UTP cable is easier to install than coaxial because you can pull it around corners more easily due to its flexibility and small size. Twisted-pair cable is more susceptible to interference than coaxial, however, and should not be used in environments containing large electrical or electronic devices.

FIGURE 1-17

An RJ-11 connector and an RJ-45 connector



exam Watch

Be sure to know the different categories of UTP cabling for the Network+ exam.

UTP cabling has different flavors, known as grades or categories. Each category of UTP cabling was designed for a specific type of communication or transfer rate. Table 1-2 summarizes the different UTP categories—the most popular today being CAT 5e, which can reach transfer rates of over 1000 Mbps or 1 gigabit per second (Gbps).

Wiring Standards

It is important to understand the order of the wires within the RJ-45 connector for both the Network+ exam and in the real world if you intend on creating (also known as crimping) your own cables. Let's start with some basics of comparing a straight-through cable with a crossover cable.

Straight-Through Cables CAT 5 UTP cabling usually uses only four wires when sending and receiving information on the network. The four wires of the eight that are used are wires 1, 2, 3, and 6. Figure 1-18 shows the meaning of the pins on a computer and the pins on a hub (or switch), which is what you typically will be connecting the computers to. When you configure the wire for the same pin at either end of the cable, this is known as a straight-through cable.

TABLE 1-2

Different UTP Category Cabling

UTP Category	Purpose	Transfer Rate
Category 1	Voice only	
Category 2	Data	4 Mbps
Category 3	Data	10 Mbps
Category 4	Data	16 Mbps
Category 5	Data	100 Mbps
Category 5e	Data	1 Gbps (1000 Mbps)
Category 6	Data	10 Gbps

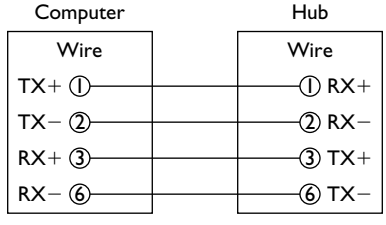
You will notice in the figure that wires 1 and 2 are used to transmit data (TX) from the computer, while wires 3 and 6 are used to receive information (RX) on the computer. You will also notice that the transmit pin on the computer is connected to the receive pin (RX) on the hub via wires 1 and 2. This is important because we want to make sure that data that is sent from the computer is received at the network hub. We also want to make sure that data sent from the hub is received at the computer, so you will notice that the transmit pins (TX) on the hub are connected to the receive pins (RX) on the computer through wires 3 and 6. This will allow the computer to receive information from the hub.

The last thing to note about Figure 1-18 is that pin 1 on the computer is connected to pin 1 on the hub by the same wire, thus the term *straight-through*. You will notice that all pins are matched straight through to the other side in Figure 1-18.

Crossover Cables At some point, you may need to connect two computer systems directly together without the use of a hub, from network card to network card. To do this, you would not be able to use a straight-through cable because the transmit pin on one computer would be connected to the transmit pin on another

FIGURE 1-18

Pinout diagram for a straight-through cable



computer, as shown in Figure 1-19. How could a computer pick up the data if it was not sent to the receive pins? This will not work, so we will need to change the wiring of the cable to what is known as a *crossover cable*.

In order to connect two systems directly together without the use of a hub, you will need to create a crossover cable by switching wires 1 and 2 with wires 3 and 6 at one end of the cable, as shown in Figure 1-20. You will notice that the transmit pins on Computer A are connected to the receive pins on Computer B, thus allowing Computer A to send data to Computer B. The same applies for Computer B to send to Computer A—pins A and B on Computer B are wired to pins 3 and 6 on Computer A so that Computer A can receive data from Computer B.

exam Watch

For the Network+ exam, remember that to create a crossover cable wires 1 and 2 are switched with wires 3 and 6 on one end of the cable.

568A and 568B Standards Although only four of the wires are used to send and receive data in most environments today, some of the newer standards use all eight wires. Therefore, it is important to know the order of all eight wires in a UTP cable. There are two popular wiring standards today, 568A and 568B, but because 568B is the more popular standard for CAT 5 and CAT 5e, I will discuss the wire order for 568B. Table 1-3 shows the wire order for the 568B standard of a straight-through cable at both ends.

FIGURE 1-19

Using a straight-through cable to connect two computers will not work.

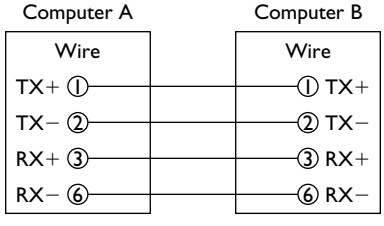


FIGURE 1-20

Pinout diagram of a crossover cable

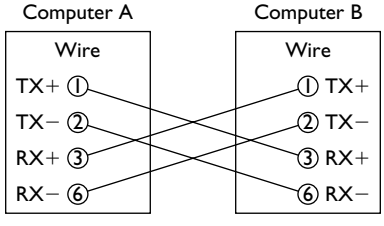


TABLE 1-3

The 568B Wiring Standard for a Straight-Through Cable

Wire	Connector #1	Connector #2
1	White wire/orange stripe (white-orange)	White wire/orange stripe (white-orange)
2	Orange wire	Orange wire
3	White wire/green stripe (white-green)	White wire/green stripe (white-green)
4	Blue wire	Blue wire
5	White wire/blue stripe (white-blue)	White wire/blue stripe (white-blue)
6	Green wire	Green wire
7	White wire/brown stripe (white-brown)	White wire/brown stripe (white-brown)
8	Brown wire	Brown wire

Following this standard and what you have learned of crossover cables, you would switch wires 1 and 2 with wires 3 and 6 at one end to create a crossover cable. After switching the wires on one end, you would have a cable that has the order of wires shown in Table 1-4.

TABLE 1-4

The 568B Wiring Standard for a Crossover Cable

Wire	Connector #1	Connector #2
1	White wire/orange stripe (white-orange)	White wire/green stripe (white-green)
2	Orange wire	Green wire
3	White wire/green stripe (white-green)	White wire/orange stripe (white-orange)
4	Blue wire	Blue wire
5	White wire/blue stripe (white-blue)	White wire/blue stripe (white-blue)
6	Green wire	Orange wire
7	White wire/brown stripe (white-brown)	White wire/brown stripe (white-brown)
8	Brown wire	Brown wire

FIGURE 1-21

A crimping tool

Before moving on to other cable types, apply what you have learned by crimping (creating) your own CAT 5 cable. To create your own network cable, you will need to have a crimper like the one shown in Figure 1-21. You can get a fairly cheap crimping tool at your local electronics store, but you can also buy some fairly expensive crimping tools.

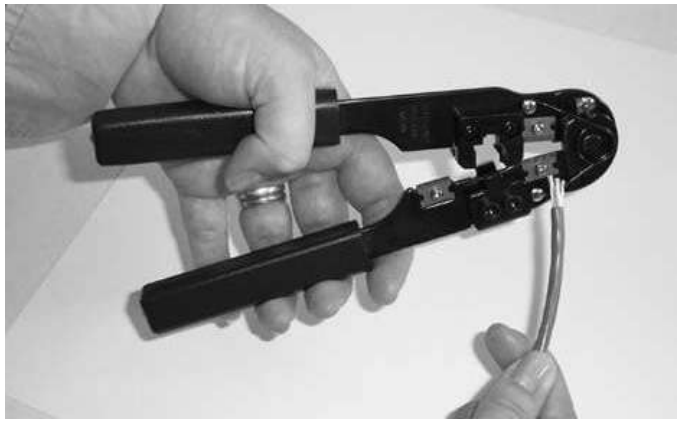
When you select a crimping tool, you want to make sure that you have one that has a built-in crimper as well as a wire stripper and a wire cutter. Exercise 1-1 demonstrates the steps needed to crimp your own CAT 5 cable.

EXERCISE 1-1

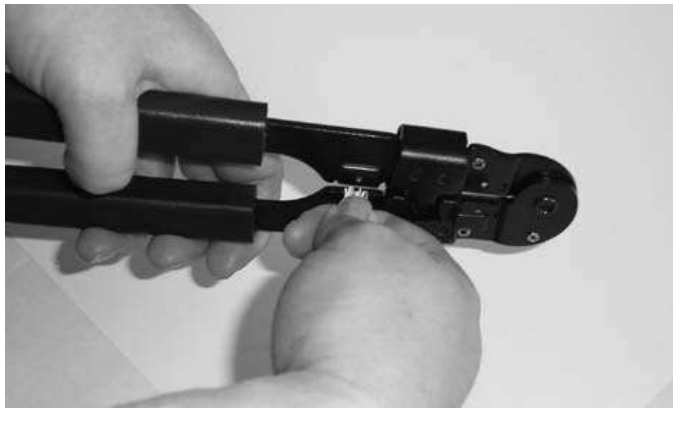
Crimping a Category 5 Cable

In this exercise, you will learn how to crimp your own CAT 5 cable. To complete this exercise, you will need to have a crimping tool, a piece of CAT 5 cabling, some RJ-45 connectors, and a little bit of patience! To create a CAT 5 cable, do the following:

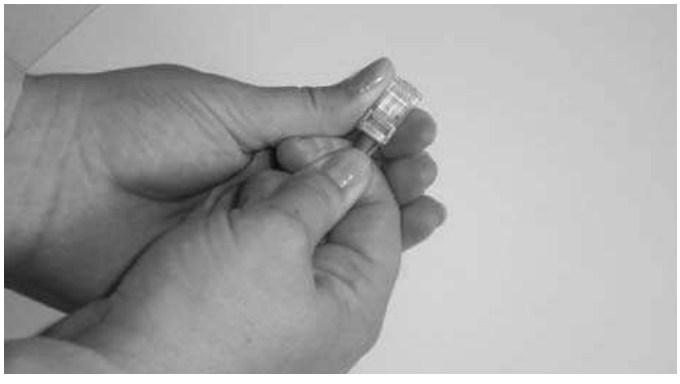
1. Ensure that you have a clean-cut end on the cable by using your wire cutters to cut a little off the end of the CAT 5 cable.
2. Once you have cut a clean end on the cable, strip about an inch off the outer jacket from the cable using the wire-stripper portion of your crimping tool, as shown in the next illustration. After stripping the outer jacket off, make sure that you have not cut into any of the individual wires. If you have, cut a clean end off the cable again and start from the beginning.



3. Once you have stripped the outer jacket off the cable, order the wires from left to right to follow the 568B standard. This is where your patience will come in, because it will take some time to get the wires in the correct order and placed tightly together so that they will go inside the RJ-45 connector.
4. Once you have the wires aligned in the correct order and you have them all nice and snug together so that they will fit inside the RJ-45 connector, you are ready to insert them into the connector. Before inserting the wires into the connector, make sure that their ends are of equal length; if they are not, just cut the tips a bit with your wire cutters, as shown in the following illustration, to be certain that they will fit nicely into the RJ-45 connector.



5. Slide the wires into the RJ-45 connector, as shown in the next illustration, and make sure that all wires have made contact with the metal contacts inside the RJ-45 connector by looking at the end of the connector. This is where mistakes happen frequently; there is usually one wire in the middle that is not pushed up to the end of the connector.



6. Once you are certain that all wires have made contact, you can "crimp" the wire, which will enclose the RJ-45 connector on the wires, creating a permanent fit. Insert the connector into the crimping tool and squeeze the handle tight, as seen in the following illustration.

Rollover A *rollover* cable is a popular cable type in the networking world and is used to connect to a Cisco device such as a router or a switch. Also known as a console cable, this cable connects from the computer's serial port to the console port of the router or switch. Once the network administrator connects to the console port, he or she is then able to configure the router or switch.

Shielded Twisted-Pair (STP) Cable

exam Watch

Both UTP and STP cabling have a maximum distance of 100 meters.

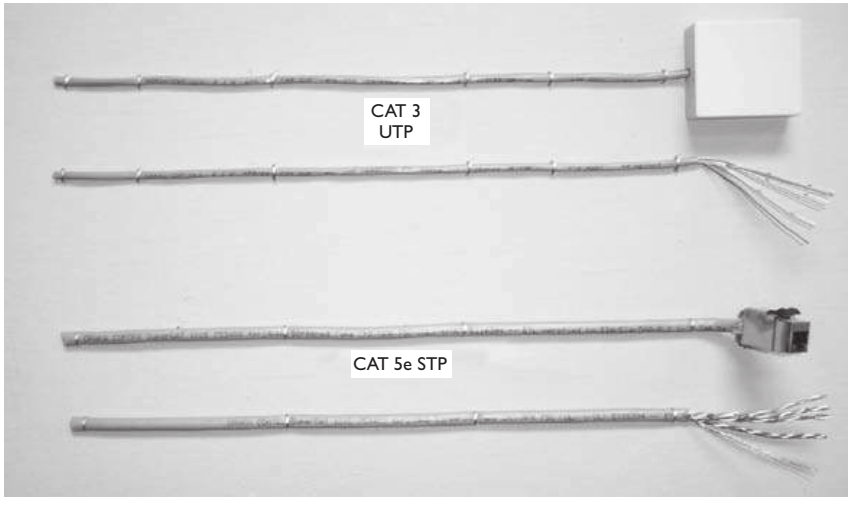
Shielded twisted-pair (STP) cable is very similar to UTP cabling, but it differs from UTP in that it uses a layer of insulation within the protective jacket, which helps maintain the quality of the signal. Figure 1-22 shows the size of STP cabling as compared to UTP.

Fiber-Optic Cable

The third type of cabling that we want to discuss is fiber-optic cabling. Fiber-optic cabling is unlike coax and twisted-pair, because both of those types have a copper wire that carries the electrical signal. Fiber-optic cables use optical fibers that carry digital data signals in the form of modulated pulses of light. An optical fiber consists of an extremely thin cylinder of glass, called the core, surrounded by a concentric layer of glass, known as the cladding. There are two fibers per cable—one to

FIGURE 1-22

UTP cabling versus STP cabling



transmit and one to receive. The core also can be an optical-quality clear plastic, and the cladding can be made up of gel that reflects signals back into the fiber to reduce signal loss. Figure 1-23 shows fibers in a fiber-optic cable.

There are two types of fiber-optic cables: single-mode fiber (SMF) and multimode fiber (MMF).

- **Single-mode fiber** Uses a single ray of light, known as a mode, to carry the transmission over long distances.
- **Multimode fiber** Uses multiple rays of light (modes) simultaneously, with each ray of light running at a different reflection angle to carry the transmission over short distances.

Fiber-optic cable supports up to 1000 stations and can carry the signal up to and beyond 2 kilometers. Fiber-optic cables are also highly secure from outside interference, such as radio transmitters, arc welders, fluorescent lights, and other sources of electrical noise. On the other hand, fiber-optic cable is by far the most expensive of these cabling methods, and a small network is unlikely to need these features. Depending on local labor rates and building codes, installing fiber-optic cable can cost as much as $500 per network node.

exam Watch

You have learned of two electrical phenomena that can disrupt a signal traveling along your network: crosstalk and outside electrical noise. Crosstalk is caused by electrical fields in adjacent wires, which induce false signals in a wire. Outside electrical noise comes from lights, motors, radio systems, and many other sources. Fiber-optic cables are immune to these types of interference because they do not carry electrical signals—they carry pulses of light.

Fiber-optic cables can use many types of connectors, but the Network+ exam is concerned only with the two major connector types: the straight-tip (ST) connector and the subscriber (SC) connector. The ST connector is based on the BNC-style connector but has a fiber-optic cable instead of a copper cable. The SC connector is square and somewhat similar to an RJ-45 connector. Figure 1-24 shows the ST (the connector on the left side) and the SC (the connector on the right side) connector types.

FIGURE 1-23

A fiber-optic cable

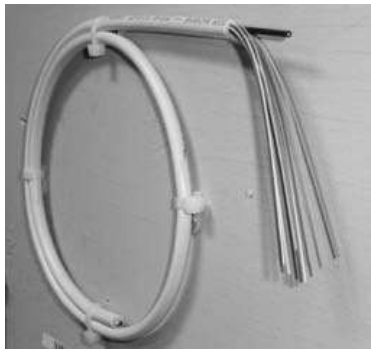
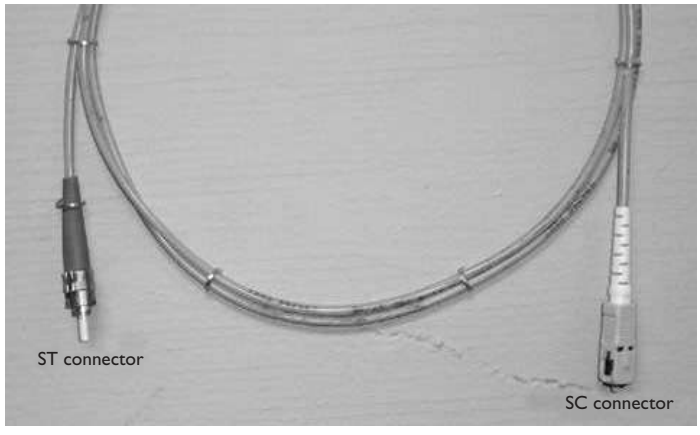


FIGURE 1-24

Fiber-optic ST and SC connector types



Regardless of the connector type, the fiber-optic cable still functions at the same speed, which is typically 1000 Mbps and faster. The only thing that you need to worry about is that the connector matches the device to which it is being connected, since the two-connector types are not interchangeable.

To better understand all of the cable types and when to use some specific types, see Exercise 1-2.

Be sure to take a look at Exercise 1-2 in the LabBook.pdf file that is found on the CD-ROM.

When preparing for the Network+ exam, it is sometimes helpful to have a table listing the differences between the different cable types. Table 1-5 summarizes the different cable types—be sure to review it for the Network+ exam.

TABLE 1-5

Summary of Cable Types

Cable	Max Distance	Transfer Rate	Connector Used
Thinnet	185 m	10 Mbps	BNC
Thicknet	500 m	10 Mbps	AUI
CAT 3 (UTP)	100 m	10 Mbps	RJ-45
CAT 5 (UTP)	100 m	100 Mbps	RJ-45
CAT 5e	100 m	1 Gbps	RJ-45
CAT 6	100 m	10 Gbps	RJ-45
Fiber	2 km	1+ Gbps	SC, ST

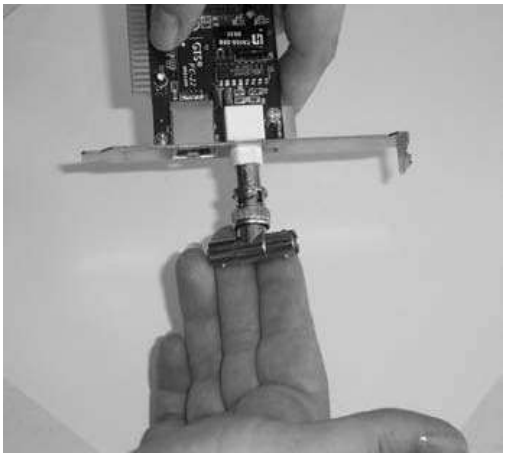
Connector Types

Coaxial Connectors

We have discussed coaxial cabling, and you saw the BNC connector that goes on the end of the cable and connects to the network card, but there are a few other BNC connector types you should be familiar with. The BNC-T connector is used to connect to coax cable from either side (so that the cable length can continue on), while a third end of the connector tees out to have a cable length connect to the network card on the client machine. Figure 1-25 displays the BNC-T connector being placed on a network card. Notice the connector on the card that the T-connector connects to, and also notice where the coax cable would continue on through.

FIGURE 1-25

A BNC-T connector connecting to the network card



We also discussed the terminator that needs to go at both ends of the coax cable. For example, if we use the BNC-T connector to connect our last system to the network, we would need to terminate one of the ends on the T-connector, as shown in Figure 1-26. Notice that the terminator goes on one end of the T-connector and that the coax cable would connect into the other end.

Twisted-Pair Connectors

We have discussed two major twisted-pair connectors, the RJ-11 for four-wire telephone cable and the RJ-45 for eight-wire network cables. There are also barrel connectors, which are female connectors on both ends that allow you to join two cable lengths together and reach greater distances, not exceeding 100 meters. Figure 1-27 shows an RJ-45 barrel connector connecting two cable lengths together. There are also BNC barrel connectors.

FIGURE 1-26

A 50-ohm BNC terminator

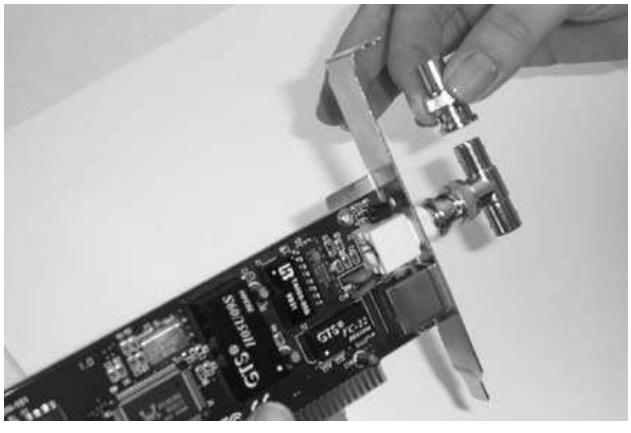


FIGURE 1-27

An RJ-45 barrel connector

Other Connectors

There are a number of additional connector types that you will come across in networking environments, some of which are listed here:

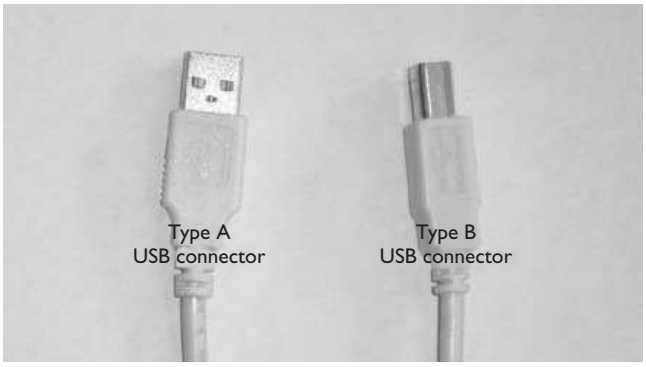
- **F-type connector** Another connector style for coax cabling, it is the same connector style that runs to your TV.
- **Fiber local connector (LC) and mechanical-transfer registered jack (MT-RJ)** Additional fiber-optic connector types that are similar to the registered jack and fiber SC shape. The Fiber LC is the preferred connector of the two for communications exceeding 1 Gbps due to its small form factor.
- **Universal serial bus (USB)** A high-speed serial bus that supports 127 devices in the chain. USB uses a standard connector type that is used by most devices, including mice, printers, network cards, digital cameras, and flash drives. There are two USB standards: USB 1.1, which has a transfer rate of 12 Mbps, and USB 2.0, which has a transfer rate of 480 Mbps. There are two standard USB connectors, Type A and Type B. Type A connectors connect to the computer, whereas Type B connectors connect to the device. Figure 1-28 displays these two connector styles.
- **IEEE 1394 (FireWire)** An ultra-high-speed bus that supports 63 devices in the chain and is ideal for real-time applications and devices such as for video. FireWire has two standards: 1394a, which has a transfer rate of 400 Mbps, and 1394b, which has a transfer rate of 800 Mbps.
- **RS-232** The standard for serial connections using the serial port on a computer. The serial port was a popular way to achieve a point-to-point connection between two hosts or was used for modems. The RS-232 standard defines a transfer rate of 20,000 bits per second, but serial devices support higher transfer rates.

Now that you understand some of the different cable types and connectors, Exercise 1-3 will demonstrate to you the steps to install a bus network using thinnet and BNC connectors.

Be sure to take a look at Exercise 1-3 in the LabBook.pdf file that is found on the CD-ROM.

FIGURE 1-28

USB Type A and Type B connectors



CERTIFICATION OBJECTIVE 1.04

Access Methods

You now know that a network uses a network topology—which is the layout of the network—and you know that some form of media such as cabling connects all hosts on the network. We have discussed the three major types of cabling: coax, twisted-pair, and fiber-optic cabling.

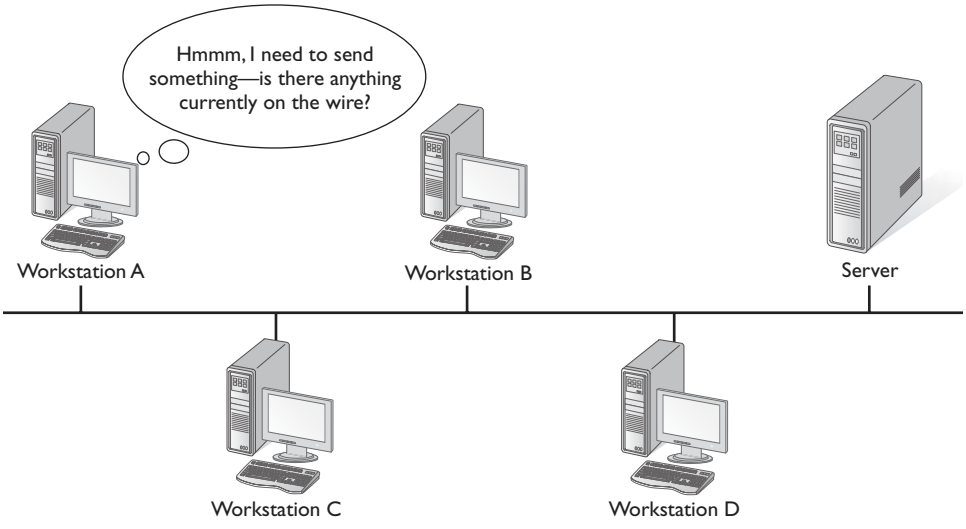
This section will identify what are known as access methods. An access method determines how a host will place data on the wire—does the host have to wait its turn or can it just place the data on the wire whenever it wants? The answer is determined by three major access methods: CSMA/CD, CSMA/CA, and token passing. Let's look at each of these access methods.

CSMA/CD

Carrier sense multiple access with collision detection (CSMA/CD) is one of the most popular access methods in use today. With CSMA/CD, every host has equal access to the wire and can place data on the wire when the wire is free from traffic. If a host wishes to place data on the wire, it will "sense" the wire and determine whether there is a signal already on the wire. If there is, the host will wait to transmit the data; if the wire is free, the host will send the data, as shown in Figure 1-29.

FIGURE 1-29

A host "sensing" the wire to see if it is free of traffic



The problem with the process just described is that, if there are two systems on the wire that "sense" the wire at the same time to see if the wire is free, they will both send data out at the same time if the wire is free. When the two pieces of data are sent out on the wire at the same time, they will collide with one another, and the data will be destroyed. If the data is destroyed in transit, the data will need to be retransmitted. Consequently, after a collision, each host will wait a variable length of time before retransmitting the data (they don't want the data to collide again), thereby preventing a collision the second time. When a system determines that the data has collided and then retransmits the data, that is known as collision detection.

exam Watch

All Ethernet environments use CSMA/CD as the access method.

To summarize, CSMA/CD provides that before a host sends data on the network, it will "sense" (CS) the wire to ensure that the wire is free of traffic. Multiple systems have equal access to the wire (MA), and if there is a collision, a host will detect that collision (CD) and retransmit the data.

CSMA/CA

Carrier sense multiple access with collision avoidance (CSMA/CA) is not as popular as CSMA/CD and for good reason. With CSMA/CA, before a host sends data on the wire, it will "sense" the wire as well to see if the wire is free of signals. If the wire

is free, it will try to "avoid" a collision by sending a piece of "dummy" data on the wire first to see whether it collides with any other data. If it does not collide, the host in effect assumes "If my dummy data did not collide, then the real data will not collide," and it submits the real data on the wire.

Token Passing

With both CSMA/CD and CSMA/CA, the possibility of collisions is always there, and the more hosts that are placed on the wire, the greater the chances of collisions, because you have more systems "waiting"' for the wire to become free so that they can send their data.

Token passing takes a totally different approach to deciding on how a system can place data on the wire. With token passing, there is an empty packet running around on the wire—the "token." In order to place data on the wire, you need to wait for the token; once you have the token and it is free of data, you can place your data on the wire. Since there is only one token and a host needs to have the token to "talk," it is impossible to have collisions in a token-passing environment.

For example, if Workstation 1 wants to send data on the wire, the workstation would wait for the token, which is circling the network millions of times per second. Once the token has reached Workstation 1, the workstation would take the token off the network, fill it with data, mark the token as being used so that no other systems try to fill the token with data, and then place the token back on the wire heading for the destination host.

All systems will look at the data, but they will not process it, since it is not destined for them. However, the system that is the intended destination will read the data and send the token back to the sender as a confirmation. Once the token has reached the original sender, the token is unflagged as being used and released as an empty token onto the network.

CERTIFICATION OBJECTIVE 1.05

Network Architectures

This section will discuss the different network architectures that are popular in today's networking environments. This section is very important from an exam point of view as well, so be sure to understand how the different architectures are pieced together.

Before we can discuss the different network architectures, we need to start our discussions by defining two terms: broadband and baseband transmissions.

Broadband and Baseband

There are two different techniques that may be used to transmit the signal along the network wire—baseband communication and broadband communication. Let's take a look at each of these techniques.

- **Baseband** Sends digital signals through the media as a single channel that uses the entire bandwidth of the media. The signal is delivered as a pulse of electricity or light, depending on the type of cabling being used. Baseband communication is also bidirectional, which means that the same channel can be used to send and receive signals.
- **Broadband** Sends information in the form of an analog signal, which flows as electromagnetic waves or optical waves. Each transmission is assigned to a portion of the bandwidth, so unlike with baseband communication, it is possible to have multiple transmissions at the same time, with each transmission being assigned its own channel or frequency. Broadband communication is unidirectional, so in order to send and receive, two pathways will need to be used. This can be accomplished either by assigning a frequency for sending and assigning a frequency for receiving along the same cable or by using two cables, one for sending and one for receiving.

Ethernet

To start us out, I first want to point out that network architecture is something that came about one day when someone sat down and said, "We are going to design a network architecture; let's use CAT 3 cabling, a star topology, and CSMA/CD as an access method. Oh, and let's call this architecture 10BaseT!"

In this example, 10BaseT was the name assigned to the architecture because 10 Mbps is the transfer rate of the network, baseband communication is the technique used to transmit the signal, and the T means our cable type—in this case twisted-pair. Now, we have discussed different types of twisted-pair cabling, but CAT 3 is the one that runs at 10 Mbps, so it is the cable used in 10BaseT.

exam Watch

Ethernet is defined as the IEEE 802.3 standard.

The first types of network architecture to look at are the different Ethernet architectures. When designing networks, one of the first decisions we usually make is "Do we want to use Ethernet or the competing network architecture called Token Ring? Oh, we want to use Ethernet. What flavor of Ethernet?" This section will help you understand what the different flavors of Ethernet are.

10Base2

The 10Base2 Ethernet architecture is a network that runs at 10 Mbps and uses baseband transmissions. 10Base2 typically is implemented as a bus topology, but it could be a mix of a bus and a star topology. The cable type that we use is determined by the character at the end of the name of the architecture—in this case a 2. The 2 implies 200 meters. Now, what type of cable is limited to approximately 200 m? You got it; thinnet is limited to approximately 200 m (185 m, to be exact). The only characteristic we have not mentioned is the access method that is used. All Ethernet environments use CSMA/CD as a way to put data on the wire.

exam Watch

10Base2 and 10Base5 follow what is known as the 5-4-3 rule, which means that there can be only five network segments in total, joined by four repeaters (more on repeaters in Chapter 3), but only three of those network segments can be populated with nodes.

The following list summarizes features of 10Base2:

- Baseband communication
- 10 Mbps transfer rate
- Maximum distance of 185 meters per network segment
- 30 hosts per segment
- 0.5 meters minimum distance between hosts

10Base5

The 10Base5 Ethernet architecture runs at 10 Mbps and uses baseband transmission as well. It was also implemented as a bus topology. The cable it uses is limited to approximately 500 meters, which is thicknet, and it uses CSMA/CD as the access method. The thicker copper core in the wire allows the signal to travel farther than is possible with thinnet.

The following list summarizes features of 10Base5:

- Baseband communication
- 10 Mbps transfer rate
- Maximum distance of 500 meters per network segment
- 100 hosts per segment
- 2.5 meter minimum distance between hosts

10BaseT

The 10BaseT Ethernet architecture runs at 10 Mbps and uses baseband transmission. It uses a star topology with a hub or switch at the center, allowing all systems to connect to one another. The cable it uses is CAT 3 UTP, which is the UTP cable type that runs at 10 Mbps. Keep in mind that most cable types are backward compatible, so you could have CAT 5 UTP cabling in a 10BaseT environment. But because the network cards and hubs are running at 10 Mbps, that is the maximum transfer speed you will get, even though the cable supports more. Like all Ethernet environments, 10BaseT uses CSMA/CD as the access method.

10BaseFL

The 10BaseFL Ethernet architecture allows for a 10 Mbps Ethernet environment that runs on fiber-optic cabling. The purpose of the fiber-optic cabling is to use it as a backbone to allow the network to reach greater distances.

Fast Ethernet (100BaseTX and 100BaseFX)

These two standards are part of the 100BaseX family, which is known as fast Ethernet. The different fast Ethernet flavors run at 100 Mbps, use a star topology, use CSMA/CD as an access method, but differ in the type of cabling used. 100BaseTX uses two pairs (four wires) in the CAT 5 cabling, whereas 100BaseFX uses two strands of fiber instead of twisted-pair cabling.

Gigabit Ethernet

Gigabit Ethernet is becoming the de facto standard for network architectures today. With Gigabit Ethernet we can reach transfer rates of 1000 Mbps (1 Gbps), using traditional media such as coaxial, twisted-pair, and fiber-optic cabling. There are

two standards (more on the IEEE standards in Chapter 2) for Gigabit Ethernet: IEEE 802.3z and IEEE 802.3ab.

IEEE 802.3z The IEEE 802.3z standard defines Gigabit Ethernet that runs over fiber-optic cabling or coaxial cabling. There are three types of Gigabit Ethernet that fall under this standard:

- **1000BaseSX** The Gigabit Ethernet architecture that runs at 1000 Mbps over multimode fiber (MMF) optic cabling. This architecture is designed for short distances of up to 550 meters.
- **1000BaseLX** The Gigabit Ethernet architecture that runs at 1000 Mbps over single-mode fiber (SMF) optic cabling. This architecture supports distances up to 3 kilometers.
- **1000BaseCX** The Gigabit Ethernet architecture that runs at 1000 Mbps over coaxial cable and supports distances of up to 25 meters.

IEEE 802.3ab The IEEE 802.3ab standard, known as 1000BaseTX, defines Gigabit Ethernet that runs over twisted-pair cabling and uses characteristics of 100BaseTX networking, including the use of RJ-45 connectors and the access method of CSMA/CD. Like 100BaseTX, 1000BaseTX uses CAT 5e or CAT 6 unshielded twisted-pair; the difference is that 100BaseTX runs over two pairs (four wires) while 1000BaseTX runs over four pairs (all eight wires).

10-Gigabit Ethernet

There are standards for 10-Gigabit Ethernet (10,000 Mbps) that have been developed that use fiber-optic cabling:

- **10GBaseSR** Runs at 10 Gbps and uses "short-range" multimode fiber-optic cable, which has a maximum distance of 100 meters.
- **10GBaseLR** Runs at 10 Gbps and uses "long-range" single-mode fiber-optic cable, which has a maximum distance of 10 kilometers.
- **10GBaseER** Runs at 10 Gbps and uses "extra-long-range" single-mode fiber-optic cable, which has a maximum distance of 40 kilometers.
- **10GBaseT** Runs at 10 Gbps using CAT 6 UTP cabling, which has a maximum distance of 100 meters.

There are special WAN versions of 10-Gigabit Ethernet that use fiber-optic cabling to connect to a SONET network (more on SONET in Chapter 9).

- **10GBaseSW** The 10-Gigabit Ethernet standard for short-range, multimode fiber-optic cable, which has a maximum distance of 100 meters
- **10GBaseLW** The 10-Gigabit Ethernet standard for long-range, single-mode fiber-optic cable, which has a maximum distance of 10 kilometers
- **10GBaseEW** The 10-Gigabit Ethernet standard for extended-range, single-mode fiber-optic cable, which has a distance of up to 40 kilometers

exam Watch

Be familiar with the 100 Mbps and 1 Gbps/10 Gbps architectures for the exam. Be familiar with the speeds, cable types, connectors, and maximum distance of each architecture.

Token Ring

A big competitor to Ethernet in the past was Token Ring, which runs at 4 Mbps or 16 Mbps. Token Ring is a network architecture that uses a star ring topology (a hybrid, looking physically like a star but logically wired as a ring) and can use many forms of cables. IBM Token Ring has its own proprietary cable types, while more modern implementations of Token Ring can use CAT 3 or CAT 5 UTP cabling. Token Ring uses the token-passing access method.

exam Watch

Token Ring is defined as the IEEE 802.5 standard.

Looking at Token Ring networks today, you may wonder where the "ring" topology is, because the network appears to have a star topology. The reason this network architecture appears to use a star topology is that all hosts are connected to a central device that looks similar to a hub, but with Token Ring, this device is called a multistation access unit (MAU or MSAU). An example is shown in Figure 1-30. The ring is the internal communication path within the wiring.

Token Ring uses token passing; it is impossible to have collisions in a token-passing environment, because the MAUs do not have collisions lights as an Ethernet hub does (remember that Ethernet uses CSMA/CD and there is potential for collisions).

FIGURE 1-30

A Token Ring MAU

INSIDE THE EXAM

Unraveling the Ethernet Name Jargon

Most people get very confused by the jargon used to describe the various Ethernet types, but Ethernet is explained easily by breaking down the name of the architecture. Ethernet types follow a ##BaseXX naming convention and are designated as follows:

- ## stands for the speed of the network; examples are 10 (for 10 Mbps), 100 (for 100 Mbps), 1000 (for 1000 Mbps or 1 Gbps), and 10G (for 10 Gbps).
- Base stands for baseband transmission.
- XX stands for the cable type or medium.
  - For example, if there is a 5 at the end of the architecture name, 5 represents the cable medium thicknet. The 5 in the name indicates the maximum length of thicknet, which is 500 meters. A 2 at the end of the name would mean that the medium is thinnet, which gets its name from the fact that thinnet has a maximum length of 200 meters (actually, 185 meters).
- T stands for twisted-pair cabling and can be further used to show the number of pairs; for example, 10BaseT4 requires four pairs of wires from a twisted-pair cable.
- F is for fiber-optic cable.
- X represents a higher grade of connection, and 100BaseTX is twisted-pair cabling that can use either UTP or STP at 100 Mbps. With fiber-optic cable such as 100BaseFX, the speed is quicker than standard 10BaseF.

If we look at an example such as 100BaseTX, the 100 means 100 Mbps using baseband transmission and twisted-pair cable. Since we know that the speed is 100 Mbps, we also can assume that the type of twisted-pair cable will be at least CAT 5.

FDDI

Fiber distributed data interface (FDDI) is a network architecture that uses fiber-optic cabling, token passing, and a ring topology, but FDDI also uses two counter-rotating rings for fault tolerance on the network. For more information on FDDI, please refer to Chapter 9.

Be sure to take a look at Exercise 1-4 in the LabBook.pdf file that is found on the CD-ROM.

Once again, a table summarizing the core facts is always useful when preparing for an exam. Table 1-6 summarizes the popular network architectures. Be sure to review these before taking the Network+ exam.

TABLE 1-6 Network Architecture Summary

Network Architecture	Topology	Cable	Transfer Rate	Access Method
10Base2	Bus	Thinnet	10 Mbps	CSMA/CD
10Base5	Bus	Thicknet	10 Mbps	CSMA/CD
10BaseT	Star	CAT 3	10 Mbps	CSMA/CD
100BaseT	Star	CAT 5	100 Mbps	CSMA/CD
1000BaseTX	Star	CAT 5, 5e, 6	1 Gbps	CSMA/CD
10GBaseLR	Star	Fiber (single mode)	10 Gbps	CSMA/CD
Token Ring	Star ring	UTP	4 Mbps/16 Mbps	Token passing

CERTIFICATION OBJECTIVE 1.06

Network Operating Systems

Now that you have a general idea of the network topologies, cable types, and network architectures, let's look at the network operating system (NOS). We focus on the three most widely used network operating systems available today:

- Windows 2000 Server and Windows Server 2003/2008
- Novell NetWare
- UNIX

INSIDE THE EXAM

The Role of Network Topology, Cabling, and Connectors

A thorough understanding of how network topology, cabling, and connectors coexist is a very valuable skill set to possess for the Network+ exam. This is especially the case if you are a network engineer who must design and implement a network from the ground up. You must know the characteristics of each network topology and be able to apply them in each unique situation you encounter.

For example, let's say that you are designing a network for a small investment firm with ten users and a minimal budget. Instantly, you may be thinking "star topology," which is relatively inexpensive and easy to implement for smaller networks such as this one.

Your choice of network topology also dictates other characteristics of the network, such as what your choice of cabling will be and whether additional hardware is required. In our example, we have implemented a star topology, which is conducive to twisted-pair cabling—more importantly of at least CAT 5 UTP. The UTP cables will be connected to a network hub or switch using an RJ-45 connector, which leads us to our final specification: the network connector. Just as the network topology dictates the choice of cabling, it also dictates our choice of connector. The RJ-45 connector is the cornerstone of twisted-pair cabling.

Although this example seems fairly straightforward, the secret lies in understanding the characteristics of each type of network, such as cable types, connectors, and supporting devices. This will come in handy during your Network+ exam, which will definitely test your knowledge of these concepts.

Once you have connected the cables to the hubs and the clients to the cables, it is time to install a network operating system. The network operating system is responsible for providing services to clients on the network. These services could be the sharing of files or printers; the server could be providing name resolution through DNS services or logon services by being a directory server.

Let's take a look at some of the popular network operating systems that provide network services to their clients. For this discussion, any time that we mention Windows 2000 or Windows Server 2003, we can also include Windows NT Server, because Windows 2000 and Windows Server 2003 were built off Windows NT technologies and are the successors to Windows NT.

Windows Servers

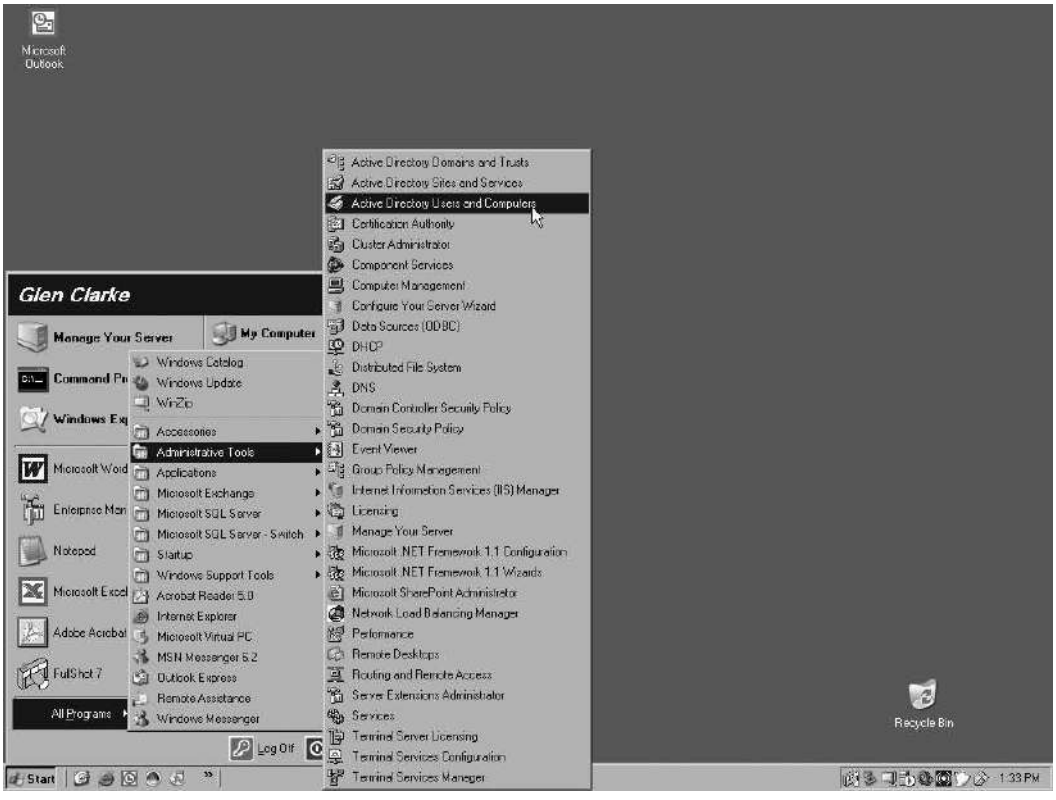
Developed from the VMS platform many years ago, Microsoft Windows NT and its successors, Windows Server 2003 and 2008, have grown into very popular network operating systems that provide a number of built-in network services, including

- **File and print services** These allow the administrator to share files and printers among Windows clients.
- **DNS and WINS services** These allow the administrator to configure DNS and NetBIOS name resolution.
- **DHCP services** These allow the administrator to configure the server to assign IP addresses to clients on the network.
- **Directory services** These allow the administrator to build a central list of objects, such as user accounts that may be used by clients to log on to the network. Microsoft's directory service is known as Active Directory.
- **Web services** These allow the administrator to build Internet or corporate intranet sites that are hosted on the server.
- **E-mail services** These allow the administrator to configure the server to send e-mail using the Simple Mail Transfer Protocol (SMTP). This feature was designed to allow application developers to build e-mail functionality into their applications.
- **Group policies** These allow an administrator to deploy settings down to the client operating systems from a central point. Some of the types of settings that can be applied to clients through group policies are folder redirection, file permissions, user rights, and installation of software.

We will look at those network services in a later chapter; the point now is that the network operating systems usually come with these features and all you need to do is install or configure them on the server.

One of the major factors that led to the popularity of the Windows-based server operating systems is that Microsoft developed a user interface on the server that was similar to the client operating systems, such as Windows 98, Windows 2000 Professional, and Windows XP Professional. This dramatically reduces the learning curve that someone new to network operating systems has to go through. Figure 1-31 displays the user interface of a Windows server.

FIGURE 1-31 The Windows server user interface



The fact that the user interface on the server operating system is the same as that on the client operating system means that the learning curve for the server operating system is dramatically reduced. The other thing that led to the rapid growth of the installed base for Windows-based servers is the fact that Windows servers made it very easy to configure the services that were mentioned previously. For example, to install a DNS server, WINS server, or DHCP server, you simply go to Add/Remove Programs and install those services as you would install solitaire on a desktop operating system.

Be sure to take a look at Exercise 1-5 in the LabBook.pdf file that is found on the CD-ROM.

Clients and Resources

A major component of successful networking with NOS is the client operating system. The client operating system needs to have client software installed known as the redirector. The term *redirector* comes from the fact that when the client makes the request for a network resource, the redirector redirects the request from the local system to the network server. Whether the workstations are in a workgroup environment (peer-to-peer) or a client/server environment, you need to have client software installed on the client operating systems to connect to the servers. Some examples of client operating systems that can connect to a Windows server are Windows XP Professional, Windows 2000 Professional, Windows NT Workstation 4.0, Windows 95/98, and Windows for Workgroups.

Another reason Windows servers have been so successful is that they support many different client operating systems. Not only can Windows clients such as Windows 98 and Windows XP connect to the Windows servers, but also non-Microsoft clients such as Macintosh clients, NetWare clients, and UNIX clients can connect to Microsoft servers. Microsoft has been very focused on coexisting with other environments.

Directory Services

With Windows servers, the server that holds the central list of user accounts that may log on to the network is called a domain controller. Windows 2000 Server and Windows 2003 Server call the database of user accounts that resides on the domain controllers the Active Directory Database. Active Directory is Microsoft's implementation of a directory service. Typically when users log on to the network, they will sit at a client machine and type a username and password. In the Microsoft world, this username and password combination is sent to the domain controller so that the domain controller can verify that the logon information is correct. If the logon information is correct, the user is allowed to use network resources. A directory service also enables users to locate objects on the network such as printers because the directory stores more than user accounts—it stores additional network objects such as printers and folders so that users can search the directory for these objects.

Novell NetWare

It started as a college project for one individual many years ago; today Novell NetWare is still used in many large organizations. NetWare has evolved into a very powerful network operating system, supporting a number of network services

out of the box and an industry-leading directory service. Some of the core services supported by a NetWare server include

- **File and print services** These allow the administrator to share files and printers among NetWare clients.
- **DNS services** These allow the administrator to configure a DNS server for DNS name resolution.
- **DHCP services** These allow the administrator to configure the server to assign IP addresses to clients on the network.
- **Directory services** These allow the administrator to build a central list of objects (such as user accounts) that may be used by clients to log on to the network. Novell's directory service is known as NDS in NetWare 4 and 5, or eDirectory in NetWare 6.
- **Web servers** These allow the administrator to build Internet or corporate intranet sites that are hosted on the server by using Apache web servers provided with the NetWare operating system.

The major difference between Windows servers and NetWare is at the server. Until NetWare 5, the server in NetWare was truly a text-based console with many of the administrative tasks done at a client workstation. As a NetWare administrator, you could manage certain administrative items from the server console, but most of the day-to-day administration such as user account management and file system administration was done from a workstation. This meant that you had to have a workstation with the management tools installed, while with a Windows server you have the management tools already installed on the server and can use them at any time. Figure 1-32 shows a screenshot of a NetWare 6 server console.

FIGURE 1-32

A NetWare 6 server console

```
File server name: DA1
Server Up Time:  54 Minutes 38 Seconds

Novell Ethernet NE1500/2100 and PCnet (ISA, ISA+, PCI, Fast)
     Version 1.39    January 23, 1998
     Hardware setting: Slot 2, I/O ports 1080h to 109Fh, Interrupt Bh
     Node address: 000C295D3FDB
     Frame type: ETHERNET_II
     PACKET EVENT2E_OFF
     Board name: CNEAMD_1_EII
     LAN protocol: ARP
     LAN protocol: IP Addr:192.168.1.10 Mask:255.255.255.0


Tree Name: .DIGITALAIR-TREE.
Bindery Context(s):
     .IS.SLC.DA

DA1:_
```

Clients and Resources

NetWare supports a wide variety of clients. The main ones, of course, are the Windows platform of operating systems, such as Windows 98, Windows 2000 Pro, and Windows XP Pro. It should be noted that NetWare now fully supports Linux client workstations; as a matter of fact, all previously mentioned Novell services can run on Linux server operating systems. Novell client software is required to connect to NetWare 4 and NetWare 5 servers but is no longer required for NetWare 6.*x*, because files, printers, e-mail, and administrative tools are all available using a web browser. The Network+ exam will assume that the Novell client always is required to connect to NetWare servers. The Novell Client software can be downloaded from the Novell web site at download.novell.com.

on the job

Although Microsoft operating systems come with a "Client for NetWare Networks," it is recommended to install Novell's client to connect to NetWare 4 and 5 networks to ensure that you are getting the full benefit of the networking environment.

Directory Services

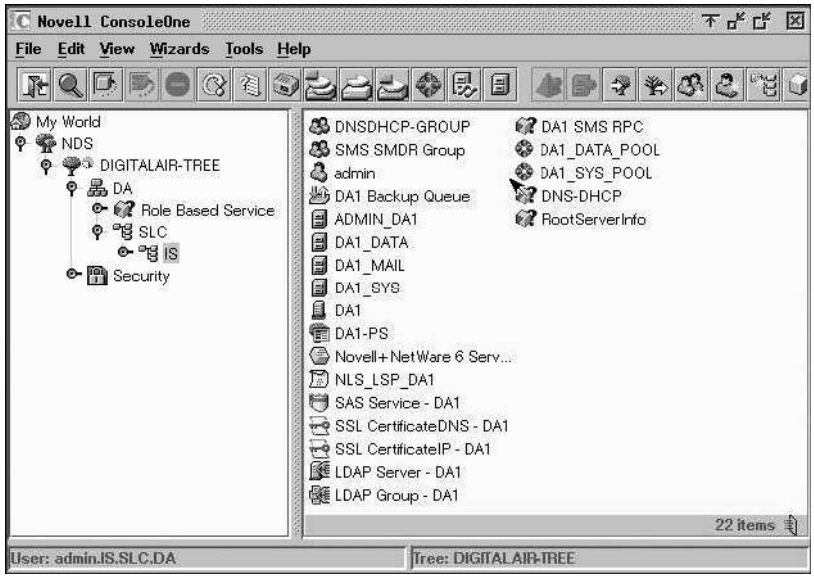
One of the driving features of NetWare since version 4 has been Novell's directory services, known as eDirectory (formerly NDS). eDirectory supports a hierarchical grouping of objects that represent resources on the network, as shown in Figure 1-33. The objects in the directory tree can be users, printers, volumes, and servers, along with others.

The directory services built into NetWare make administration easier because everything is organized and centralized within one utility. Some of the features provided by eDirectory include

- **Platform independence** eDirectory can run on NetWare servers, Windows servers, Linux servers, and UNIX servers.
- **DirXML** eDirectory uses DirXML software drivers to synchronize directory information with other directories, such as Microsoft Active Directory or Oracle's PeopleSoft.
- **Partitioning and replication** eDirectory can be split (partitioned) into smaller portions, and these smaller portions (replicas) can be placed on strategically selected servers.

FIGURE 1-33

Objects organized in Novell eDirectory using the ConsoleOne tool



UNIX/Linux

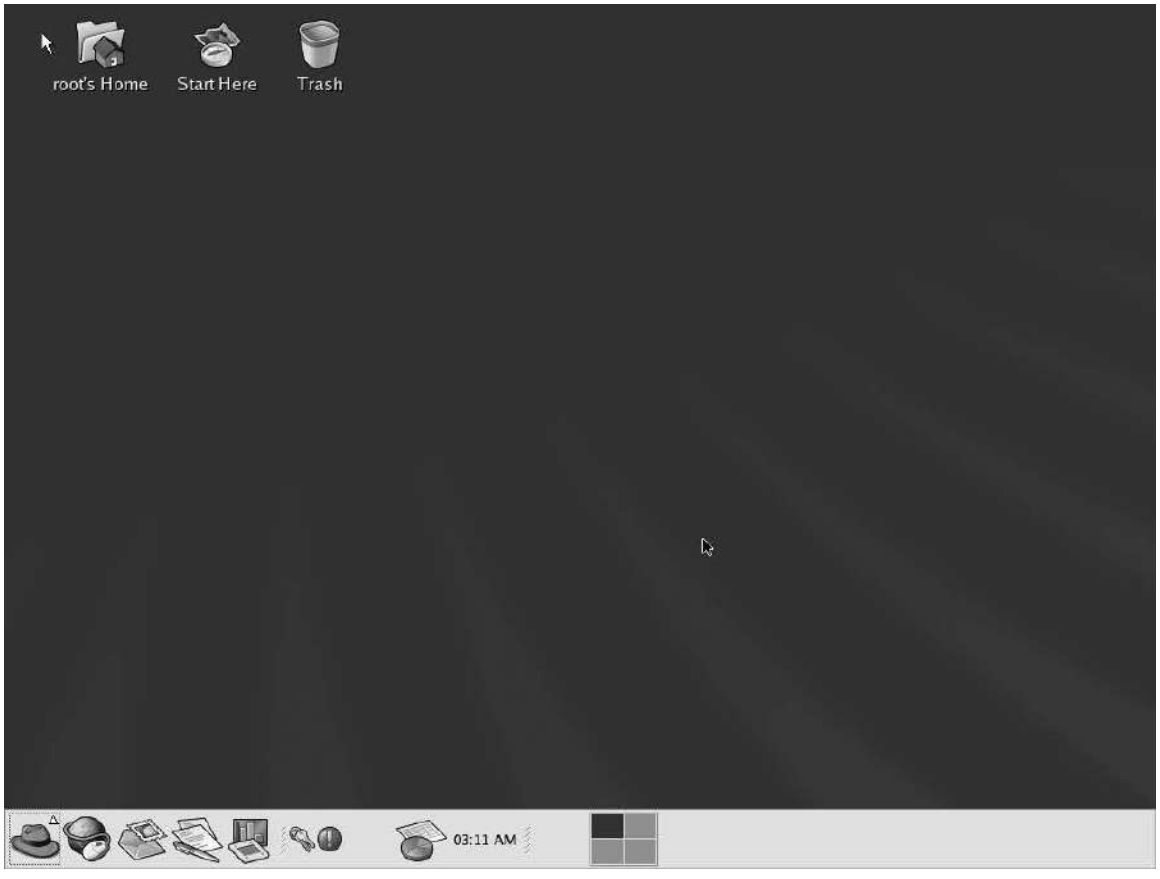
Originally developed by Bell Labs, UNIX is a very popular operating system for powerful networking and database management. UNIX boasts three key features that make it powerful: multitasking, multiusers, and networking capabilities.

UNIX is a very powerful multitasking operating system that can run many processes in the background while enabling users to work in the foreground on an application. The last feature, networking capability, has been standard for some time. UNIX has been the leader in several powerful and diverse utilities that have been ported over to other operating systems. UNIX has a very popular cousin, known as Linux, which is starting to pick up some market share as both servers and clients. Figure 1-34 displays the Linux operating system.

Clients and Resources

Today's versions of UNIX and especially Linux are different than the older versions of UNIX. Today, like Windows, most Linux versions have a graphical shell loaded automatically that allows a user to use the operating system with a mouse. Today's

FIGURE 1-34 The Linux user interface



versions of Linux have programs automatically installed that allow you to configure the operating system and change its settings. Like Windows, most Linux operating systems have popular programs installed for you to use—programs such as a text editor and a calculator. The point is that although most people have traditionally associated Linux or UNIX with the command line only, you can do a lot from the graphical shell as well.

Directory Services

The UNIX and Linux standard directory service is called Network Information Service (NIS), which as been superseded by NIS+ and LDAP. As a matter of fact, Microsoft Services for UNIX and NetWare Services for UNIX both include an NIS service, which allows UNIX and Linux clients to authenticate to Active Directory or eDirectory. These services also allow for the objects from Active Directory and eDirectory to be copied or synchronized with the NIS directory, allowing UNIX clients to authenticate with NIS when the account was built originally in the other directory. Similar to Active Directory and eDirectory, NIS is a central repository of network resources (for example, users, group, printers) that is synchronized to other UNIX and Linux servers on the network.

exam Watch

NIS is the directory service used by UNIX and Linux to store a central list of network objects, such as users, groups, and printers.

CERTIFICATION SUMMARY

This chapter plays a significant role in this book. It serves as an introduction to some very key elements of networking, such as network topologies, cabling, and network architectures. Understanding the basic network structure takes a little knowledge of computing and information sharing. First, remember that for a network to exist, we need to have two things: the entities that want to share information or resources and the medium that enables the entities to communicate (a cable, such as coaxial or unshielded twisted-pair, or a wireless network). In this chapter, you looked at the various topologies that exist in networks: bus, star, ring, mesh, and wireless. You also looked at network terms, such as segments and backbones.

You also looked at the various networking media and connectors. Knowing the various grades of cable can be important for the exam, as well as knowing what connectors go with what type of cabling. Make sure to review this before taking your exam.

You also learned about some of the network operating systems for client/server networks: Windows 2000 Server, Windows Server 2003, Novell NetWare, and UNIX.

TWO-MINUTE DRILL

Identifying Characteristics of a Network

- A network is made up of two basic components: the entities that need to share information or resources and the medium that enables the entities to communicate.
- A peer-to-peer network is a network that has a number of workstations that connect to one another for the purpose of sharing resources. There is no dedicated server on a peer-to-peer network.
- A server-based network is a network that has a central server installed with each client requesting resources from the server.

Identifying Network Topologies

- Topology is the physical layout of computers, cables, and other components on a network.
- Many networks are a combination of these topologies:
  - Bus
  - Star
  - Mesh
  - Ring
  - Wireless
- A bus topology uses a main trunk to connect multiple computers. If there is a break in a cable, it will bring the entire network down.
- In a star topology, all computers are connected through one central hub or switch. If there is a break in a cable, only the host that is connected to that cable is affected.
- With a mesh topology, every workstation has a connection to every other component of the network. This type of topology is seen more commonly in something like the national telephone network.

- ❑ In a ring topology, all computers are connected in a ring with no beginning or end. Each system in the ring regenerates the signal. If there is a break in the ring, the entire network goes down.
- ❑ In a wireless topology, radio frequencies are used instead of physical cables. Wireless clients connect to cells, or access points, through the use of a wireless network card.
- ❑ A backbone is the main cable segment in the network.

Network Media and Connectors

- ❑ Cabling is the LAN's transmission medium.
- ❑ Three primary types of physical media can be used: coaxial cable, twisted-pair cable, and fiber-optic cable.
- ❑ Coax uses a copper core that carries an electrical signal. There are two types of coax: thinnet and thicknet. Hosts connect to thinnet through BNC connectors, whereas vampire taps and drop cables are used to connect to thicknet.
- ❑ Twisted-pair cabling is a cable type similar to telephone cable, but there are eight wires instead of four. Telephone cables use an RJ-11 connector, whereas network cabling uses an RJ-45 connector.
- ❑ Fiber-optic cabling has a glass or clear-plastic core that carries pulses of light. The straight tip (ST) and subscriber connector (SC) are connectors used with fiber-optic cabling.

Access Methods

- ❑ An access method determines how systems access the network or place data on the wire.
- ❑ CSMA/CD is the access method used by Ethernet networks and involves a host sensing traffic on the wire. When the wire is free of traffic, the host can send its data.
- ❑ Token passing is the access method used by Token Ring. When a system on a Token Ring network wants to send data it must wait to receive the token.

Network Architectures

- A network architecture is made up of a certain cable type, access method, and topology.
- Two popular Ethernet architectures are 10BaseT and 100BaseT. 10BaseT uses twisted-pair cabling at 10 Mbps (CAT 3) and uses CSMA/CD as the access method. 100BaseT runs at 100 Mbps using CAT 5 UTP cabling. Both architectures use a star topology.
- Token Ring is a network architecture that uses token passing as the access method and is configured in a star topology.

Network Operating Systems

- The three most widely used network operating systems available are
  - Microsoft Windows Server 2003/2008
  - Novell NetWare
  - UNIX

SELF TEST

The following questions will help you measure your understanding of the material presented in this chapter. Read all the choices carefully because there may be more than one correct answer, but you will need to select the most correct answer.

Identifying Characteristics of a Network

1. Which of the following is an example of a network?
   A. A computer attached to a printer and a scanner to input and output information
   B. Computer systems sharing a common communication medium for the purpose of sharing information or devices
   C. Several printers connected to a switch box going to a single terminal
   D. Several diskettes holding information for one workstation
2. In which type of network is there no dedicated server, with each node on the network being an equal resource for sharing and receiving information?
   A. Client/server
   B. Peer-to-peer
   C. Windows Server 2003
   D. Novell NetWare 6.*x*
3. What is the Microsoft term for a peer-to-peer network?
   A. Client/server
   B. Domain
   C. Workgroup
   D. Active Directory
4. A company has offices in Halifax and Toronto. Both networks are connected to allow the two locations to communicate. This is considered what type of network?
   A. LAN
   B. JAN
   C. MAN
   D. WAN

5. Which type of server is responsible for storing files for users on the network?
   A. File and print server
   B. Web server
   C. Directory server
   D. Application server
6. You wish to extend your intranet to certain business partners. What type of network are you building?
   A. Intranet
   B. Internet
   C. Extranet
   D. LAN

Identifying Network Topologies

7. The physical layout of computers, cables, and other components on a network is known as which of the following?
   A. Segment
   B. Backbone
   C. Topology
   D. Protocol
8. Which topology has a centralized location in which all of the cables come together to a central point such that a failure at this point brings down the entire network?
   A. Bus
   B. Star
   C. Mesh
   D. Ring
   E. Wireless
9. Which topology has a layout in which every workstation or peripheral has a direct connection to every other workstation or peripheral on the network?
   A. Bus
   B. Star
   C. Mesh
   D. Ring
   E. Wireless

10. Which network topology requires the use of terminators?
- A. Bus
- B. Star
- C. Mesh
- D. Ring
- E. Wireless

Networking Media and Connectors

11. Which of the following is not a common type of medium used in networking?
- A. Coaxial cable
- B. Twisted-pair cable
- C. Fiber-optic cable
- D. RJ-45

12. What is the distance limitation of 10Base2, or thinnet?
- A. 100 meters
- B. 185 meters
- C. 250 meters
- D. 500 meters

13. Which cable type sends the signal as pulses of light through a glass core?
- A. Thinnet
- B. Thicknet
- C. Fiber optic
- D. CAT 5e

14. What is the maximum distance of CAT 3 UTP cabling?
- A. 100 meters
- B. 185 meters
- C. 250 meters
- D. 500 meters

15. What is the maximum distance of cabling used on a 10Base5 network?
- A. 100 meters
- B. 185 meters
- C. 250 meters
- D. 500 meters

16. You wish to install a 100BaseT network. What type of cabling will you use?
- A. CAT 3 UTP
- B. CAT 5 UTP
- C. Thinnet
- D. Fiber optic

17. Fiber-optic cabling uses which types of connectors? (Select two.)
- A. SC
- B. RJ-45
- C. BNC
- D. ST

18. What is the maximum distance of single-mode fiber (SMF)?
- A. 300 meters
- B. 500 meters
- C. 2 km
- D. 850 meters

19. Which cable type is immune to outside interference and crosstalk?
- A. Thinnet
- B. Thicknet
- C. Twisted-pair
- D. Fiber optic

20. Which type of connector is used on 10Base2 networks?
- A. SC
- B. BNC
- C. RJ-45
- D. RJ-11

21. You want to create a crossover cable to connect two systems directly together. Which wires would you have to switch at one end of the cable?
- A. Wires 1 and 2 with wires 3 and 6
- B. Wires 2 and 3 with wires 6 and 8
- C. Wires 1 and 2 with wires 3 and 4
- D. Wires 2 and 3 with wires 3 and 6

Access Methods

22. Which access method does 100BaseT use?
- A. Baseband
- B. CSMA/CD
- C. CSMA/CA
- D. Token passing

23. Which access method does Token Ring use?
- A. Baseband
- B. CSMA/CD
- C. CSMA/CA
- D. Token passing

Network Architectures

24. Which network architecture is defined as the IEEE 802.3 standard?
- A. Token Ring
- B. FDDI
- C. Fiber
- D. Ethernet

25. Which network architecture uses single-mode fiber-optic cabling?
- A. 1000BaseLX
- B. 1000BaseSX
- C. 1000BaseCX
- D. 1000BaseTX

26. How many populated network segments can exist with 10Base2?
- A. 1
- B. 2
- C. 3
- D. 5

27. Which type of cabling is used in a 10BaseFL network?
- A. STP
- B. CAT 3 UTP
- C. Thinnet
- D. Thicknet
- E. Fiber optic

28. Which Gigabit architecture uses multimode fiber cabling?

A. 1000BaseLX
B. 1000BaseSX
C. 1000BaseCX
D. 1000BaseTX

Network Operating Systems

29. Which network operating system was developed from the VMS platform?

A. NetWare
B. UNIX
C. Windows 95
D. Windows NT

30. Which operating system was originally developed by Bell Labs and has multitasking, multiuser, and built-in networking capabilities?

A. UNIX
B. Windows NT
C. Windows 95
D. NetWare

31. Which of the following are network operating systems and not simply desktop operating systems? (Choose all that apply.)

A. Novell NetWare
B. Microsoft Windows 98
C. Microsoft Windows XP
D. Microsoft Windows Server 2003

32. Novell's directory service is called _____?

A. Active Directory
B. NDS / eDirectory
C. DNS
D. StreetTalk

33. Microsoft's directory service is called _____?

A. Active Directory
B. NDS
C. DNS
D. StreetTalk

SELF TEST ANSWERS

Identifying Characteristics of a Network

1. ☑ **B.** Computer systems sharing a common communication medium for the purpose of sharing information or devices is what a network is all about. The entities are usually workstations, and the medium is either a cable segment or a wireless medium such as an infrared signal.
   ☒ **A, C,** and **D** are incorrect because a network, by definition, is two or more computers connected to share information. These three choices do not allow two or more PCs to share information; they are only setups of several connected devices or a PC connected to a peripheral device.

2. ☑ **B.** A peer-to-peer network has no dedicated servers. There are no hierarchical differences between the workstations in the network; each workstation can decide which resources are shared on the network. In a peer-to-peer network, all workstations are clients and servers at the same time.
   ☒ **A** is incorrect because this network type has a dedicated server. **C** and **D** are incorrect because a Windows Server 2003 and Novell NetWare 6.*x* constitute the server portion of the client/server network.

3. ☑ **C.** The Microsoft term for a peer-to-peer network is a workgroup environment. If you have not installed your Windows clients in a domain (client/server), then they are sitting in a workgroup environment.
   ☒ **A** is incorrect because a client/server network is the opposite of a peer-to-peer network; a client/server network uses a central server. **B** is incorrect because domain is the term for a Microsoft server-based environment. **D** is incorrect because Active Directory is the term for Microsoft's implementation of a directory server.

4. ☑ **D.** Two remote offices that are spread over geographic distances constitute a wide area network (WAN).
   ☒ **A** is incorrect because it is the opposite of a WAN; a LAN is a network in a single geographic location. **B** is incorrect because there is no such thing in networking as a JAN. **C** is a metropolitan area network.

5. ☑ **A** is correct. A file and print server is responsible for providing files and printers to users on the network.
   ☒ **B, C,** and **D** are incorrect because they are each their own type of server. A web server will host web sites; a directory server is a server that contains a central list of objects, such as user accounts on the network; and an application server runs a form of networking application, such as an e-mail or a database server program.

6. ☑ **C.** An extranet allows selected individuals to see your corporate intranet.
☒ **A, B,** and **D** are incorrect. An intranet allows only individuals within your company to access the site; allowing anyone on the Internet to access it would make it an Internet-type application.

Identifying Network Topologies

7. ☑ **C.** The topology is the physical layout of computers, cables, and other components on a network. Many networks are a combination of the various topologies.
☒ **A** is incorrect because a segment is a part of a LAN that is separated by routers or bridges from the rest of the LAN. **B** is incorrect because a backbone is the main part of cabling that joins all of the segments together and handles the bulk of the network traffic. **D** is incorrect because a protocol is a set of rules governing the communication between PCs; a protocol can be thought of as similar to a language.

8. ☑ **B.** In a star topology, all computers are connected through one central hub or switch. A star topology actually comes from the days of the mainframe system. The mainframe system had a centralized point at which the terminals connected.
☒ **A** is incorrect because a bus topology uses one cable to connect multiple computers. **C** is incorrect because the mesh network has every PC connected to every other PC and can resemble a spider's web. **D** is incorrect because a ring topology resembles a circle or ring. **E** is incorrect because there is no physical cabling to represent the topology; it is represented by a bubble or cell.

9. ☑ **C.** A mesh topology is not very common in computer networking, but you have to know it for the exam. The mesh topology is seen more commonly with something like the national telephone network. With a mesh topology, every workstation has a connection to every other component of the network.
☒ **A** is incorrect because a bus topology uses one cable to connect multiple computers. **B** is incorrect because a star topology is made up of a central point or hub with cables coming from the hub and extending to the PCs. **D** is incorrect because this topology resembles a circle or ring. **E** is incorrect because there is no physical cabling to represent the topology; it is represented by a bubble or cell.

10. ☑ **A.** A bus topology uses terminators on any loose end of the bus. The terminator is designed to absorb the signal so that it does not bounce back on the wire and collide with other data.
☒ **B** is incorrect because a star topology does not use terminators; it uses a central hub or switch that connects systems to the network. **C** is incorrect because a mesh topology has each system connecting to each other system. **D** is incorrect because a ring topology has no beginning and no end, so there are no "loose ends" to put a terminator on. **E** is incorrect because a wireless network does not use cables at all.

Networking Media and Connectors

11. ☑ **D.** RJ-45 is not a network medium. Three primary types of physical media can be used: coaxial cable, twisted-pair cable, and fiber-optic cable. Transmission rates that can be supported on each of these physical media are measured in millions of bits per second (Mbps). RJ-45 is a connector type for twisted-pair cabling.
☒ **A, B,** and **C** are incorrect because they are all common network media.

12. ☑ **B.** 10Base2 (thinnet) has a distance limitation of 185 meters. 10Base5 (thicknet) has a distance limitation of 500 meters, and 10BaseT (twisted-pair) has a distance limitation of 100 meters.
☒ **A, C,** and **D** are incorrect because these are not the distances covered by thinnet.

13. ☑ **C.** Fiber-optic cabling sends pulses of light through a glass core.
☒ **A, B,** and **D** are incorrect because each carry an electrical signal.

14. ☑ **A.** All twisted-pair cabling is limited to 100 meters.
☒ **B** is incorrect because 185 meters is the maximum distance of thinnet cabling; **D** is incorrect because 500 meters is the maximum distance of thicknet cabling. **C** is incorrect; there is no cable type that has a 250-meter maximum distance.

15. ☑ **D.** 500 meters is the maximum distance of thicknet cabling.
☒ **A** is incorrect because all twisted-pair cabling is limited to 100 meters. **B** is incorrect because 185 meters is the maximum distance of thinnet cabling. **C** is incorrect because there is no cable type that has a 250-meter maximum distance.

16. ☑ **B.** 100BaseT uses twisted-pair that runs at 100 Mbps. CAT 5 is twisted-pair cabling type that runs at 100 Mbps.
☒ **A** is incorrect because CAT 3 runs at 10 Mbps. **C** is incorrect because thinnet runs at 10 Mbps and is known as 10Base2. **D** is incorrect. Although fiber optic can run at 100 Mbps, it is not used in 100BaseT.

17. ☑ **A** and **D.** Fiber-optic cabling uses a number of connector styles—two of which are the SC and ST connectors.
☒ **B** and **C** are incorrect. RJ-45 is used by twisted-pair cabling, and BNC is used by thinnet.

18. ☑ **C.** Single-mode fiber-optic cabling has a maximum distance of approximately 2 km.
☒ **A, B,** and **D** are incorrect distances for single-mode fiber, although 300 meters is the maximum distance of multimode fiber.

19. ☑ **D.** Fiber-optic cabling is immune to outside interference and crosstalk.
☒ **A, B,** and **C** are incorrect. Thinnet, thicknet, and twisted-pair cabling are susceptible to outside interference.

20. ☑ **B.** The BNC connector is the connector used by 10Base2.
☒ **A, C,** and **D** are incorrect. The SC connector is used by fiber optic, the RJ-45 connector is used by twisted-pair, and the RJ-11 connector is used by the telephone cable.

21. ☑ **A.** To create a crossover cable, you would switch wire 1 and 2 with wire 3 and 6 on one end of the cable.
☒ **B, C,** and **D** are incorrect. These combinations are not used to create crossover cables.

Access Methods

22. ☑ **B.** Carrier-sense multiple access with collision detection (CSMA/CD) is the access method that 100BaseT uses. With CSMA/CD, a host will sense the wire to see if it is free; only if the wire is free of data will the host send data on the wire.
☒ **A, C,** and **D** are incorrect. Baseband is not an access method. CSMA/CA and token passing are access methods but are not used by 100BaseT.

23. ☑ **D.** Token Ring uses the token-passing access method. With token passing, a host must have the token before submitting data on the wire.
☒ **A, B,** and **C** are incorrect. Baseband is not an access method, CSMA/CA is used in AppleTalk networks, and CSMA/CD is used in Ethernet environments.

Network Architectures

24. ☑ **D.** Ethernet (CSMA/CD) is defined by IEEE 802.3
☒ **A, B,** and **C** are incorrect. These architectures are not defined by 802.3, but be aware that Token Ring is defined by IEEE 802.5.

25. ☑ **A.** 1000BaseLX uses single-mode fiber-optic cabling.
☒ **B, C,** and **D** are incorrect. 1000BaseSX uses multimode fiber-optic cabling, 1000BaseCX uses coaxial cabling, and 1000BaseTX uses CAT 5e or above.

26. ☑ **C.** Following the 5-4-3 rule, you are allowed to have five network segments, joined by four repeaters, while three of those segments are populated with nodes.
☒ **A, B,** and **D** are all incorrect because they are not the number of populated segments in a 10Base2 network.

27. ☑ **E.** 10BaseFL uses fiber-optic cabling. Remember to watch the characters at the end of the architecture name to determine what the cable type is—"FL" is for fiber link.
☒ **A, B, C,** and **D** are incorrect. STP, thinnet, thicknet, and CAT 3 UTP are all cable types but are not used in 10BaseFL.

28. ☑ **B.** 1000BaseSX uses multimode fiber cabling. Remember that multimode cannot go as far as single mode, and also the "SX" in the architecture is for "short range"—multimode for short range, single mode for long range.
☒ **A, C,** and **D** are all incorrect. 1000BaseLX uses single-mode fiber, 1000BaseCX uses coaxial cable, and 1000BaseTX uses twisted-pair.

Network Operating Systems

29. ☑ **D.** Developed from the VMS platform many years ago, Microsoft Windows NT has grown into a very popular network operating system with a new and different interface.
☒ **A, B,** and **C** are incorrect. The graphical interface and look and feel of the other operating systems in the Windows family made Windows NT very popular among users and network administrators. Windows 95 was simply a great enhancement of Windows for Workgroups. NetWare and UNIX were not based on VMS.

30. ☑ **A.** Originally developed at Bell Labs, UNIX is a very popular operating system for powerful networking and database management. UNIX boasts three key features that make it powerful: multitasking, multiuser, and networking capabilities.
☒ **B, C,** and **D** are incorrect. Windows 95 and NT were developed by Microsoft; NetWare was developed by Novell.

31. ☑ **A** and **D.** Novell NetWare and Microsoft Windows Server 2003 are NOSs. The major difference between Windows servers and NetWare is at the server.
☒ **B** and **C** are incorrect. Windows 98 and Windows XP are client operating systems and not true servers.

32. ☑ **B.** Novell's directory service is known as NDS or eDirectory.
☒ **A, C,** and **D** are incorrect. Active Directory is the name of Microsoft's directory service, DNS is the name of a service that performs FQDN–to–IP address name resolution, and StreetTalk is Banyan's directory service.

33. ☑ **A.** Active Directory is the name of Microsoft's directory service.
☒ **B, C,** and **D** are incorrect. Novell's directory service is known as NDS, DNS is the name of a service that performs FQDN–to–IP address name resolution, and StreetTalk is Banyan's directory service.