40555A Networking Fundamentals

Module 2: Local area networks and wide area networks

Contents

Learning objectives based on the Microsoft Technology Associate (MTA) exam objectives

#	Lesson title	Learning objectives	Exam objectives mapped
1	Local area networks	• Describe a local area network (LAN). • Describe how to implement perimeter networks. • Explain the difference between wired and wireless LANs.	1.2.1 Perimeter networks 1.2.5 Wired LAN and wireless LAN
2	Wide area networks	• Describe a wide area network (WAN). • Explain leased lines. • List considerations for implementing WANs.	1.3.1 Leased lines 1.3.2 Dial-up, Integrated Services Digital Network (ISDN), virtual private network (VPN), T1, T3, E1, E3, Digital Subscriber Line (DSL), cable modem, and more, and their characteristics (speed, availability)
3	Network topologies and access methods	• List and describe physical network topologies. • List and describe logical network topologies. • Describe Ethernet.	1.5.1 Star, mesh, ring, bus, logical and physical topologies

Module overview

Historically, the earliest networked systems spanned only single offices. They connected a small number of personal computers for the primary purpose of facilitating access to shared resources such as files and printers.

As the usefulness of personal computer networks became more apparent, the need arose to extend those networks. Initially, this was to overcome distance and signaling limitations that some of the networking components imposed. Later, it was to extend networks across sites, countries/regions, and eventually continents.

Throughout this period, several networking standards were devised. The various standards implemented a variety of different structures and access methods to link devices over local and wide areas.

In this module, you'll learn about local area networking and wide area networking, and you'll discover the various network topologies and access methods you use to create them.

Objectives

After completing this module, you will be able to:

- Describe LANs.
- Describe WANs.
- Identify and explain various network topologies and access methods.

Lesson 1: Local area networks

A LAN is just that: a network over a specific local area. But what is local? A room? A building? A city? In this lesson, you'll learn to identify LANs and describe the components that are typically used to create a LAN. You'll also learn about both wired and wireless LANs.

Objectives

After you complete this lesson, you will be able to:

- Describe a LAN.
- Describe how to implement perimeter networks.
- Explain the difference between wired and wireless LANs.

Making it real

Let's examine a real-world example for a moment. Remember our old friends at Fourth Coffee? As we progress through this chapter, let's try to apply what we're learning to helping Josh, the boss, with his plans for his startup business. Josh started his coffee shop a little while ago, and although he's not especially tech-savvy, he knows enough to realize he could benefit from some kind of network for his business.

What is a LAN?

A *LAN* is a collection of devices that can communicate over relatively short distances. At one time, connecting devices over a LAN was expensive and something that you might only find in business organizations. Today, however, it's extremely common to find LANs in homes. They interconnect TVs, media players, smart phones, tablets, printers, and of course, computers. Home LANs also enable connectivity to the internet.

Implementing a LAN provides several benefits:

- Sharing content. Networks enable you to share files or media content and to provide shared access to databases.
- Enabling communications. Email, social media, online conferencing, location sharing, and instant messaging are prevalent these days. A network enables you to use a connected device such as a tablet, smartphone, or computer to participate in shared communications.
- Enabling peripheral devices and device sharing. You don't often need a printer for every user in your business or home. By using a network, you can share peripheral devices and other devices such as printers, scanners, copiers, media players, and display devices such as large screens.
- Bringing improved organization. A LAN enables you to bring order to chaos by centralizing data and using access control (file and object permissions) to determine who can access files and devices. You can also use a LAN to distribute apps to connected devices and to manage application licensing. Most networked operating systems enable you to perform centralized management of connected devices by using configuration policies.
- Increasing productivity. People often work in teams, and networked devices make it easier and more efficient for people to collaborate.

A LAN at Fourth Coffee?

Think about our example coffee shop with its patrons in the morning rush. Some are checking email on their phones, and others want to sit and enjoy their coffees while working on their laptops. Think about the baristas taking the orders. Do they use paper and pencil, or do they enter orders into devices? Josh would like to stream music from the internet and play it over a speaker system he had installed. Can Josh address any of these needs by implementing a LAN? Discuss this with the rest of the class.

Components of a LAN

A LAN consists of the following components:

- Computing devices
- Network protocol stack
- Topology
- Physical infrastructure

Computing devices

Typically, a LAN contains a collection of computing devices, each installed with a network adapter that supports physically wired and wireless connections. Each device on the LAN has a hardware address. Usually, this is the serial number of the network adapter and is a unique 48-bit binary number expressed in hexadecimal to make it shorter. This unique hardware address is known as the *media access control* (MAC) address.

You might typically connect several types of devices to a LAN, as Figure 1 depicts:

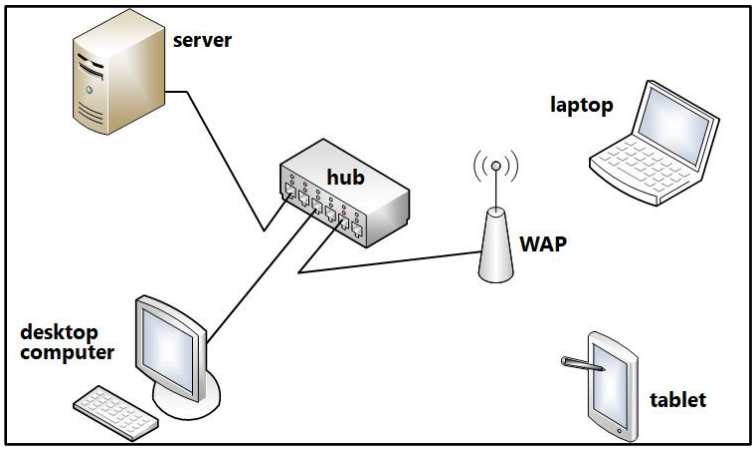

Figure 1. LAN computing devices

Devices that you typically connect to a LAN include:

- Desktop computer. A computer that typically remains on a user's desk. Desktop computers usually use wired connections to a LAN.

- Laptop. This device runs the same operating systems as a desktop computer but is portable. In business scenarios, laptops often use docking stations that allow the device to connect more quickly and easily to additional peripherals, such as external keyboards, mice, and monitors. Most laptops support wired and wireless connections to a LAN.
- Tablet. A smaller device, typically with screen dimensions between 7 and 10 inches diagonally, tablets usually require a wireless connection to a LAN. Those designed to run the Windows operating system run the same one as is available for laptop and desktop computers (Windows 10). Tablets such as the iPad run the Apple iOS operating system, which is specifically designed to support a touch interface. Tablets are also available that run the Google Android operating system.
- Convertible laptop. Increasingly common, convertible laptops are devices that cross the laptop-tablet boundary. Some laptop displays support touch and enable orientation of the screen around the hinge so that the device becomes a tablet. Other tablet devices support the attachment of keyboards and mice to make the device more like a laptop.
- Server. To share files, databases, or to enable shared communications such as email or instant messaging, you need one or more servers. These computers are more powerful than their desktop counterparts, and they have more memory, larger storage capacity, and sometimes, multiple network adapters to enable higher network throughput. Microsoft provides the Windows Server 2019 platform in a variety of editions to support different organizational sizes and requirements, and other vendors also provide server operating systems. As your network grows, you might decide to deploy additional servers for specific tasks such as a database server, file server, email server, or web server.

Network protocol stack

In addition to a network adapter, each device has networking software known as a *network protocol stack* that enables the device to communicate with other devices on a LAN. Often, this protocol stack is part of the computer's operating system. In Windows 10, iOS, macOS, Linux, and Android, the protocol stack is an integrated component of the operating system.

As you'll remember from Module 1, "Overview of networking," the most commonly used protocol stack is TCP/IP. But whichever protocol you use to implement a LAN, you must implement an addressing scheme to assign each device a unique logical address. In TCP/IP, this is known as an *IP address*.

Note

TCP/IP implements two logical addressing schemes at the internet layer of the protocol stack. These addressing schemes form part of the Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) network protocols. We will examine these in detail later in this course.

The protocol stack is responsible for taking messages from the applications on a device and packaging them up for transmission onto a physical network. It's also responsible for receiving packets on a physical network and passing the encapsulated data up to the appropriate application.

Topology

The way in which devices interconnect follows prescribed rules, known as the *network topology*. There are both physical topologies (the way things are actually joined together) and logical topologies (the way data logically flows between devices). We'll discuss topologies later in this module.

Physical infrastructure

Various physical components are necessary to connect devices together, as Figure 2 depicts:

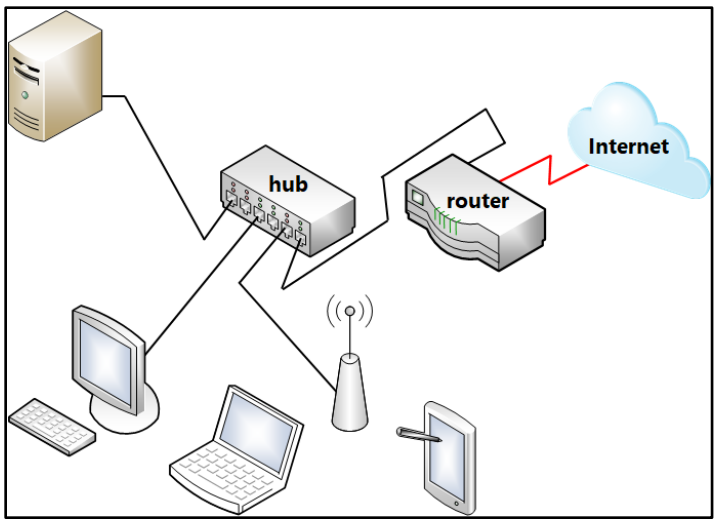

Figure 2. Components in a physical infrastructure

The components will vary depending on your needs and the complexity and size of the LAN. However, they typically include the following components:

- Hub. There are many ways to wire a network, but at very least, you'll need some sort of wiring concentrator, often known as a *hub*. All devices are connected to this hub with appropriate cabling.

  Hubs can support various sizes of LAN by providing more or fewer ports. For example, a 32-port hub can support up to 32 connected devices. You can extend a network by interconnecting multiple hubs, which we'll talk about later. Note that devices such as hubs are comparatively rare these days, being relatively old technology.

- Wiring. Each device (or node) on the network requires a connection to the hub. You achieve this by installing wiring. For large networks, wiring might already be installed in the building as part of the process of fitting out an office. In a smaller network, you might need to lay cabling between devices. The type of cable that you use and the rules governing distances for cable runs vary depending on the type of network (its *topology*) that you're deploying. We'll examine these rules later.

Note

Over the years, the maximum distances supported by LAN standards and protocols have changed, and to some extent, this blurs the distinction between a LAN and a WAN.

- Wireless access point. If your devices support or require a wireless network connection, you'll need a wireless access point (WAP). Some WAPs, typically those designed for home networks, also support physical ports for wired connections. In a small network, this might be all you need. For larger networks, however, you must physically connect WAPs to the hubs that you deploy. In some situations, a single WAP is sufficient, such as for a small office or home network. For larger, more complex LANs, you might need to deploy several WAPs to accommodate your users' needs.

- Router. A router device is required to connect a LAN to other LANs or to the internet. Sometimes routing functionality is built into a hub. This is common with domestic devices, which combine a wiring concentrator, a WAP, and an internet router in a single box. If you use a separate device as a router, you must connect it to the hub.

Infrastructure for Fourth Coffee

Thinking about Josh and his customers, what type of physical infrastructure would you install so that coffee shop customers can use their devices to send emails? How would you go about this?

Implement perimeter networks

As discussed in the last module, you can create security zones in a LAN by positioning firewall devices between networks. This creates isolated areas on a network to and from which you can define network traffic flow. When you need to make network services available on the internet, it's not advisable to connect hosting servers directly to the internet, because this can expose those devices to security risks. You can help avoid these risks by placing these servers in a perimeter network. This way, you can make them available to internet users without allowing those users access to your organization's intranet.

You can create a perimeter network in several ways depending on how many networks and firewalls you have.

Back-to-back configuration

In a *back-to-back configuration*, you create a perimeter network by deploying two firewall devices: the external firewall is connected to the internet on one interface, and the second interface connects to a hub, as Figure 3 depicts:

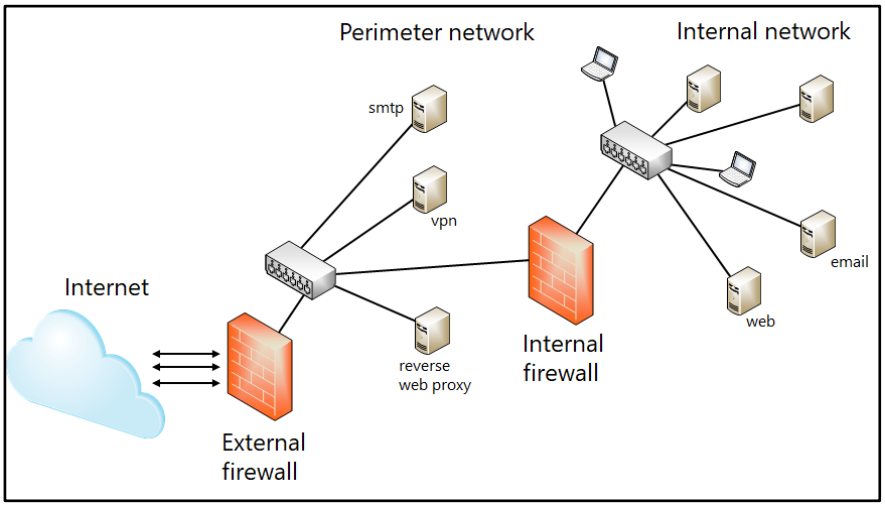

Figure 3. Back-to-back firewall configuration

Also connected to this hub are the server devices that you want to make accessible from the internet. Typically, this might be a web server, a Simple Mail Transfer Protocol (SMTP) relay, a VPN server, and a reverse web proxy.

Note

A reverse web proxy enables you to publish services from your internal network to the internet. This means that if you want to make your web server accessible across the internet, you can publish the web service on the internal network to the internet. Doing so means that you don't have to place a web server in your perimeter network. However, be careful what you put in the perimeter network. For security and privacy, place only the servers that you must in the perimeter network.

Three-part configuration

As the name suggests, a *three-part configuration* has three connections to a single firewall device. One connects to the internet while the other two connect to the perimeter network and the internal network. Traffic that passes between the internal and perimeter network must pass through the firewall, as Figure 4 depicts:

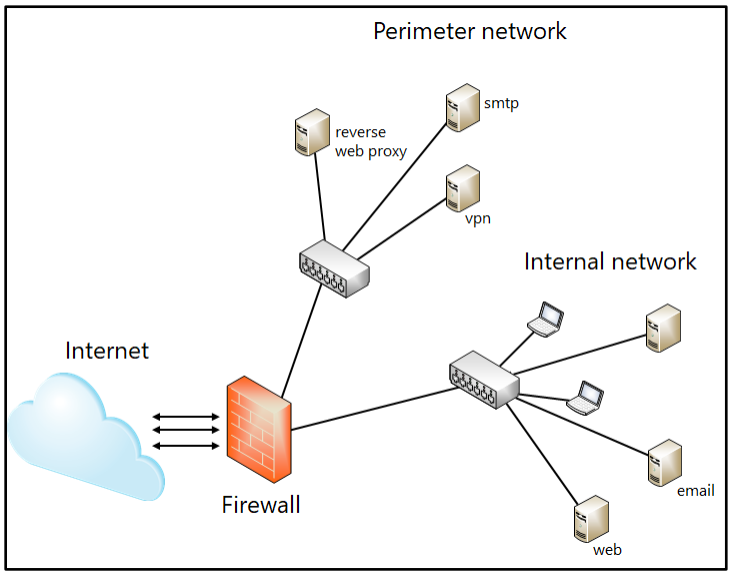

Figure 4. Three-part firewall configuration

This arrangement is simpler and requires less equipment and administration. However, it's not as secure, because a malicious hacker need only transit a single firewall to gain access to the internal network.

Note

A typical network at home probably doesn't involve multiple firewall devices in a back-to-back configuration. In fact, the firewall function is built into the hub device that your telecom company provides. However, you might be able to set up this hub device to create a three-part configuration.

Security zones at Fourth Coffee?

Because Josh wants to create a facility for his customers to connect wirelessly to the internet through the Fourth Coffee network, it might be beneficial to create several internal networks: a perimeter network with services he wants to make available on the internet, an internal network for employees, and a third network for customers to use. These security zones enable control of network traffic between the various networks that are connected to the firewall. What do you think? Will this work?

Wired and wireless LANs

Before wireless networks, all LANs were a collection of devices that were wired together by using cables. However, using wireless LANs provides many more benefits, not least of which is that you don't necessarily need to install cabling for networked devices. Let's examine wired and wireless networks in more detail.

Wired LANs

To implement a wired LAN, you must deploy a cabling system that facilitates a connection for all your networked devices. Like wireless LANS, wired LANs also have some benefits:

- Security. If you don't provide wireless capability, then anyone who wants access to your network must physically connect to the network cabling. This means that you control access to your network by monitoring physical access to the buildings where you installed the cabling. This is inherently more secure than using a wireless network because connecting to a wireless network merely requires being in range of a WAP—you don't need access to the building.
- Speed. Wired network connections tend to be faster. A typical wired network adapter supports a speed of 1,000 megabits per second (Mbps), or 1 gigabit per second (Gbps). A typical wireless network adapter can operate at speeds around 54 to 100 Mbps.

Note

Speed isn't really the correct term, but it's widely used. The term *bandwidth* is more appropriate, which describes the capacity of a network in a measured period of time. You can think of bandwidth as being the volume of network traffic that can pass between devices in a specific period. Speed is actually a measure of how fast electrical signals can transmit across network media.

- Interference. Wired network adapters are less prone to interference than wireless network adapters. That's not to say they can't be affected by electromagnetic interference, but if appropriately shielded cabling is used, this is significantly reduced.
- Distance. Wired LANs support physically bigger networks. To connect to a WAP, you must be near it. If you move a device more than a few dozen yards from a WAP, you might suffer reduced bandwidth or lose the signal altogether.
- Architecture. You can design a wired LAN to accommodate the physical characteristics of the building where it's deployed. This means that even if a device is connecting from a basement through a thick concrete floor, it can connect with the same bandwidth and reliability as a device that's connected anywhere else in the building. Wireless devices are affected by thick walls, floors, and other architectural elements.

Wireless LANs

Using wireless networks is convenient. If you think about the 21st century home, most have a LAN, and almost all of those will be based on wireless technologies. Wireless is almost everywhere—schools, businesses, and even supermarkets have their own wireless LANs. Wireless LANs are so popular for several reasons:

- Cost. Because a wireless LAN can be established with little physical infrastructure beyond a simple WAP, the cost is extremely low. For example, you can buy a WAP for home use that connects to the internet for less than $30. Because many consumer devices are equipped with wireless network adapters, after you set up a WAP, you're good to go.

- Simplicity. Laying cabling in a building to meet wired LAN needs requires considerable skill. It also requires specialized tools and a particular skill set to configure the cables that attach to a hub at one end, and the network adapter at the other. None of those skills or tools are necessary to enable a wireless LAN.
- Easy to extend. Adding devices to a wired LAN might require installing additional hubs and wiring. This is usually not the case when adding wireless devices.

Which to use?

Although there are advantages and disadvantages to both wired and wireless LANs, most networks—certainly those in a workplace—are a combination of both. WAPs deploy throughout an organization to facilitate convenient connections for devices with wireless network adapters. Structured cabling is used to interconnect these WAPs with network servers and resources elsewhere on the network infrastructure.

Security is a major consideration, especially for larger organizations, and the benefits of wired LANs in this area might be a factor. For a small business or a home office user, a wireless approach probably makes sense, thereby taking advantage of the low cost and simplicity that wireless networking offers.

Wireless LAN at Fourth Coffee

If you think about Fourth Coffee and Josh's requirement to support his customers' internet access, using a wired LAN wouldn't be appropriate. After all, phones and tablets don't have wired network adapters. What are the considerations for implementing a wireless LAN to support Josh's customers, but also to enable business usage for Josh's employees?

Lesson 2: Wide area networks

A *WAN* is a collection of several LANs joined together over a distance that LAN technologies can't support. For example, if you have two LANs in two cities, LAN technologies don't support the interconnection of those offices. Therefore, as an organization grows and begins to occupy offices and other buildings in multiple locations, its IT staff must begin to consider how best to connect those locations.

When considering WANs and how best to interconnect an organization's locations, you'll need to think about which technologies will satisfy your requirements. Some WAN technologies provide faster connections, support more reliable connections, and have a higher associated cost. You'll need to consider these factors when planning a WAN.

Objectives

After you complete this lesson, you will be able to:

- Describe a WAN.
- Explain leased lines.
- List considerations for implementing WANs.

What is a WAN?

As we have learned, a WAN is simply a collection of LANs that are connected over a wide area. To connect a LAN to another LAN over a WAN, you must install a device at each end of the connection that can take the LAN traffic and convert it to a format suitable for transiting the WAN. The device must also be capable of receiving a WAN packet and converting its payload to a structure suitable for onward transmission to the LAN.

In the past, dial-up devices known as *modems* were used to achieve this. Modems used telephone lines to send and receive data. The digital data on the LAN was converted into an analog signal and transmitted—fairly slowly—across the telephone network to the remote modem. At the remote end, the analog signal was converted back into a digital signal and transmitted onto the LAN. This approach was unreliable and slow and was discontinued after

packet switching and cell switching networks became available. Lately, routed networks have replaced packet and cell switching.

The following table describes WAN technologies.

WAN technology	Explanation
PSTN	Public switched telephone network (PSTN) connections support analog connections by using modem devices. Speeds are low and reliability isn't high. This technology is largely, if not entirely, discontinued in favor of other options.
ISDN	Integrated Services Digital Network (ISDN) provides a digital (non-analog) version of a telephone line. Better suited to support data connections, ISDN provides packet-switched data connections at speeds that increment in 64 kilobits per second (Kbps). Although still available from telecom providers, this technology isn't often used to support WANs anymore, although some organizations use ISDN for video conferencing and as a backup internet connection. ISDN was never particularly popular in the United States but was more widespread in Europe.
DSL	Digital Subscriber Line (DSL) provides data access over standard telephone lines. There are a few DSL options: • Asymmetrical Digital Subscriber Line (ADSL). Small businesses and home users typically use this DSL technology to connect to the internet, and it's often given the generic name *broadband*. Speeds (bandwidth) can vary greatly depending on the quality of the underlying telephony cabling and the distance from the telephone exchange. Users can expect download speeds up to around 30 Mbps, with lower upload speeds. Subscribers can use voice and data simultaneously. • Symmetrical digital subscriber lines (SDSL). Businesses rather than home users typically use SDSL. Their upload and download speeds are almost the same. However, you can use only data with SDSL; it doesn't support simultaneous voice.

WAN technology	Explanation
Broadband cable	Broadband cable provides higher speed (bandwidth) connections, typically in the range of 36 Mbps to over 300 Mbps. Usually delivered via coaxial cable to homes or offices, it provides improved throughput over the twisted-pair copper wiring that telephone systems use.
X.25	A packet switching network that became popular in the early days of wide area networking, X.25 isn't widely used now. However, it's still used to some extent for supporting niche applications such as the credit card payment system that some banks use.
Frame relay	Frame relay largely began replacing X.25 in the 1990s. Frame relay packages data into "frames" and sends the frames between the LANs within a larger WAN. For the most part, frame relay itself is now becoming obsolete. Some organizations are still using the technology, but most are migrating to other WAN technologies.
Leased lines (T-carrier)	Leased lines from telecoms carriers are usually found in large organizations. These lines are private and dedicated lines for an organization and connect two or more locations. There are a number of T standards, including: • T1, also known as DS1, provides speeds up to 1.544 Mbps. • T2, or DS2, provides speeds up to 6.312 Mbps. • T3, or DS3, provides speeds up to 44.736 Mbps. • T4, or DS4, provides speeds up to 274.176 Mbps. • T5, or DS5, provides speeds up to 400.352 Mbps. The higher speeds achieved by T2 through T5 is achieved by combining multiple T1 lines. Thus, T4 is achieved with 168 T1 connections. In Japan, these T-carriers are known as J-carriers, and in Europe, they are known as E-carriers. Thus, T3 is known as J3 and E3 respectively.

WAN technology	Explanation
ATM	Asynchronous transfer mode (ATM) is a cell-based switching technology. Again, this isn't widely used anymore.
SONET	A Synchronous Optical Network (SONET) uses optical connections based on the Optical Carrier standards, which are: • OC-1 51.84 Mbps • OC-3 155.52 Mbps • OC-12 622.08 Mbps • OC-24 1.244 Gbps • OC-48 2.488 Gbps • OC-192 9.953 Gbps SONET was originally devised to replace the T-carrier system.
FDDI	Not strictly speaking a WAN technology, Fiber Distributed Data Interface (FDDI) uses fiber optic cable at high speeds (bandwidth) over fairly long distances. As opposed to WAN technology, FDDI is often considered more useful for interconnecting buildings in large campuses.

Leased lines

Leased lines provide dedicated and private connections between LANs to create a WAN. You can also use leased lines to support other WAN technologies, such as frame relay.

As mentioned previously, there are a number of leased line (T-carrier) standards and worldwide equivalents. The following table summarizes them.

Standard	USA	Europe	Japan
DS0	64 Kbps	64 Kbps	64 Kbps
DS1	1.544 Mbps, known as T1	2.048 Mbps, known as E1	1.544 Mbps, known as J1
DS3	44.736 Mbps, known as T3	34.368 Mbps, known as E3	32.064 Mbps, known as J3
DS4	274.16 Mbps, known as T4	139.264 Mbps, known as E4	97.728 Mbps, known as J4

Practical considerations for implementing WANs

As discussed in the last module, it's becoming more popular to connect offices together by using VPNs. With site-to-site VPN connections, also known as *router-to-router VPN connections*, you can connect offices together over the internet. Security and privacy are maintained by using authentication and encryption at each end of the VPN, as Figure 5 depicts:

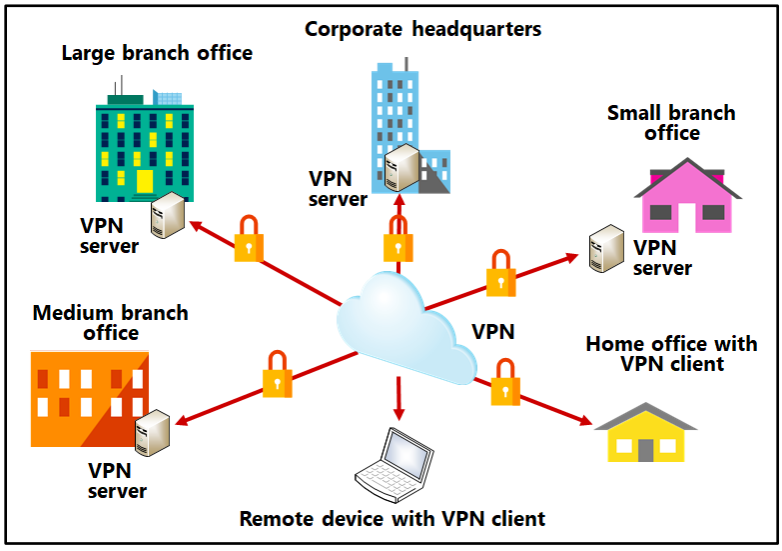

Figure 5. Overview of VPNs

A routed VPN connection across the internet operates logically as a WAN link. When networks connect over the internet, a router forwards packets across a VPN connection to another router. By using VPN connections in this way, you can take advantage of existing internet connections. This means that you can select between DSL, broadband cable, and wireless data connections to facilitate your WAN.

Wireless data technologies, which have been evolving at an impressive rate, currently include the following technologies:

- Enhanced Data rates for GSM Evolution (EDGE), also known as 2G. This is based on the General Packet Radio Service (GPRS), and it supports speeds (bandwidth) from 40 Kbps up to 1 Mbps. This is hardly ideal for the volume of traffic you might expect to support over a WAN link.
- Evolution-Data Optimized (EV-DO), also known as 3G. This supports speeds of around 8 Mbps download and 2 Mbps upload. Again, this is probably insufficient for most WANs.
- Evolved High Speed Packet Access (HSPA+), also known as 3.5G. This increased speeds to around 42 Mbps for download and 22 Mbps for upload. At these bandwidths, WAN connections become feasible.
- Long-Term Evolution (LTE), also known as 4G. Theoretically, download speeds of from around 150 to 300 Mbps are possible, with uploads at around half of that. In practice, the bandwidth is probably significantly lower; however, 4G is certainly a viable option for supporting a WAN connection.

Connecting the shops of Fourth Coffee

Business is thriving at Fourth Coffee, and Josh now has six coffee shops around New York City. He wants to be able to interconnect them, but he doesn't have a huge amount of money to spend on infrastructure. What are his options?

Lesson 3: Network topologies and access methods

We previously talked about implementing wired networks, and we mentioned constraints and rules regarding precisely how devices can be linked together. These rules define the network topology.

In the 1990s, several different network topologies were used, with the most popular being Ethernet and token ring. Ethernet is a logical bus topology that's physically wired by using the star topology. Token ring is a logical ring topology, usually star wired as well. In this lesson, we'll examine these two network topologies in more detail.

Objectives

After you complete this lesson, you will be able to:

- List and describe physical network topologies.
- Explain logical network topologies.
- Describe Ethernet.

Physical topologies

Physical topologies determine how things are arranged—that is, how devices are physically connected. There are several common ways of physically wiring networks, including bus, ring, star, tree, and mesh. Let's examine these more closely.

Bus topology

In a *bus network*, a main cable passes each device in the network, as Figure 6 depicts. A short cable connects the network adapter in the device to the main cable; this short connecting cable is often known as a *drop cable*. The interconnecting cable is typically a long piece of coaxial cable, like the kind of cable you connect to your TV to receive terrestrial broadcasts.

A terminator is installed at each end of the cable. The terminator absorbs network traffic, preventing network frames from bouncing back down the cable.

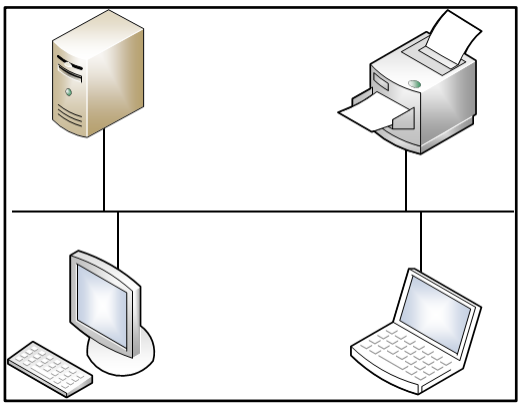

Figure 6. A bus topology network

Bus topology networks were extremely popular when LANs were first being installed. They used comparatively inexpensive cabling components and were relatively easy to deploy. However, a significant drawback of using bus networks is that if the cable that interconnects the devices is damaged or broken, communication on that cable is lost.

Star topology

By far the most common physical topology is a *star*. It's called this because each device is wired back to a central point, the wiring concentrator (or hub), as Figure 7 depicts:

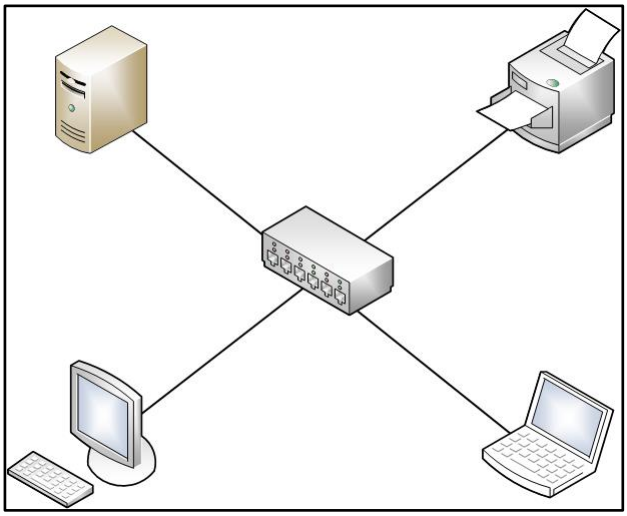

Figure 7. A star topology network

In typical implementations of star-wired networks, if a cable that connects a device to the hub is disconnected or broken, communications continue across all other wired devices without interruption.

This makes star-wired networks far more attractive than bus topology networks because they're more fault-tolerant. Specifics about the type of wiring that you can use is discussed later in the course.

Mesh topology

A *mesh topology* uses multiple cables to interconnect all devices, as Figure 8 depicts. While this topology avoids using a central wiring concentrator and the single point of failure of the bus network (the cable), it does use a complex and expensive wiring system.

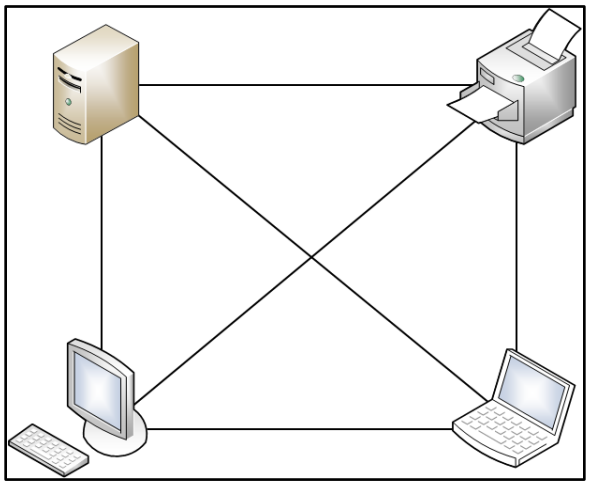

Figure 8. A mesh topology network

This is because each device requires *N*-1 wires, where *N* is the number of devices in the LAN. However, for specialist networks, this can be an attractive solution.

Ring topology

In a *ring topology*, a single cable (typically coaxial cable) loops between all devices on the LAN. Each is connected to the cable, as Figure 9 depicts. Network traffic loops around the ring, passing each device in turn.

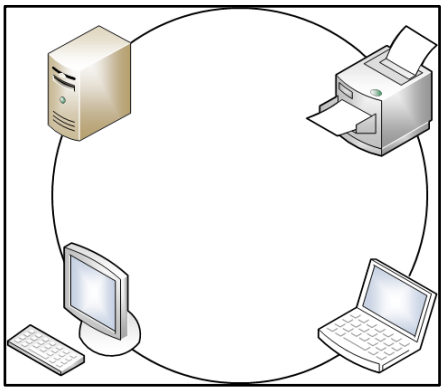

Figure 9. A ring topology network

As with the bus topology, the single point of failure here is the cable. A break in the cable causes the ring to fail, and no communications can occur.

Logical topologies

When you examine the various physical topologies, one stands out as having the most to offer in most situations: the star-wired network. Arguably, its biggest benefit is its fault-tolerance. However, neither of the two most popular network topologies are based on a star topology. Ethernet is a bus topology, and token ring, as the name suggests, is a ring topology.

However, if you think about it, you could collapse the Ethernet bus down into a wiring concentrator and make the drop cables much longer, thereby creating a star. In this situation, you have a physical, star-wired, logical bus topology.

Likewise, token ring is often wired using a special wiring concentrator called a multistation access unit (MAU). Each node is star-wired back to the MAU, creating a physical, star-wired network based on a logical ring topology.

Therefore, the logical topology of the network defines how communication occurs between nodes on the network, while the physical topology defines the wiring characteristics of the network. Let's briefly examine the characteristics of the two most popular networks of the last 30 years: Ethernet, and token ring.

Ethernet

As mentioned previously, Ethernet is a logical bus topology. This doesn't mean that it's based on a bus-length of cable, as you might infer. Rather, it describes how traffic moves up and down the single cable that (logically) connects all devices.

Although Ethernet is quite an old networking standard, it's still widely used and is by far the most popular network topology in use today. It's a *contention-based system*, which means that devices compete for available bandwidth. Consequently, under heavy load, Ethernet isn't the most efficient network topology. You'll learn more about Ethernet in the next topic.

Token ring

Token ring was developed by IBM in the late 1980s. It uses a logical ring, and usually, a star-wired ring. Unlike Ethernet, it uses a deterministic system rather than a contention system to manage access to media from connected devices. Essentially, a token loops around a ring of devices, but only one device can use the token at a time. Think of the token as being a flag. When you have the flag, you can speak. When a device wants to communicate, it captures the token, preventing other devices from trying to use the media. For the time that the device holds the token, it has exclusive use of the media. When it finishes transmitting data, the device releases the token.

Under load, token ring is an effective system because it enables all devices to use available bandwidth equally. However, under low loads, it's inefficient because time is wasted when the token rotates around the ring to devices that don't wish to communicate on the media.

Token ring was comparatively expensive to deploy compared with Ethernet. For this reason, and perhaps because Ethernet was already so widely deployed, it failed to secure a foothold in the marketplace.

Overview of Ethernet

Ethernet has become an international standard that virtually every networking organization has adopted. Originally developed by Xerox and later supported by Intel and DEC in the 1970s, the Institute of Electrical and Electronic Engineers (IEEE) standardized Ethernet as IEEE 802.3. This standard defined exactly how communications occur between connected devices.

IEEE 802.3—and therefore Ethernet—is a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) network. Essentially, connected nodes observe the media to which they're connected. If they can't detect other network traffic, they can transmit data. If another device transmits at the same time as the first device, all data, known as *frames* in Ethernet, is destroyed in what's called a collision. The two devices recognize the occurrence as a collision and then back off for a while before retransmitting their respective frames.

Note

When you implement Ethernet over wireless networks, it implements a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) system. We'll review wireless networks in more detail later in the course.

One of the significant problems with Ethernet networks is that they suffer from degraded performance under load. This occurs because time is spent checking for media use by other devices and retransmission of data following a collision. For example, think of a telephone call. With two parties talking, you seldom speak over one another; but it does happen, and when it does, you both automatically wait and then try again. However, if your call had dozens of parties, like telephone party lines, the likelihood of a collision increases. There comes a point when sufficient people are on the call that no data is ever delivered. All that happens is people try to talk, wait, and try to repeat themselves again.

Early Ethernet standards defined the speed (bandwidth) of the network at 10 Mbps. However, most devices are now equipped with 1 Gbps network adapters (1,000 Mbps) and infrastructure, enabling frames to be more quickly transmitted. This results in media being occupied for significantly shorter periods of time, effectively enabling more devices to connect on the same infrastructure.

Wiring standards

Originally, Ethernet was wired by using a single length of thick coaxial cable known as RG-8/U. Because the maximum cable length of the segment was 500 meters, and because a baseband transmission system was used, the original Ethernet system was known as 10Base5, or simply, *ThickNet*. Up to 100 nodes could connect to a single segment.

Thick coaxial cable is unwieldy, and so 10Base2 was developed. This Ethernet standard was based on thinner RG-58 coaxial cable and was often called *ThinNet*. Cable runs were up to 185 meters, and up to 30 nodes could connect to a single segment.

As discussed earlier, most modern Ethernet systems are star wired using unshielded twisted pair (UTP) cabling. This arrangement is known as 10Base-T. Because higher speeds are possible over UTP, later standards were developed to reflect this: 100Base-T, for example, defines 100 Mbps connections over UTP. Note that the maximum UTP cable length is 100 meters from hub to node.

802.3 standards

Ethernet has been around for so long that the IEEE has revised the standards and added new standards to support emerging technologies. The following table identifies the most common of these IEEE standards and explains how they relate to bandwidth and cabling.

IEEE 802.3 standard	Bandwidth	Cabling
802.3	10 Mbps	10Base5 over thick coaxial cable
802.3a	10 Mbps	10Base2 over thin coaxial cable
802.3i	10 Mbps	10Base-T over UTP cable
802.3j	10 Mbps	10Base-F over fiber optic cable
802.3ab	1 Gbps	1000Base-T over UTP cable
802.3z	1 Gbps	1000Base-X over fiber optic cable
802.3an	10 Gbps	10GBase-T over twisted-pair cable
802.3ae	10 Gbps	10GBase-SR over fiber optic cable

Extending an Ethernet network with repeaters, bridges, and routers

As you might have noticed, the early Ethernet standards provided fairly short cable runs—500 meters over thick coaxial cable and 200 meters over thin coaxial cable, respectively. One way to get around this limitation is to extend your network by using repeaters, bridges, and routers.

Repeater

The simplest way to extend an Ethernet network is to install a repeater. As the name suggests, a *repeater* is a device that repeats a signal by amplifying or regenerating it. You connect a repeater to both coaxial segments, and it simply repeats the electrical signal it receives on one interface on the other interface.

Repeaters operate at the physical layer of the network protocol stack. A maximum of four repeaters are allowed between any two Ethernet devices.

Note

Another way to think of a hub is as a multiport repeater.

Bridge

A *bridge* operates at the data-link layer. You can use a bridge to extend a network when you reach the maximum number of repeaters in sequence. However, a bridge can do more than just repeat an electrical signal. Because it works with frames, it can perform error-checking and won't forward damaged frames between connected interfaces.

You can also implement bridges over WAN links to extend a network between locations. However, bridges aren't the ideal device for WAN connections, because they don't support multiple paths efficiently.

The key features of a bridge are:

- A bridge operates at the data-link layer (MAC layer) and is therefore protocol independent.
- A bridge is transparent to communicating hosts. In other words, they don't realize that their frames are traveling through a bridge to reach the destination host.
- Bridges always pass broadcast and multicast traffic.

Note

A bridge isn't addressed by an end node. That is, when a device wants to communicate with another device, it's not aware that it does so over a bridge. A bridge is usually transparent to the communicating nodes.

Router

We'll discuss routers in much more detail later in the course; however, it's worth briefly discussing them now. A router operates at the network layer of the Open Systems Interconnection (OSI) protocol stack. When implemented over a TCP/IP network, a router operates at the internet layer. Unlike a bridge, when nodes communicate through a router, they knowingly do so—that is, a node on the network addresses the router it wants to use to communicate with a remote host.

To summarize, a router is an internetwork store and forwarding device that differs from a bridge in several important ways:

- A router operates at the network layer.
- A router is protocol dependent.
- A router is addressed by the hosts on the network.
- Routers can optimize network availability by managing multiple routes effectively.
- Routers can be used to connect LANs together that differ in their topology (e.g. token ring to Ethernet).
- Routers provide more reliable, available networks.

Learning in action: Planning LANs and WANs

Scenario

You have just taken a new job in IT with Lucerne Publishing in London. This small publishing company is about to take off in a big way, having signed some great new authors and secured the movie rights for several of its books. Lucerne Publishing just opened a number of small branch offices in cities throughout the United Kingdom. It's important that these be connected to the corporate network.

Answer the following questions.

1. **You want to implement star-wired Ethernet networks at the branch offices. What critical components must you install at each location to facilitate a star-wired Ethernet network? Choose all that apply.**

   A. A hub

   B. A suitable cabling system based on twisted pair

   C. Network adapters in each networked device, if necessary

   D. A WAP

2. **You want to make a web application available to users in the branch offices. What device must you put in the perimeter network at the London office to make a web server in the private network at London available?**

   A. Web server

   B. Proxy server

   C. Reverse proxy server

   D. VPN server

3. **What element should you add to each network to enable wireless communications in each branch office?**

   A. A firewall

   B. A WAP

   C. A reverse proxy server

   D. A repeater

4. **You want to implement a security zone network at the head office in London. What's the best firewall configuration?**

   A. An all-in-one WAP containing a firewall component

   B. A back-to-back firewall configuration

   C. A three-part firewall configuration

Test your knowledge

1. **You want to interconnect your computers and media players at home. What kind of network should you implement?**

   A. A WAN

   B. A LAN

2. **Which of the following devices should you use to connect your computing devices together?**

   A. Router

   B. Firewall

   C. Bridge

   D. Hub

3. **A network adapter has what kind of unique address?**

   A. MAC address

   B. IPv4 address

   C. IPv6 address

Fill in the blanks for the following statements.

4. **( ) is the most popular network protocol stack.**
5. **You need to install a ( ) to support connections from tablets and phones.**
6. **A ( ) firewall configuration requires two firewalls and creates a perimeter network between the internet and your private network or networks.**
7. **True or false: One of the advantages of wireless network adapters is that they can operate at higher bandwidths than wired network adapters.**

   True

   False

8. **True or false: You can use wireless data connections and VPNs to facilitate a WAN.**

   True

   False

Study the scenario and answer the question.

9. **You pop into Fourth Coffee on your way to the office. Josh, the owner, is an old college friend. He knows you work in IT, and he wants some advice. Sipping your espresso, you listen to Josh explain what he thinks he needs. Josh says he wants to be able to install networking equipment to support the following requirements:**

   - Provide his customers free access to the internet.
   - Enable a pair of desktop computers in the office to connect to the workplace network and the internet.

   How can you achieve these objectives? List the components you must install and list any special configuration you might need to make.

Study the scenario and answer the question.

10. **On your way home from the office, you again pop into Fourth Coffee. Sipping your second espresso of the day, you and Josh, the owner and an old friend, discuss the changes he'd like to make to the LAN he installed in the coffee shop. Josh says he wants to be able to install networking equipment to support the other coffee shops he has throughout the city. He wants to interconnect them cost-effectively.**

    How can you achieve this objective? List the components you must install and list any special configurations you might need to make.

Glossary

Term	Definition
Binary	A numbering system that uses base 2—that is, ones and zeros
Bridge	A device that's running at the data-link layer of the network. It forwards all frames that it receives. It's used to interconnect LAN segments and is a way to extend a LAN. In the past, bridges were used to interconnect LANs across distances to create WANs, but a bridge isn't ideally suited to this task.
Extranet	Enables an organization to extend its network to other organizations.
Firewall	A device or software component that filters network traffic based on its characteristics and determines whether to allow or block that traffic
Hexadecimal	A numbering system that uses base 16. Numbers 0 through 9 and letters A through F are used to express numbers 0 to 16
Internet	The public network that individuals and organizations widely use to distribute and share information and to support networked services such as email, databases, web browsing
Intranet	A private network that typically consists of multiple subnets
Local area network (LAN)	A collection of networked devices that are relatively close to one another. Typically, a LAN can span devices within a building, or several buildings in close proximity, such as a university campus.
Media access control (MAC) address	A unique 48-bit binary address (usually expressed in hexadecimal) that identifies a network adapter. Typically, the MAC address is the serial number of the network adapter.
Network adapter	A device found in network hosts that connects the host to the network infrastructure via wiring or wireless protocols

Term	Definition
Protocol stack	The protocol stack takes messages from applications and packaging and addressing them for transmission to remote hosts. At the remote end, the protocol stack handles passing the received data up the stack to the appropriate application.
Router	An internetwork device that propagates and receives network packets at layer 3 of the OSI reference model. Routers enable network administrators to separate networks into distinct subnets to help manage network traffic. You can also use routers to join remote LANs to create WANs. A router is network transport–specific—that's to say, it runs a specific network protocol, such as TCP/IP.
Switch	A wiring concentrator with advanced software that enables you to change the way frames and packets are handled between devices that are connected to ports on the switch. Layer 2 switches behave like bridges on configured ports. Layer 3 switches emulate router functionality.
Wide area networks (WAN)	Uses network devices and protocols to interconnect devices that potentially span the globe