CHAPTER 1

# Network Fundamentals



**Exam objectives in this chapter**

- What Is a Network?
- Logical Network Topologies
- Physical Network Topologies
- Network Types

## WHAT IS A NETWORK?

The basic concept of networking is the difference between standing alone and being part of a group. Computers can also be standalone or part of a network. Networks are the systems that interconnect computers and other devices and provide a method of communication and the capability to share data.

### Fast Facts

A computer network exists when two or more machines are connected together, thereby allowing them to share data, equipment, and other resources. By using a combination of software and hardware, the computers gain added functionality, including the capability to

- transfer data between machines
- save and access files on the same hard disks or other storage devices
- share printers, scanners, modems, and other peripheral devices
- allow messages to be exchanged via e-mail, instant messaging, and other technologies.

### Network Elements

Although networks may provide similar functions, they can be very different. Some of the elements that will define your network and make it different from others include the following:

- **Network interface cards** (NIC) or **network adapters** allow computers to transmit and receive data across the network; *routers*, *switches*, and *hubs* pass the data to other computers or networks.
- **Media** consist of cables or wireless technologies that carry the data across the network.
- **Protocols** are sets of rules that control how the data is sent between computers. The most popular of these is the protocol used on the Internet, Transmission Control Protocol/Internet Protocol (TCP/IP), while other protocols used on networks include Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) and AppleTalk.
- **Topology** is the shape of the network. It defines how the network is designed and describes how computers are connected together.
- **Network type** defines the size of the network and its scale within a geographical area.
- **Network model** determines the levels of security that are available to the network and the components needed to connect the computers together.
- **Access** determines who can use the network and how, and if features of the network are available for private or public use.
- **Network operating systems** (NOSes), such as Windows, NetWare, and Linux, may be used for a server, which is a computer that provides services to numerous computers, and/or installed on computers that are used by individual users of the network. In some cases, such as Novell NetWare, additional software may need to be installed on computers that use the server, who are referred to as clients.
- **Other software and services,** such as whether the network provides access to internal Web sites, e-mail, databases, and so forth, are also included in the network.

Networks may use different protocols, topologies, and other elements that make them unique. This means you can look at two networks in two different homes or businesses, and they can be completely different from one another. However, because the same basic set of protocols, topologies, media, and other elements are used to build these networks, they will all have similarities.

## LOGICAL NETWORKING TOPOLOGIES

There are different network models that can be chosen. The network model you choose will affect a network infrastructure's design and how it is administered. The model or models used can have an impact on the location of computers, how users access resources, and the number of computers and types of operating

systems required. Some models and topologies available to choose from are as follows:

- Centralized
- Decentralized (distributed)
- Peer-to-peer
- Client/server
- Virtual private network (VPN)
- Virtual local area network (VLAN)

Selecting a network model is the first important step in completing a network design. Another important decision involves determining how resources will be accessed. Centralized, decentralized, or a mixture of both are possible choices.

## Centralized

When a centralized network model is used, a network's resources are centrally located and administered.

Here are the key points about centralized network models that you should know:

- A centralized model will affect the physical location of servers and other resources on your network by situating them within a specific area.
- Servers are generally located in a secure, central location, such as a dedicated server room. This secured room can also be used to house other resources, such as routers, switches, firewalls, Web servers, and other devices.
- The centralized network model can also mean that fewer servers or other devices are needed. Rather than each building having their own server on the premises, users can save their work to a dedicated server in a central location. This would keep everyone's files on one or more servers, allowing their work to be kept secure and regularly backed up.

### DID YOU KNOW?

Additional work may be required to manage devices stored in a central location. For example, let's say you had a plotter that was kept in a server room. Anytime anyone needed the plotter installed as a printer on his or her computer, you would need to set up permissions on the plotter granting them usage rights. If the user sent a print job to this plotter, someone from the IT staff would need to enter the secure room to get the user's printout. In addition, there would also be the need to replace paper and toners used in the device. In a centralized model, administration of the resources is also centralized.

Despite the scenario described in the preceding sidebar, in some ways, managing resources can be easier with this model. By keeping these resources in one area, a network administrator can easily change backup tapes, replace hard disks, or fix other issues as required. Imagine the issues of having servers in offices throughout a city or region and having to visit each of them whenever a tape needed to be

replaced after a tape backup. By keeping resources centralized, administrative work can be reduced.

### Decentralized (Distributed)

When a decentralized network model is used, a network's resources are distributed through different areas of the network, and administration is shared by designating responsibility to system administrators or individual users.

Here are the key points about decentralized network models that you should know:

- A decentralized network model has a variety of servers, equipment, and other resources distributed across the geographical area making up the network, which aren't readily physically accessible. Cost factors or other issues may influence the requirement for a decentralized network.
- Distributing servers may improve network performance since users would no longer have to authenticate across wide area network (WAN) links or use slow connections to access remote servers.

### Peer-to-Peer

In a peer-to-peer network, computers on the network are equal, with each workstation providing access to resources and data. This is a simple type of network where computers are able to communicate with one another and share what is on or attached to their computer with other users. It is also one of the easiest types of architectures to create. Here are some of the characteristics of a peer-to-peer network:

- Individual users have responsibility over who can access data and resources on their computers.
- Operating systems such as Windows XP and Windows Vista allow accounts to be set up that will be used when other users connect to an individual user's computer.
- Accounts, passwords, and permissions are saved in a local database and are used to determine what someone can do when connecting to your computer.

#### DID YOU KNOW?

One important issue with peer-to-peer networks is security. Each computer on this type of network may allow or deny access to other computers, as access to data and resources is controlled on each machine. For example, a user could share a folder containing payroll information on his or her computer, allowing other users to access the files in that folder. Because users can control access to files and resources on their computers, network administration isn't controlled by one person. As such, peer-to-peer networks are generally used in small deployments and in situations where security isn't a major concern, as in the case of home networks or small businesses.

**EXAM WARNING**

A peer-to-peer network is decentralized, because resources and administration are handled locally on each participating machine, while a client/server network can be either centralized or decentralized. Remember the differences and relationships between different network types for the exam, as they may be covered either directly or incorporated in the scenarios used to cover other material.

## Client/Server

When you use a peer-to-peer network model, each machine can house data and also request data from other machines, so the computers act as both clients and servers, depending on the action performed. In a client/server network, model machines have a distinct role. Here are some characteristics of the client/server model:

- Roles are distinct since the client/server model involves dedicated servers that provide services and data, and dedicated clients, which do not house data content.
- The client/server model consists of high-end computers serving clients on a network, by providing specific services upon request.
- Each server may perform a single role, or a mixture of roles can be combined on a single server machine.

### Crunch Time

Examples of various client/server roles include the following:

- **File server** allows clients to save data to files and folders on its hard drive.
- **Print server** redirects print jobs from clients to specific printers.
- **Application server** allows clients to run certain programs on the server and enables multiple users to common applications across the network.
- **Database server** allows authorized clients to view, modify, and/or delete data in a common database.

- The server needs to have an NOS like Windows Server 2003, Windows Server 2008, or Linux installed.
- These server operating systems provide features specifically for servicing clients and can respond more efficiently to a greater number of client requests than operating systems intended for client roles such as Windows XP or Windows Vista.
- Once a high-end computer has server software installed, the services provided by it need to be configured and other programs may need to be installed.
- Many of the server's functions are dependent on the server software installed on it. For example, a server that acts as a database server needs to have a

program like Microsoft SQL Server or mySQL installed on it. In the same way, a Windows Server 2008 server which must act as a Web server would need Internet Information Services (IIS) configured.

- By installing server software on the dedicated server, you define the role that the server will play on your network.

## Virtual Private Network

A VPN provides users with a secure method of connectivity through a public network, such as the Internet, into the internal network of an organization. Most companies use dedicated connections to connect to remote sites. However, when users want to connect to that same corporate network from home over the Internet, it is important to consider security and require the additional security offered by encryption of the data using a VPN. It may also make sense to connect a small branch office using a VPN, which would cost less than a dedicated connection.

### *WHAT IS A VPN?*

When a VPN is implemented properly, it provides wide area security, reduces costs associated with traditional WANs, improves productivity, and improves support for users who telecommute. Cost savings are twofold. First, companies save money by using public networks such as the Internet instead of paying for dedicated circuits between remote offices. Second, telecommuters do not have to pay long-distance fees to connect into centrally-located, corporate remote access servers. They can simply dial into their local Internet service providers (ISPs) and create a virtual tunnel to the office. A tunnel is created by encapsulating a data packet inside another data packet and transmitting it over a public medium.

### Crunch Time

*Tunneling* requires three different protocols:

- **Carrier Protocol** The protocol used by the network (IP on the Internet) that the information is traveling over.
- **Encapsulating Protocol** The protocol, such as Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), IPsec, or Secure Shell (SSH), that is wrapped around the original data.
- **Passenger Protocol** The original data being carried.

Essentially, there are two different types of VPNs: site-to-site and remote access.

- **Site-to-site VPNs** are normally established between corporate offices that are separated by a physical distance extending further than normal local area network (LAN) media covers.

- VPNs are available as software implementations such as Windows VPN, available on Windows 2003 and 2008.
- VPNs are available as hardware implementations which may be deployed on firewall devices such as Cisco PIX and Check Point.
- Common protocols associated with VPN transmission security include the following:
  - PPTP – a tunneling protocol used to establish a secure tunnel connection between two sites
  - L2TP – a tunneling protocol used to establish a secure tunnel connection between two sites
  - SSH – an encryption protocol used to secure data passing through the tunnel
  - IPSec – an encryption protocol used to secure data passing through the tunnel
  - Secure Sockets Layer/Transport Layer Security (SSL/TLS) – an encryption protocol used to secure data passing through the tunnel

- **Remote access VPN,** also known as a *private virtual dial-up network* (PVDN), differs from a site-to-site VPN in that end users are responsible for establishing the VPN tunnel between their workstation and their remote office.
  - Users connect to the Internet or an ESP through a point of presence (POP) using their particular VPN client software and then authenticate with the VPN server, usually by username and password.
  - Allows employees to transmit data to their home offices from any location.
  - Good solution choice for a company with many employees working in the field.

### Virtual Local Area Network

VLANs allow network administrators to divide the network by designating certain switch ports as part of a logical network. While several computers or devices can be connected to the same physical network, they can all be separated logically through the use of a VLAN. Characteristics of VLANs are as follows:

- VLAN databases can provide important details to any individual who is trying to discern the logical breakup of the network.
- VLANs logically divide the network and affect the traffic and security of a switched network.
- VLANs are commonly used in the enterprise or corporate computing networks to segment networks.

## PHYSICAL NETWORKING MODELS

The topology of a network is the physical layout of computers, hubs, routers, cables, and other components. It provides a map of where things are and how the network is configured.

While networks are unique, the topology of each network will share characteristics with other networks.

## Crunch Time

Networks may use a single topology or a combination of any of the following topologies:

- Bus
- Star
- Ring
- Mesh
- Point-to-point
- Point-to-multipoint
- Hybrid
- Wireless

### EXAM WARNING

You must be able to identify a topology based on either the description given or by looking at a picture of a topology. Make sure you know each of the topologies covered in this section and can identify them via diagrams. Figure 1.1 displays examples of some of the topologies.

### The Bus Topology

All the computers in a bus topology are connected together using a single cable, which is called a *trunk*, *backbone*, or *segment*. Characteristics of a bus topology are as follows:

- Coaxial cable is commonly used for the trunk.
- The computers in a bus topology are attached to the cable segment using T-connectors.
- Because all these computers use the same cable, only one computer can send packets of data onto the network at a time.
- When a computer sends a packet of data onto the trunk, it is sent in both directions so that every computer on the network has the chance to receive it.
- When a computer listens to the network, any packets that aren't addressed to it are discarded, while any packets specifically sent to it are examined further.
- A broadcast is made when packets are destined for every computer on the network.
- To prevent data signals from staying on the cable indefinitely, the cable needs to be terminated at each end so electronic signals are absorbed when they reach the cable's end.
- Without termination, packets sent would bounce back-and-forth along the length of the cable causing the entire network to fail.

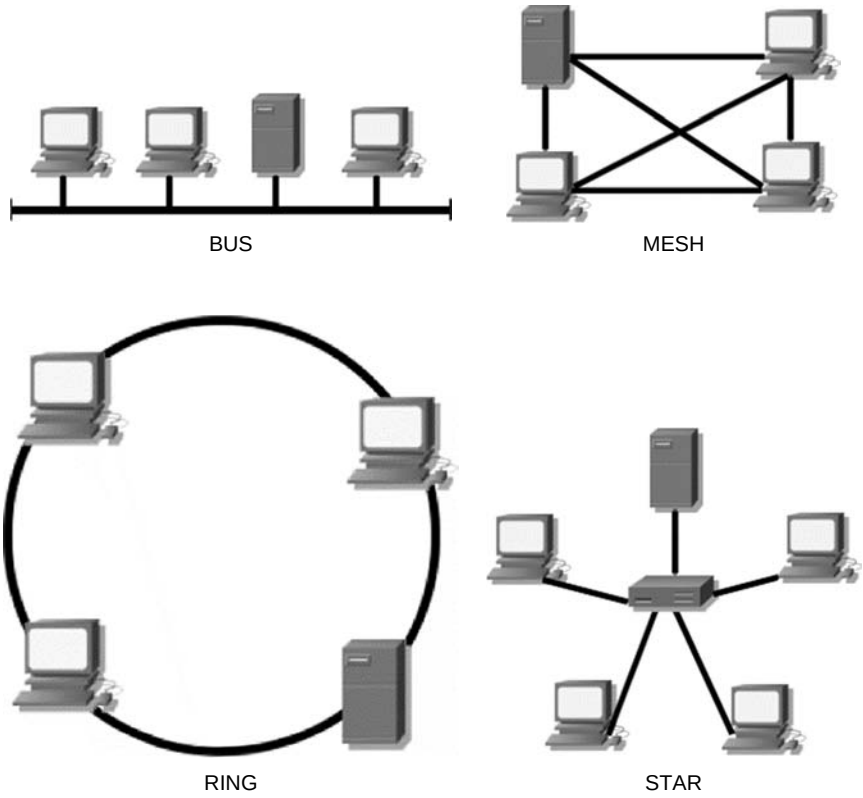


**FIGURE 1.1**
Sample network topologies

### DID YOU KNOW?

In a bus topology, every computer is connected to a single cable. If the cable breaks, then each segment has an end that isn't terminated, and the entire network goes down. If the trunk is long enough, this can make it difficult to isolate where the break is.
Another disadvantage of this topology is that it isn't very scalable. The number of computers is limited to the length of the cable, and as your company grows, it can be difficult changing the size and layout of the network. Also, while changes or repairs are made to the cable, the network is down because there is no redundancy and termination of the cable is required.

## The Star Topology (Hierarchical)

In a star topology, computers aren't connected to one another but are all connected to a central hub or switch. When a computer sends data to other computers on the network, it is sent along the cable to a central hub or switch, which then

determines which port it needs to send the data through for it to reach the proper destination. Characteristics of a star topology are as follows:

- All cables run to a central connection point.
- If one cable breaks or fails, only the computer that is connected to that cable is unable to use the network.
- A star topology is scalable.
- As the network grows or changes, computers are simply added or removed from the central connection point, which is usually a hub or a switch.
- Because there is so much cabling used to connect individual computers to a central point, this may increase the cost of expanding and maintaining the network.

## The Mesh Topology

A mesh topology has multiple connections, making it the most fault tolerant topology available. Every component of the network is connected directly to every other component. Characteristics of a mesh topology are as follows:

- A mesh topology provides redundant links across the network.
- If a break occurs in a segment of cable, traffic can still be rerouted using the other cables.
- This topology is rarely used because of the significant cost and work involved in having network components directly connected to every other component.
- It is common for partial mesh topologies to be deployed. This balances cost and the need for redundancy.

## The Ring Topology

A ring topology consists of computers connected to a cable that loops around forming a ring. Characteristics of a ring topology are as follows:

- The topology forms a closed loop, so there are no unconnected ends to the ring, so terminators aren't required.
- Data passes around the loop in one direction.
- A signal called a *token* is passed from one computer to the next in the ring. When a computer has the token, it has access to the ring and can send data.
- Each computer examines each packet and checks to see if there are any that are meant for it. If there aren't, the computer sends the packet on to the next computer in the ring.
- Each computer acts as a repeater.
- When any packet reaches the originating computer, it removes the packet from the network.
- In a ring topology, if one computer fails, the entire network goes down.

- If a computer is down or a cable is broken, the ring can't be completed, so the network can't function properly.
- Some ring implementations have features that detect and disconnect failed computers from the ring or beacons that notify the network if a break is detected.

#### *POINT-TO-POINT*

A point-to-point topology is any network that connects two hosts in a dedicated fashion. For example, if you were to configure a router in Miami, Florida, to connect and use resources on a network in Atlanta, Georgia, you would want to make sure you had a link between them that can support your needs. If you need a permanent connection that is constantly available and dependable, you may need a T1 circuit. Although costly, you will be able to connect your two sites together resulting in a point-to-point connection that is dependable and reliable.

#### *POINT-TO-MULTIPOINT*

A point-to-multipoint topology is any network that connects three or more hosts and can grow exponentially based on the hardware and software you choose to manage it. For example, if you wanted to create a large network of many sites (that is, New York, Georgia, Florida and Michigan), you may need to create a point-to-multipoint network. The main connection could be your headquarters location, and the other three sites could be smaller sites accessing resources in the main "hub" site. This type of network is also called a "*hub-and-spoke*" topology.

#### *HYBRID*

A hybrid topology is any mixture of at least two or more of any network topologies. Most networks aren't purely configured as one type of topology but are deployed in some form of hybrid network.

### Wireless

A wireless topology broadcasts data over the air, so very few cables are used to connect systems together.

Characteristics of radio frequency-based wireless environments are as follows:

- This topology uses transmitters called *cells*, which broadcast the packets using radio frequencies.
- The cells extend a radio sphere around the transmitter in the shape of a bubble that can extend to multiple rooms and possibly different floors in a building.
- Each cell is connected to the network using cabling so that it can receive and send data to the servers, other cells, and networked peripherals.

- Computers and other devices have a device installed in them that transmits and receives data to and from the cell, allowing them to communicate with the network.
- Wireless networks can also extend their transmission to wireless devices by implementing radio antennas that are situated on buildings or towers. The antenna serves as a cell that will cover a wider area, such as a building or campus.

Characteristics of infrared-based wireless environments are as follows:

- Infrared communications require a direct line of site and close proximity for the communication to work.
- This type of wireless networking is similar to using a remote control for a TV, where each device needs to be lined up and within range of one another.
- Because of its limitations, it isn't generally used for networking but may be seen in a networked environment for connecting laptops and other computers to devices like printers.

Here are some of the potential issues that may occur in wireless networks:

- There is a chance of transmissions being blocked or experiencing interference.
- Machinery and other devices can emit radio frequencies or electrical interference that disrupts signals being exchanged between the cell and wireless devices.
- Some buildings using cinderblocks, large amounts of metal, or insolated to prevent transmissions from interfering with equipment can keep a wireless network from working between rooms.

## NETWORK TYPES

A network can be in a single building or comprising computers connected together over a broader geographical area. To categorize the scope of a network, different terms have been created to classify these different network types. The types of networks that could be created include the following:

- Local area network (LAN)
- Wide area network (WAN)
- Metropolitan area network (MAN)
- Storage area network (SAN)
- Personal area network (PAN)
- Campus area network (CAN)

### Local Area Network and Wide Area Network

LANs and WANs were the first types of networks to be classified by the area they covered. Although each of the names refers to an area, an exact range has never been firmly established and is left vague. LANs are networks spanning a limited

distance, whereas a WAN is a network that is larger than a LAN. The distance difference that distinguishes a LAN from a WAN in terms of area is ambiguous and speculative.

Characteristics of a LAN are as follows:

- LANs are small to medium-sized networks and generally connect network devices that are no more than a few miles of one another, which Institute of Electrical and Electronics Engineers, Inc. (IEEE) defines as being 4 km or less in diameter.
- LANs include networks that have been set up in homes, offices, the floor of a building, an entire building, a campus or group of nearby buildings, or facilities that are relatively close to one another.
- Typically, a LAN is owned by a single person or organization and is managed by a single person or group of people.

Characteristics of a WAN are as follows:

- WANs can span great geographical distances and connect different LANs together using high-speed solutions or telephone lines.
- A WAN may connect LANs in different cities, regions, states/provinces, or even countries.
- With WANs, ownership isn't a defining factor. WANs are often owned and managed by more than one organization.
- Each LAN that is part of the WAN may be managed by individuals or IT departments, and either the former or the latter maintains its connection to the rest of the LAN or hires outside parties to perform that function.

## Crunch Time

An effective way of understanding how a local area network is related to a WAN is to look at how they are connected and how data is sent. This may differ from organization to organization, as there are several different ways of getting data from a LAN to a WAN, including the following:

- **Modem** is a device that allows you to connect to other computers and devices using telephone lines. Generally, when a modem is mentioned, it refers to a dial-up modem (as opposed to the digital modems used for other methods mentioned below). This type of connection is slow and allows connections at a maximum of 56 Kbps (meaning that 56,000 bits of data can be sent or received per second)
- **Integrated Services Digital Network (ISDN)** sends data over telephone lines but at higher speeds up to 128 Kbps but averaging at 64 Kbps using an ISDN modem or router.
- **Digital subscriber line (DSL)** sends data across telephone lines at speeds ranging from 1.5 million bits per second (Mbps) using a router or digital modem and configured phone lines.
- **Cable** transmits the data across cable lines using the same lines used for cable television at speeds of up to 1.5 Mbps.
- **Satellite** transmits data to a satellite at speeds of up to 400 Kbps.
- **T1 and T3** are dedicated connections that provide extremely high speeds. A T1 line provides speeds of 1.544 Mbps, while a T3 line provides speeds ranging from 3 Mbps to 44.736 Mbps

To illustrate the relationships between LANs and WANs, let's look at a situation that may be familiar to you: sending an e-mail to another person. Here is a general overview of the process:

1. Using the e-mail program on your home computer, you would address, compose, and send an e-mail message.
2. Your e-mail is sent to the network adapter, where it is broken up into smaller chunks called *packets* that can be sent more efficiently over the network.
3. These packets are transmitted over the connection in your home LAN to the router that is used to connect to the Internet.
4. The router examines the information pertaining to the packet's end destination, and the router determines if the destination is for a computer on the LAN or if the packets need to be sent to the ISP that provides your Internet connection.
5. Since in this case you're sending an e-mail to someone who isn't on your home network, the router would use the WAN connection between your LAN and the ISP's LAN to send the e-mail.
6. When the ISP receives your e-mail, it also looks at where the data is destined. Because the ISP also has a LAN, it looks at whether the e-mail is destined for someone else who uses their service, a computer on their network, or another network connected to the Internet.
7. Since you're sending the e-mail to someone who uses a different ISP, the e-mail is broken into packets and sent over the Internet, which is a giant WAN, to be received by the other ISP's e-mail server.
8. When the other ISP receives the data, it will store the e-mail you sent on its e-mail server, until your friend dials into the Internet using a modem.
9. Your friend's computer connects to the ISP's server and then requests any e-mail that the e-mail server might have.
10. This data is again broken into packets and sent over the telephone line so that your friend's modem can receive the data, and their computer can reassemble these packets and display them in your friend's e-mail program.

As you can see by this example, there are many different kinds of LANs and WANs that data may pass through. LANs may be as small as a couple of computers networked together, and a WAN may be as large as the Internet or as small as two LANs (yours and your ISP's) interconnected together using routers. In each case, the LAN consists of computers that are part of the same network and the WAN consists of geographically dispersed LANs that are internetworked.

## Metropolitan Area Network

While most people refer to a network in terms of being either a LAN or a WAN, an additional category that exists is called a metropolitan area network (MAN). A MAN will generally cover a metropolitan area like a city, but this isn't always

the case. When LANs are connected together with high-speed solutions over a territory that is relatively close together (such as several buildings in a city, region, or county), it can be considered a MAN. A MAN is a group of LANs that are internetworked within a local geographic area, which IEEE defines as being 50 km or less in diameter.

### Storage Area Network

A SAN is used to connect storage devices together using high-speed connections. It is a segment of a network that allows storage devices to be accessed by computers within the larger LAN or WAN. These storage devices consist of hard disks or other methods of storing data and allow users of the network to view and/or save data to a centralized location.

### Personal Area Network

A PAN is a wireless network that allows devices to exchange data with computers. Personal digital assistants (PDAs), cell phones, and other devices that someone can carry on their person and support this technology have a wireless transmitter in them. When they are within a certain distance of a receiver that's installed on a computer, data can be exchanged between the computer and the device. Using a PAN allows you to do such things as update a calendar in a PDA, address book in a cell phone, and other tasks that are supported by the device.

### Campus Area Network

A CAN refers to a series of LANs that are internetworked between several nearby buildings. This is a common type of network that's used in organizations with facilities that are close to one another, such as when there is a pool of office buildings or a campus. It is larger than a LAN but smaller than a MAN.

## Summary of Exam Objectives

We have reviewed the various network types, topologies, and models available for a network. A network can use a centralized or distributed model and be designed as a client/server model or peer-to-peer. In creating a network, you will use one or more topologies, which represents the physical layout of network components. The topologies we covered in this chapter were bus, star, ring, mesh, and wireless. Finally, the geographic scope of a network will determine what type of network you have. LANs are small networks within a limited area of a few miles, MANs are within a metropolitan area, and WANs interconnect LANs over a wide area. These characteristics define your network and will affect a wide variety of elements including security, media, and other features that make up your network as a whole.

## Top Five Toughest Questions

1. A new intranet has been created in your organization, and it includes a File Transfer Protocol (FTP) site to download files and a news server for sharing information. The network is internetworked with a network belonging to a subsidiary of the company. The subsidiary's network uses Apple computers and uses AppleTalk as a network protocol. To access the intranet, which of the following protocols would need to be installed on your computer?
   **A.** IPX/SPX
   **B.** NWLink
   **C.** TCP/IP
   **D.** AppleTalk

2. Your company's network is on several floors of a building. Because of the amount of data being stored, there are three file servers, a Web server for the intranet, an e-mail server for internal e-mail, and an SQL Server that is used for several databases that have been developed in house. Because of security reasons, floppy disks and other devices to transfer or transmit data to and from the computer have been removed and aren't permitted. What type of network model is being used?
   **A.** Client/server
   **B.** Peer-to-peer
   **C.** MAN
   **D.** PAN

3. A company has multiple offices that are internetworked. Office A has a single computer that has the capability to dial into the Internet but isn't connected to the other offices. Office B is in another part of the country from the other offices but doesn't have its network interconnected to the other offices. Offices C and D are in separate states but have a dedicated connection between them. Office C has 20 computers that access each other's machines and provide services and data to one another. Office D has 50 computers that log onto the network using a single server. Based on this information, which of the Offices are part of a LAN and a WAN?
   **A.** Offices A and B
   **B.** Offices B and C
   **C.** Offices C and D
   **D.** The entire network (Offices A, B, C, and D)

4. You receive a call that the network is down. In this network, all the computers are connected together using a single cable, which they are connected to using T-connectors. Looking at the situation, you find that there is no break through the trunk. Which of the following is most likely the cause of the problem?
   **A.** A failed network card
   **B.** One of the computers is turned off
   **C.** T-connectors are missing from the ends of the cable
   **D.** Terminators are missing from the ends of the cable

5. Your network has 10 computers that are networked together using a star topology. Which of the following is a possible point of failure for this topology that could bring down the entire network?
   **A.** Cable
   **B.** Network card
   **C.** T-connector
   **D.** Hub

## Answers

1. Correct answer and explanation: **C**. TCP/IP. Intranets use the same technologies as the Internet, which uses TCP/IP. To access an intranet using a Web browser, and fully take advantage of the services it provides, you would need to have TCP/IP installed just as you would if you were going to access the Internet.

   Incorrect answers and explanations: **A**, **B**, and **D**. Answer **A** is incorrect because IPX/SPX is a protocol used on Novell NetWare networks but isn't a protocol that's used to access Internet sites (such as FTP sites that require TCP/IP). Although IPX/SPX was a default protocol for NetWare, recent versions use TCP/IP as a default protocol. Answer **B** is incorrect for similar reasons, as NWLink is an IPX/SPX compatible protocol that's used by Microsoft operating systems to connect to NetWare networks. Answer **C** is incorrect because AppleTalk is used for Apple networks but isn't the protocol used by various Internet technologies (such as FTP Sites).

2. Correct answer and explanation: **A**. Client/server. A decentralized network model has network resources and administration distributed throughout the network. Administration is shared by designating responsibility to system administrators or individual users, while resources such as servers and other devices are installed at various locations throughout the network. By sharing administrative burdens in this way, certain resources can now be managed by other members of the organization.

   Incorrect answers and explanations: **B**, **C**, and **D**. Answer **B** is incorrect because servers are being used, so this isn't a peer-to-peer network. On a peer-to-peer network, computers on the network are equal and aren't in the role of dedicated servers. Answers **C** and **D** are incorrect because these aren't network models and are types of networks. Because the network doesn't extend across a metropolitan area, it isn't a MAN, and because personal devices aren't being used to network with computers or other network devices, it isn't a PAN.

3. Correct answer and explanation: **C**. Offices C and D. Both these offices have LANs. Office C has a peer-to-peer network, while Office D has a client\server network. They are interconnected to one another and thereby part of a WAN.

   Incorrect answers and explanations: **A**, **B**, and **D**. Answer **A** is incorrect because Office A doesn't have a network but only an Internet connection.

It is also wrong because Office B isn't part of a WAN. Answer **B** is incorrect because although it has a LAN, it isn't connected to the other networks and therefore isn't part of the WAN. Answer **D** is incorrect because not every office has a LAN, and the others connected together form a WAN.

4. Correct answer and explanation: **D**. Terminators are missing from the ends of the cable. The topology described in the question refers to a bus topology and states that the entire network is down although there is no cable break. Terminators are needed on a bus topology because they prevent packets from bouncing up and down the cable. Terminators need to be attached to each end of the cable to absorb electronic signals. This clears the cable to allow other computers to send packets on the network. If there is no termination, the entire network fails.

   Incorrect answers and explanations: **A**, **B**, and **C**. Answer **A** is incorrect because a failed network card would only affect one computer. Answer **B** is incorrect because a bus topology is passive and doesn't require each computer to be present to receive and resend data along the cable. Answer **C** is incorrect because T-connectors are used to connect the computers to the cable. They aren't used to terminate the ends of a cable.

5. Correct answer and explanation: **D**. Hub. In a star topology, all computers are connected through one central hub. Computers are cabled to this hub making it a centralized point where the network is connected. If the hub fails, the network would go down.

   Incorrect answers and explanations: **A**, **B**, and **C**. Answer **A** is incorrect because if a cable broke or failed in some way, it would only remove the computer connected to it from the network. Answer **B** is incorrect because a failed network card in a computer would only prevent that particular computer from being able to access the network. Answer **C** is incorrect because a T-connector is used to connect computers to a cable in a bus topology. A star topology is being used in this situation.