CCNA™
CISCO® CERTIFIED NETWORK ASSOCIATE

1

Networking Technologies

CERTIFICATION OBJECTIVES

This chapter offers a brief introduction to networking and some basic networking terms and concepts. This material should be a review of many already known concepts. You should be familiar with the various networking topologies used in networks, as well as different types of networks, such as local area networks (LANs) and wide area networks (WANs).

CERTIFICATION OBJECTIVE 1.01

Networks

A *network* is basically all of the components (hardware and software) involved in connecting computers across small and large distances. Networks are used to provide easy access to information, thus increasing productivity for users. This section covers some of the components involved with networking, as well as the basic types of topologies used to connect networking devices, including computers.

Components

One of the main components of networking is applications, which enable users to perform various tasks. Many applications are *network-aware*. These applications allow you to access and use resources that are not located on your local computer. Some of the more common networking applications include e-mail (sending mail electronically), FTP (transferring files), and WWW (providing a graphical representation to information). The number of networking applications ranges in the thousands, but those listed are the most commonly used.

To build a network, you need three types of devices or components: computers, networking devices, and cabling. Computers—devices such as PCs and file servers running Microsoft Windows, Macintosh OS, Unix (including Linux), or other operating systems—are responsible for providing applications to the users. Networking devices—such as hubs, bridges, switches, routers, firewalls, modems, NT1s (an ISDN network termination device), and channel service units / data service units (CSU/DSUs)—are responsible for moving information between computers.. Cabling, such as copper or fiber cabling, is needed to connect the computers and networking devices so that information can be shared between components. Wireless communication also falls in this category.

TABLE 1-1 Networking Locations

Term	Definition
Small office/home office (SOHO)	Users working from a home or small office (a handful of people)
Branch office	A small group of users connected in a small area, called a LAN, geographically separated from a corporate office
Mobile users	Users who can connect to a network from any location, LAN or WAN
Corporate office	The location where most users in an organization and their resources are located

Locations

Network components can be located in various locations. Table 1-1 shows some common terms used to describe the location of network components.

CERTIFICATION OBJECTIVE 1.02

Topologies

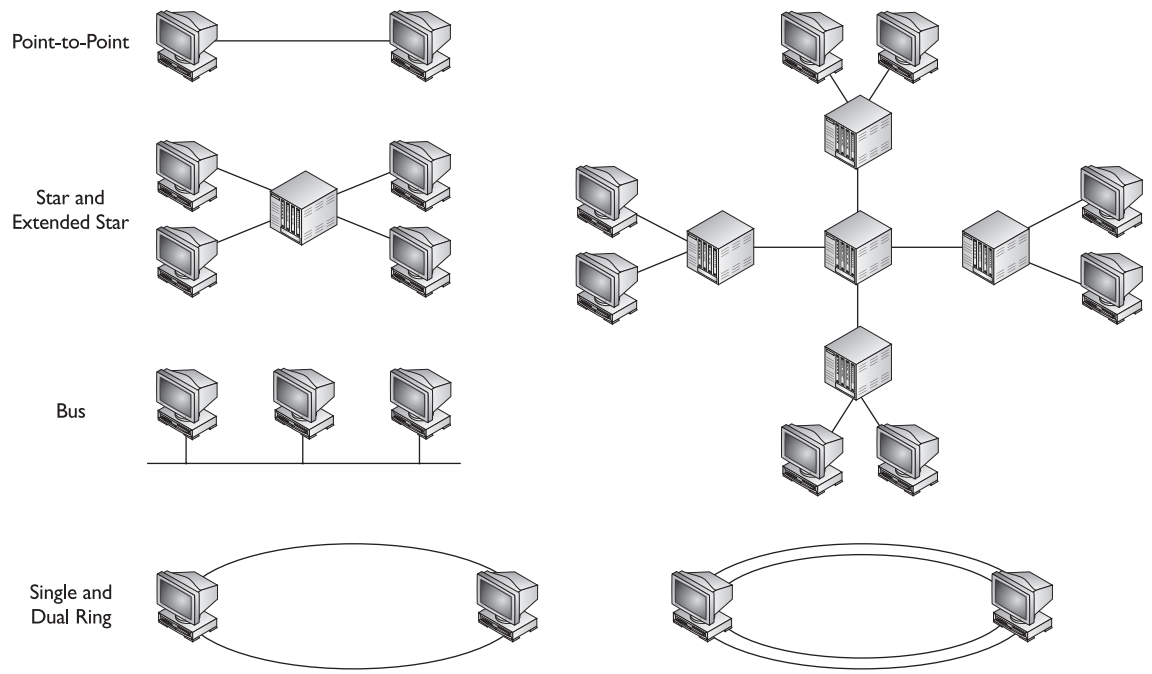
When you are cabling up your computers and networking devices, various types of topologies can be used. A topology defines how the devices are connected. Figure 1-1 shows examples of topologies that different media types use.

A *point-to-point* topology has a single connection between two devices. In this topology, two devices can directly communicate without interference from other devices. These types of connections are not common when many devices need to be connected together. An example of a point-to-point topology is when you connect two routers across a dedicated WAN circuit.

In a *star* topology, a central device has many point-to-point connections to other devices. Star topologies are used in environments where many devices need to be connected. An example of a media type that uses a star topology is 10BaseT Ethernet. When connecting devices together, you connect your computers to a hub or switch (the center of the star). An extended star topology is basically multiple star topologies interconnected.

A *bus* topology uses a single connection or wire to connect all devices. Certain media types, like 10Base5 and 10Base2 Ethernet, use a bus topology. Typically, special

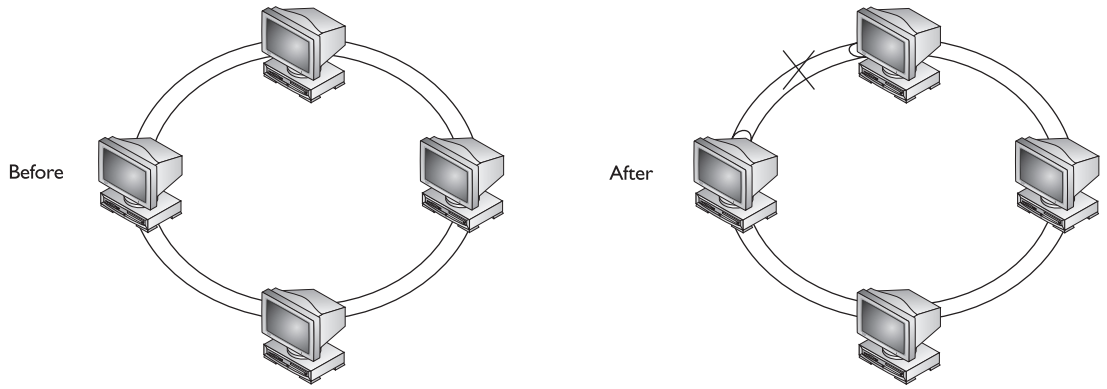
FIGURE 1-1 Network topologies



types of connectors or transceivers are used to connect the cables in order to provide the bus topology. In 10Base2, for example, each device connects to a single strand of coaxial cable via a vampire tap. This device taps into the single strand of coaxial cable and provides the physical connection from a networking device to the single strand of cable.

In a *ring* topology, device one connects to device two, device two connects to device three, and so on to the last device, which connects back to device one. Ring topologies can be implemented with a single ring or a dual ring. Dual rings are typically used when you need redundancy. For example, if one of the devices fails in the ring, the ring can wrap itself, as shown in Figure 1-2, to provide a single, functional, ring. Fiber Distributed Data Interface (FDDI) is an example of a media technology that uses dual rings to connect computer devices.

FIGURE 1-2 Dual rings and redundancy



Physical Versus Logical Topologies

A distinction needs to be made between physical and logical topologies. A *physical* topology describes how devices are *physically* cabled together. For instance, 10BaseT has a physical star topology and FDDI has a physical dual ring topology. A *logical* topology describes how devices communicate across the physical topology. The physical and logical topologies are independent of each other. For example, any variety of Ethernet uses a logical bus topology when devices communicate. This means that in Ethernet, you might be using 10BaseT with a physical star topology to connect devices together; however, these devices are using a logical bus topology to communicate.

Token Ring is actually a good example of a media type that has a different physical topology from its logical one. Physically, Token Ring uses a star topology, similar to 10BaseT Ethernet. Logically, however, Token Ring devices use a ring topology to communicate. This can create confusion when you are trying to determine how devices are connected together and how they communicate. FDDI, on the other hand, is straightforward. FDDI's physical and logical topologies are the same: a ring. Table 1-2 shows common media types and their physical and logical topologies.

TABLE 1-2 Examples of Physical and Logical Topologies

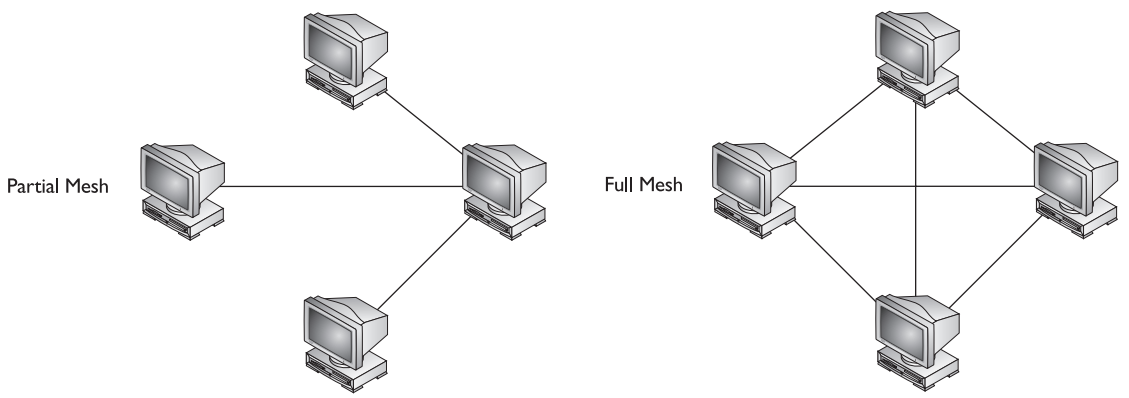
Media Type	Physical Topology	Logical Topology
Ethernet	Bus, Star, or Point-to-Point	Bus
FDDI	Ring	Ring
Token Ring	Star	Ring

Meshing

Meshing generically describes how devices are connected together. There are two types of meshed topologies: partial and full. In a partially meshed environment, every device is *not* connected to every other device. In a fully meshed environment, every device *is* connected to every other device. Figure 1-3 shows examples of these two types of topologies.

Note that like the topologies in the preceding section, partial and full mesh can be seen from both a physical view and a logical one. For example, in a physical bus topology, all the devices are fully meshed, since they are all connected to the same piece of wire—this is both a physical and logical fully meshed topology. This is common in LAN topologies. WANs, on the other hand, because of their cost, commonly use partially meshed topologies to reduce the cost of connected devices. For example, in the partially meshed network shown in the top part of Figure 1-3, the top, right, and bottom devices can all communicate via the device on the right-hand side. This communication introduces a delay in the transmission, but it reduces the cost, since not as many connections are needed.

FIGURE 1-3 Partial- and full-mesh topologies



CERTIFICATION OBJECTIVE 1.03

Network Types

Networks come in a wide variety of types. The most common are LANs and WANs, but there are many other types of networks, including metropolitan area networks (MANs), storage area networks (SANs), content networks (CNs), intranets and extranets, VPNs, and others. The following sections provide a brief overview of each of these network types.

Local Area Networks

Local area networks (LANs) are used to connect networking devices that are in a very close geographic area, such as a floor of a building, a building itself, or a campus environment. In a LAN, you'll find PCs, file servers, hubs, bridges, switches, routers, multilayer switches, voice gateways, firewalls, and other devices. The media types used in LANs include Ethernet, Fast Ethernet (FE), Gigabit Ethernet (GE), Token Ring, and FDDI. Today, most networks use some form of Ethernet. Ethernet is discussed in Chapter 2.

Wide Area Networks

Wide area networks (WANs) are used to connect LANs together. Typically, WANs are used when the LANs that must be connected are separated by a large distance. Whereas a corporation provides its own infrastructure for a LAN, WANs are leased from carrier networks, such as telephone companies. Four basic types of connections, or circuits, are used in WAN services: circuit-switched, cell-switched, packet-switched, and dedicated connections.

A wide array of WAN services are available, including analog dialup, ATM, dedicated circuits, cable, DSL (digital subscriber line) Frame Relay, ISDN, Switched Multi-megabit Data Services (SMDS), and X.25. Here, analog dialup and ISDN are examples of circuit-switched services, ATM and SMDS are examples of cell-switched services, and Frame Relay and X.25 are examples of packet-switched services.

Circuit-switched services provide a temporary connection across a phone circuit. These are typically used for backup of primary circuits and for temporary boots of bandwidth. A dedicated circuit is a permanent connection between two sites where the bandwidth is dedicated. These circuits are common where you have a variety of

services, such as voice, video, and data, that must traverse the connection and you are concerned about delay issues with the traffic and guaranteed bandwidth.

Cell-switched services can provide the same features that dedicated circuits offer. Their advantage over dedicated circuits is that a single device can connect to multiple devices on the same interface. The downside of these services is that they are not available at all locations, they are difficult to set up and troubleshoot, and the equipment is expensive when compared to using dedicated circuits.

Packet-switched services are similar to cell-switched services. Whereas cell-switched services switch fixed-length packets, called cells, packet-switched services switch variable-length packets. This feature makes them better suited for data services, but they can nonetheless provide some of the Quality of Service (QoS) features that cell-switched services provide. All of these service types are discussed in more depth in Chapter 15.

exam Watch

Circuit-switched connections, like analog and ISDN are typically used for temporary or backup connections. Dedicated circuits, like leased lines, are used to provide guaranteed bandwidth for applications across short distances. Cell-switched services and cell-switches services are used when you only want to use a single connection to the WAN, but provide a partially or full-meshed network. Cell-switched services, like ATM and SMDS, can provide a granular level of quality of service (QoS) for an application and are typically used to provide voice and video connections. Packet-switched services, like Frame Relay and X.25, provide a more cost-effective solution than cell-switched services, but not with the same level of QoS support.

Two newer WAN services that are very popular in the U.S. are cable and DSL. DSL provides speeds up to 2 Mbps and costs much less than a typical WAN circuit from the carrier. It supports both voice and video and doesn't require a dialup connection (it's always enabled). Cable access uses coaxial copper connections—the same medium used to provide television broadcast services. It supports higher data rates than DSL, but like DSL, it provides a full-time connection. However, it has one major drawback: it is a shared service and functions in a logical bus topology (discussed in Chapter 2) much like Ethernet—the more customers in an area that connect via cable, the less bandwidth each customer has.

Examples of networking devices used in WAN connections include cable and DSL modems, carrier switches, CSU/DSUs, firewalls, modems, NT1s, and routers.

Metropolitan Area Networks

A metropolitan area network (MAN) is a hybrid between a LAN and a WAN. Like a WAN, it connects two or more LANs in the same geographic area. A MAN, for example, might connect two different buildings or offices in the same city. However, whereas WANs typically provide low- to medium-speed access, MANs provide high-speed connections, such as T1 (1.544 Mbps) and optical services.

The optical services provided include SONET (the Synchronous Optical Network standard) and SDH (the Synchronous Digital Hierarchy standard). With these optical services, carriers can provide high-speed services, including ATM and Gigabit Ethernet. These two optical services (covered in Chapter 2) provide speeds ranging into the hundreds or thousands of megabits per second (Mbps). Devices used to provide connections for MANs include high-end routers, ATM switches, and optical switches.

Storage Area Networks

Storage area networks (SANs) provide a high-speed infrastructure to move data between storage devices and file servers. A storage device, sometimes referred to as a storage unit, includes disk drives, disk controllers, and any necessary cabling. This infrastructure can be dedicated to just these devices or can include other devices. Typically, fiber channels are used for the connections. A *fiber channel* is an optical cable that connects the file servers, disk controllers, and hard drives at rates exceeding 1 gigabit per second (Gbps). The advantages of separating the storage device from the file services are more flexibility and centralization of storage, which eases management.

SANs are becoming very popular in LAN environments, and some ISPs and carrier companies are starting to offer these services in MAN environments. However, SANs are not currently being used in WAN environments, because of the connection types and access speeds required.

Since optical connections are used, you gain the following advantages over normal storage techniques (keeping the data local to the server):

- Performance is fast.
- Availability is high because of the redundancy features available.
- Distances can span up to 10 kilometers.
- Management is easy because of the centralization of data resources.
- Overhead is low (uses a thin protocol).

The main disadvantage of SANs is their cost. If you are using fiber channels, you must buy special disk controller cards for your file servers and buy a SAN storage

unit, and you must lay down the necessary fiber. Of course, if you are using your own network infrastructure, you only need to buy a storage unit and lay down any necessary cabling for it. Plus, if you are concerned about redundancy, your cost will increase because you'll need to ensure that your network infrastructure has redundant paths between your servers and the SAN storage unit(s).

Content Networks

Content networks (CNs) were developed to ease users' access to Internet resources. CNs are aware of layers 4–7 of the OSI Reference Model (discussed in Chapter 2) and use this information to make intelligent decisions about how to obtain the information for the user or users. CNs come in the following categories: content distribution, content routing, content switching, content management, content delivery, and intelligent network services, which include QoS, security, multicasting, and virtual private networks (VPNs).

Companies deploy basically two types of CNs:

- Caching downloaded Internet information
- Distributing Internet traffic loads across multiple servers

For the first item, CNs are used to reduce the amount of bandwidth that you need for your users' Internet connections. When users download content, it is cached on a local server. And then when a user make another request, that request is first checked with the local server to determine if the content exists there. If it does, the local server sends the information to the user, thus providing higher data rates, since the client is acquiring its information from the LAN instead of having to download it again from the Internet. If not, the local server will obtain the information from the Internet resource. Because many items, especially GIFs and JPEGs, are included on every page from a web site, this information doesn't have to be repeatedly downloaded. The main problem with this solution, however, is that all traffic to and from the network must go through a CN device, commonly called a proxy server, which can reduce your throughput.

CNs are also used to reduce the overhead for external users that want to access internal resources in your network. In the old days of networking, if your web server was overwhelmed with requests, your only solution was to upgrade its processor, memory, disk drive, and interface card to larger sizes or faster speeds. And if you have ever upgraded a server, you know that this is not always an easy process. With the introduction of CNs, you can distribute the traffic load from external users across multiple internal servers, thus reducing network congestion to the servers and reducing the resources required to handle the external users' requests.

Because of the advantages that CNs provide, they are commonly used in LAN environments. Customers use them to access external resources more efficiently and to provide better throughput and redundancy for local resources. ISPs also commonly use CNs in their LANs to help reduce some congestion by providing caching services for commonly accessed web pages.

Intranets, Extranets, and Internets

Now that you have a basic understanding of various types of networks, let's discuss some other terms that are used to describe locality: intranet, extranet, and internet. An *intranet* is basically a network that is local to a company. In other words, users from within this company can find all of their resources without having to go outside of the company. An intranet can include LANs, private WANs and MANs, and SANs.

An *extranet* is an extended intranet, where certain internal services are made available to *known* external users or external business partners at remote locations. The connections between these external users and the internal resource are typically secured via a firewall and a VPN, a feature that is briefly discussed in the next section.

exam Watch

Understand the difference between intranet, extranet, and internet.

An *internet* is used when *unknown* external users need to access internal resources in your network. In other words, your company might have a web site that sells various products, and you want any external user to be able to access this service. There is a difference between the terms *internet* and *Internet*. The lowercase *internet* refers to any type of network connection where external users access publicly available resources. The *Internet* is the main public network that most companies and people use when accessing external resources. Typically, a firewall is used to secure your internal resources from external users.

Virtual Private Networks

A virtual private network (VPN) is a special type of secured network. A VPN is used to provide a secure connection across a public network, such as an internet. Extranets typically use a VPN to provide a secure connection between a company and its known external users or offices. A VPN typically provides authentication, confidentiality, and integrity to create a secure connection between two sites or devices. *Authentication* is provided to validate the identities of the two peers. *Confidentiality* provides encryption of the data to keep it private from prying eyes. And *integrity* is used to ensure that the data sent between the two devices or sites has not been tampered with.

TWO-MINUTE DRILL

Networks

- A network includes all of the hardware and software components to connect computers across a distance in order to provide easy access to information and increase productivity. To build a network, you need computers, networking devices, and cabling (or wireless connections).
- A SOHO describes people working from home or a small office. A branch office describes a small group of users connected in a small area. Mobile users connect to a network from any remote location, including LANs, MANs, and WANs.

Topologies

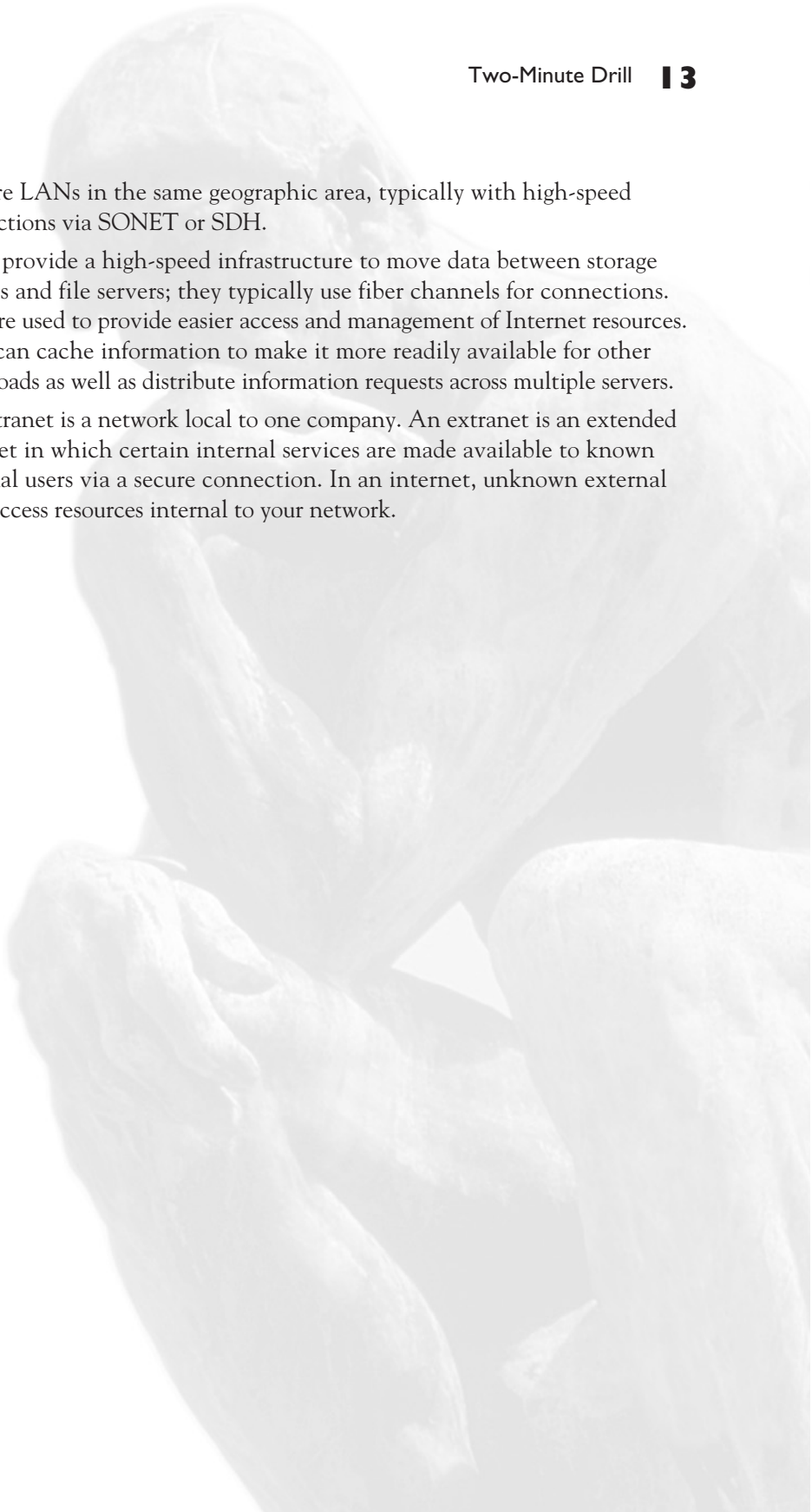
- A point-to-point topology uses a single connection between two devices and is typically used in WAN environments. In a star topology, a central device makes many point-to-point connections to other devices. A 10BaseT hub is an example of a central device in a star topology. A bus topology uses a single connection between all devices; Ethernet 10Base5 is an example of this topology. A ring topology connects one device to the next, where the last device is connected to the first. FDDI is an example of a ring topology.
- A physical topology defines how the computing devices are physically cabled together. A logical topology describes the method by which devices communicate across a physical topology. The two topologies can vary with the media type used.
- Meshing generically describes how devices are connected. A partially meshed network is one where not every device has a connection to every other device. In a fully meshed network, each device has a connection to all other devices.

Network Types

- LANs are used to connect networking devices in a very close geographic area. Media types used include varieties of Ethernet, Token Ring, and FDDI. WANs are used to connect LANs across large distances. WAN services include analog dialup, ATM, dedicated circuits, cable, DSL, Frame Relay, ISDN, SMDS, and X.25. MANs are hybrid networks used to connect two

or more LANs in the same geographic area, typically with high-speed connections via SONET or SDH.

- ❑ SANs provide a high-speed infrastructure to move data between storage devices and file servers; they typically use fiber channels for connections. CNs are used to provide easier access and management of Internet resources. They can cache information to make it more readily available for other downloads as well as distribute information requests across multiple servers.
- ❑ An intranet is a network local to one company. An extranet is an extended intranet in which certain internal services are made available to known external users via a secure connection. In an internet, unknown external users access resources internal to your network.



SELF TEST

The following Self Test questions will help you measure your understanding of the material presented in this chapter. Read all the choices carefully, as there may be more than one correct answer. Choose all correct answers for each question.

Networks

1. A _____ is basically all of the components, hardware and software, involved in connecting computers across small and large distances.
   - A. LAN
   - B. WAN
   - C. Network
   - D. SAN
2. _____ describe(s) users working from home.
   - A. SOHO
   - B. Branch office
   - C. Regional office
   - D. Corporate office
3. _____ describe(s) users that can connect to a network from any location.
   - A. SOHO
   - B. Branch office
   - C. Mobile users
   - D. Corporate office

Topologies

4. A _____ topology uses a single connection to connect all devices together.
   - A. Bus
   - B. Star
   - C. Point-to-point
   - D. Ring

5. _____ has both physical and logical ring topologies.
   A. Ethernet
   B. FDDI
   C. Token Ring
6. Ethernet _____ has/have both a physical and logical bus topology.
   A. 10BaseT
   B. 10Base2 and 10Base5
   C. 10BaseT and 10Base2
   D. 10BaseT, 10Base2, and 10Base5
7. A _____ topology describes how devices communicate with each other.
   A. Physical
   B. Logical
8. _____ has a physical star topology but a logical ring topology.
   A. Ethernet
   B. FDDI
   C. Token Ring
   D. FDDI and Token Ring

Network Types

9. A _____ is used to connect networking devices that are in a very close geographic area, such as a floor of a building, a building itself, or a campus environment.
   A. WAN
   B. LAN
   C. MAN
   D. LAN and MAN
10. A _____ uses Gigabit Ethernet as a media type
   A. WAN
   B. LAN
   C. MAN
   D. LAN and MAN

11. A _____ connects two or more LANs in the same geographic area.

A. LAN
B. WAN
C. MAN
D. SAN

12. A _____ provides a high-speed infrastructure to move data between storage devices and file servers.

A. SAN
B. LAN
C. CN
D. SAN and CN

13. Which of the following is a disadvantage of SANs?

A. Distance limitation
B. Cost
C. Overhead
D. Management

14. A _____ looks at OSI Reference Model layers 4–7 to make intelligent decisions about how to obtain information for a user.

A. SAN
B. LAN
C. CN
D. SAN and CN

15. A _____ is a network that provides a secure connection from a company to other business partners.

A. Intranet
B. Extranet
C. Internet

SELF TEST ANSWERS

1. ☑ **C.** A network is basically all of the components, hardware and software, involved in connecting computers together across small and large distances.
   ☒ **A** is true for small, but not large, distances. **B** is true for large distances only. **D** describes how a file server accesses remote storage devices.

2. ☑ **A.** The term SOHO describes users working from a home or small office.
   ☒ **B** is a small group of users connected via a LAN at one location. **C** is users that can dynamically connect from either a LAN or a WAN. **D** describes the central site, where most of the users and resources are located.

3. ☑ **C.** Mobile users are users that can dynamically connect from either a LAN or a WAN.
   ☒ **A** describes users working from home or a small office. **B** is a small group of users connected via a LAN at one location. **D** describes the central site, where most of the users and resources are located.

4. ☑ **A.** A bus topology uses a single connection to connect all devices together.
   ☒ **B** uses a central device, which has point-to-point connections to other devices. **C** is a single connection between two devices. **D** is where one device is connected to another and so on until the last device is connected to the first device, forming a ring.

5. ☑ **B.** FDDI has both physical and logical ring structures.
   ☒ **A**, depending on the type, uses a physical star or bus topology, but all types use a logical bus topology. **C** uses a physical star topology and a logical ring topology.

6. ☑ **B.** Ethernet 10Base2 and 10Base5 have physical and logical bus topologies.
   ☒ **A** has a physical star topology and a logical bus topology. **C** and **D** are incorrect because 10BaseT has a physical star topology and a logical bus topology.

7. ☑ **B.** A logical topology describes how devices communicate with each other.
   ☒ **A** defines how devices are connected to each other.

8. ☑ **C.** Token Ring has a physical star topology but a logical ring topology.
   ☒ **A** uses a logical bus topology. **B** uses a physical ring topology. **D** is incorrect because FDDI uses a physical ring topology.

9. ☑ **B.** A LAN is used to connect networking devices together that are in a very close geographic area, such as a floor of a building, a building itself, or a campus environment.
   ☒ **A** connects LANs together across large distances. **C** connects two or more LANs together in a small geographic area, such as between two buildings in a city. **D** is incorrect because it includes MAN.

10. ☑ **D.** LANs and MANs use Gigabit Ethernet media types for connections.
☒ **A** typically uses lower-speed connections. **C** is incorrect because it omits MAN, and **D** is incorrect because it omits LAN.

11. ☑ **C.** A MAN connects two or more LANs in the same geographic area.
☒ **A** connects networking devices together that are in a very close geographic area, such as a floor of a building, a building itself, or a campus environment. **B** connects LANs together across large distances. **D** connects storage devices to file servers.

12. ☑ **A.** A SAN provides a high-speed infrastructure to move data between storage devices and file servers.
☒ **B** connects networking devices together that are in a very close geographic area, such as a floor of a building, a building itself, or a campus environment. **C** looks at OSI Reference Model layers 4–7 to make intelligent decisions about how to obtain information for a user. **D** is incorrect because it includes CN.

13. ☑ **B.** The main disadvantage of SANs is cost.
☒ **A**, **C**, and **D** are advantages.

14. ☑ **C.** A CN looks at OSI Reference Model layers 4–7 to make intelligent decisions in order to obtain information for a user.
☒ **A** provides a high-speed infrastructure to move data between storage devices and file servers. **B** connects networking devices that are in a very close geographic area, such as a floor of a building, a building itself, or a campus environment. **D** is incorrect because it includes SAN.

15. ☑ **B.** An extranet is a network that provides a secure connection from a company to other business partners or known external users.
☒ **A** is a network local to one company. **C** is where unknown external users access internal resources in your network.