LESSON

17

Networking

Networking is perhaps the most complex aspect of PC troubleshooting. When you interconnect computers and attempt to transfer information between them, this information is broken down into small pieces, formatted, converted, sent across a network medium, converted again, placed into the correct order, reformatted, and then reassembled. As you can probably guess, these interactions add a significant level of complexity to the entire configuration and troubleshooting process.

As you advance in your career, you are likely to take on more and more responsibilities that relate to networking. As a PC technician, you will likely be required to perform only simple networking tasks, such as installing network cards, drivers, and protocols. However, even these tasks require an understanding of basic networking principles and the features of various networking technologies. In this lesson, we will work on building a strong foundation upon which you can base future networking knowledge.

Goals

In this lesson, you will learn how to identify common networking technologies and the features of those technologies. Additionally, you will learn how to connect systems to a network and troubleshoot network connectivity.

Lesson 17 Portable systems

Skill	A+ Hardware Objective
1. Introducing Networking	6.2 Identify basic networking concepts, including how a network works.
2. Understanding Network Topology	6.2 Identify basic networking concepts, including how a network works.
3. Comparing Ethernet Technologies	6.2 Identify basic networking concepts, including how a network works.
4. Identifying Network Hardware	6.1 Identify the common types of network cables, their characteristics, and connectors.
5. Examining Ethernet Data Transmission	6.1 Identify the common types of network cables, their characteristics, and connectors. 6.2 Identify basic networking concepts, including how a network works.
6. Understanding Network Protocols	6.2 Identify basic networking concepts, including how a network works.
7. Connecting to a Network	1.8 Identify proper procedures for installing and configuring common peripheral devices. Choose the appropriate installation or configuration sequences in given scenarios. 1.9 Identify procedures to optimize PC operations in specific situations. Predict the effects of specific procedures under given scenarios.
8. Connecting to the Internet	6.3 Identify common technologies available for establishing Internet connectivity and their characteristics.
9. Examining Wireless Networking	6.1 Identify the common types of network cables, their characteristics, and connectors. 6.2 Identify basic networking concepts including how a network works.
10. Troubleshooting Connectivity	2.1 Recognize common problems associated with each module and their symptoms, and identify steps to isolate and troubleshoot the problems. Given a problem situation, interpret the symptoms and infer the most likely cause.

Requirements

This lesson requires a PC running Windows 98 or later, a network interface card, and a wireless network interface card.

skill 1 Introducing Networking

A+ Hardware Objective

6.2 Identify basic networking concepts, including how a network works.

overview

Networks are infrastructures designed to support communication between various computing devices. Networks are designed so that users can access shared resources on the network from devices like file servers and printers. Each device capable of communicating on the network is known as a **node**. The nodes communicate with each other by transmitting data over the **network medium,** which may be cabled or wireless.

To understand the interactions that occur in networking, it is important that you understand some basic concepts related to all networking technologies.

Topology defines the network layout **(Figure 17-1)**. In networking, there are actually two topologies with which you should be familiar: **physical topology** and **logical topology**. Physical topology defines the physical layout of the network and how the network devices and cables are physically configured and connected.

Logical topology, on the other hand, describes how the data is passed through the network medium. Network topologies are discussed in greater detail in the next skill.

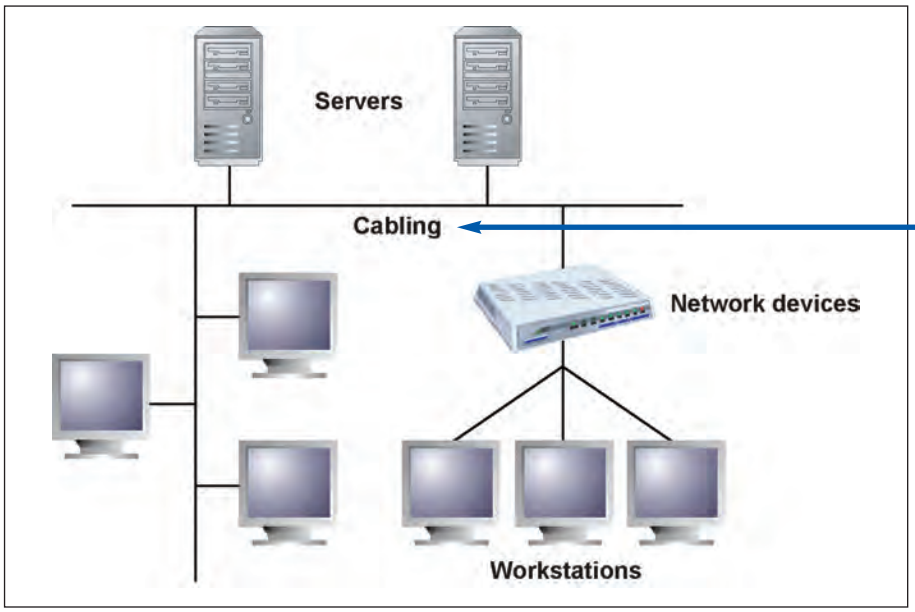
Bandwidth is a term used to describe the maximum theoretical speed of data transmissions over the network medium. Bandwidth is typically measured in bits per second (bps). This means that to arrive at bytes per second (Bps) speed for a network connection, you must divide the bps rate by 8. For instance, a 10 Mbps connection is capable of maximally transmitting 1.25 MBps under ideal conditions.

The terms **baseband** and **broadband** define the communication channels used in the network medium. Baseband communications use the entire communications channel for each data stream **(Figure 17-2)**. This is because baseband communications utilize the entire usable frequency range of the medium to transmit data. This functionality makes baseband devices simpler and generally more cost effective, but does so at the expense of allowing only a single communications channel over the medium. Broadband, on the other hand, divides the frequency range of the medium into distinct channels, allowing multiple communications streams to pass across a single medium simultaneously. This functionality generally increases costs because broadband devices must be capable of selecting different frequency ranges. The advantage of broadband, multiple signals traversing the network medium simultaneously, allows for higher total throughput in many cases. Cable television is an example of broadband communication. In cable television, the data for all channels is transmitted through the medium at the same time, and the cable tuner simply tunes itself to the requested channel, ignoring the other channels.

Regardless of the mechanism used for data transmission, all networking technologies are also defined by the duplex of the connection. **Duplex** defines the ability of the technology to transmit and receive data simultaneously **(Figure 17-3)**. A telephone conversation is an example of duplex communications. **Half-duplex** technologies can only send or receive at any given time. When one device transmits on the channel, all other devices on that channel must receive, similar to a CB radio. **Full-duplex** devices, on the other hand, are capable of both sending and receiving data simultaneously on a given channel, similar to a telephone. In most full-duplex devices, this is accomplished by providing separate signal paths (typically provided by separate cables) for the transmit and receive channels.

Next, all network mediums use some form of **physical addressing**. To understand physical addressing, you must realize that each host on the network must be able to determine if the data they receive is destined for them or is simply passing through on its way to a different host. (A **host** is any device that is active on the network and requires a logical address, such as an IP address.) Without a physical addressing mechanism, each device on a multi-access network would be required to process every data transmission.

Figure 17-1 Network layout



The configuration of the cables and devices constitute the physical topology of this network

Figure 17-2 Baseband vs. broadband

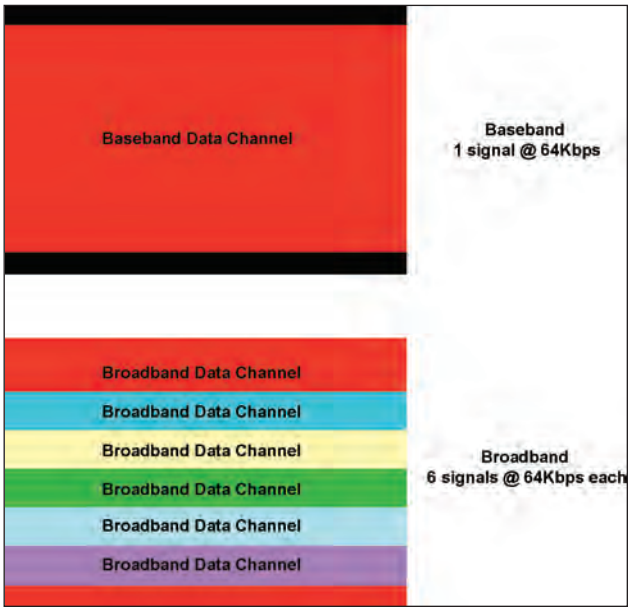
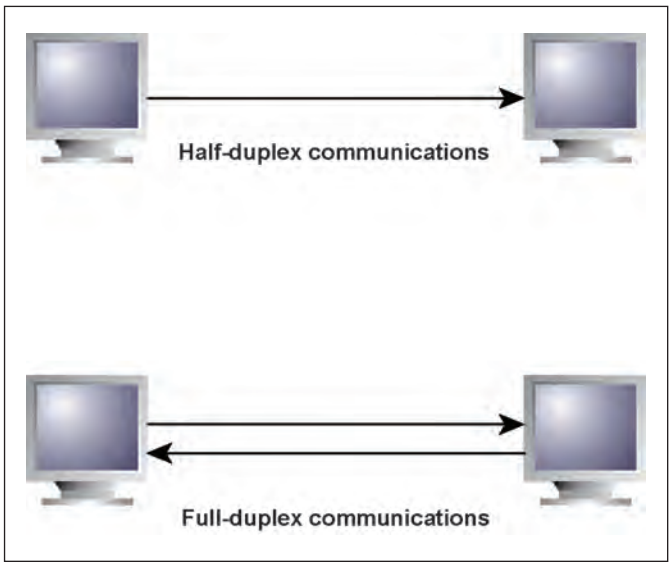


Figure 17-3 Duplex transmission modes



skill 1

Introducing Networking (cont'd)

A+ Hardware Objective

6.2 Identify basic networking concepts, including how a network works.

overview

Finally, **framing** defines how the data in each network communication is divided, reassembled, and formatted. To fully understand this, you must realize a few key points. First, all data sent is sent as an analog signal of some type. In most technologies, this signal is electrical, but in some, light or radio waves are used. This analog signal is converted by the **network interface card (NIC)** to a binary digital representation of the data **(Figure 17-4)**. Of course, the binary representation of the data is useless without formatting. For example, the binary data 0100110100010101110010010101111010101111010101101, is useless without a means or mechanism for determining which portion of that data is the address, which portion is the data, which portion is for error correction, etc. If our formatting divides the data into sections as shown in **Figure 17-5**, we can easily see the purpose of each section of the data.

The rest of the network framing mechanism involves determining how to disassemble the data sent to the NIC and then reassemble the data on the remote receiving host computer. Framing defines the maximum and minimum sizes of these individual units, called **frames**, and the mechanism used to reassemble them along with the mechanism used for detecting and correcting errors in one or more frames.

Figure 17-4 Converting analog to digital

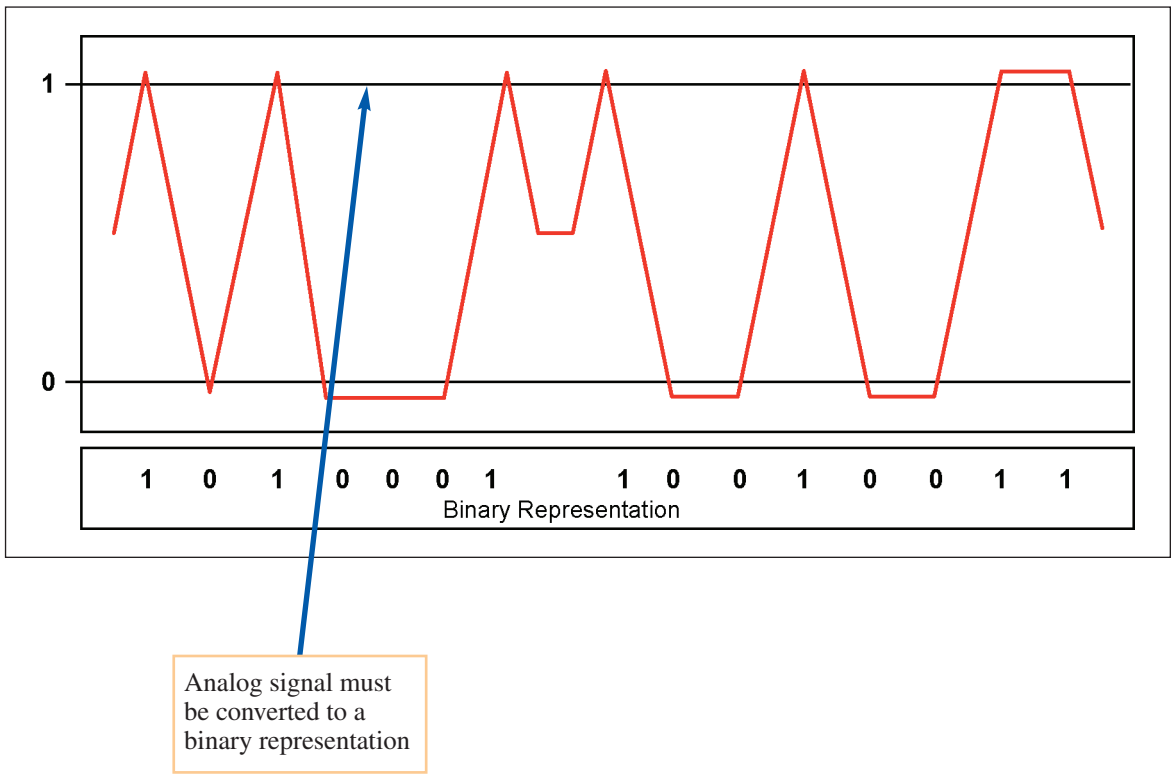
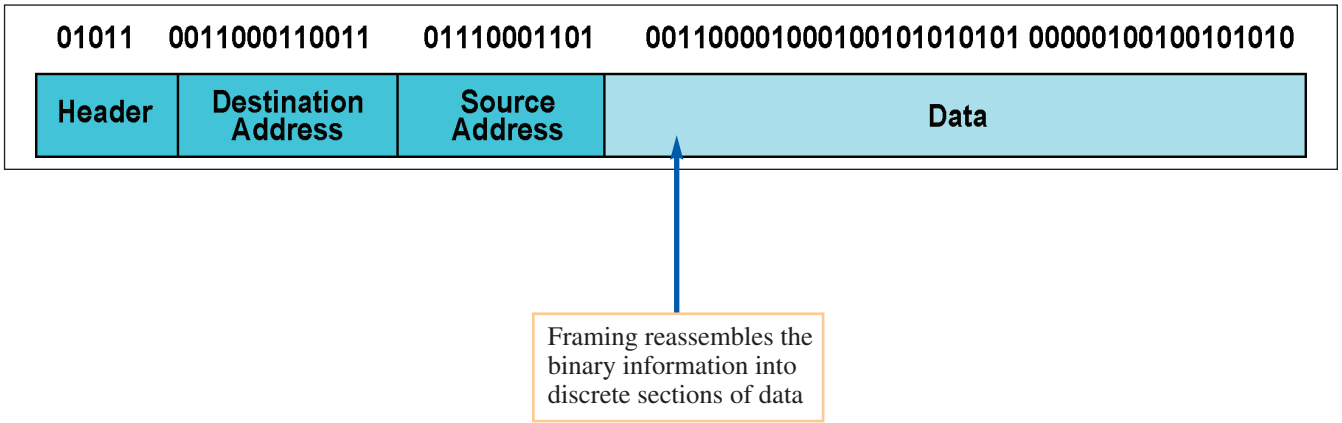


Figure 17-5 Network framing



skill 2 Understanding Network Topologies

A+ Hardware Objective

6.2 Identify basic networking concepts, including how a network works.

overview

As discussed in the previous skill, physical network topologies describe how network hardware, including workstations, servers, and network devices, such as hubs, routers, and cabling, are connected. Various physical topologies are shown in **Figure 17-6**, and described more fully in **Table 17-1**.

A logical topology, on the other hand, describes how data or information flows through the network devices. The two logical topologies we are concerned with are bus and ring. **Bus** topologies are so called because the data transmitted proceeds from the source to all nodes on the network at a set rate **(Figure 17-7)**, regardless of the actual intended recipient. In a **ring topology**, however, the data is passed from node to node in the order of position within the ring in a clockwise direction **(Figure 17-8)**.

Physical and logical topologies, when combined, define how the network operates at a basic level. Networks are typically described using the combination of their physical and logical topologies. For instance, 10base-T Ethernet network is described as a **star-bus topology**, which means that it is cabled in a star configuration, but uses a bus topology for data transfer.

Ethernet is a fairly simple and cheap networking technology. It is also the most prevalent and widespread technology for local area networking. Ethernet operates on a bus or star-bus topology model. What does this mean? Well, **Thicknet** network cable, also known as **10base5**, and **Thinnet** network cable, also known as **10base2**, operate like a series of bus stops. No stop may be skipped, even if there is no data to transmit to those stops. If you send a frame or packet to Computer B from Computer C, that packet will also be transmitted to Computer A and Computer D, as shown in Figure 17-7.

Even though the packet is not destined for the other PCs, due to the electrical properties of the bus architecture, it must travel to all PCs on the bus. This is because, in a physical bus topology, all PCs share the same network cable. Although there may be multiple physical segments of cable, they are all coupled to one another and share the same electrical signal. Also, the electrical signal travels down all segments or paths in the bus at exactly the same rate. For instance, in the previous example, the electrical signal from Computer B will reach Computer A and Computer C at exactly the same time, assuming all cable segment lengths are exactly the same.

Another problem with the physical bus topology is that if a cable breaks, all PCs are affected. This is because a physical bus must have a resistor, called a terminator, placed at both ends of the bus. Failure to do this causes a change in the cable's impedance, leading to problems with the electrical signal. Any break in the cable, at any point, effectively creates two segments, neither of which is properly terminated.

10baseT and 10base2 are both a logical and a physical bus. They are a physical bus because all PCs share a common cable segment. They are a logical bus because every PC in the network receives exactly the same data because the bandwidth is shared.

The star-bus architecture, which is much more prevalent today, operates differently. The star bus is a physical star and a logical bus. The physical star means that all of the devices connected to the network have their own physical cable segment. These segments are generally joined in a central location by a device known as a hub. This device has absolutely no intelligence. Its entire purpose is to amplify and repeat the signals heard in any port out all other ports. This function creates the logical bus required by Ethernet. The advantage of a physical star is that if any one cable segment breaks, only the device on that cable is affected; no other devices are affected by the break. The port the cable is connected to on the hub is inoperative until the cable is repaired or replaced.

tip

Wireless networks also have a physical topology, which describes how devices actually connect to the wireless networks.

Table 17-1 Physical topologies

Topology	Description	Advantages	Disadvantages
Star	All hosts connect to a central device, such as a hub. Each host has its own cable.	Failure of a single cable does not affect other systems.	Increased cabling costs when compared to a bus.
Bus	All hosts connect to a single segment of cable.	Low cabling costs, simple to install.	Cable problems at any point cause the entire segment to fail.
Ring	Hosts connect to a single segment of cable that goes from host to host in a ring.	Equal access to the medium; no host can monopolize the network.	Failure on any node causes the entire segment to fail.
Mesh	All hosts are connected to all other hosts with a dedicated cable.	High speed and redundancy.	Complex configuration and high costs.

Figure 17-6 Physical topologies

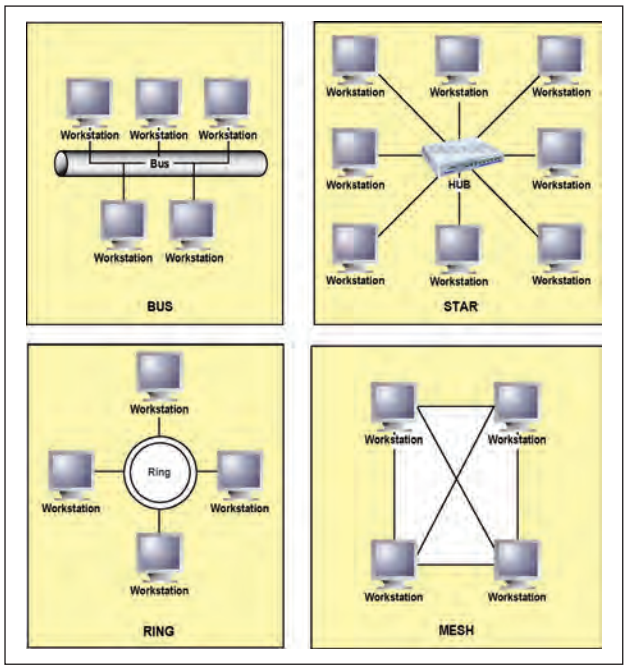


Figure 17-7 Bus topology

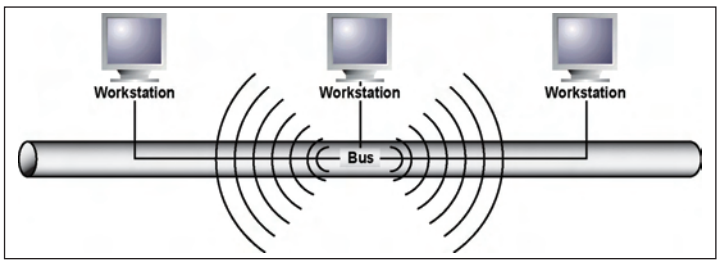
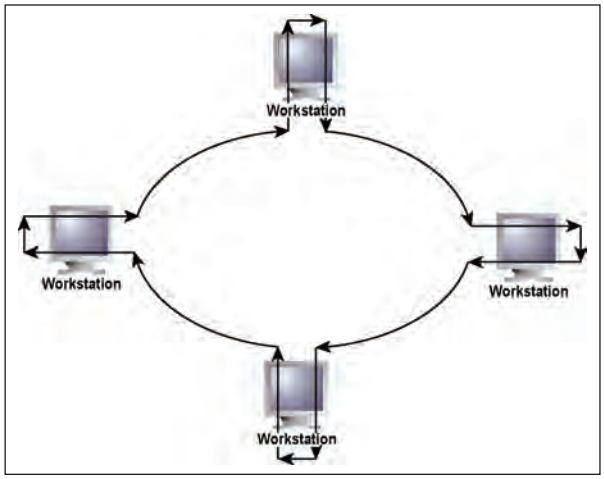


Figure 17-8 A ring topology



skill 2

Understanding Network Topologies *(cont'd)*

A+ Hardware Objective

6.2 Identify basic networking concepts, including how a network works.

overview

As for the logical bus in star-bus Ethernet, it operates exactly as in the physical bus architecture. If a signal is sent to Computer B, from Computer C, it still must be transmitted to Computer A and Computer D. This is demonstrated in **Figure 17-9.**

Token Ring, on the other hand, uses a star-ring topology. In Token Ring, the physical topology is a star, just like 10baseT Ethernet, but the logical topology is a ring. In a ring topology data transits from host to host in order around the ring **(Refer to Figure 17-8)**. Because of this logical topology, each host has equal access to the ring, meaning that all hosts have equal data transmission. Additionally, this topology does not suffer from collisions like a bus based topology. Token Ring uses a star physical topology to allow systems to leave or join the ring at any time without causing connectivity problems for other systems. All systems connect to a Token Ring "hub," known as a Multi-Station Access Unit (MAU), and the MAU forwards the data properly in order around the ring **(Figure 17-10)**.

Fiber Distributed Data Interface (FDDI), however, utilizes a physical and logical ring topology. This means that FDDI systems are wired in a physical ring, and transmit data in a logical ring **(Figure 17-11)**. Because of the physical ring topology of FDDI, disconnecting a system, powering down a system, or a break in the cabling would cause the entire ring to go down. For this reason, most FDDI networks actually utilize a dual ring topology **(Figure 17-12)**. Like Token Ring, FDDI provides equal access to the network and does not suffer from collisions.

Figure 17-9 Star-bus operation

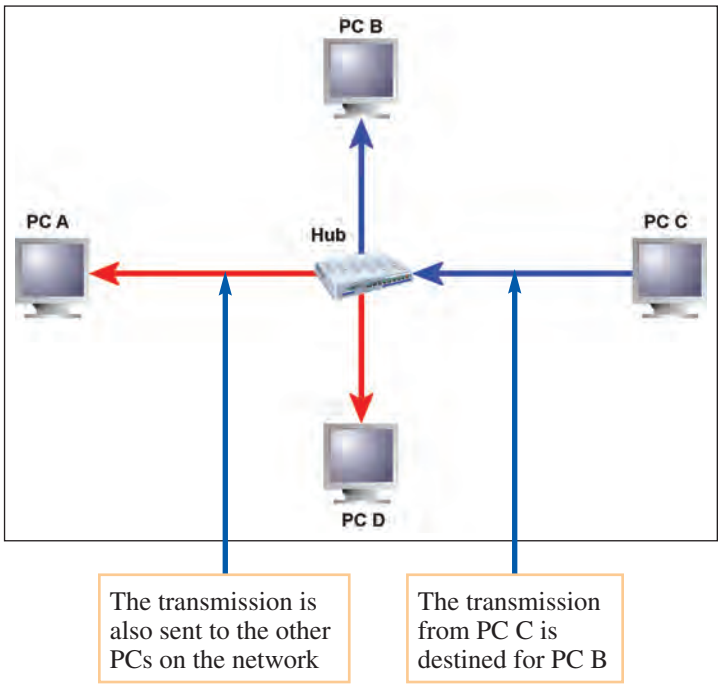


Figure 17-10 Token Ring topology

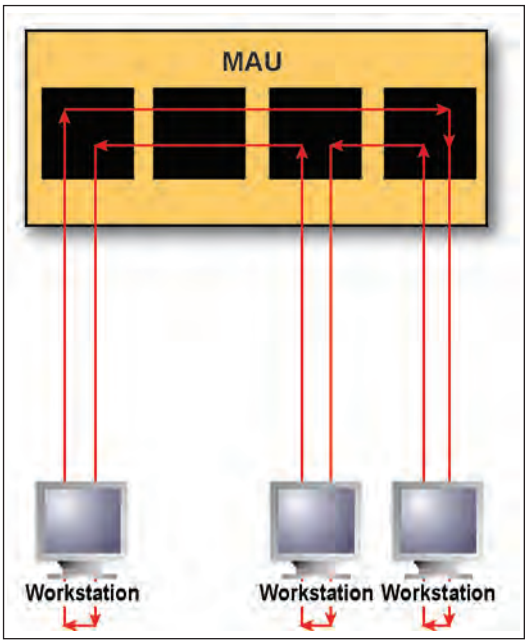


Figure 17-11 FDDI ring topology

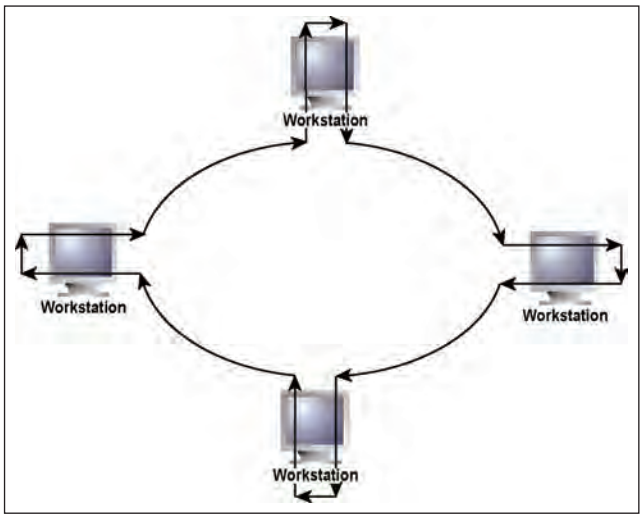
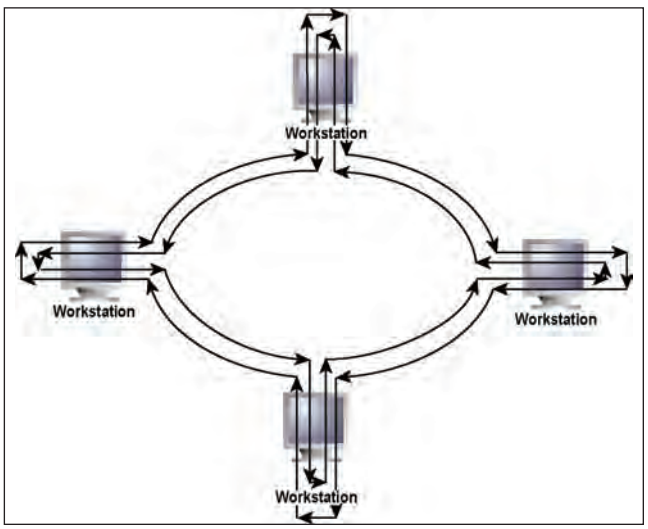


Figure 17-12 FDDI dual ring topology



skill 3 Comparing Ethernet Technologies

A+ Hardware Objective

6.2 Identify basic networking concepts, including how a network works.

overview

In comparing the various standards used for Ethernet networking, it is important to note some key commonalities between all standards.

- **Baseband signaling method**: All common Ethernet technologies use the Baseband signaling method.
- **Speed/base/cable type naming scheme**: All Ethernet specifications conform to the following naming scheme: Speed/Base/Cable Type. Speed is the speed in Mbps. Base stands for baseband, the signaling technology. The cable type is represented with a variety of terms, such as T (for twisted-pair) and 2 (for thinnet coaxial, a .25-inch cable). For example, 10baseT means 10 Mbps, baseband signaling, using twisted-pair cable.
- **5/4/3 rule**: All Ethernet specifications conform to what is known as the 5/4/3 rule. This rule basically states that you can have up to five segments and four repeaters, with no more than three segments populated with users. In star-bus Ethernets, this works slightly differently, but the rule is that no two hosts should be separated by more than four repeaters or five times the maximum segment length in meters of cable.
- **Auto negotiation**: Most Ethernet networks support auto negotiation, which allows the hub or switch to automatically configure the network link to be 10 Mbps or 100 Mbps, full-duplex or half-duplex. However, you should also be aware that the recommended network practice is to configure the duplex manually, because auto negotiation (especially between products from different vendors) has been known to fail.

There are several variants of Ethernet technology that are categorized according to the cabling speed **(Table 17-2)**.

- **10 Mbps Ethernet**: 10 Mbps Ethernet comes in many flavors, the most common of which uses 10baseT cable. All versions of 10 Mbps Ethernet, however, conform to the same standards. The main variations in these types are due to the type of cable used.
- **100 Mbps Ethernet**: 100 Mbps Ethernet, also known as **Fast Ethernet** comes in many varieties, but most varieties only differ in the media supported. Note that 100baseT4 uses all four pairs of cable while 100baseTX only uses two of the four network cable pairs. Also, the distance limitations of half-duplex, Fast Ethernet are due to propagation (broadcast) delay, and may vary according to the types of hubs and switches used.
- **1 Gbps Ethernet**: 1 Gbps Ethernet comes in several varieties, each of which has its own unique requirements. The most common forms of 1 Gbps Ethernet networks are **1000baseT** and 1000baseSX. Note that very few products from any vendor have been designed for 1000baseCX. Also note that 1000baseLH (for Long Haul) is drastically different from the other types in regard to timing constraints.
- **10 Gbps Ethernet**: A new ratified standard for 10 Gbps Ethernet is defined for use with fiber-optic cabling. However, 10 Gbps Ethernet is still rare, and supported by only a few very high-end network devices. You can find out more information about 10 Gbps Ethernet from **http://www.10gea.org.**

Table 17-2 Ethernet standards

Standard	Cable Type	Max Segment Length (m)	Max Overall Length (m)	Max Nodes per Segment	Topology	Capable of Full Duplex?
10 Mbps Ethernet Standards						
10base5	RG-8	500	2500	100	Bus	No
10base2	RG-58 A/U	185	925	30	Bus	No
10baseT	Category 3,4, or 5 UTP*	100	500	2	Star-bus	Yes
10baseFL	Fiber Optic (SM or MM)**	2000	2500***	2	Star-bus	Yes
100 Mbps Ethernet Standards						
100baseTX	Category 5 UTP	100	500 FD**** ~250 HD	2	Star-bus	Yes
100baseT4	Category 3, 4, or 5 UTP, STP	100	~250	2	Star-bus	No
100baseFX	Fiber Optic (SM or MM)	2000	2500	2	Star-bus	Yes
1 Gbps Ethernet Standards						
1000baseCX	STP	25	25	2	Star-bus	Yes
1000baseT	Category 5e UTP	100	200	2	Star-bus	Yes
1000baseSX	Fiber-optic (MM)	550	2750	2	Star-bus	Yes
1000baseLX	Fiber-optic (SM or MM)	550 MM 5000 SM	2750 MM 20,000 SM	2	Star-bus	Yes
1000baseLH	Fiber-optic (Single Mode)	100,000	Varies	2	Star-bus	Yes

* UTP = unshielded twisted-pair; STP = shielded twisted-pair

** SM = single mode; MM = multi mode

*** Due to timing constraints

****HD = half-duplex; FD = full-duplex

skill 4 Identifying Network Hardware

A+ Hardware Objective

6.1 Identify the common types of network cables, their characteristics, and connectors.

overview

NIC: The network interface card (NIC) provides the connection to the physical network for each host. As such, the NIC will be specifically designed to connect to a particular type of network, such as an Ethernet network. Additionally, a NIC typically only supports certain types of cabling. For instance, most Ethernet adapters typically support only a single connection type, such as RJ-45. A few Ethernet adapters will include multiple connection types (such as RJ-45, BNC, and AUI), such as the one shown in **Figure 17-13**, but these are very rare in modern networks. Adapters that support multiple network connection types are commonly called combo cards. Additionally, most Ethernet adapters will have status indicators, most commonly a link indicator and an activity indicator **(Figure 17-14)**. The link indicator simply informs you that the NIC is receiving an Ethernet "heartbeat" signal, which is typically a good sign that the cables are correctly connected. The activity indicator simply shows current network activity. In some 10/100 Ethernet cards (cards that can run at both 10 Mbps and 100 Mbps), you may also have an additional indicator that shows the current link speed (either 10 Mbps or 100 Mbps).

Workstations/Servers: In most networks, the primary distinction between a workstation and a server lies in the hardware and OS employed. Workstations tend to be standard PCs running a client OS, such as Windows XP, while server systems tend to be high-performance systems with large quantities of RAM, storage, and in some cases, multiple processors running a server OS, such as Windows 2003 Server. However, the technical description of the difference in the two is much simpler. A workstation is simply a system that does not host or share resources, while a server is a system that does **(Figure 17-15)**. For example, a file server is a server that shares large quantities of files to be accessed by workstations on the network.

Cabling: Network cabling is primarily defined by the type of cable used **(Figure 17-16)**. While there are numerous types of network cabling, the ones you are most likely to see are:

- Coaxial
- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair (STP)
- Fiber Optic

Each type of cable has distinct advantages and disadvantages **(Table 17-3)**. Coaxial cabling comes in many varieties, but for most network connections, you will likely see either RG8, or RG58A/U. RG8 is the cabling used in "thicknet" Ethernet, or 10base5. It is approximately ½ inch thick, very inflexible, and generally expensive and difficult to install. RG58A/U, on the other hand, is only ¼ inch thick, is very flexible, and is relatively cheap and easy to install. RG58A/U is used for "thinnet" Ethernet, 10base2 **(Figure 17-17)**. All types of coaxial cables are so named because they include two conductors, one in the center of the cable, and one before the outer layer of sheathing. The center conductor is typically solid copper wire, while the outer conductor is usually a mesh made from fine copper wiring. Due to the cable arrangement of coaxial cabling, it fairs reasonably well against Electromagnetic Interference (EMI).

UTP, on the other hand, uses either four or eight conductors twisted around each other along the length of cable. UTP also comes in several different varieties, known as categories. In general, each category is defined by the size of the conductors, quality of the conductors, and number of twists in the cable per foot. Category 3 is the lowest category of cabling generally used for data transmission, and is only recommended for transmission rates of 10 Mbps or lower. Category 5 cabling is perhaps the most common cabling installed in Ethernet networks, and is recommended for transmission rates up to 100 Mbps. Category 5e is an enhanced version of Category 5 cabling, and can be expected to support gigabit Ethernet (1Gbps). Finally, Category 6 is a mostly unused category of cabling that is designed to provide more bandwidth support than Category 5e.

Figure 17-13 Combo card

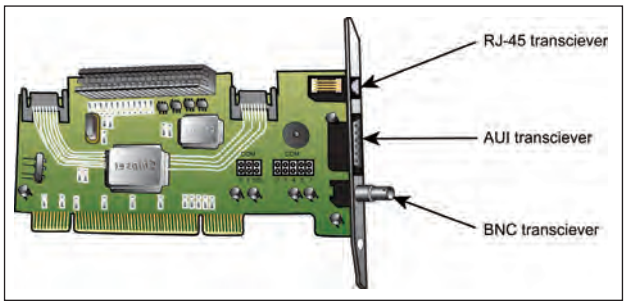


Figure 17-14 Status indicators on Ethernet

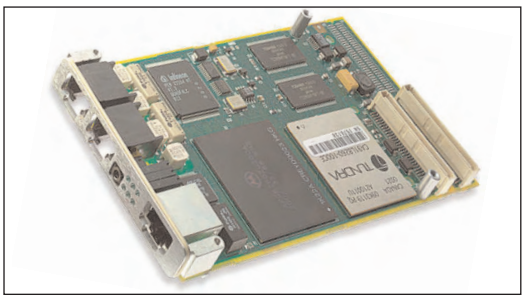


Figure 17-15 Workstations

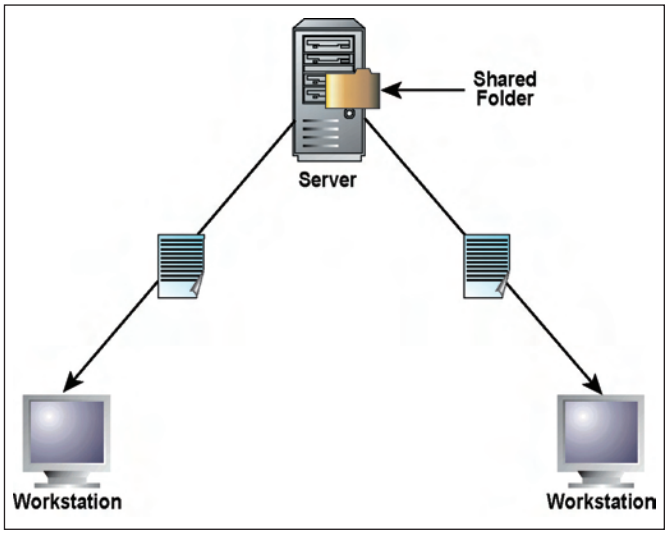


Figure 17-16 Network cabling

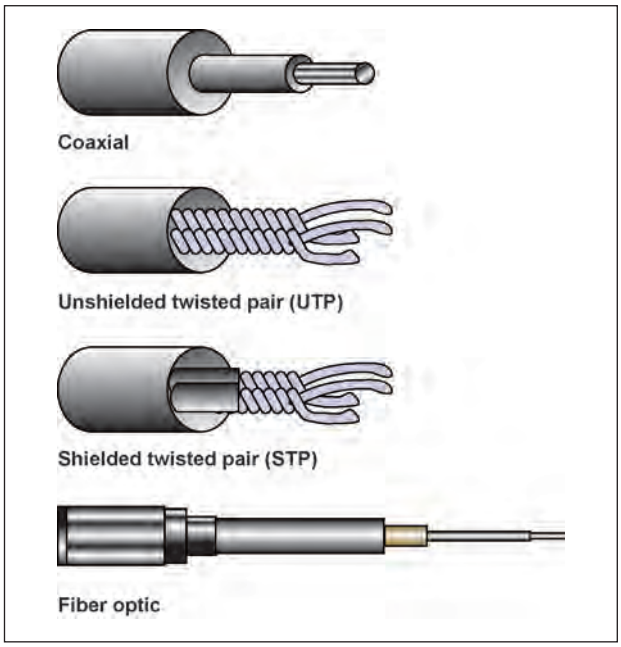


Figure 17-17 Coaxial cabling

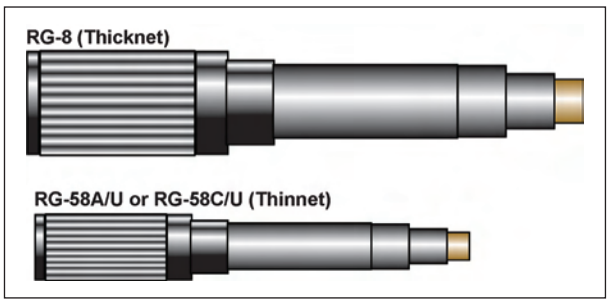


Table 17-3 Ethernet cabling

Cable Type	Maximum Speed	Duplex	Topology	Benefits	Drawbacks
UTP (unshielded twisted-pair)	1 Gbps (Cat 5e cable)	Both	Star-bus	Easy to install, cheap, plentiful, wide support	Moderately susceptible to electromagnetic interference (EMI)
Thicknet coaxial (RG8)	10 Mbps	Half	Bus	Long distances, decent EMI resistance	Difficult to install, expensive, hard to find
Thinnet coaxial (RG 58 A/U)	10 Mbps	Half	Bus	Good for fast, temporary connections, decent EMI resistance	Prone to problems
Fiber optic	10 Gbps	Full	Star-bus	Very, very fast, extremely long distances, immune to EMI	Somewhat difficult to install, can be expensive

skill 4

Identifying Network Hardware (cont'd)

A+ Hardware Objective

6.1 Identify the common types of network cables, their characteristics, and connectors.

overview

However, there are currently no Ethernet standards that require the use of Category 6 cabling (though it is recommended for Gigabit Ethernet).

All UTP cabling suffers from high susceptibility to EMI, though the higher category cables suffer less than the lower categories. The primary benefits of UTP cabling are the low cost and ease of installation of the cabling. UTP cabling is used for many different forms of Ethernet, including 10baseT, 100baseTX, 100baseT4, and 1000baseT. UTP cabling is also very common in modern Token Ring networks. STP cabling is very rarely seen in modern networks. STP cabling is mostly identical to UTP, with the exception of having an additional conductor used as a shield surrounding the other conductors within the cable. This additional conductor allows STP to withstand EMI much better than UTP, but also makes the cabling much less flexible and more costly. STP is quite common in older Token Ring networks, however.

Fiber optic cabling **(Figure 17-18)** comes is a wide variety of types and sizes, typically listed by the size of the optical fiber in microns. In general, the smaller the core diameter, the more bandwidth the cable supports. However, unless you are working for a telecom company and running fiber for extreme distances (hundreds of miles), you will not need to concern yourself with the size of the core. Multi-mode fiber is the least expensive type of fiber, and consists of a 50 or 65.5 micron plastic core. Multi-mode fiber is the most common type of fiber used in LAN installations, and supports 10 Gbps for distances up to one mile. Single-mode fiber is much more expensive, and uses an 8.5 micron glass core that is very pure to support high bandwidth over hundreds of miles.

The advantages of fiber optic cabling are high speed, complete immunity to EMI, and support for extremely long distances. Multi-mode fiber is reasonably priced and relatively easy to install, while single-mode fiber is extremely expensive and rather difficult to install.

Additionally, all cables are defined by the type of shielding they use. Most cables you will come in contact with are known as plenum cables, because the shielding they use is made from a chemical compound that is approved for installation in ventilation ducting. Polyvinyl Chloride (PVC) cabling is cabling that specifically cannot be used in ducting, as the cable creates deadly chlorine gas when burned.

Crossover cables: Crossover cables are a special type of UTP Ethernet cable where the leads are crossed, sending the transmit end of one side of the cable to the receive end of the other side **(Figure 17-19)**. Crossover cables are used to connect two UTP-based Ethernet hosts without using a hub.

Connectors: Many different connector types have been utilized in networking **(Figure 17-20)**. Most connector types are specific for a particular network technology and cabling specification. The connector types you are expected to be familiar with are:

- Bayonet Neill Concelman (BNC): Used with 10base2 and 10base5 networks.
- Registered Jack 45 (RJ-45): Used with most varieties of UTP.
- Attachment Unit Interface (AUI): Used with some Ethernet networks to connect an external transceiver to the NIC. Very rare in modern networks.
- ST/SC: Used for fiber-optic connections. ST connectors use a BNC-style twist-on connector and are round in shape, while SC connectors use a push/pull style and are square in shape. ST connectors are no longer recommended for new installations.
- Universal Data Connector (UDC): Also known as an IBM Data Connector (IDC) and IBM type-1 connector, these connectors are hermaphroditic, meaning that they do not utilize the standard male/female connector pairs. Each connector can directly mate to any

Figure 17-18 Fiber optic cable

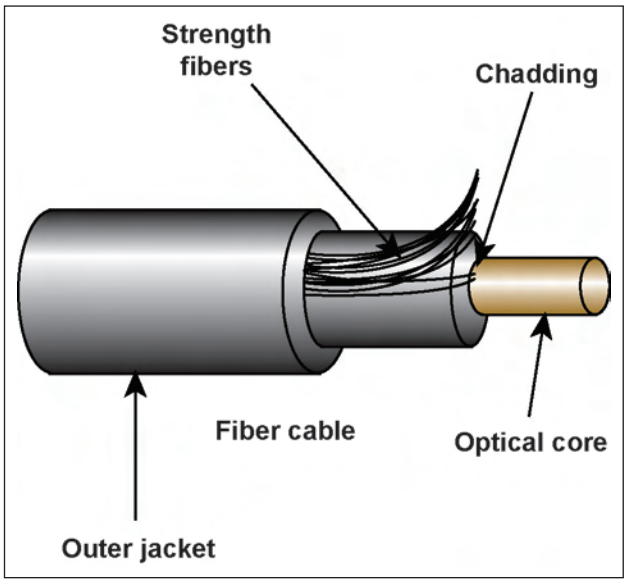


Figure 17-19 Crossover cables

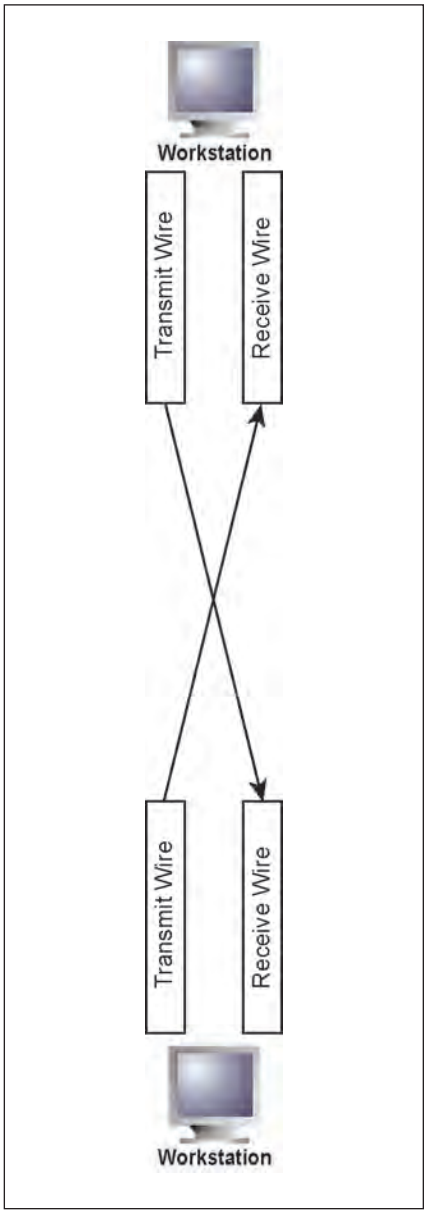
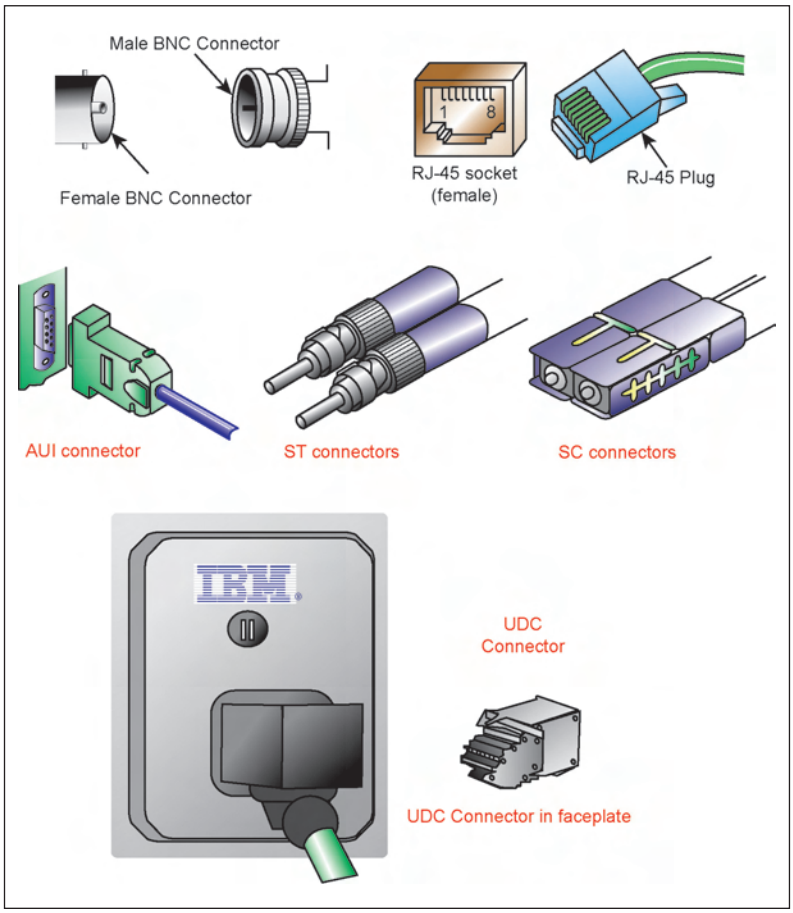


Figure 17-20 Cable connectors



skill 5 Examining Ethernet Data Transmission

A+ Hardware Objective

6.1 Identify the common types of network cables, their characteristics, and connectors.
6.2 Identify basic networking concepts, including how a network works.

overview

other connector. These connectors are extremely rare, and are typically only seen in older Token Ring networks.

Ethernet operates at various transmission speeds, from 10 Mbps (megabits per second) to 10 Gbps (gigabits per second). The common speed currently used on most networks is 100 Mbps, though you must take this speed with a grain of salt. Because of data collisions, the use of half-duplex mode, the best average sustained data rate attainable at this network speed is around 60 Kbps.As discussed earlier in this lesson, Ethernet operates at one of two transmission modes: half- or full-duplex.

- **Half-duplex:** At half-duplex, you can either send or receive at any given instant, but not both. This means that if another device is currently sending data (which you are receiving), you must wait until that device completes its transmission before you can send. This also means that collisions are not only possible, but likely. Imagine half-duplex Ethernet as a single-lane road. Then imagine packets as city buses screaming down the road. If one is coming toward you, and your bus is screaming toward it, there will be a collision **(Figure 17-21)**. This results in the loss of both buses, or network packets.
- **Full duplex:** Full-duplex Ethernet solves this dilemma by allowing a two-lane road. With full-duplex, you can send and receive at the same time. This is accomplished by using separate physical wires for transmitting and receiving. However, this requires that the hub support full-duplex, as it must do a bit of a juggling act. In full-duplex, whenever something comes in to the hub from a transmit pair, the hub must know to send that signal out to all receive pairs. Generally, today's hubs have a small buffer (512 KB to 1 MB) in case the hub is overloaded with traffic. Full-duplex communication is also accomplished between two devices by using a cable known as a crossover cable. A crossover cable is a cable in which the send and receive wires are crossed or flipped, so that the send on one end goes to the receive on the other. This is very similar to a lap link cable. In this scenario, no hub is needed. All networks use addressing schemes in order to deliver data to the intended recipient. Ethernet utilizes **MAC (Media Access Control) Addresses** for its addressing structure. MAC addresses are 12-digit hexadecimal addresses that are unique for each Ethernet device **(Figure 17-22)**.

The data is sent in segments called frames, and whenever you send an Ethernet frame, the first two fields in the frame header are the destination MAC address and the source MAC address. These fields must be filled in. Using Ethernet, although every client normally receives every frame (due to the logical bus topology), the host will not process any frame whose destination MAC address field does not equal their own. There are two exceptions to this rule, however. The first is a **broadcast**, and the second is called **promiscuous mode**.

- **Broadcast mode:** If the MAC address of the intended recipient is unknown, or if the message is delivered to all hosts on the network, then a special MAC address, called a broadcast address, is used. The broadcast address is all Fs or FF-FF-FF-FF-FF-FF. The reason behind broadcasting is that sometimes you need to send a message to all PCs. Generally, only one PC actually needs the message, but you have no idea which PC that is. So you send the frame to all PCs, and the PC that actually needs to receive the frame will respond. The rest of the PCs will discard the frame. The downside to broadcasts is that they require processing on every machine in the broadcast domain and can waste bandwidth on networks.
- **Promiscuous mode:** When a NIC is placed in promiscuous mode, it keeps all frames, regardless of the intended destination for that frame. Usually, this is done so that you can

tip

Full-duplex communication cannot be accomplished on a physical bus topology (such as with 10base2 or 10base5).

Figure 17-21 Half-duplex collisions

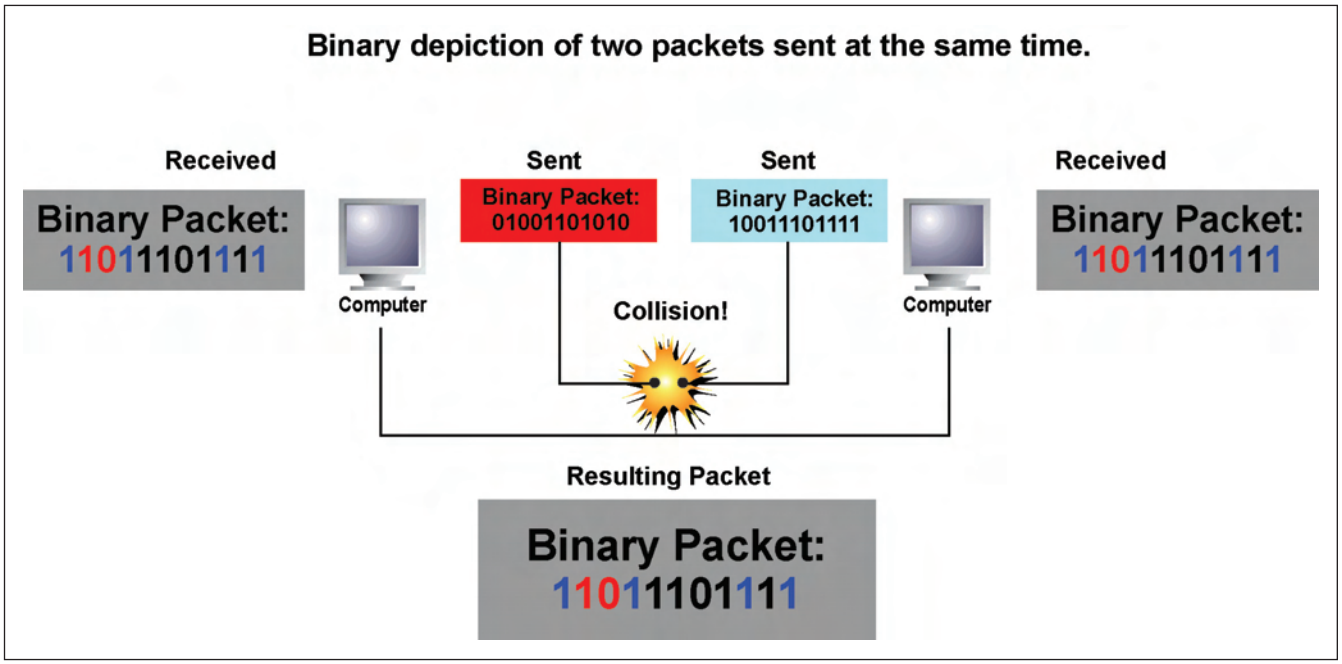
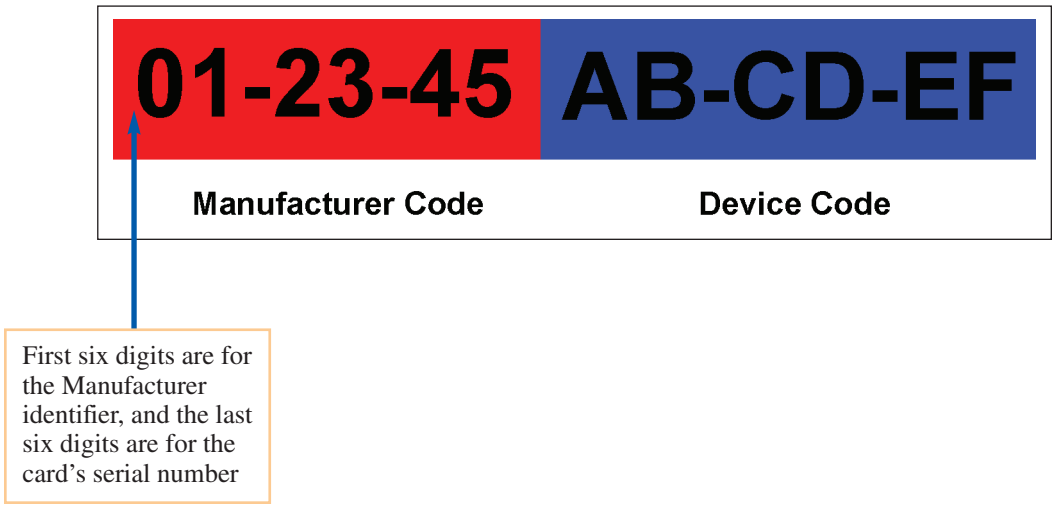


Figure 17-22 MAC addressing



skill 5

Examining Ethernet Data Transmission (cont'd)

A+ Hardware Objective

6.1 Identify the common types of network cables, their characteristics, and connectors.
6.2 Identify basic networking concepts, including how a network works.

overview

analyze each individual packet. Analyzing packets can be performed using a device known as a network analyzer (more commonly called a sniffer). A sniffer is extremely useful. If you understand the structure of a frame and the logic and layout of the PDUs (protocol data units; a fancy way of saying packets), you can troubleshoot and solve a great many seemingly unsolvable network problems in a very short time. However, sniffers also have a bad reputation, because they can also be used to view and analyze data that you aren't supposed to see (such as unencrypted passwords).

Note that full-duplex communication cannot be accomplished on a physical bus topology such as with 10base2 or 10base5. **Arbitration** is the method of controlling how multiple hosts can access the wire, and specifically, what to do if multiple hosts attempt to send data at the same instant. Because multiple devices can potentially send at the same time and cause data errors, all half-duplex mediums are required to use an arbitration mechanism. Although there are several arbitration mechanisms in use today, the most common one used is the **Carrier Sense Multiple Access (CSMA)**, which is used by a number of technologies, including Ethernet, WLANs, and LocalTalk. The CSMA technique relies on the ability of each host to sense when a signal is being sent, informing the node that another node is transmitting. Ethernet uses Carrier Sense Multiple Access With Collision Detection (CSMA/CD) as an arbitration method **(Table 17-4)**.

Although the entire Ethernet specification uses CSMA/CD as an arbitration method, it is needed only for half-duplex operation. In full-duplex environments, there are no collisions, so CSMA/CD is disabled.

Ethernet **repeaters (Figure 17-23)** are devices that repeat the signal sent to them onto multiple segments of the network cable. The simplest type of repeater is a passive repeater, which essentially splices multiple segments of cable together and significantly reduces the overall signal strength. Passive repeaters, however, are obsolete. Modern repeaters are active repeaters, which increase or amplify the strength of the incoming signal before sending the signal out multiple ports. All repeaters, regardless of type, repeat the signal heard on one port out all ports. Hubs are an example of a repeater.

Although older repeaters amplified the incoming signal, this technique results in a reduced signal-to-noise ratio (SNR) for each repeater the signal passes through. In modern repeaters, the signal is actually buffered and re-created before being repeated, which essentially results in a new signal. However, you should remember that each repeater reduces the SNR of the signal, despite this fact.

Layer 2 Ethernet switching (also known as **transparent bridging**) is actually a fairly simple concept. Unlike a hub, an Ethernet switch processes and maintains a record of the MAC addresses used on a network and builds a table (called a channel access method, or CAM) linking these MAC addresses with ports. It then forwards an incoming frame out of the port specifically associated with the destination MAC address in the frame. It builds its CAM table by listening to every transmission occurring on the network and noting which port each source MAC address enters through. Until the CAM table is built, it forwards the frame out of all ports except the originating port, as it doesn't yet know which port to send it to. This is known as flooding **(Figures 17-24** through **17-26)**.

The major benefit of switching is that it separates, or logically segments, your network into collision domains. A **collision domain** is defined as an area in which collisions can occur.

Table 17-4 Carrier Sense Multiple Access with Collision Detection (CSMA/CD)	
Carrier Sense	Before sending data, Ethernet listens to the wire to determine if other data is being transmitted. Picture multiple phones hooked to the same phone line. If you pick it up and hear someone else talking, you must wait until they finish. If not, you can use the line. This is what Ethernet does.
Multiple Access	Multiple machines have the ability to use the network at the same instant in time, leading to collisions.
Collision Detection	Ethernet can sense when a collision has occurred and resend the data.

Figure 17-23 Repeater

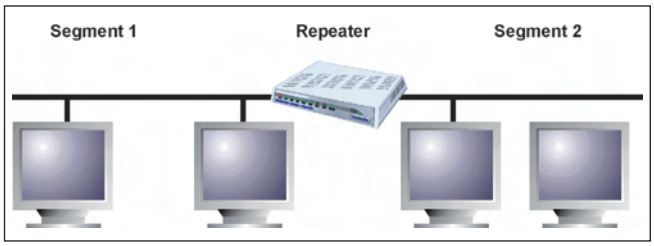
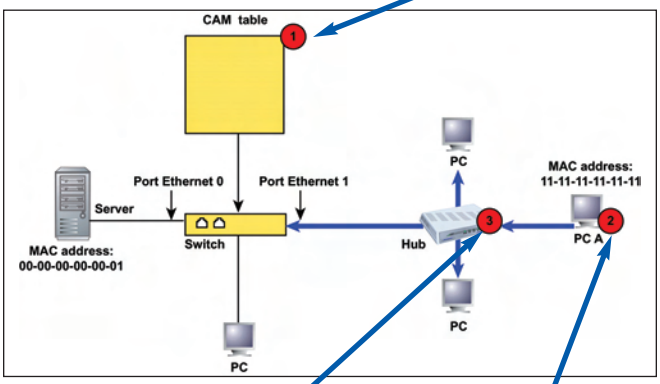


Figure 17-24 Switching - I

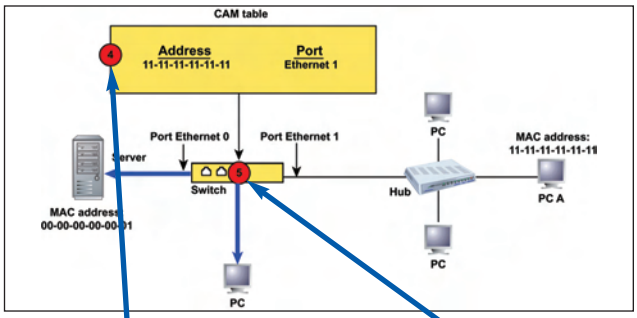
Switching configuration directly after powered on: The switch starts with a blank CAM table



The hub repeats the frame out to all ports

PCA sends a frame destined for the server to its local hub

Figure 17-25 Switching - II



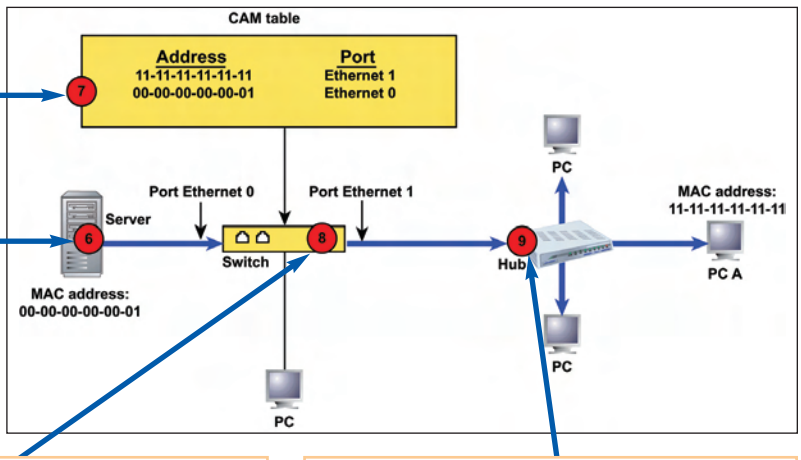
The switch adds the source address to its CAM table

The switch cannot find the destination address in its CAM table, so it forwards the data to all ports except for the originating port

Figure 17-26 Switching - III

The switch adds the server's MAC address to the CAM table

The server responds



The switch looks up the MAC address and forwards the packet out Ethernet Port 1

The packet reaches the hub, which repeats the frame out to all ports

skill 5

Examining Ethernet Data Transmission (cont'd)

A+ Hardware Objective

6.1 Identify the common types of network cables, their characteristics, and connectors.
6.2 Identify basic networking concepts, including how a network works.

overview

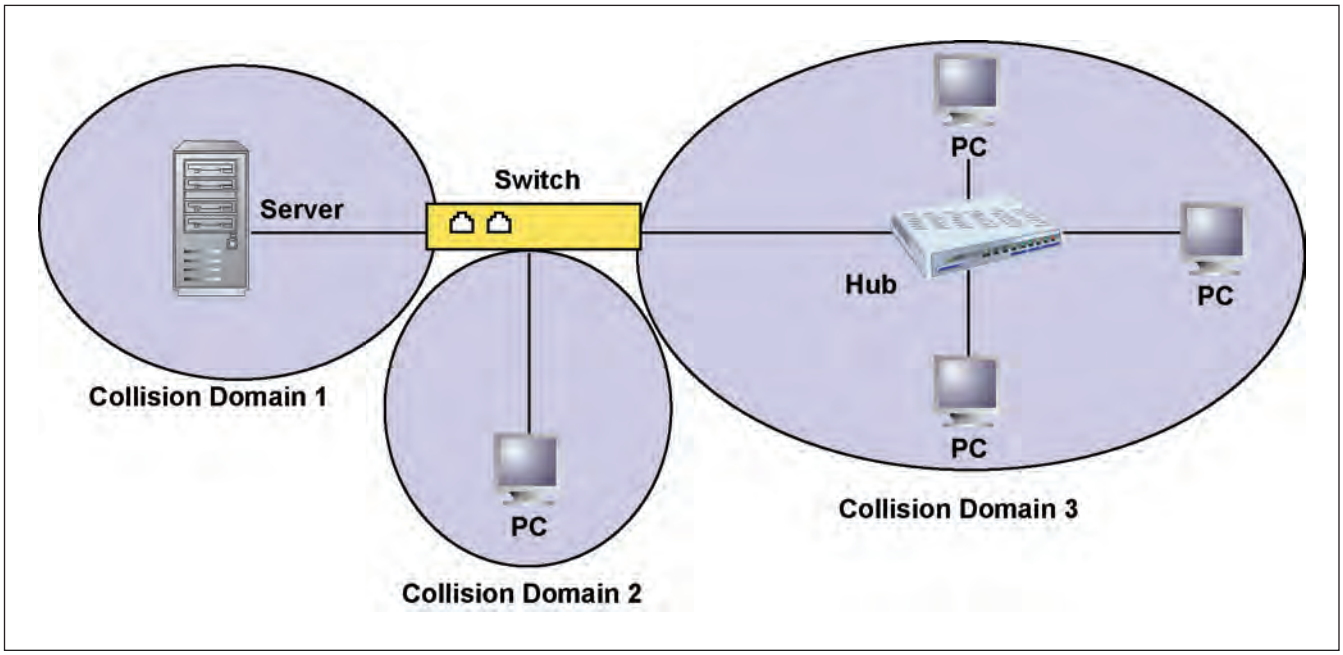
If you are in a given collision domain, the only devices that your frames can collide with are devices in the same collision domain.

Segmenting a network into collision domains provides two main benefits. The first is obviously a reduction in the number of collisions. In **Figure 17-27**, it is very unlikely that there will ever be a collision in collision domain 1 or 2, as only one device is residing in these domains. You are only able to collide with the host you are directly transmitting to at any given time). This benefit cuts collisions on this network by 40 percent, as now only three PCs (all on collision domain 3) are likely to have a collision. In addition, segmenting the network with a switch also increases available bandwidth. In Figure 17-27, if the central switch is replaced with a hub, returning the network to one collision domain, there is only 1.2 Mbps of bandwidth available to each device (assuming 10 Mbps Ethernet links). This is because all devices connected to the hub have to share the same bandwidth. If one device is sending, all the rest must wait before sending. Therefore, to determine the available bandwidth in one collision domain, you must take the maximum speed (only around 6 Mbps is possible with 10 Mbps Ethernet, due to frame size and gaps between the frames) and divide it by the number of hosts (5). However, using a segmenting switch, each collision domain has a full 6 Mbps of bandwidth. So the server in collision domain 1 and the PC in collision domain 2 can both transmit a full 6 Mbps speed. The three PCs in collision domain 3, however, can transmit at only 2 Mbps.

more

When sending a frame, Ethernet will listen to its own frame for the first 64 bytes just to make sure that it doesn't collide with another frame. The reason it doesn't listen to the entire transmission is because by the time the sixty-fourth byte is transmitted, every other machine on the network should have heard at least the first byte of the frame, and therefore will not send. The time this takes is known as propagation delay. The **propagation delay** on standard 10 Mbps Ethernet is around 51.2 microseconds. On 100 Mbps Ethernet, this drops to 5.12 microseconds. This is where distance limitations involved with timing begin to appear in Ethernet, because if your total cable length on a logical Ethernet segment (also known as a collision domain) is near or greater than the recommended maximum length, you can have a significant number of late collisions. Late collisions are collisions that occur after the slot, or 64 byte time in Ethernet, and are therefore undetectable by the sending NICs. This means that the NIC will not retransmit the data and the client will not receive it. In any case, assuming a collision that is detectable by the NIC occurs, the NIC waits a random interval (so that it does not collide with the other station yet again), and then resends the data. It does this up to a maximum of 16 times, at which point it gives up on the frame and discards it.

Figure 17-27 Example network segmentation



skill 6 Understanding Network Protocols

A+ Hardware Objective

6.2 Identify basic networking concepts, including how a network works.

overview

Protocols are similar to languages that define the network communication. Although numerous protocol suites have been defined, the ones you will most likely encounter are **Transmission Control Protocol/Internet Protocol (TCP/IP)**, Internetwork Packet Exchange/Sequenced Packet Exchange (**IPX/SPX**, also known as NWLink), and **NetBIOS** Extended User Interface (NetBEUI). TCP/IP is by far the most commonly used network protocol for both private **local area networks (LANs)** and public **wide area networks (WANs)**. Nearly every OS supports TCP/IP, and TCP/IP is the de facto protocol supported on the Internet. TCP/IP is a robust, medium-sized, and scalable protocol, and is controlled by public committees. The fact that TCP/IP is controlled by public entities is perhaps its biggest advantage, because anyone can extend the protocol suite if they are willing to write a proposal for the change and submit it in the form of a Request for Comments (RFC). This fact is one of the primary reasons that TCP/IP is used as the protocol suite for the World Wide Web.

TCP/IP consists of many individual protocols responsible for different tasks within the suite. Some of the more common protocols in the TCP/IP suite are:

- **IP:** The addressing protocol for TCP/IP is the Internet Protocol (IP). IP defines the format and structure of logical addressing for the TCP/IP suite. The current version of IP, version 4, defines IP addresses as 32-bit addresses composed into four octets represented decimally **(Figure 17-28)**. This 32-bit address space provides for roughly 4 billion host addresses, which is now woefully inadequate. For this reason, the newest version of IP, version 6, supports an address space 128 bits long represented as 32 hexadecimal digits **(Figure 17-29)**. This address space supports 2^{128} addresses, for a total of 3.4×10^{38} addresses, which is more than enough addresses to last a lifetime. IPv6 is not expected to be in widespread use for several years.
- **TCP:** The Transmission Control Protocol is the transport protocol responsible for session establishment, error correction and retransmission. TCP ensures that lost data is retransmitted, and that it is reassembled in the proper order.
- **UDP:** The User Datagram Protocol is another transport protocol within TCP/IP, but unlike TCP, UDP only provides a "best effort" transport service, and does not guarantee that data is received at all. UDP is commonly used for real-time data transmissions where low overhead is needed and the retransmission functions of TCP are not required (such as live multimedia applications).
- **ICMP:** The Internet Control Messaging Protocol is primarily an error notification protocol that also has a number of other uses. ICMP is responsible for reporting transmission problems, such as when a destination is not reachable. ICMP is also the protocol responsible for issuing ECHO and Time Exceeded messages used in the commonly used connectivity testing utilities **ping** and **tracert**.
- **DHCP:** The **Dynamic Host Configuration Protocol** is used to allocate IP addresses to clients in a dynamic fashion, reducing configuration requirements for each client. A DHCP server is provided with a scope (range of IP addresses) to allocate to clients. When a client requests an address, the DHCP server allocates, or leases, the addresses on a first-come first-served basis and keeps track of which addresses are used.
- **DNS:** The **Domain Name System** is a hierarchical naming system designed to provide a scalable, distributed naming scheme. DNS utilizes **fully qualified domain names (FQDNs)** to describe the full path to a host **(Figure 17-30)**. DNS servers are used to resolve FQDNs into IP addresses (and vice versa).
- **HTTP:** Hypertext Transfer Protocol is perhaps the second most widely used protocol on the Internet, after the Simple Mail Transfer Protocol (SMTP). HTTP is responsible for transferring Hypertext Markup Language (HTML) documents to browsers, and is also partially responsible for the formatting of those documents.

Figure 17-28 IP v4 address format

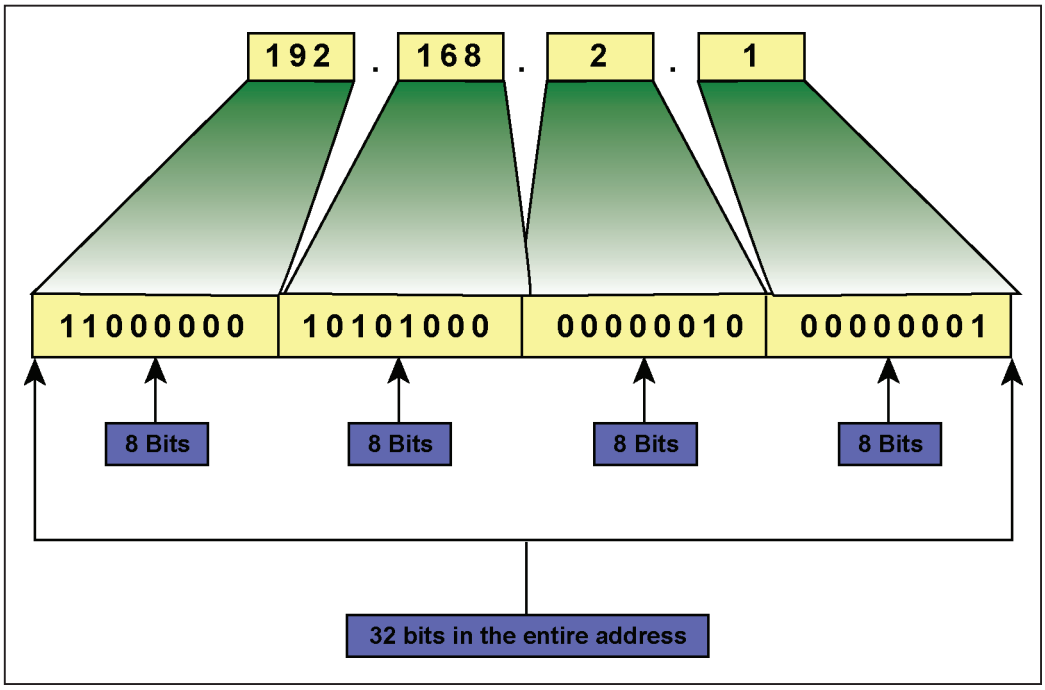


Figure 17-29 IP v6 address format

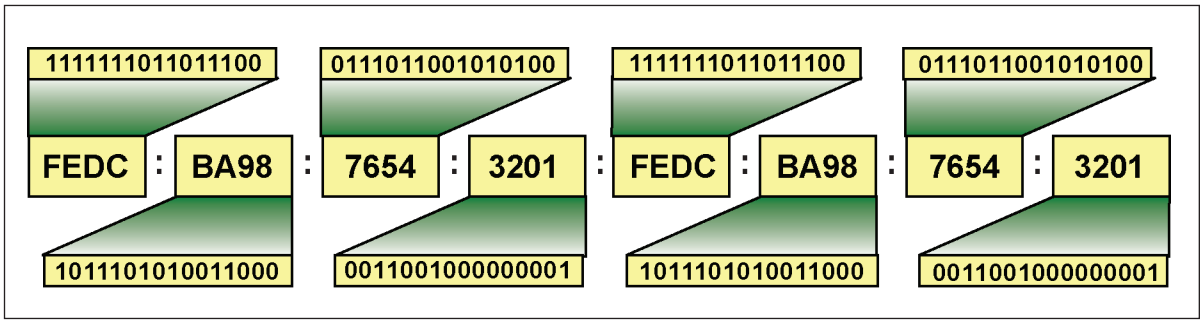
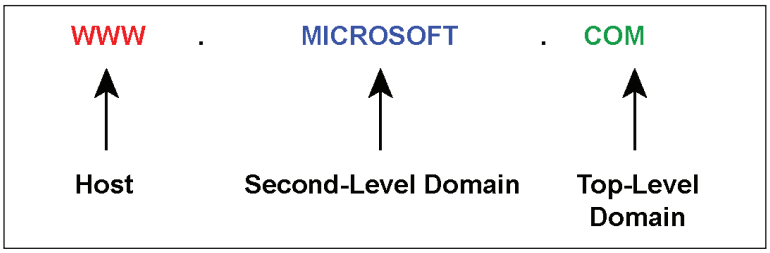


Figure 17-30 An FQDN



skill 6

Understanding Network Protocols (cont'd)

A+ Hardware Objective

6.2 Identify basic networking concepts, including how a network works.

overview

- **FTP:** The File Transfer Protocol is a commonly used protocol with one purpose: transferring and managing file and folder structures. FTP supports simple authentication mechanisms to help protect files, and allows users to create, delete, copy, and move files and folders.
- **POP3:** Post Office Protocol version 3 is responsible for logging users into mail servers and ensuring that users access the correct mailbox. Contrary to popular belief, POP3 does not transfer e-mail, it simply logs the user in. SMTP is used to transfer the e-mail.
- **SMTP:** Simple Mail Transfer Protocol is responsible for transmitting and receiving e-mail, making it a widely used protocol on the Internet. SMTP is capable of transmitting only plain text, though other standards allow other types of data to be converted into text from transmission via SMTP.

tip

Do not confuse NetBIOS with NetBEUI. NetBIOS is simply a naming convention, while NetBEUI is a protocol suite. While NetBEUI is based off of the NetBIOS naming convention, NetBEUI is still a full protocol suite.

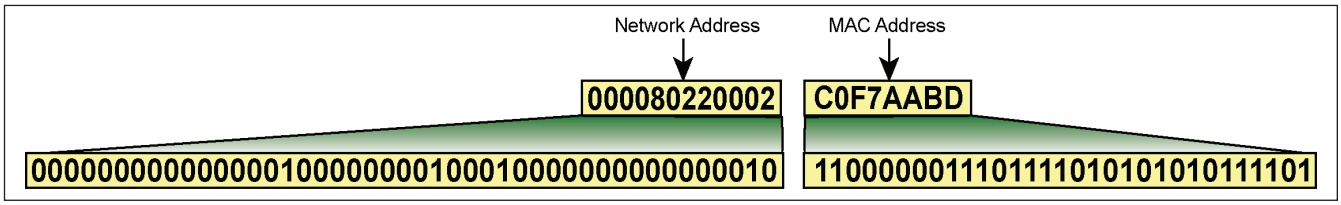
These protocols are provided for reference purposes, but even with this short list, you can see some of the variety included in the TCP/IP suite. In contrast to the vendor independence of TCP/IP, IPX/SPX is a vendor-specific protocol used primarily with the Novell NetWare platform. Although IPX/SPX can be used in environments consisting purely of Windows clients, in practice this type of configuration is rare.

In many ways, IPX/SPX is perhaps even more scalable than TCP/IP, and it is without a doubt more user friendly. IPX is the addressing protocol in the IPX/SPX suite, and IPX addresses are 80-bit addresses written in hexadecimal **(Figure 17-31)**. This address space allows for approximately 12 x 10^{23} total addresses, which is a significantly larger address space than IPv4 provides. However, because IPX/SPX is vendor-specific, it has proven to be much less versatile and extensible than TCP/IP.

IPX/SPX client configuration is generally dynamic, and occurs without user intervention. In general, you simply load IPX/SPX on a client system to provide IPX connectivity, with no further configuration required. NetBEUI, unlike the previously mentioned protocols, is very limited in terms of scalability. NetBEUI does not include any provisions for routing, which means that it cannot be used to transfer data between networks. This limits NetBEUI to small networks, typically fewer than 100 hosts. In practice, however, NetBEUI is rarely used for networks larger than 20 hosts. NetBEUI, like IPX/SPX, is configuration-free. In fact, NetBEUI has no user configurable settings. You simply load the suite to provide connectivity. This makes NetBEUI a standout choice for very simple networks. Additionally, NetBEUI is a very low overhead suite when used on small networks, making it very fast. However, NetBEUI relies heavily on broadcasts, which makes it prone to collisions on larger, half-duplex Ethernet networks.

Although each protocol suite mentioned in this skill has its own distinct advantages and disadvantages, in general practice, your protocol selection is dependant on the network you are installing the system to. Most modern networks utilize TCP/IP as the only protocol suite, though a few still utilize IPX/SPX. NetBEUI networks are still used somewhat in very small peer-to-peer networks.

Figure 17-31 IPX address format



skill 7 Connecting to the Network

A+ Hardware Objective

1.8 Identify proper procedures for installing and configuring common peripheral devices. Choose the appropriate installation or configuration sequences in given scenarios.

1.9 Identify procedures to optimize PC operations in specific situations. Predict the effects of specific procedures under given scenarios.

overview

Connecting to a network involves installing a network adapter card (NIC) and configuring the appropriate protocols and services to support connectivity.

Installing the network card itself involves the same steps as installing any other adapter. First, you locate a free expansion slot of the required type. Most modern network adapters will be Peripheral Component Interconnect (PCI) devices, but Industry Standard Architecture (ISA) NICs are still available, although rarely used today.

After the adapter is properly installed, you must configure resources for the adapter. In general, this process is automatic with PCI-based adapters. With ISA adapters, however, you need to manually configure the card, utilizing jumpers, DIP switches, or a software utility provided by the manufacturer. Although the network adapter can be configured to use any available IRQ and I/O address, the most common settings for ISA cards are IRQ 5 and I/O address 300h.

Once you configure the hardware resources for the adapter, the drivers for the adapter are next installed. Although Windows automatically installs Plug and Play PCI network adapters, ISA network adapters may need to be manually installed. Installing the drivers for the network adapter follows the same process as installing drivers for any other expansion card.

The final step is physical connectivity and involves physically connecting the adapter to the network media. For Ethernet networks, this is accomplished by connecting the network cable to the appropriate port on the NIC. The Ethernet standards that Ethernet connectors are typically used with are shown in **Table 17-5**. Once the adapter and drivers are properly installed and the NIC is connected to the network medium, you need to configure Windows to support the desired network connectivity. This process involves configuring the appropriate protocols and services.

how to

Configure Windows to support network connectivity.

1. To install a protocol suite, first open the Properties dialog box for your network adapter. In Windows 9x, this is accomplished by right-clicking on the **Network Neighborhood** icon and choosing **Properties**. In Windows 2000/XP, right-click on **My Network Places** and choose **Properties**.
2. Right-click on the desired adapter and choose **Properties.**
3. Once the adapter properties dialog is open (**Figure 17-32**), click the **Install** button and choose protocols in the dialog that appears.
4. Select the appropriate protocol and click **Add**.
5. To configure TCP/IP, navigate again to the Properties dialog box for your network adapter.
6. Click on the Internet Protocol (TCP/IP) component and select **Properties (Figure 17-26)**.
7. In the TCP/IP properties dialog, you see fields for **IP address, subnet mask, default gateway,** and preferred **DNS** server addresses **(Figure 17-33)**. Of these, the only two that are absolutely required for Windows 9x are the IP address and subnet mask. For Windows XP/2000 you need all of them to connect to the Internet. If you are using DHCP in your network, select the option to obtain addresses and DNS settings automatically. This setting allows the client to request an IP address from a DHCP server.
8. Additionally, if you want to connect to other networks (including the Internet), you must configure the default gateway field, which points your PC to a router, enabling it to reach other networks. Finally, if you want to resolve FQDNs, you will need to enter at least one DNS server address. Entering a secondary DNS server address provides for redundancy in case the first DNS server is unreachable.

Figure 17-32 Adapter Properties (Windows XP)

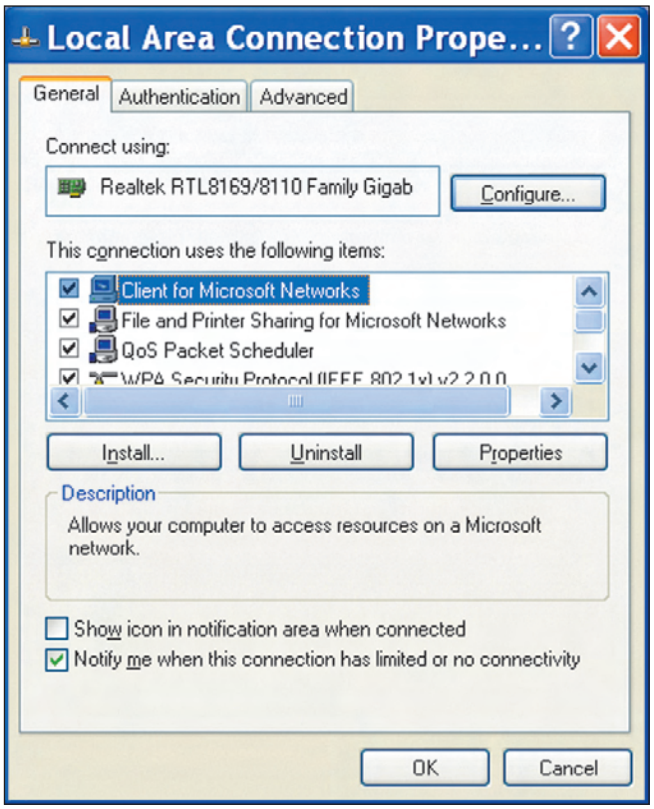
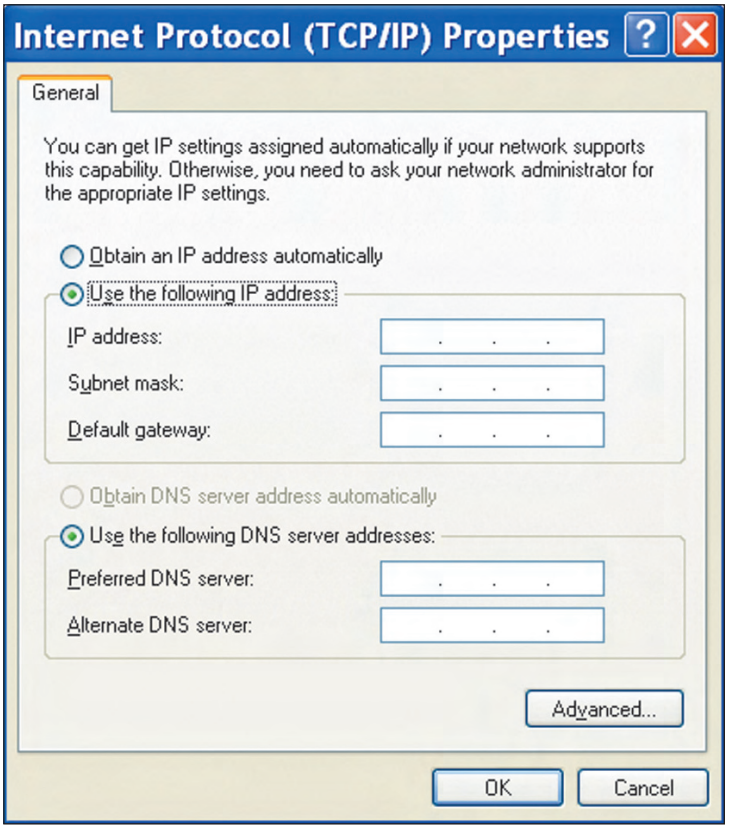


Figure 17-33 IP Properties dialog box (Windows XP)



skill 7

Connecting to the Network (cont'd)

A+ Hardware Objective

1.8 Identify proper procedures for installing and configuring common peripheral devices. Choose the appropriate installation or configuration sequences in given scenarios.

1.9 Identify procedures to optimize PC operations in specific situations. Predict the effects of specific procedures under given scenarios.

more

Once you have installed and configured the appropriate protocol suite or suites, you should ensure that the appropriate network services are installed on the system. Each Windows host can be configured with a variety of network services, but for this discussion, only two are of importance: the server service and the workstation service. The server service is the service that is used to provide shared resources to clients. To share a resource, the server service must be enabled. The server service is installed in the same manner as protocol suites, via the adapter properties. In this dialog, the server service is listed as File and Print sharing for Microsoft Networks.

The workstation service (also known as the redirector), on the other hand, allows you to connect to remote shared resources. Like the server service, the workstation service is installed through the adapter Properties dialog box. The workstation service is listed as Client for Microsoft Networks in the adapter properties.

Table 17-5 Ethernet connectors

Connector	Cabling used with
RJ-45	UTP (Category 3, 5, 5e, and 6)
AUI	Thicknet (RG8)
BNC	Thinnet (RG58A/U)
ST/SC	Fiber-optic

skill 8 Connecting to the Internet

A+ Hardware Objective

6.3 Identify common technologies available for establishing Internet connectivity and their characteristics.

overview

Many different network connections are used to connect to the Internet. Although they differ in speeds, capabilities, and support, all utilize an Internet service provider (ISP) to provide connectivity.

An ISP is an organization that has one or more uplink connections to the Internet and provides smaller connections to clients. However, when you get right down to it, the term "Internet" is very ambiguous. The Internet is not a single entity; rather, it is a collection of organizations that allow you to transit parts of their network to a more remote network. Most ISPs are small entities with only a few dedicated circuits. These ISPs connect to larger ISPs, which connect to even larger providers, in effect creating one very large network by allowing data to flow freely among the many smaller networks **(Figure 17-34)**. Although a detailed discussion of the topology of the Internet is beyond the scope of this book, suffice it to say that an ISP is an organization that allows connectivity and transmission to other public networks, thereby connecting you to the Internet.

Obviously, the primary concern for the end user connecting to the Internet is the speed of the connection. Reliability is also a concern, and latency of the connection (how long it takes for your request to be responded to) is also important.

Not all Internet connectivity options are available in all areas. Rural areas, in particular, tend to have few options available. In some cases, you have a particular connection method available but find that speed and/or latency for that connection suffers. Finally, cost is always a factor with Internet connectivity, and depending on your location and the competition in the area, costs are variable. Due to all of these factors involved, picking an Internet connection can be a daunting task. For this reason, to determine and choose the correct method of Internet connectivity, you must examine various connectivity options in detail. For quick reference and summarization, the major features of each option are also detailed in **Table 17-6**.

The most commonly available and early method of Internet access is **dial-up access** using standard telephone lines. To connect to a provider using dial-up, you need an analog modem installed in your PC. Connection speeds with this method are limited to a maximum of 53 Kbps (federal regulations prevent modems from reaching the 56 Kbps advertised speeds), though speeds in the high 40 Kbps range are more common. The maximum obtainable speed with this connection type is primarily dependant on line noise of the connection. For this reason, some providers offer higher quality phone lines developed for use by computers with better noise resistance properties.

The advantages of dial-up access using standard phone lines are cost (both the equipment and monthly charges are the lowest) and availability. The disadvantages of this method of Internet access are speed and latency, both of which are quite poor. In general, dial-up access using standard phone lines is considered an option of last resort.

Another form of dial-up access is **Integrated Services Digital Network (ISDN)**. ISDN comes in two forms: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). ISDN BRI is the most common form of ISDN, and is capable of up to 128 Kbps of data transmission over standard phone lines. ISDN PRI is much different, using a T-1 connection to provide a total of 1.544 Mbps of data throughput. ISDN BRI is the most commonly used form of ISDN for personal Internet access, whereas ISDN PRI is more commonly used to provide large numbers of voice connections in conjunction with data traffic for businesses **(Figure 17-35)**.

Although the speeds associated with ISDN BRI are not particularly impressive, one major benefit of the technology is that it allows both data and voice connections to be established simultaneously over a single line, though this does split the speed of the data throughput in half. Also, because ISDN is digital, the connection process is fast when compared to analog phone lines.

tip

The diagram presented in Figure 17-28 is for illustration only, and is significantly simplified. For some excellent, detailed diagrams of the Internet in various formats, visit http://www.cybergeography.org/atlas/topology.html

Figure 17-34 A simple Internet diagram

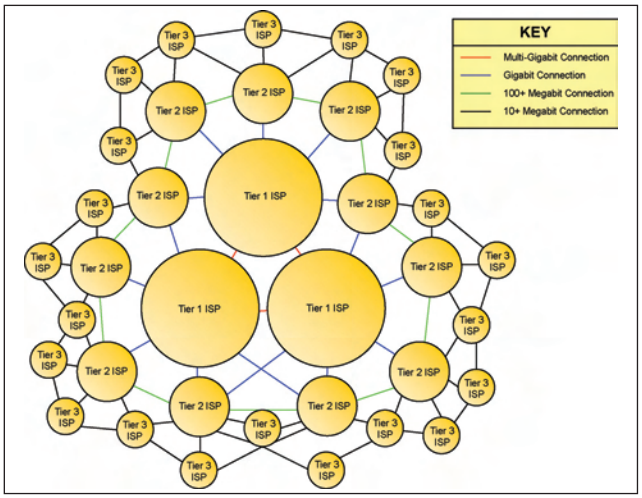
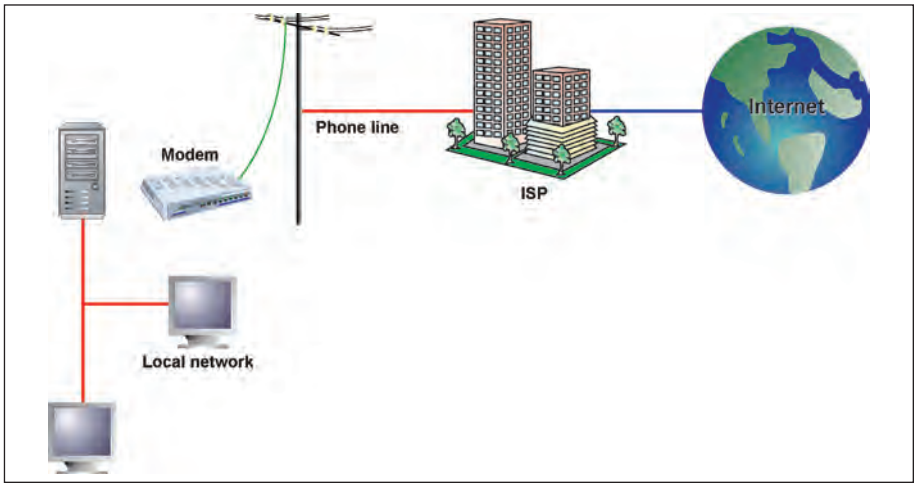


Table 17-6 Internet connectivity options

Connectivity Type	Upload Speed	Download Speed	Latency	Reliability	Availability	Cost
Dial-up	Up to 53 Kbps	Up to 53 Kbps	High	Medium	Widely available	Very low
ISDN BRI	Up to 128 Kbps	Up to 128 Kbps	Medium	Medium	Widely available	Medium to high
ADSL	Up to 1 Mbps	Up to 5 Mbps	Low	High	Limited	Low to medium
SDSL	Up to 1.5 Mbps	Up to 1.5 Mbps	Low	High	Limited	Medium to high
Cable	Up to 5 Mbps	Up to 5 Mbps*	Low	High	Limited	Low to medium
Satellite	Up to 1.5 Mbps	Up to 128 Kbps	Very high	Low	Widely available	Medium to high
WLAN	Up to 54 Mbps	Up to 54 Mbps	Low to moderate	Medium	Very limited	Medium to high

* Many cable providers artificially limit the cable upload speeds.

Figure 17-35 ISDN PRI connectivity example



skill 8

Connecting to the Internet (cont'd)

A+ Hardware Objective

6.3 Identify common technologies available for establishing Internet connectivity and their characteristics.

overview

ISDN connections are made using an ISDN adapter. Although the device is typically labeled a modem, the term adapter is more fitting, because the line is digital and no modulation or demodulation is performed. Both internal and external modems are available, and external models typically connect using serial or Universal Serial Bus (USB) ports.The advantages of ISDN are faster connections than dial-up, simultaneous voice and data capability, and relatively low latency. Major phone companies offer ISDN services, and availability has been around a long time. Additionally, ISDN access is available in many areas.

The disadvantages of ISDN include low data speeds and moderately high costs. In some areas, costs are increased beyond the base monthly rate because the lines have additional charges attached to them, such as fees for connection time in addition to your standard monthly fee.

A more recent standard for high-speed Internet access over phone lines is **Digital Subscriber Line (DSL)**. DSL comes in many forms, but the two most common are **Asynchronous DSL (ADSL)** and **Synchronous DSL (SDSL)**. ADSL provides a much higher download speed than upload speed (typically, the download is around 8 to 10 times the upload speed), and is well suited to activities that require high-speed downloads, such as Web surfing and multimedia applications. However, the low upload speed of ADSL makes it a poor choice for dedicated servers providing large files, such as for FTP servers.

SDSL, on the other hand, provides equal bandwidth in both directions. SDSL service is typically reserved for business customers, and at a significantly higher cost than ADSL. Although SDSL speeds rival some dedicated lines (such as T-1 connections), and the costs are significantly cheaper, SDSL is typically both slower and more costly than cable connections.

Unlike most other forms of dedicated Internet access, DSL speeds are largely dependant on the distance from the central office (CO) of the subscriber. Users closer to the CO experience very high data rates, whereas users farther away experience much slower rates. As of this writing, the effective maximum distance for DSL is around three miles from the CO, though this figure is in flux as new standards and hardware improve upon the distance limitations.

Both forms of DSL connect over standard phone lines using DSL modems. Like ISDN, these devices are more accurately termed adapters. Most modern DSL adapters also include routing functionality, so they can also be classified as routers. Connecting to a DSL modem is typically performed using either USB or more commonly Ethernet. An example of DSL connectivity is shown in **Figure 17-36**. Like ISDN, DSL is capable of sending both voice and data over the line simultaneously. Like ISDN, speed is impacted when using DSL's voice channel, but the speed impact is generally much less severe with DSL. Unlike ISDN, DSL does not have to dial the provider to connect to the network. DSL connections are always on and can be considered a dedicated (24/7) connection.

The advantages of DSL are dependant upon the type of DSL used. ADSL provides high download speeds, a dedicated connection, low latency, and perhaps the lowest cost for high-speed access. Additionally, the fact that ADSL supports voice and data on the same line which helps to reduce the effective overall cost of the connectivity, making the monthly cost more attractive ($50 a month for both voice and data as opposed to $50 for data and $20 for voice). ADSL's biggest disadvantage is limited upload speeds.

SDSL, on the other hand, provides high upload speeds in addition to low latency, dedicated connectivity. However, at present, SDSL prices are not very attractive when compared to competing consumer products, such as cable. Still, SDSL presents an attractive alternative to dedicated T-1 access.

Figure 17-36 DSL connectivity

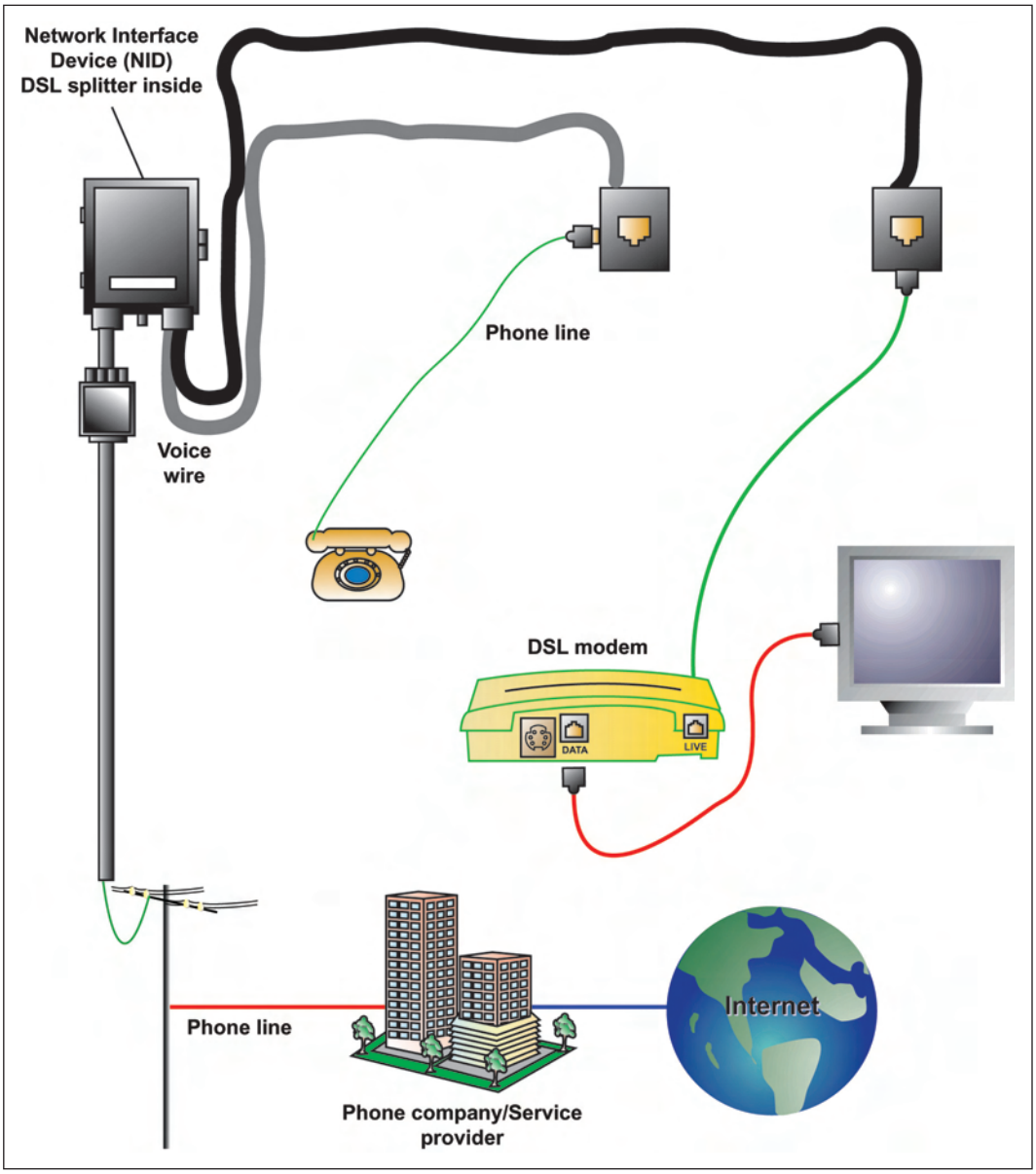
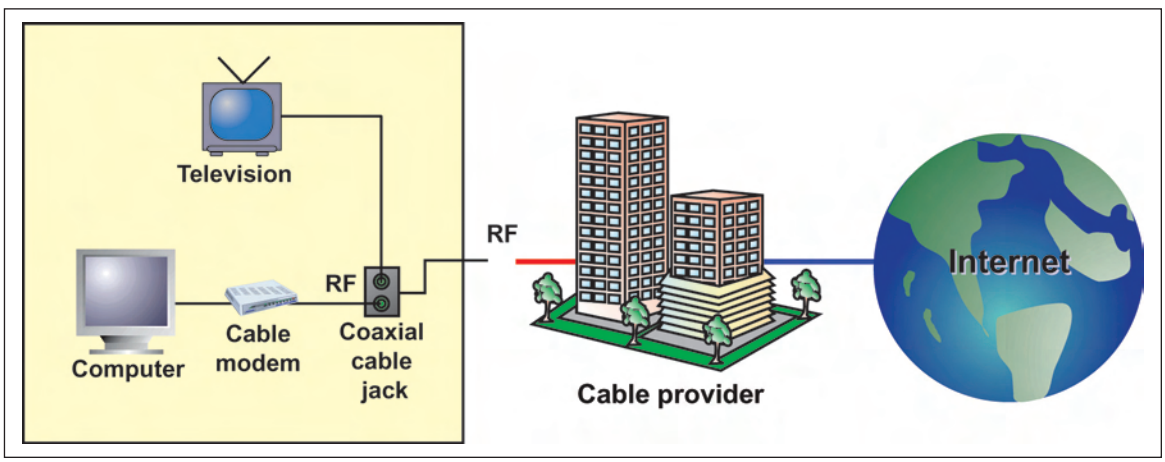


Figure 17-37 Cable connectivity



skill 8

Connecting to the Internet (cont'd)

A+ Hardware Objective

6.3 Identify common technologies available for establishing Internet connectivity and their characteristics.

overview

Cable connectivity is another consumer-level Internet access mechanism, and is perhaps the most popular form of broadband Internet connectivity. Cable Internet access is provided over coaxial cable (Figure 17-37), which is typically arranged in a bus topology, with a single bus servicing a local geographic region (such as a housing development).

Cable connectivity provides equal upload and download bandwidth, and is capable of very high bit rate service. However, cable speeds are generally limited by the provider to a predefined maximum. Additionally, cable is bus-based, which means that the total cable bandwidth is shared among all users of that bus. In addition to the speed decrease this causes, in some cases, it can also raise significant security concerns.

Cable connectivity is generally available in areas where cable television is available. Cable pricing is slightly higher at present than ADSL rates, but cable rates do not include voice capability, which implies that the effective cost can be more than double ADSL in some areas. Of course, this factor must be weighed against the additional bandwidth cable provides.

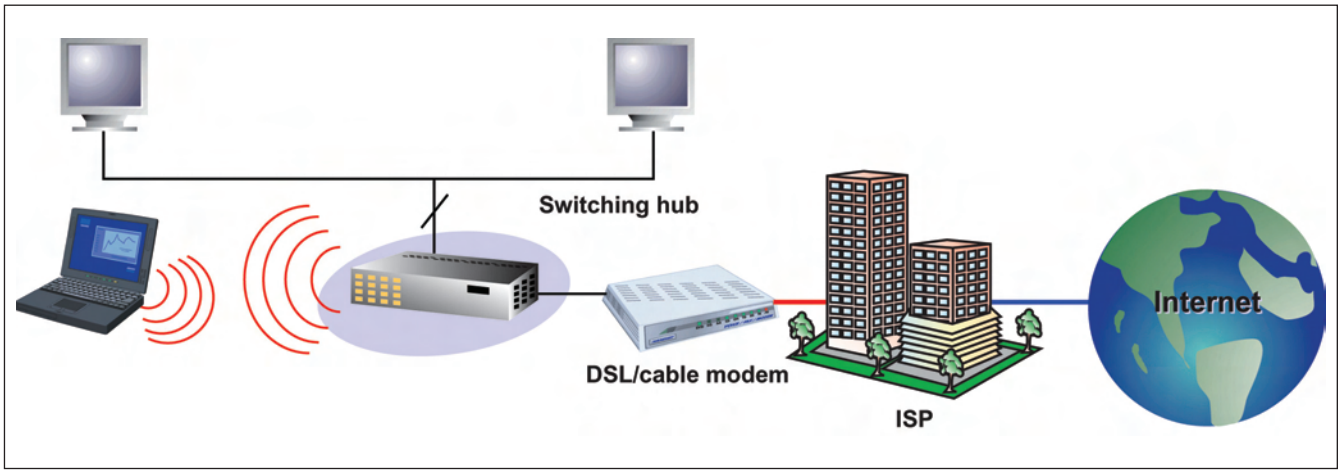
Similar to ADSL, cable connections are made with cable modems, which are more accurately termed adapters and/or routers. Connections to the cable modem are made using USB or more commonly Ethernet, similar to DSL.

Cable's biggest advantages are dedicated connectivity, high upload and download speeds, and low latency. Cable's biggest disadvantages are the shared nature of the medium and the slightly greater overall cost of the service when compared to DSL.

Satellite connectivity is another alternative for high-speed access, that, unlike the other forms of access, is available virtually anywhere. Satellite Internet connectivity at present is not nearly as popular as the other forms of Internet connectivity for several reasons. First, the pricing of satellite connectivity is generally higher than all other forms of high-speed access. Second, satellite access suffers from high latency, in some cases as much as 1 second per transfer. Third, satellite connectivity, until recently, has been confined to one-way transfers (download only). Uploads were limited to the speeds provided by a modem. Although some providers are offering two-way satellite service now, the overall cost is not as attractive when compared to the other alternatives. Finally, satellite connectivity can be unreliable, especially when weather conditions are poor. For these reasons, satellite connectivity is generally used when no other method of high-speed connectivity is available.

WLAN (wireless LAN) access **(Figure 17-38)** is another method that is gaining popularity in densely populated areas. By installing access points in strategic locations, WLAN coverage is provided to a geographic location without the expense of running additional cabling. Currently, WLAN Internet access is highly popular in certain environments, such as hotels, where running additional cabling would be prohibitively expensive. However, the difficulty associated with controlling access, higher costs, and security means that this method of Internet access is likely to remain a niche player for the foreseeable future.

Figure 17-38 WLAN connectivity



skill 9 Examining Wireless Networking

A+ Hardware Objective

6.1 Identify the common types of network cables, their characteristics. and connectors.
6.2 Identify basic networking concepts, including how a network works.

overview

Wireless LAN technologies are a bit different from everything we have discussed so far. First, wireless LAN technologies must contend with many more obstacles than their wired counterparts. Things like radio interference, walls and doors, metal girders in the floor, even microwave ovens can cause signal loss.

Currently, there are two major technologies in use for short-range wireless communication. The first is infrared (IR). IR is a line of sight technology, meaning that to communicate, a clear path must exist between the sending station and the receiving station. Even window glass can obstruct the signal. Because of this, IR is typically used only for very short-range (1 meter or less) communications at a limited bandwidth (around 1 Mbps), such as data exchange between two laptops or other handheld devices. For this reason, because the standard is more like a lap link standard than a networking standard, we will focus most of our discussion on the other technology, radio.

Radio-based wireless LANs (also known as WLANs) are defined in the IEEE 802.11 specification. This specification defines a spread-spectrum radio technology over the unlicensed 2.4 GHz frequency channel, running at 1 to 2 Mbps, with a range between 30 and 300 meters. The specification also allows the use of IR, as well as two differing types of spread spectrum technologies. However, the only one of these three technologies that has yet to make it to high speed is **DSSS (Direct Sequence Spread Spectrum)**. The other two technologies only reach 1 to 2 Mbps, making them somewhat unattractive for common use. For this reason, all of the issues I will cover in this chapter assume the use of DSSS technology.

The 802.11 technology specification was updated later to the 802.11b standard, which defines a speed improvement from 2 Mbps to 11 Mbps. This **IEEE 802.11b** standard, using DSSS, is widely adopted, and this is the technology we focus our attention on. Another, newer, wireless standard is 802.11g, which upgrades the speed to 54 Mbps and is backward-compatible with 802.11 and 802.11b devices. A competing standard, 802.11a, also operates at 54 Mbps, but uses the 5 GHz range and is, therefore, not compatible with earlier standards **(Table 17-7)**.

Wireless network communication are enabled by network **wireless access points (WAPs).** The AP acts as a bridge device, with a port for the wired LAN (usually Ethernet), and a radio transceiver for the wireless LAN **(Figure 17-39)**. The 802.11b standard allows for two modes of operation, Infrastructure Mode, and Ad Hoc Mode.

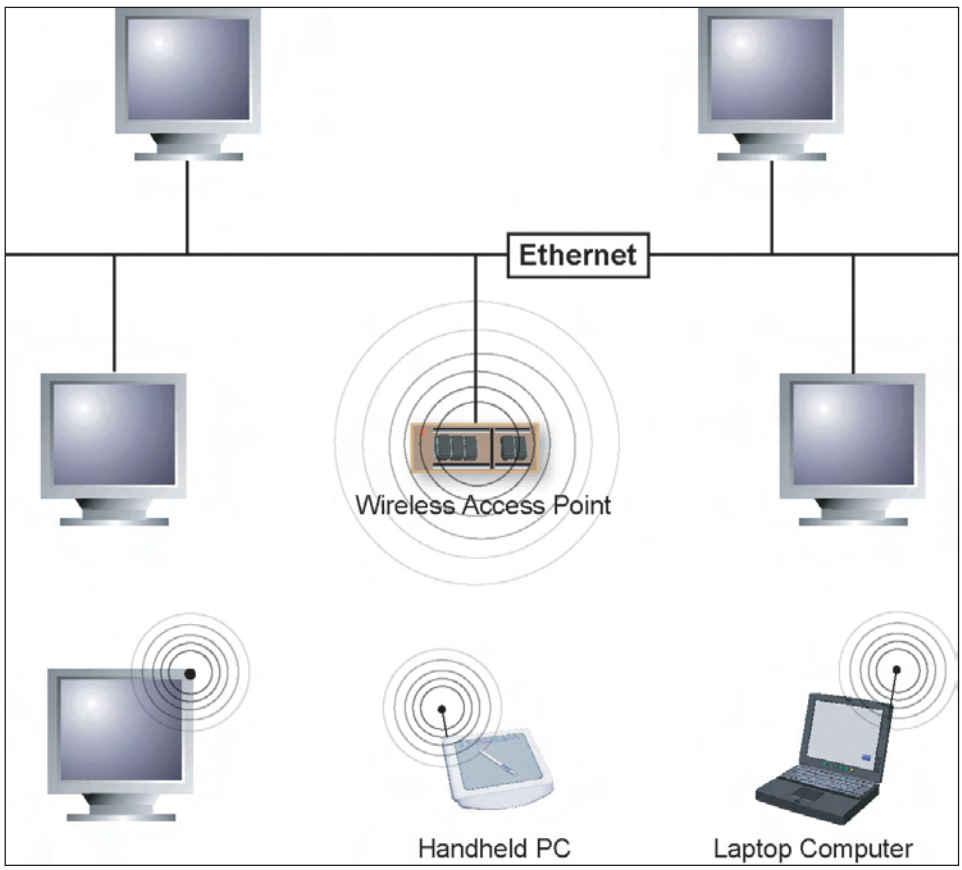
- With **Infrastructure Mode** all STAs (stations) connect to the WAP to gain access to the wired network, as well as to each other. This is the most commonly used mode, for obvious reasons. The WAP controls all access to the wired network, including security, which we will discuss in more detail later. In this environment, you typically place the WAP in a centralized location inside the room in which you want to allow wireless connectivity (such as a room of cubicles). In addition, multiple WAPs may be set up within the building to allow roaming, or extend the range of your wireless network.
- With **Ad Hoc Mode** no WAP is required. Rather, the STAs connect to each other in a peer-to-peer fashion. Although this allows no connectivity to the wired network, it is useful in situations where several PCs need to be connected to each other within a given range.

Initially, radio communication for network traffic seems to be a fairly simple proposition. It sounds like you just plug a NIC into a walkie-talkie or laptop and go cruising.

Table 17-7 Wireless LAN specifications

Specification	Frequency Range	Distance Range (m)	Maximum Speed	Backward Compatibility	Notes
IEEE 802.11	2.4 GHz	~100	2 Mbps	1 Mbps	First WLAN specification
IEEE 802.11b (WiFi)	2.4 GHz	~100	11 Mbps	802.11	Also called WiFi
Bluetooth	2.4 GHz	10	Up to 1 Mbps	N/A	Used for short range communication and data synchronization
IEEE 802.11a	5 GHz	~100	54 Mbps	Not backward compatible	An alternate specification that uses the 5 GHz frequency range, making it incompatible with other 802.11 specifications
IEEE 802.11g (SuperG)	2.4 GHz	~100	54 Mbps	802.11, 802.11b	The latest WLAN specification. Also known as SuperG

Figure 17-39 A wireless network



skill 9 Examining Wireless Networking (cont'd)

A+ Hardware Objective

6.1 Identify the common types of network cables, their characteristics. and connectors.
6.2 Identify basic networking concepts, including how a network works.

overview

Unfortunately, it's not quite that simple. With a fixed frequency (like that of two-way radios), you run into a number of problems, the biggest of which are lack of security and interference. For networking, you need a method for reducing the ability of someone to tap your communications, and in the case of interference, some way to recover and resend the data. This is why wireless networking uses a technology called spread spectrum.

The 802.11b standard specifies the use of the unlicensed radio range from 2.4465 GHz to 2.4835 GHz. In this range, the frequencies are split up into fourteen 22 MHz channels which are useable by wireless networking devices. Wireless LAN devices hop frequencies within a given channel at regular intervals. Because of this, if another device is causing interference in one frequency, the wireless LAN will simply hop to another frequency. This technique also helps improve LAN security, because someone scanning one particular frequency will only have limited success in intercepting the transmissions.

WLANs are by their very nature security nightmares, because you eliminate most of the physical security inherent in your network by sending the data over radio waves. However, three techniques can be used to help improve security and eliminate most of the problems in WLANs: the Wired Equivalent Privacy (WEP) protocol, data encryption, and access control lists.

- **WEP (Wired Equivalent Privacy):** WEP requires that each STA associated with an AP be configured to use the WAP's preprogrammed Extended Security Set ID (ESSID).
- **Data encryption:** AP can be configured to encrypt all data with a 40-bit shared key algorithm. WLANs also support all standard LAN encryption technologies.
- **ACLs:** ACLs (access control lists) are used to secure communications by requiring that every STA associated with the WAP be listed in the access control entry. However, these entries are MAC addresses, so maintenance and upkeep can be difficult in a large environment.

how to

Install a wireless NIC

1. Open the case and insert the NIC into a free expansion slot.
2. Secure the NIC and close the case.
3. Power on the system.
4. If the system automatically detects the adapter, follow the prompts to install the adapter. Once installed, you are finished with this how-to.
5. If the system does not detect the adapter but you have an installation CD that came with the adapter, insert the installation CD and follow the directions to install the adapter. Once installed, you are finished with this how-to.
6. If you do not have a driver CD, open the Control Panel (click start, point to Settings, and click Control Panel) and double-click on Add Hardware to open the Add Hardware Wizard.
7. Click Next > and allow the wizard to complete searching for your new hardware.
8. When asked if the hardware is installed, choose yes, and click Next >.
9. Under the list of installed devices, scroll to the last device and select Add a new hardware device **(Figure 17-40)**. Click Next >.
10. In the next page **(Figure 17-41)** choose Install the hardware that I manually select and click next.

Figure 17-40 Selecting to install new hardware

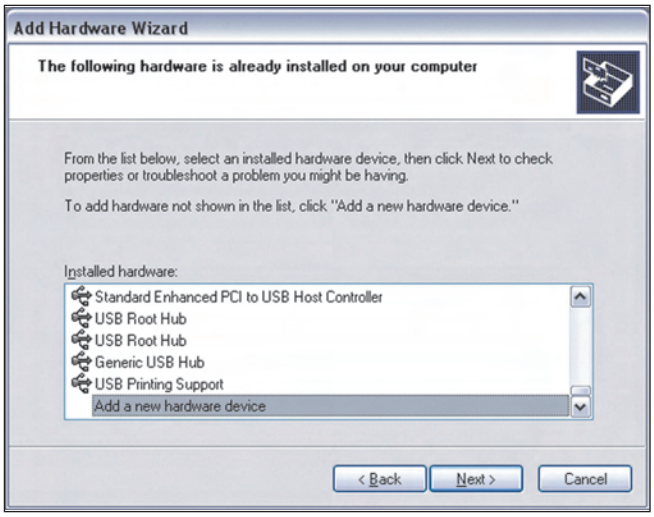


Figure 17-41 Selecting to install manually selected hardware

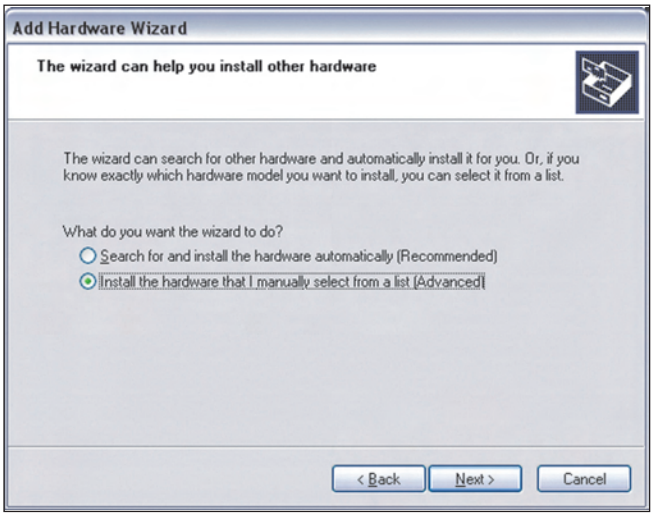
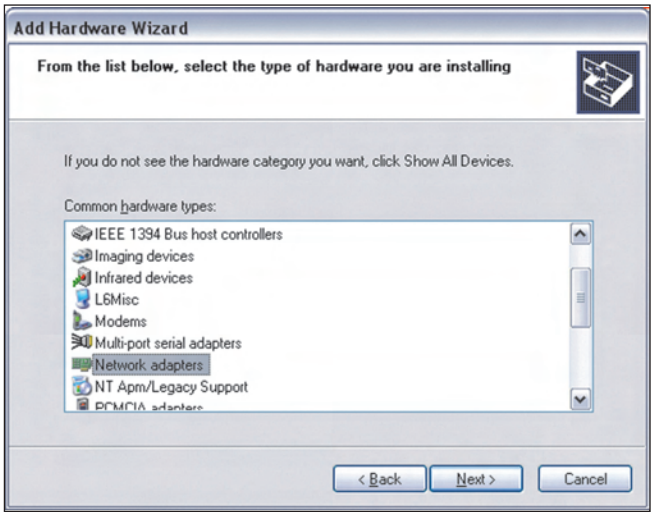


Figure 17-42 Selecting network adapter as the device type to install



skill 9 Examining Wireless Networking (cont'd)

A+ Hardware Objective

6.1 Identify the common types of network cables, their characteristics. and connectors.
6.2 Identify basic networking concepts, including how a network works.

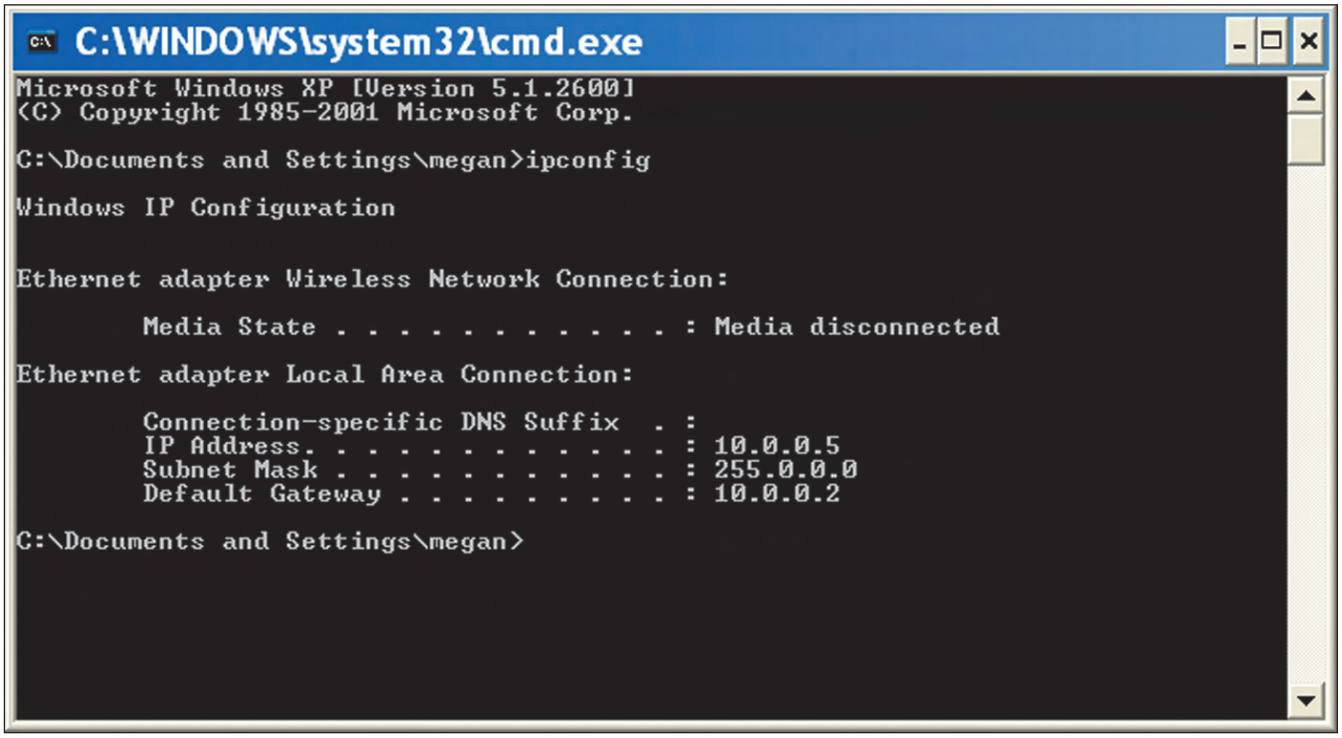
how to

11. In the hardware category list, choose network adapters and click Next > (**Figure 17-44**). Finally, choose the correct vendor and model for your adapter and click Next > to install it.

more

The range for modern WLANs is very dependant upon the environment in which the WLAN is deployed. Some environments are able to support distances of 300 feet, some will struggle to connect at 40 feet. The speed and distance attainable with radio technology is limited by a number of factors. The amount of metal in the structure, the number of walls, the amount of electrical interference, and many other things contribute to lower the attainable bandwidth and range. In addition, even though amplifying the power of the signal can overcome most of these issues, because the 2.4 GHz range is an unlicensed range, the FCC limits power output for devices in this range to 1 watt.

Figure 17-44 Using the ipconfig command



skill 10

Troubleshooting Network Connectivity

A+ Hardware Objective

2.1 Recognize common problems associated with each module and their symptoms, and identify steps to isolate and troubleshoot the problems. Given a problem situation, interpret the symptoms and infer the most likely cause.

overview

Troubleshooting network connectivity problems can be a daunting task due to the complexity associated with network interactions. However, troubleshooting network problems involves the same steps as troubleshooting any other system problem.

First and foremost, you want to ensure that your physical connections are correct. For most Ethernet devices, this can be checked quickly and easily by looking for the presence of a link light on the adapter **(Figure 17-43)**. In most cases, Windows 2000 and XP inform you of a problem with the network connection by displaying the "A Network Cable is Unplugged" message in the task bar tray for adapters without an Ethernet heartbeat. Although it is possible to have an Ethernet heartbeat (signal), along with the corresponding link light, and still not be able to transmit or receive data, these cases are rare.

Along the same lines, if you are using an network adapter with more than one transceiver or port (commonly referred to as a combo card), ensure that the correct transceiver is selected on the card. While most current combo cards will auto-detect the cable connection and select the appropriate transceiver, many older ISA models require that you change a jumper or DIP switch to change the transceiver setting.

Next, ensure that the correct drivers are installed for the NIC and that the hardware resources (IRQ, I/O address) are correctly configured. If you find a problem at this stage, reconfigure the NIC or remove and reinstall the NIC and drivers.

Once physical connectivity is verified, ensure that the computer NIC has a valid IP address. This is performed in Windows 9x by running the command **winipcfg**. In Windows NT, 2000, and XP, run the **ipconfig** command from a command prompt to display IP address information **(Figure 17-44)**. An IP address of 0.0.0.0 or and IP address beginning with 169.254 indicates that there is a problem obtaining an IP address from a DHCP server. This could be because the DHCP server is down or because it has run out of addresses. If you have no address or an invalid IP address, click on the renew button in winipcfg (Windows 9x) or issue the ipconfig /renew command (Windows NT, 2000, and XP). In Windows XP, you can also use the repair network connection parameter to obtain an IP address.

tip

If a firewall is used on the network, it may block ICMP packets for security reasons. In these cases, you can transfer data between the PCs but you may be unable to ping.

When settings are all verified, attempt to **ping** various systems on the network using both name and IP address. The ping utility is a analysis utility that sends an Internet Control Message Protocol (ICMP) echo request packet to remote systems. Upon receiving the echo request, the remote system will reply with an echo reply, which confirms connectivity at a basic level.

If the ping command succeeds when using IP addresses of remote hosts, but fails when using the host's DNS name, then the problem is related to DNS name resolution. To resolve the problem, enter the correct addresses for the DNS (Windows 2000 and XP) and/or Windows Internet Naming Service (WINS) (Windows 9x and NT servers on your network in the IP properties of the adapter. If you can ping some hosts on the network but not others, examine the network layout to determine which devices are used to separate the network. For instance, if a hub or switch is being used to connect two sections of the network, a failure in the link between the two could be the cause of the problem **(Figure 17-45)**. If a router separates the two segments, ensure that the default gateway address is entered properly on PCs on both segments. The default gateway address should be configured for the local interface of the router on that subnet **(Figure 17-46)**.

In some cases, you may be able to perform all of these tests but can still not locate the remote system in **My Network Places** or **Network Neighborhood.** This is a common issue in all

Figure 17-43 Ethernet link light

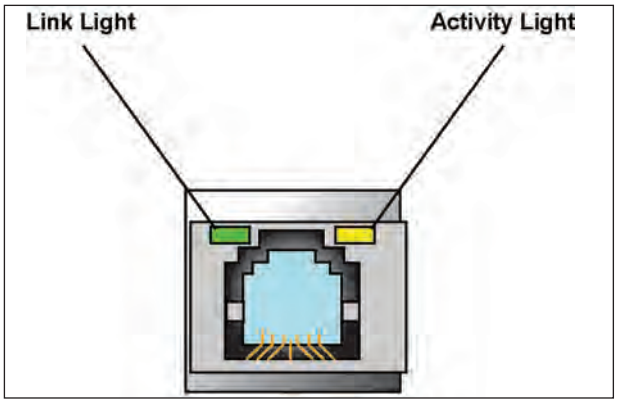


Figure 17-45 An example of a hub failure

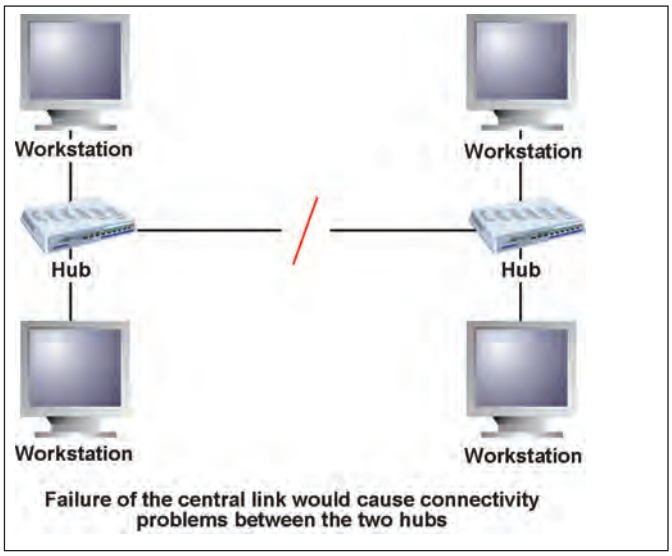
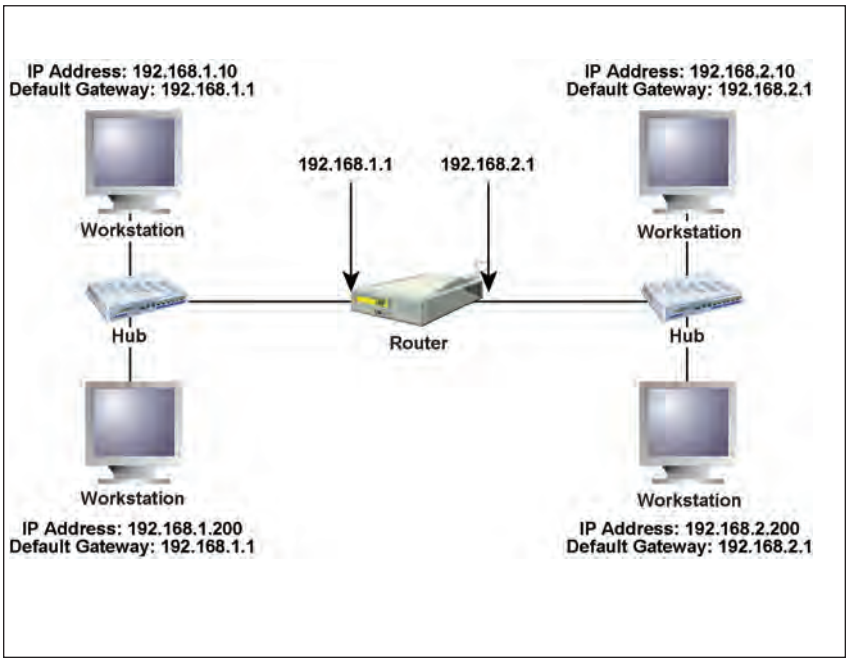


Figure 17-46 Configuring the default gateway



skill 10

Troubleshooting Network Connectivity (cont'd)

A+ Hardware Objective

2.1 Recognize common problems associated with each module and their symptoms, and identify steps to isolate and troubleshoot the problems. Given a problem situation, interpret the symptoms and infer the most likely cause.

overview

Windows systems, and is caused by a large number of different factors, not all of which are technically errors, including the following:

- A system is only listed in My Network Places or Network Neighborhood if the computer system is sharing files. Systems that are not sharing files do not have the server service running, which means that they do not "advertise" any computer resources.
- If you are not using a WINS server and are not a member of a domain, you will not be able to browse to any computers on the other side of a router in My Network Places or Network Neighborhood. This is due to the broadcast-based nature of the browser service, which is responsible for building the list of resources (called the browser list) shown in My Network Places or Network Neighborhood.
- The browser list takes some time to build. In general, around 12 to 15 minutes is generally enough time to build a browser list, but in a few cases, this process can take over an hour. If you cannot connect to the resource through My Network Places or Network Neighborhood, try connecting to the computer by typing *systemname*, where *systemname* is the Network Basic Input/Output (NetBIOS) name or IP address of the remote system. If this works and browsing didn't, then the problem is related to the browser service itself, and will not impact network connectivity.

more

Additionally, data transmissions over networks also suffer from transmission loss or data degradation due to several key factors: attenuation, chromatic dispersion, and electromagnetic interference (EMI) (**Table 17-8**).

Although not solely an issue with Ethernet, **attenuation** is a major concern in Ethernet. Attenuation is defined as the degradation of a signal over time or distance. This occurs because the cable itself provides some resistance to the signal flow, causing a reduction in the electrical signal as the signal travels down the cable. You can think of this like a car traveling down a road. If you accelerated to 60 MPH, the minimum speed was 40 MPH, and you had just enough gas to accelerate but not enough to maintain your speed, it will only take a short distance before your car falls below the minimum speed. This is like Ethernet. The signal is sent at a certain voltage and amperage, but over distance, resistance in the cable causes the signal to degrade. If the signal degrades too much, the signal to noise ratio (how much signal is present compared to noise in the wire) drops below minimum acceptable levels, and the end device is not be able to determine the difference between signal and noise. See **Table 17-8** for ways to deal with attenuation and other signal degradation.

Table 17-8 Managing signal degradation and attenuation

Degradation Type	Occurs with	Description	Solutions
Attenuation	Copper-based media.	Degradation of a signal over time or distance due to resistance in the cable itself to the signal flow, causing a reduction in the electrical signal as the signal travels down the cable.	Setting maximum cabling lengths helps alleviate the problem by establishing maximum limits on the total resistance based on cable type. Repeating, or amplifying,the signal helps alleviate the problem to a degree by amplifying the signal when it gets low.
Chromatic dispersion	Fiber-optic cabling; especially multi-mode fiber-optic media that allows greater dispersion due to its physical size and greater glass impurities.	Occurs with the transmission "impure" wavelength of light, composed of many differing wavelengths, broken into its separate wavelengths. Because wavelengths define transmission speed, some rays of light in a single bit transmission may reach the other end sooner, causing false bits to be detected.	Start by reducing the frequency of signals sent down the cable. Use high quality components, such as single-mode fiber and actual laser transmitters.
Electromagnetic interference (EMI)	Copper cabling, especially (unshielded twisted-pair). cabling.	Caused by magnetic fields created in electrical devices or along copper cabling too close to other copper cabling.	Move data cables as far away as possible from high-powered, non-shielded electrical devices.
Crosstalk	Copper cabling, especially UTP (unshielded twisted-pair) cabling.	Caused by EMI, when two cables near each other generate "phantom" electrical pulses in each other, corrupting the original signal.	This problem is reduced considerably in UTP cabling by twisting the cables around each other (in fact, the number of twists per foot is one of the major differences between Category 3 and Category 5 cabling).

Summary

- Physical and logical topology, when combined, defines how the network operates on a basic level.
- Bandwidth is typically measured in bits per second (bps). This means that to arrive at bytes per second (Bps) speed for a network connection, you must divide the advertised bps rate by 8.
- Baseband devices are simpler and generally more cost effective than broadband devices, but only allow a single communications channel over the medium.
- Broadband divides the frequency range of the medium into distinct channels allowing multiple communications streams to pass across a single medium simultaneously.
- Ethernet operates on a bus or star-bus topology model.
- In a physical bus topology, if a cable breaks, all PCs are affected.
- The star bus is a physical star, but a logical bus.
- A crossover cable is a cable in which the send and receive wires are crossed or flipped, so that the send on one end goes into the receive on the other.
- If the signal degrades too much, the signal to noise ratio (SNR, how much signal is present compared to noise in the wire) will drop below minimum acceptable levels, and the end device is not able to determine what is signal and what is noise.
- Your two real problems with electromagnetic interference (EMI) are that your cabling can interfere with other cabling, and that other electronic devices (such as high-powered lights) can interfere with your cabling.
- For two hosts to communicate directly, they must understand the same frame types.
- Ethernet uses CSMA/CD as an arbitration method.
- Although the entire Ethernet specification uses CSMA/CD as an arbitration method, it is actually only needed for half-duplex operation.
- Ethernet repeaters are devices that repeat the signal sent to them onto multiple segments of cable.
- Unlike a hub, an Ethernet switch processes and keeps a record of the MAC address used on a network and builds a table (called a CAM) linking these MAC addresses with ports.
- If you are in a given collision domain, the only devices your frames can collide with are devices in the same collision domain.
- Infrared (IR) is a line of sight technology, meaning that to communicate, a clear path must exist between the sending station and the receiving station.
- Radio-based wireless LANs (WLANs) are defined in the IEEE 802.11 specification. This specification defines a spread-spectrum radio technology over the unlicensed 2.4 GHz frequency channel, running at 1 to 2 Mbps, with a range between 30 and 300 meters.
- The 802.11 technology specification was updated later to the 802.11b standard, which defines a speed improvement from 2 Mbps to 11 Mbps.
- Another, newer, standard is 802.11g, which upgrades the speed to 54 Mbps and is backward-compatible with 802.11 and 802.11b devices.
- With Infrastructure Mode, all STAs connect to the wireless access point (WAP) to gain access to the wired network, as well as to each other.
- With Ad Hoc Mode, no WAP is required. Rather, the STAs connect to each other in a peer-to-peer fashion.
- WLANs generally operate in a cellular topology, with access points placed around a building to allow users to roam from place to place.
- The Wired Equivalent Privacy (WEP) protocol is used to prevent hackers from associating their STA with your private WAP.
- Range for modern WLANs is very dependant upon the environment in which the WLAN is deployed. Some environments are able to support distances of 300 feet, some struggle at 40 feet.
- Connecting to a network involves installing a network adapter and configuring the appropriate protocols and services to support connectivity.
- Protocols are similar to languages and define the network communication method.
- TCP/IP is by far the most commonly used network protocol for both private local area networks (LANs) and public wide area networks (WANs).
- Nearly every OS supports TCP/IP, and it is the only protocol suite supported over the Internet.
- TCP/IP consists of literally hundreds of individual protocols responsible for different tasks within the suite.
- If you are using TCP/IP with static addressing, at the minimum you will need to enter in the proper IP address and subnet mask.
- IPX/SPX is a vendor-specific protocol used with the Novell NetWare platform.
- IPX/SPX client configuration is generally dynamic, and occurs without user intervention.
- NetBEUI does not include any provisions for routing, which means that it cannot be used to transfer data between networks.
- NetBEUI is a very low overhead suite when used on small networks, making it very fast.
- Most modern networks use TCP/IP as the only protocol suite, though a few still use IPX/SPX. NetBEUI networks are rare and used only by very small peer-to-peer networks.
- The server service is the service used to provide shared resources to clients. To share a resource, the server service must be enabled.

- The workstation service (also known as the redirector) allows you to connect to remote shared resources.
- An ISP is an organization that has one or more uplinks to the Internet and provides smaller connections to clients.
- The Internet is not a single entity; rather, it is a collection of organizations that allow you to transit parts of their network on your way to a more remote network.
- Not all Internet connectivity options are available in all areas. Rural areas, in particular, tend to have very few options available.
- Dial-up modems are limited to 53 Kbps.
- The advantages of dial-up access using standard phone lines are cost (both the equipment and fees are the lowest of any method) and availability.
- ISDN BRI is the most common form of ISDN, and is capable of up to 128 Kbps of data transmission over standard phone lines.
- The advantages of ISDN are fast connections, simultaneous voice and data capability, and relatively low latency. Additionally, ISDN access is available in most areas.
- ADSL provides a much higher download speed than upload speed (typically, the download is around 8 to -10 times the upload speed), and is well suited to activities that require high-speed downloads, such as Web surfing and multimedia applications.
- SDSL provides equal bandwidth in both directions.
- DSL speeds are largely dependant on the distance from the central office (CO) of the subscriber.
- Both forms of DSL connect over standard phone lines using DSL modems.
- Unlike ISDN, DSL does not have to dial the provider to connect to the network. DSL connections are always on, and can be considered a dedicated connection.
- ADSL provides high download speeds, a dedicated connection, low latency, and perhaps the lowest cost for high speed access. Additionally, the fact that ADSL supports voice and data on the same line can reduce the effective cost of the connectivity, making the monthly cost more attractive.
- SDSL provides high upload speeds in addition to low latency, dedicated connectivity.
- Cable Internet access is provided over coaxial cable, which is typically arranged in a bus topology, with a single bus servicing a local geographic region (such as a housing development).
- Cable's biggest advantages are dedicated connectivity, high-speed uploads and downloads, and low latency.
- Satellite access suffers from extremely high latency, in some cases as much as 1 second per transfer.
- Satellite connectivity can be unreliable, especially when weather conditions are poor.
- Currently, WLAN Internet access is highly popular in certain environments, such as hotels, where running additional cabling would be prohibitively expensive.
- Although it is possible to receive an Ethernet heartbeat and the corresponding link light, and still not be able to transmit or receive data, these cases are rare.
- Although most current combo cards will auto-detect the cable connection and select the appropriate transceiver, many older ISA NIC models require that you change a jumper or DIP switch to change the transceiver setting.
- If a firewall is being used on the network, it may block ICMP packets for security reasons. In these cases, you are able to transfer data between the PCs but be unable to ping.
- If you can ping some hosts on the network but not others, examine the network layout to determine which devices are used to segment or separate the network.
- In some cases, you may be able to perform all of these tests but can still not locate the remote system in My Network Places or Network Neighborhood.

Key Terms

1000baseT
10base2
10base5
10baseT
Ad Hoc mode
Arbitration
Asynchronous DSL (ADSL)
Attenuation
Bandwidth
Baseband
Broadband
Broadcast
Bus
Bus topology
Carrier Sense Multiple Access (CSMA)
Collision domain
Dial-up access
Digital Subscriber Line (DSL)
Domain Name System (DNS)
DSSS (Direct Sequence Spread Spectrum)
Duplex
Dynamic Host Configuration Protocol (DHCP)
Fast Ethernet
Fiber Distributed Data Interface (FDDI)
Frames
Framing
Full-duplex
Fully qualified domain names (FQDNs)
Half duplex
Host
IEEE 802.11b
Infrastructure mode
Integrated Services Digital Network (ISDN)
Ipconfig
IPX/SPX
Layer 2 Ethernet switching
Local area networks (LANs)
Logical topology

Media Access Control (MAC) addresses
NetBEUI (NetBIOS Extended User Interface)
Network Interface Card (NIC)
Network medium
Node
Physical addressing
Physical topology
Ping
Promiscuous mode
Propagation delay
Protocols
Repeaters
Ring topology
Star-bus topology
Synchronous DSL (SDSL)
TCP/IP
Thicknet
Thinnet
Token ring
Topology
Tracert
Transmission Control Protocol/Internet Protocol (TCP/IP)
Transparent bridging
Wide area networks (WANs)
Winipcfg
Wireless access points (WAPs)
Wireless LAN (WLAN)

Test Yourself

1. You are having difficulty connecting to remote hosts on a network running TCP/IP. Which of the following tools or steps would you perform to diagnose the problem? (Choose all that apply.)
a. Ipconfig /all
b. Ping
c. Repair network connection feature
d. Reinstall the OS
e. Examine Device Manager
f. Unplug the router or hub
g. Examine the network cable

2. What is the current version of IP used by most systems?
a. Version 1
b. Version 8
c. Version 6
d. Version 4

3. Your company is setting up a small presentation in a convention center. Two presentation systems, along with a presentation server, will be sent to the convention. These systems will have to be networked on-site by the sales staff, who have little or no networking expertise. These systems require a high-speed networking solution, but do not require access to other networks. You ensure that the systems contain 100 Mbps Ethernet adapters, and ensure that the appropriate number of 10/100baseT patch cables, along with a 10/100 hub, are sent to the convention center. What protocol suite would be best for this scenario?
a. AppleTalk
b. NetBEUI
c. IPX/SPX
d. TCP/IP

4. Which of the following WLAN standards supports the highest data rate while remaining backward-compatible?
a. 802.11
b. 802.11b
c. 802.11g
d. 802.11a

5. You and a friend are in a shopping mall when you notice several walkie-talkies on display. You immediately test the devices by proceeding to talk to one another using them. You notice that when you speak, your friend cannot, and when he speaks, you cannot. What would this functionality be called in networking?
a. Full-duplex communication
b. Half-duplex communication
c. Reliable communication
d. Complex communication

6. Which of the following are advantages of Layer 2 Ethernet switching on half-duplex Ethernet? (Choose all that apply.)
a. Greater cabling distances
b. Less attenuation and crosstalk
c. Reduced number of collisions
d. Increased available bandwidth

7. Which of the following best describes 10baseT Ethernet's physical topology?
a. Star
b. Bus
c. Ring
d. Mesh
e. Busted star

8. You are utilizing a wireless network at work, and need to increase the speed of the network to support some hosts without needing to upgrade all wireless NICs to support the new technology. All wireless hosts currently use Wi-Fi NICs and APs. Which of the following could you upgrade the APs to and still retain down-level compatibility?
a. 802.11
b. 802.11a
c. 802.11g
d. Bluetooth
e. 802.11b

9. Which of the following cable types are compatible with 10baseT Ethernet (choose all that apply)?
   a. RG58
   b. Multi-mode Fiber
   c. Category 5 UTP
   d. RG8
   e. Category 3 UTP
   f. Category 5
   e. UTP

10. Which of the following best describes the 5/4/3 rule in 10base2 Ethernet?
   a. 5 repeaters, 3 segments with hosts, 4 total segments
   b. 5 total segments, 3 segments with hosts, 4 repeaters
   c. 5 total segments, 3 repeaters, 4 segments with hosts

Projects: On Your Own

1. Examine your local IP configuration.
   a. Log on to the system as an Administrator.
   b. Open a command prompt.
   c. Type **ipconfig /all** (Windows NT, 2000, and XP) or winipcfg (Windows 9x) and press [**Enter**].
   d. View your IP information for each network adapter. Is your IP address statically configured, or obtained via DHCP? Which router do you use to reach the Internet?
   e. Close the all windows/dialogs and log off of the system.

2. Ping your local gateway to ensure connectivity, then trace the path to **www.yahoo.com**.
   a. Log on to the system as an Administrator.
   b. Open a command prompt.
   c. Ping your default gateway by typing **ping GATEWAY_ADDRESS,** where GATEWAY_ADDRESS is the IP address of your default gateway as listed in the last project.
   d. Was the ping successful? If so, continue to the next step. If not, try to troubleshoot the error.
   e. Type **tracert www.yahoo.com** and hit [**Enter**]. Analyze the results. See if you can determine the path to yahoo.com using the information returned by the tracert command.
   f. Close the all windows/dialogs and log off of the system.

Problem Solving Scenarios

1. You have a client that cannot connect with two specific systems on a remote network. The client is connected to a hub (hub1), which is connected to a router, which is connected to another hub (hub2). The two systems the client cannot connect to are connected to hub 2. You verify that the client can connect to all systems, including other systems attached to hub 2, except these two systems. List the steps you would take to troubleshoot this problem. List the most likely causes of this problem based on the information given.

2. You are attempting to design a basic network for a small company with two offices. The offices are on a single campus, with only 300 meters separating them. You wish to use the highest speed media possible for connectivity, but for financial reasons, you cannot utilize fiber optics. Draw a basic network design for this company.