Understanding Network Hardware

Lesson Objectives

In this lesson, you will learn about networking devices and the transmission media that connects them. By the completion of this lesson, you will be able to:

- ☐ Identify the seven layers of the Open Systems Interconnection (OSI) reference model.
- ☐ Explain the process of data encapsulation and packet creation.
- ☐ Identify the four layers of the TCP model, and describe how they correspond to layers of the OSI model.
- ☐ Review concepts and terms related to network traffic.
- ☐ Understand the function and characteristics of network switches.
- ☐ Understand the function and benefits of virtual LANs (VLANs).
- ☐ Understand the function and characteristics of routers.
- ☐ Describe the routing function.
- ☐ Understand network address translation (NAT).
- ☐ Identify various transmission types, such as synchronous, asynchronous, baseband and broadband.
- ☐ Identify the characteristics of different types of transmission media such as twisted-pair, coaxial, and fiber-optic cable, including transmission speeds and susceptibility to interference and interception.
- ☐ Understand twisted-pair Ethernet wiring.
- ☐ Describe technologies for free-space transmission.
- ☐ Identify proper cabling procedures.

Exam Objectives

1.2 Understand local area networks (LANs)
2.1 Understand switches
2.2 Understand routers
2.3 Understand media types
3.1 Understand the OSI model
3.2 Understand IPv4

Networking Models

Objective
3.1

In Lesson 1, you learned that adherence to standards and protocols makes networking possible and even seamless between devices created by different manufacturers. Standards are developed around models for how communication should take place.

Several models exist for networking and for networking over the Internet. A basic familiarity with these models will help you understand how networking hardware and protocols work. The two models we will investigate in this course are the Open Systems Interconnection reference model (OSI/RM) and the TCP/IP four-layer model.

The OSI Reference Model

The *Open Systems Interconnection reference model (OSI/RM)* is a seven-layer networking function model. Adherence to the model ensures that systems from various vendors will be able to communicate with one another. As you will see shortly, the model also describes the sequence of data encapsulation. The model was defined by the International Organization for Standardization (ISO).

The seven layers of the OSI/RM are briefly described in the following table.

Layer #	Layer Name	Comments
7	Application	The user interface resides at this layer. Web browsers and e-mail clients work at this layer of the model. This is the only layer a user actually sees; the functions of the other layers are transparent to the user.
6	Presentation	User input and other information is transformed at this layer into a standardized format recognized by all operating systems.
5	Session	Connections between systems that are communicating with each other are set up and torn down at this layer.
4	Transport	Mechanisms that ensure data is accurately and completely sent and received between communicating systems operate here.
3	Network	Data is organized into discrete units called *packets* at this layer, and in addition to the original data, each packet includes addressing information that is required to deliver the packet to its intended destination.
2	Data Link	At this layer, packets are divided into discrete units called *frames* before being sent across the *transmission medium*. The transmission medium is the physical wire that connects the devices on the network. This layer also controls access to the transmission medium.
1	Physical	At this layer, frames are transmitted across the transmission medium in a bitstream, that is, as a series of 1s and 0s.

It is important to understand the functions of each layer because networking hardware and protocols map to specific layers of the OSI. We will refer back to this model several times during the course.

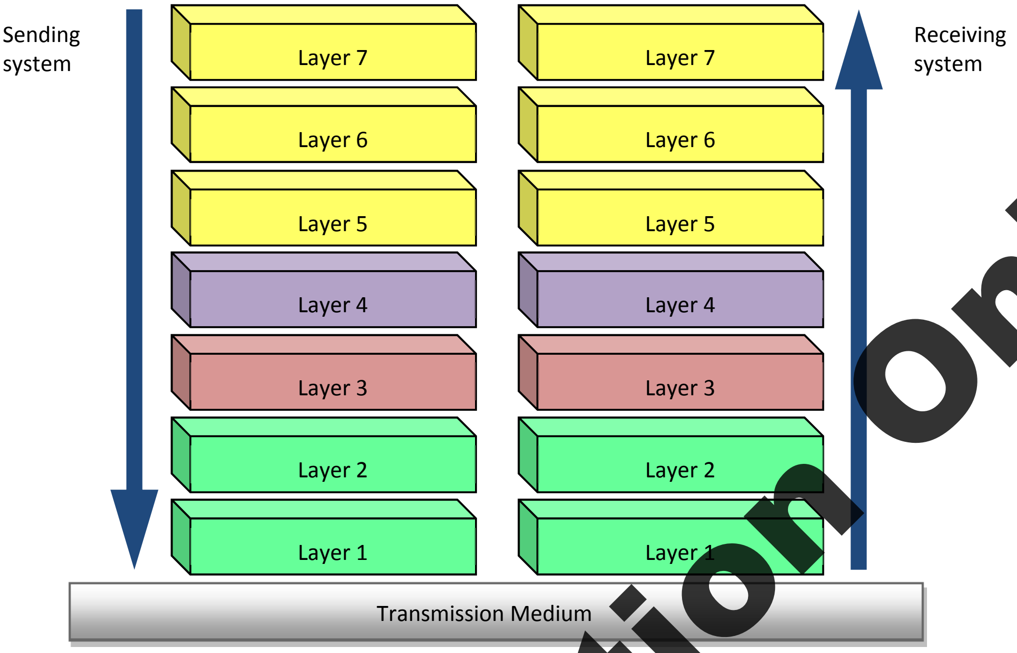
Data Encapsulation

Networking models remind us of the processes that must take place for systems to communicate with one another. For example, consider two computer systems on a network. One belongs to Ed and one belongs to Ron. If Ed's computer needs to send data to Ron's computer, Ed's computer must first "package" that data to prepare it for transport across the network. This process is called *data encapsulation*.

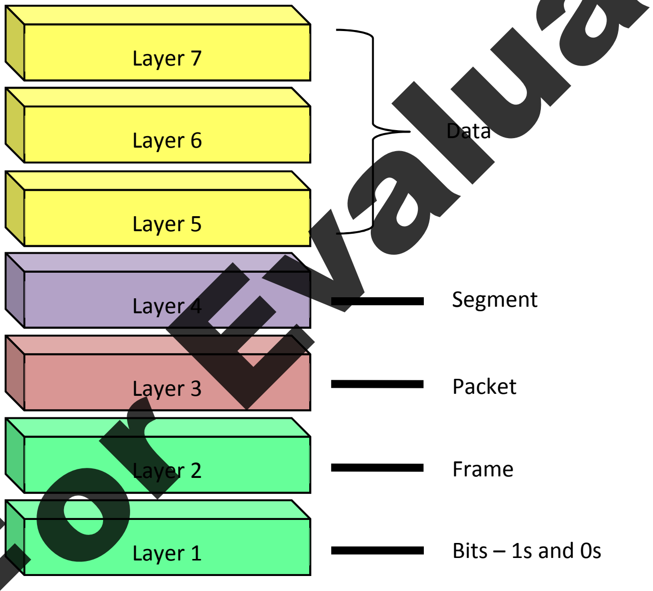
To properly encapsulate the data to be sent across the network to Ron's computer, Ed's computer will pass the data down through each of the seven layers of the OSI/RM. Each layer adds its own packaging information and passes it to the next layer below. Once the data reaches Layer 2, it is prepared to be sent across the physical transmission medium used on the network (e.g., copper wire or fiber-optic cable).

Ed's encapsulated data is sent across the transmission medium and received at Ron's computer. Ron's computer then takes the data off the transmission medium and passes it up through the seven layers of the OSI/RM. As the data is passed up through the OSI/RM on Ron's computer, the data is de-encapsulated until it reaches Layer 7, where it is once again in a usable form.

The following figure illustrates this process:



At various stages during the encapsulation process, the data being encapsulated is referred to by different names, as illustrated in the following figure.



As you learn more about protocols and networking technologies, you may see data at various stages of encapsulation referred to by these names: data, segment, packet and frame. In some literature, you may find data at all stages of encapsulation referred to simply as "packets."

How packets are created

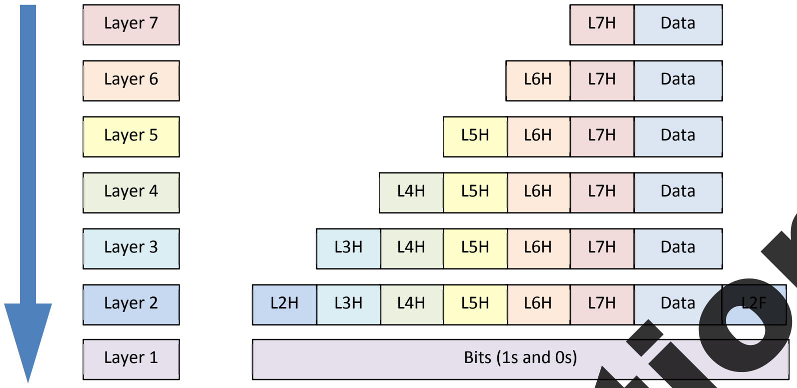
The creation of a packet begins at Layer 7 (the application layer). Looking again at Ed's computer, let us assume that he is sending data to Ron's computer. Ed enters data (for example, in an e-mail message) at Layer 7. The message he enters will undergo a transformation that will break it into smaller pieces so that it can be sent.

Layer 7 takes a manageable “piece” of the data and adds its own information (called the *header*) to it. The piece of the original data is now called the *payload*. The entire unit (the payload plus the header) is referred to as a *protocol data unit* (PDU) and it is passed down to Layer 6.

Layer 6 then treats the Layer 7 PDU as a payload, and adds its own header. The resulting PDU is then passed down to Layer 5. The process continues through all the layers of the OSI.

Each layer considers what has been passed down to it from an upper layer to be "data." It treats the entire higher-layer message as a data payload. At the end of the encapsulation process, a frame is formed.

The following figure illustrates how each layer appends a header to the PDU it receives from the layer above it. Notice that Layer2 also adds a footer (or trailer). Notice also that there is no header added at Layer 1.



As you learned earlier, the terms data, segment, packet and frame are the protocol data unit names assigned to information at specific points in the encapsulation process. An item of information is considered data as it is generated and passed down through the upper three layers of the OSI, which are often collectively known as the application layer.

At Layer 4

Data is passed down to the transport layer (Layer 4) where it is encapsulated to include source and destination port numbers that identify the applications (such as FTP or e-mail) between which the data should be passed. At this point, the data is considered a segment.

At Layer 3

A segment is passed down to the network layer (Layer 3), where it is encapsulated and given source and destination IP addresses. At this point, the segment becomes a packet.

At Layer 2

A packet is passed down to the data link layer (Layer 2), where it is encapsulated and given a source and destination MAC address. A footer is also appended to the packet. The footer contains an error-checking mechanism called a *cyclical redundancy check (CRC)*. At this point, the packet becomes a frame.

A CRC is also referred to as a frame check sequence (FCS).

The cyclical redundancy check (CRC) is a mathematical calculation that allows the receiving computer to verify whether a packet is valid. When a sending host transmits a packet, it calculates a CRC by summing all the ones in the payload and storing this sum as a hexadecimal number, which is then stored in the footer. When the receiving host reads the packet, it runs its own CRC, then compares it with the CRC stored in the footer. If the two match, the packet is not damaged, and the receiving host processes the packet. If the CRCs do not match, the receiving host discards the entire packet.

At Layer 1

Frames are passed down to the physical layer (Layer 1) where they are sent across the transmission medium as a bit stream.

Removing headers

When a receiving host processes a packet, it reverses the packet-creation process and de-encapsulates or removes each header, beginning with Layer 1 and ending with Layer 7. All that is left at the end of this process is the original, unaltered data, which the host can then process.

The TCP/IP Four-Layer Model

The TCP/IP architecture uses a four-layer model, and each layer coincides with layers of the OSI/RM, as shown in the following illustration. Each layer in the architecture has its own specific functions. Various hardware devices and protocols are mapped to specific layers. You will investigate these later in the course.

OSI/RM	TCP/IP	
Layer 7 Application	Application Layer	Upper layers or Developer layers
Layer 6 Presentation		
Layer 5 Session		
Layer 4 Transport	Transport Layer	
Layer 3 Network	Internet Layer (or Network Layer)	Lower layers or Network layers
Layer 2 Data link	Link Layer (or Access Layer)	
Layer 1 Physical		

Both the OSI and TCP models are generally divided into upper layers and lower layers. The upper layers are often referred to as *developer layers*. Applications developers write programs and procedures that work with these layers. The lower layers are referred to as the *network layers*. These are the layers that control communication across a network.

Application layer

The application layer of the TCP/IP architecture corresponds to the application, presentation and session layers of the OSI/RM. The TCP/IP application layer interacts with the transport-layer protocols to send or receive data.

Transport layer

The transport layer of the TCP/IP architecture corresponds to the transport layer of the OSI/RM. This layer accepts application-layer data and divides the data into segments. Each segment is passed to the Internet layer. This layer is also responsible for establishing a connection and controlling the flow of information between two systems.

Internet layer (or network layer)

The Internet layer of the TCP/IP architecture corresponds to the network layer of the OSI model. A segment received from the transport layer is encapsulated in an IP packet. This layer is also responsible for addressing and routing packets. Based on the destination host information, this layer determines whether to deliver the packet locally or send it to another network.

Link layer (or access layer)

The link layer of the TCP/IP architecture corresponds to the physical and data link layers of the OSI model. This layer accepts higher-layer packets, creates frames and transmits them in bitstreams over the attached network. This layer interfaces with the transmission media.

Exercise 2-1: Reviewing OSI layer functions

In this exercise, you will match each OSI layer with its function.

1.	Physical	A.	Sets up, maintains and tears down connections.
2.	Data link	B.	Handles addressing.
3.	Network	C.	Ensures that data is accurately and completely sent and received.
4.	Transport	D.	Translates data into a suitable format.
5.	Session	E.	Controls access to the transmission medium.
6.	Presentation	F.	Describes how data is transmitted across the medium.
7.	Application	G.	Provides an interface to the user.

In this exercise, you reviewed OSI layer functions.

Traffic-related Concepts

Before moving on to how network devices map to the layers of the OSI and TCP models, you should be familiar with the following concepts and terms related to network traffic.

Network segments	Large networks are frequently broken into manageable pieces called *segments*. A segment is a portion of a network on either side of a router or bridge (these devices will be discussed shortly). Within a given network segment, devices can send data to each other using a MAC address. Breaking networks into segments keeps the network functioning efficiently. In an Ethernet network, a network segment is also called a collision domain.
Collision domain	An area in a network where a group of network devices compete for access to the transmission medium. In traditional Ethernet networking, only one device can transmit at any time. When two devices attempt to transmit at the same time, their transmitted frames collide and are destroyed. The more collisions there are, the less efficient the network is.
Access methods	Rules by which networking devices abide to avoid a high number of collisions. Some technologies use collision avoidance, whereas others use collision detection. The access method is determined at Layer 2 of the OSI model.
Broadcast	A transmission from one network node that is intended to reach all other nodes on the local network segment. Broadcasts are used whenever a device needs to send out information, but does not know which device to address it to. Broadcasts are important to the function of a network, but must be handled carefully because they generate a lot of traffic.
Broadcast domain	A logical area in a network in which any connected device can transmit to any other device in the domain without having to go through a routing device. Broadcast traffic is limited to the confines of a broadcast domain. If a network has been broken into segments, each separate segment is a broadcast domain.
Simplex communication	A mode of communication in which the data can flow in one direction only (similar to a public address system).
Half-duplex communication	A mode of communication in which the data can flow in two directions, but in only one direction at a time, similar to a walkie-talkie.
Full-duplex communication	A mode of communication in which data can flow in two directions simultaneously, similar to a telephone conversation.

Exercise 2-2: Introduction to internetworking devices

In this exercise, you will watch a video that introduces networking devices and the process required to move a packet across the Internet.

1. Instructor: Present the following YouTube videos to the class:

   Warriors of the net http://www.youtube.com/watch?v=Ve7_4ot-Dzs

   Note: this video is 13 minutes long.

2. As a class, review the steps required to send a Web page request out to a Web server.
3. Do you think that all packets travel across the Internet in this way (or in a way similar to the one in the video)?
4. Do you think this system of transporting packets is efficient?

In this exercise, you were introduced to internetworking devices and to the way in which a packet is transported across an IP network.

Networking Devices

Objective
3.1

Now that you have an idea of the seven layers of the OSI model, you can understand how networking devices function. Each device is designed to operate at a specific layer (or layers) of the model, and thus, is designed to work with data at various stages of encapsulation.

NICs

As you learned in Lesson 1, the NIC is the interface between the computer and the network, providing the physical connection between the computer and the network cabling. A NIC operates at the data link layer (Layer 2), as this is where the MAC address is defined. The physical connection to the cabling, however, operates at the physical layer (Layer 1).

Hubs

A *hub* connects computers in a network so they can exchange information. It is a central connection device with several ports and each node attached to the network plugs into a port on the hub using a network cable. Most hubs regenerate the electronic signals sent to them by the nodes. Hubs operate at the physical layer (Layer 1) of the OSI model. They can be connected to other hubs, or "daisy-chained," to provide more ports for a larger network.

Technically, a hub connects multiple devices into the same collision domain and allows frame collision. Hubs do not break up a network into segments the way bridges or switches do. A hub takes a signal coming from any node and passes it on to all the other nodes on the network.

All hosts connected to the hub must share the bandwidth and only one host can transmit at a time. Each host is responsible for detecting collisions and retransmitting frames if some were lost in a collision. This traditional setup is called shared Ethernet.

In a shared Ethernet network, transmission is half-duplex. That is, data can be transmitted in only one direction at a time. Hubs have been widely replaced by switches in modern networks.

Bridges

Bridges are networking devices that determine whether a frame belongs on a local network segment, or on some other network segment. Bridges make this determination by examining the destination hardware address (MAC address) encapsulated in each frame. Bridges operate at the data link layer (Layer 2) of the OSI model. Bridges are commonly used to divide a network into separate segments, thereby reducing traffic by creating smaller collision domains. Bridges have also been largely replaced by switches in modern networks.

Switches

Objective 2.1

A *switch* is a networking device that can connect either individual systems or multiple networks. Switches include multiple Ethernet ports, with different sized switches offering a varying number of ports. A switch directs the flow of data directly from one node to another.

Basic Function

A switch is much faster than a hub or a bridge because it cross-connects all hosts connected to it, thereby providing a separate connection between any two nodes that need to communicate. A switch segments a collision domain into as many segments as there are connections between nodes. For any given connection, the collision domain consists of only the two nodes that are communicating. For this reason, the switch can give each sender/receiver pair the line's entire bandwidth; this is in contrast to communication in a hub, in which all connected devices must share the bandwidth.

Switches also provide full-duplex communication. A switch can handle multiple simultaneous communications between the computers attached to it, whereas a hub can handle only one at a time. Ethernet networks that use switches instead of hubs are called Full Ethernet networks.

In contrast to routers, switches forward broadcast traffic. The following figure shows a 24-port switch.

OSI Layer(s)

By definition, a switch operates at the data link layer (Layer 2). However, there are several types of switches that operate at different layers.

Layer 2—LAN switch

A Layer 2 switch, also called a LAN switch, provides a separate connection for each node in a company's internal network. This type of switch forwards traffic based on MAC addresses, and is much faster than a bridge.

Layer 3 switches

A Layer 3 switch, also called a routing switch, forwards traffic based on network address information as well as based on MAC addresses. Layer 3 switches are used to connect networks. These switches are much faster than routers because they can act on Layer 2 information as well as Layer 3 information, and are replacing routers in many installations in the core network.

Layer 4 switches

Layer 4 switches make forwarding decisions based on Layer 4 information (such as the specific TCP/UDP port that an application uses), as well as on Layer 2 and 3 information.

Switching Technology

A LAN switch maintains a content addressable memory (CAM) table. The CAM table maps individual MAC addresses on the network to physical ports on the switch. This allows the switch to direct data out of the physical port where the recipient is located, as opposed to broadcasting the data out of all ports as a hub does.

In a process called *packet switching*, a LAN switch enables a connection between two network segments just long enough to send the current packet. A frame coming into a switch contains an IP packet payload with a Layer 2 header that includes MAC address information for both the source and destination system. The switch reads the MAC address in the frame header and compares it to a list of addresses in its CAM table. The switch then forwards the frame accordingly.

Switches can use two methods for forwarding traffic:

Store-and-forward	Using this method, the switch saves the entire packet in its buffer and checks it for CRC errors before forwarding it. Packets that contain errors are discarded.
Cut-through	Using this method, the switch reads the MAC address as soon as the frame begins to enter the switch. After reading the destination MAC address, the switch immediately begins forwarding the frame. This method provides no error detection or correction.

Many switches combine the two methods for forwarding traffic.

Transparent bridging

Switches use a technology called *transparent bridging* to learn about the location of nodes on the network without a network administrator having to configure anything. Transparent bridging consists of five parts:

Learning	A switch receives a packet from a computer (Node A) on a particular segment (Segment A) and stores Node A's MAC address in its lookup table for Segment A.
Flooding	The packet received from Node A is addressed to Node B, which resides on Segment C. The switch does not know where Node B is located, so the switch broadcasts the packet out to all the segments (except Segment A) in order to find Node B. This process is called *flooding*, because the packet is flooded to all the ports on the switch except for the port of origination.
Forwarding	When Node B receives the packet, it sends an acknowledgment to Node A, which comes first to the switch. The switch adds the MAC address for Node B to its lookup table for Segment C. This eliminates the need for further broadcasting of packets destined for Node B. The switch forwards the packet directly to Node A.
Filtering	Switches ignore packets that have a source and destination address on the same (local) network segment. Filtering reduces network traffic.
Aging	Lookup table entries are time-stamped. Old entries are periodically purged to free up memory in the switch.

Hardware Redundancy

Redundancy in a network eliminates the possibility of single points of failure. For example, redundant switches can ensure that multiple paths are available for network traffic in the event that one of the switches fail. However, the network administrator must take care that a switching loop is not created.

A *switching loop* occurs when there is more than one path between two endpoints. A switching loop will create a broadcast storm. In a broadcast storm, redundant switches flood the same network segments searching for a destination node. Each switch will receive the broadcast from the other switch, and rebroadcast it back out again, flooding the network. Broadcast storms congest the network and can ultimately cause network failure. (If not controlled, a broadcast storm can generate enough traffic to cause a complete network failure.)

Spanning Tree Protocol (STP)

Spanning Tree Protocol (STP) is a protocol that enables the use of redundant switches on a network. STP designates one switch from each pair of redundant switches as the designated switch. The other switch is identified as the backup switch. Although there may be physical loops on the network, STP creates a loop-free logical topology because the backup switch is not counted as a potential path unless it is needed. For example, if the designated switch fails, the backup switch can detect the failure and bypass the failed switch.

The Spanning Tree algorithm senses which switch has more than one path for communicating with a node, then determines the most efficient path and blocks out the other paths. It also keeps track of the other available paths and can restore one of those should the primary path become unavailable. STP allows switches to configure themselves, resulting in a fault-tolerant network that is easy to maintain.

Switch Features

A wide variety of switches is available for both home and enterprise use. Distinguishing features of switches include:

Number of ports	The number of ports determines how many systems can be connected to the switch. Common numbers of ports on Ethernet switches are 5, 8, 10, 24 and 48 ports.
Type of ports	The ports on the switch can be rated at 10 Mbps, 100 Mbps, or 1 Gbps. Some switches support multiple speeds and will adjust automatically to match the speed of the system connected to the port. The number and type of ports directly affect the cost of a switch. The speed of a switch also usually determines how it will be used. For example, on a large network a gigabit switch might be used as a core switch. It will handle heavy traffic and offer high speed. In contrast, a slower switch, such as a 100 Mbps switch might be used as an access switch. An access switch is the switch to which individual systems connect.
Backplane speed	The backplane consists of the internal connections within the switch that move frames between the ports in the switch. Backplanes are high speed and allow full bandwidth between any two users or segments.
Number and speed of uplinks	Switches contain regular ports (into which systems are connected) and uplink ports. You use an uplink port to connect a switch to a networking device on a larger network, such as another switch or a modem or a router. (The wiring inside an uplink port differs from the wiring inside a regular port.)
Managed or unmanaged	A switch can be managed or unmanaged. Unmanaged switches are plug-and-play devices. You cannot change any configurations in these devices—you simply plug systems in and the switch makes the connections. Unmanaged switches are commonly used on home networks. A managed switch, on the other hand, can be configured by a network administrator. For example, the switch could be configured to use STP, or to set up virtual LANs (VLANs). Two subclasses of managed switches are smart switches (they provide a Web-based interface which allows manipulation of some configuration settings) and enterprise managed switches (also called fully managed switches). These provide a full set of management features as well as a command line interface for configuration purposes. Typical switch management features include: • Turning a particular port range on or off • Configuring bandwidth and duplex settings • Setting priority levels for particular ports • Using STP • Monitoring traffic and/or listening to particular types of network traffic • Enabling security or MAC address filtering

Benefits of Using Switches

Switches offer the following benefits for networks:

- Simple installation—installing a switch as a replacement for a hub or a bridge is as simple as unplugging connections from existing devices and plugging the connections into the switch ports.
- Higher speeds—as you have learned, switches have high-speed backplanes that allow full bandwidth between any two users or segments. This feature eliminates the switch as a potential network bottleneck.
- More server bandwidth—servers can connect directly to switches. This capability allows network users to utilize the network's full bandwidth when accessing server resources.
- Creation of VLANs—you can create a logical group of systems called a *virtual LAN (VLAN)*. A VLAN allows you to organize systems according to their logical functions on the network, as opposed to their physical locations. VLANs allow you to prioritize traffic, and reduce network congestion.
- Default security—one of the “default” benefits of using switches over hubs is that it is more difficult to "sniff" (examine data traveling over a network) network connections in a switch-based network than in a standard hub-based network. Each connection made in a switch is dedicated; in a hub-based network, any one system can see all connections made on the network.

- Security features—managed switches provide specific security features to protect an enterprise network. These include: port security (specifying which MAC addresses can access a particular switch port), using 802.1x for user authentication, configuring and isolating VLANs.

Exercise 2-3: Researching switches

In this exercise, you will research network switches and observe the wide variety of products available.

1. Open a browser and research the network switches available for home and enterprise use. If you are having difficulty finding information, research the products made by 3Com, Cisco, Juniper, or NetGear.
2. What types of switches could you find? How many ports are available? Were you able to find pricing information?
3. Research data center and service provider switches. How do the features available on these devices compare to the ones available on a basic 4-port network switch?
4. Are there more types of switches than you had originally thought? How vital do you think switching is on the LAN?
5. Close your browser.

In this exercise, you began to explore different types of network switches.

Virtual LANs (VLANs)

Objective
1.2

A *virtual local area network (VLAN)* is a logical subgroup within a LAN created with software instead of hardware. A VLAN is a collection of nodes that are grouped into a single broadcast domain that is based on something other than physical location. That is, VLANs do not depend on the physical topology of the LAN.

Whereas network hubs allow you to group systems only by their physical location, VLANs allow you to organize systems according to their logical functions on a network instead of their physical locations. In a VLAN, computers that are connected to separate network segments appear and behave as if they were on the same segment.

In computing, a virtual component is something you can see, although it is not really there. You can think of a virtual LAN as a virtual hub that spans across multiple switches, including selected ports from each switch.

In a typical network, everything on the same side of the router is all part of the same broadcast domain. A switch on which you have implemented VLANs has multiple broadcast domains, and there is a one-to-one correspondence between VLANs and IP subnets. Each IP subnet is its own broadcast domain and you need a router to pass information from one subnet (VLAN) to another. (You will learn about subnets shortly.)

VLANs and Switches

MMM
Configuring VLANs

VLANs are implemented on switches. You will recall that a switch provides full-duplex communication, handles multiple simultaneous communications, segments a collision domain into as many segments as there are connections between nodes, and reduces the collision domain so that only the two nodes in any given connection coexist within each collision domain.

VLANs eliminate collision domains and operate at Layer 2 of the OSI/RM. A single VLAN can span multiple switches, and you can have more than one VLAN on each switch. When you implement VLANs, the broadcast domain is split into the number of VLANs. That is, if you have five VLANs, you will have five broadcast domains. Although VLANs increase the number of broadcast domains on a network, they reduce the size of each broadcast domain. VLANs do not forward broadcast traffic. VLANs are connected by routers or Layer 3 switches.

You can create a VLAN on a switch by accessing the configuration interface and entering the parameters for the VLAN (name, domain and port assignments). After you have created the VLAN, any network segments connected to the assigned ports will become part of that VLAN.

To "see" a VLAN, you must look at the individual switch ports to which the hosts are connected. When you interconnect more than one switch, the ports that interconnect them use a *trunking protocol* that allows traffic from different VLANs to share the same physical link.

VLAN Benefits

VLANs offer several benefits to an enterprise. These include:

- Network security—the network administrator can separate systems containing sensitive data from the rest of the network, thereby reducing the chance that users can gain unauthorized access.
- Traffic control—even though they are created on switches, VLANs do not forward broadcast traffic. You can also prioritize traffic, assigning high priority to a particular VLAN, for example, and lower priority to others.
- Support for special projects—systems involved in a particular project can be grouped together into a VLAN for the duration of the project, and then reassigned accordingly at the end of the project.
- Access control—because systems are assigned to a particular VLAN, the network administrator can control which systems see particular network traffic and which systems can access other systems.

Routers

Objective
2.2

A *router* is a device that routes data packets between networks based on network layer (Layer 3) information.

Routers are similar to bridges in that they are used to divide a network into separate segments, but they operate at the network layer (Layer 3) of the OSI model. Instead of using MAC addresses, routers use the network portion of the IP address to determine where data should be forwarded or "routed."

Routers can be used to connect separate network segments on a LAN, or to connect separate LANs. Routers identify the destination machine's network address, then determine the most efficient route for sending the data to the destination. Because routers direct data packets between different networks or network segments, they do not forward broadcast traffic.

An organization typically has one router that connects to a public carrier's lines to access the Internet. This type of router is called an *access router* because it provides access to the Internet. The access router provides the path outside the LAN. Because it acts as a gateway to the Internet, this router is referred to on the network as the "*default gateway*."

Routers and Subnets

Recall that large networks are frequently broken into manageable segments. Ethernet networks use a broadcast system. A packet sent from any system on the network is seen by all the other systems on that same network. Each system examines the packet to determine whether the packet is addressed to it. The more nodes there are on the local network, the more traffic is generated and the slower the network performs. Segments are a physical construction; they are physical subdivisions of a network.

A subnet, or sub network, is a logical subdivision of a network. It serves a similar purpose as a network segment—to reduce traffic and congestion.

The practice of dividing a network into subnets is called *subnetting*. Subnets are distinct from one another, and systems on different subnets can communicate with one another only by passing their data through a router. The router manages traffic between subnets, and unlike switches, routers do not forward broadcast packets.

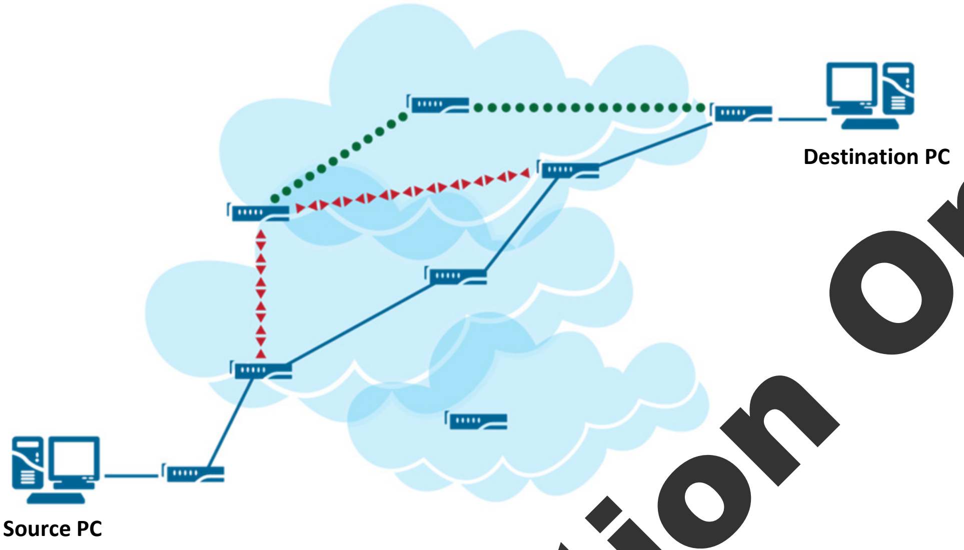
A router is considered the logical border or boundary of a subnet. All systems within a subnet are considered to be on the same side of the router. Systems in a different subnet are considered to be on the other side of the router. Each subnet in a network is served by a designated default router (one router may be the designated default router for several subnets). Systems within a subnet may still be arranged into multiple physical network segments interconnected by switches or bridges.

The Routing Function

Routing is the process of selecting a path over which to send data packets in a network. Layer 3 performs the routing function. A data packet includes the required information for routing the packet from the source host to the destination host. This information is contained in the IP address.

When routing a packet, a router always tries to select the best path. The best path may be the shortest path, or the most accessible, depending upon how the router makes its decisions. Routing across the Internet or any WAN always involves more than one router, and usually involves many routers. In fact, packets may traverse several networks before reaching their destination host.

Each router a packet is passed to along the way to its destination makes its own routing decisions on where to forward the packet next. Different packets sent between a source host and destination host may take different paths across the Internet on their way from source to destination. The following figure shows a few of the possible paths a packet may take when being sent from a source PC to a destination PC.



Direct and Indirect Routing

Routing can be classified as either direct or indirect.

Direct routing

Direct routing takes place when the source and destination hosts are on the same physical network or subnet (the systems are on the same physical network if the network portions of the source and destination addresses are the same). This type of delivery does not require a router at all. When two computers on the same physical network need to communicate, the source system binds the destination IP address to a MAC address and transmits the packet directly to its destination. The packet is considered a *local packet*.

Indirect routing

When two computers that are not on the same physical network need to communicate, they must send their IP packets to a router for delivery because they are located on remote networks. Whenever a router is involved in communication, the activity is considered indirect routing. The term “routing” generally refers to indirect routing.

The Routing Process

Routing involves two key elements:

- The source system must know where to send packets that are destined for a remote network. Packets bound for a remote network are sent to the default gateway. The default gateway is the IP address of the router on your local network; this router will take the packet from the local network and send it elsewhere on the way to its destination.
- The router must know where to send the packet. It makes this determination by using its routing information table (or routing table).

Routing Tables

A *routing table* is an in-memory database managed by the router’s hardware and software. The router uses the entries in the routing table to calculate where to send a packet is it responsible for forwarding.

Routing tables contain a list of IP addresses. Each IP address identifies a remote router or network that the local router is configured to recognize. The routing table also includes information that specifies the destination IP address ranges that the remote router will accept.

When a packet arrives at the router, the router examines the packet's destination network, and then checks its own routing table. It determines the next router to which to send the packet, and forwards the packet to that router. This part of the journey is considered a *hop*. In some cases, the destination network is attached to the router, in which case the packet has reached its destination network.

If a router does not have a route to a specific device in its routing table, it will send that packet to its default gateway, which is also specified in the router's routing table.

Home network routers use a very small routing table because they forward all outbound traffic to the ISP's gateway (usually the ISP's primary DNS server), which will handle all additional routing steps that are required. Packets bound for other systems on the home network are handled directly by the home router. Home network routers generally maintain routing tables of ten or fewer entries.

Internet backbone routers on the other hand maintain the full Internet routing table, which includes more than 100,000 entries. Enterprise routers fall somewhere in between. Their routing tables include information on remote networks relative to the router's location. Depending on the number of subnets and internal routers on the LAN, the routing table can become quite large.

Static, Dynamic and Directly Connected Routes

A *static route* is a route that is manually entered into a router's routing table by a network administrator. If static routing is used on a LAN and a route to a certain network does not exist in the static routing table, the router will be unable to communicate with that network.

Static routes are not fault-tolerant; if a specified path becomes unavailable (for example, due to a failure or a change in configuration), traffic will not be rerouted until either the failure is corrected or the administrator updates the routing tables.

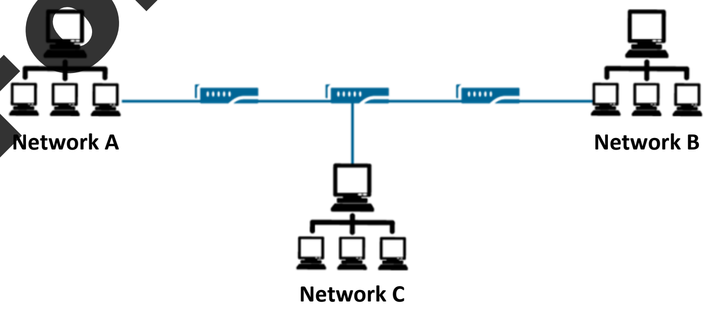
Dynamic routes are built from shared information that comes from other routers on the network. A dynamic router communicates with other dynamic routers in the network to calculate routes automatically using routing protocols (which will be discussed shortly). Dynamic routers exchange information about routes of known networks. When a route changes, the routers automatically update themselves by recalculating routes.

Home network routers set up their routing tables dynamically when they connect to the ISP, generating a routing table entry for each of the ISP's DNS servers, and an entry for routing among the home computers in the LAN. Most residential network routers do not support manual configuration of their routing tables. Enterprise routers, however, typically allow network administrators to manually update routing tables.

Directly connected routes are routes to hardware interfaces directly connected to the router. That is, a router automatically learns about the devices to which it is directly connected. (These are devices within the subnet connected to the router.) Directly connected routes are preferred over routes through other routers.

Hop Count

Aside from maintaining a list of IP addresses, the routing table also includes metrics that identify how many hops are required to reach a particular address. A *hop* is one link between two network devices. For example, in the following figure, it will take 3 hops to get from Network A to Network C, and it will take 4 hops to get from Network A to Network B.



The number of hops between any two devices is called a hop count. Routers take hop count into consideration when selecting a route for a packet that will be forwarded.

Exercise 2-4: Finding routers along the way

The tracert command determines whether a destination system is on the same local network or whether a default gateway is used to send a packet to a remote network. When a packet is passed to another network by a router, the IP address of the router displays in the command output. Each router that a packet hits on its way to a destination host is called a hop.

Output from the tracert command indicates the path between source and destination systems and provides information about the time it takes for a packet to make a round trip between each router and the source system. This time is called the round-trip propagation time. These times are returned in milliseconds.

In this exercise, you will use the tracert command to locate routers between a source and destination system. For the purposes of this exercise, select one classmate as a partner.

1. Click the **Start** button, type: `cmd` in the Search programs and files text box, then press ENTER to open a command prompt window.
2. In the command prompt window, type: `ipconfig` then press ENTER to display information about your current IP configuration, including the IP address. (You used the ipconfig command in Lesson 1.) Record your IP address here ___________________________.
3. Use the tracert command to examine the route from your machine to your partner's machine. Enter:

   ```
   tracert [ip_address]
   ```

   How many hops does it involve? ____________

   If the destination host is on the local network, this command will result in a response similar to the one shown below. The single line of output indicates that the destination is a host on the local network, and no hops are required:

   ```
   Tracing route to 192.168.3.11 over a maximum of 30 hops:
   1      <10ms  <10ms    <10ms  192.168.3.11
   Trace complete.
   ```

   If the destination host were on a remote network, the first line of output would list the IP address of the router (default gateway) and therefore constitute a hop. Additional lines of output between the first line (the default gateway) and the final line (the destination host) would also list IP addresses of routers and be counted as hops along the way.
4. Use the tracert command to determine the path from your machine to your favorite Internet site. For example, enter the following:

   ```
   tracert www.google.com
   ```

   How many hops does it take to reach Google? What is the round-trip time? Compare *tracert* output for paths from your machine with paths from machines in the United States (*www.ansi.org*) and in Europe (*www.iso.ch*).
5. Use the tracert command to trace the path to a site on a different continent. Are there more or fewer hops that it takes to reach a site on your own continent?
6. Close the command prompt window.

In this exercise, you used the tracert command to examine routers between a source and destination system.

Routing algorithms

A *routing algorithm* is the formula routers use to calculate the best route on which to send a packet. Parameters for determining the best route include hop count, time delay and the cost of packet transmission. "Cost" is determined in terms of distance to the next router, as well as the direction to the nearest router.

There are two major types of routing algorithms:

- Decentralized algorithms—each router has information about the routers to which it is directly connected. It does not know about every router in the network. These algorithms are also known as *distance vector algorithms*.

  In distance vector algorithms, each router has to follow these steps:

  1. It counts the cost of the links directly connected to it and saves the information to its table.
  2. It sends its table to its neighbor routers (not to all routers on the network) and receives the routing table of each of its neighbors.
  3. Based on the information in its neighbors' routing tables, it updates its own.

- Global routing algorithms—each router has complete information about all the other routers in the network and has information about the traffic conditions on the network as well. These algorithms are also called *link state algorithms*.

  In link state algorithms, every router has to follow these steps:

  1. Identify the routers that are physically connected to them and get their IP addresses.
  2. Send echo packets to neighbor routers in order to measure their delay time and/or average traffic.
  3. Broadcast its information over the network for other routers and receive the other routers' information. In this way, every router learns the structure and status of the network.
  4. Build a graph of the network that shows the location of routers and their links to each other. Assign a cost to each link, and then identify the best route to every node on the network.

Default Routes

A *default route* is the network route used by a router when no other known route exists for a given destination IP address, such as an IP address outside the LAN. The default route is usually to a router that has a connection to the network service provider (or ISP)—the default gateway. It is common for the default gateway to also provide firewall and/or proxy services to the LAN.

Routing Protocols

Routing protocols are required for dynamic routing. They determine how routers share information and report routing table changes to one another. When routing protocols are used, networks can be expanded or reconfigured without requiring an administrator to update routing tables.

There are two basic types of routing protocols:

- Interior routing protocols are used to communicate routing information between routers within an autonomous system. An autonomous system is managed by a single organizational entity, and includes all networks and routers managed by that entity. Routers within an autonomous system are called interior gateways. Interior routing protocols include:

  – Routing Information Protocol (RIP and RIPv2)—an efficient choice for small networks (2 or 3 routers) with a relatively static structure. RIP maintains only the best route to a destination (that is, the route that contains the fewest hops). Regular routing table updates are sent across the network.

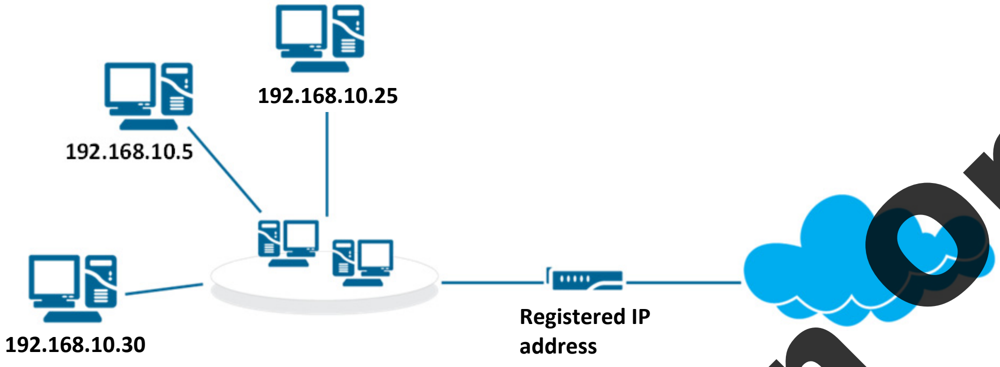
  – Open Shortest Path First (OSPF)—a good choice in larger networks where multiple alternative routes are available. Routing decisions in OSPF can take available bandwidth, security settings and multiple paths into consideration. Routing table updates occur only when necessary.

- Exterior routing protocols are used to send information between autonomous systems. Routers that belong to different autonomous systems that exchange information with one another are called exterior gateways. Border Gateway Protocol (BGP) is the exterior routing protocol used on the Internet.

Network Address Translation (NAT)

Objective
3.2

Network Address Translation (NAT) is the process of translating one IP address into another. There are many applications for NAT. For example, if you are using a private IP addressing scheme inside your LAN, you must convert the private IP addresses into one or more registered IP addresses in order to access the Internet. NAT allows a router or firewall to alter the IP packet and replace the private IP address with one that can be routed across the Internet.



NAT is important to network security because it hides internal systems from systems outside the LAN (for example, from systems on the Internet). NAT is included in a router and is often part of a corporate firewall. Proxy servers also provide NAT services. By translating addresses, these devices form a buffer between the core LAN and the Internet. Using private addresses on the LAN protects the internal hosts because they cannot be reached directly from the Internet.

Typically, a company maps its local internal network addresses to one or more public IP addresses, and unmaps the public IP addresses on incoming packets back into local IP addresses.

Address translation tables

A network administrator creates address-translation tables that map public-to-private and private-to-public addresses. These addresses can be statically defined, or can be set up to dynamically translate to and from a pool of IP addresses.

Types of NAT

Three types of NAT exist:

Port Address Translation (PAT)	Multiple IP addresses are translated into one valid IP address. For example, if you are given only one valid IP address for multiple hosts, PAT would be your only option.
Static address translation	Multiple IP addresses are mapped to valid IP addresses in a one-to-one relationship.
Dynamic address translation	Multiple IP addresses are mapped to valid IP addresses randomly.

Exercise 2-5: Do you use NAT?

In this exercise, you will determine whether your network uses network address translation.

1. Recall from Lesson 1 that the ICANN has reserved the following IPv4 address ranges as private IP addresses:

   10.0.0.0 to 10.255.255.255
   172.16.0.0 to 172.31.255.255
   192.168.0.0. to 192.168.255.255

2. Consider the IP address you recorded in the previous exercise (or open a command prompt window and find your IP address if necessary). Are you using a private IP address or a registered IP address? ___________________________

3. Open a browser and visit your favorite Internet site. If you are using a private IP address and you are able to access the Internet, a device on your network (router, proxy server or firewall) performs network address translation. You may be able to find the IP address of your router by typing the following URL in the browser address bar: `http://checkip.dyndns.org/`

4. Close any open windows.
5. Does your classroom network use NAT? ________________ Which network device performs NAT? _____________
6. If it does, list at least two reasons why NAT is employed on your school network. ____________________________

    ____

In this exercise, you determined whether your network uses network address translation.

Router Features

There are a wide variety of routers available suited for different settings. They differ in their degree of programmability, number and type of ports, amount of routing table memory, functions supported, and supported transmission speeds.

Home/Broadband routers

A home broadband router, such as the one shown in the figure, generally includes four 10/100 Mbps Ethernet ports and a WAN port (or Internet port) for connection to a DSL or cable modem. You connect the router to your modem by attaching one end of an Ethernet cable to the router's WAN port, and the other end of the cable to the Ethernet port on the cable modem. This connection allows the router access to your Internet service.

The other Ethernet ports on the broadband router are LAN ports. When you want to connect other computers to the network, you attach them (via Ethernet cable) to the LAN ports. Wireless broadband routers also support wireless connections at speeds based upon the standard in use (e.g., 11 Mbps, 54 Mbps, 300 Mbps).

These routers do not require much memory as their routing tables are generally short. They are designed to work “out-of-the-box” and are not highly configurable. Most of these devices are combination boxes that also perform switching functions, and DHCP and firewall functions.

Enterprise routers

Enterprise routers are used in medium to large businesses, data centers and ISPs. These can be highly complex and administrator-configurable devices that support large routing tables (60,000 routes or more), and support connections to various types/speeds of WAN interfaces (e.g., ISDN, T1, E3, high-speed fiber lines, etc.). These devices often feature separate and redundant power supplies, expandable memory slots for flash cards and DRAM, and modular components for upgrades and expansion.

The number and speed of the ports on these devices also vary, but many include gigabit and 10-gigabit Ethernet ports. These routers perform load balancing, prioritize traffic, and guarantee quality of service (QoS) for specific types of traffic (such as VoIP traffic).

Core routers

A core router is designed to operate in the Internet backbone (or core). It must be able to support multiple telecommunications interfaces operating at the highest speed in use in the core (in 2007, the Internet core link speed was 10 Gbps, with a few links at 40 Gbps). The core router must also be able to forward IP packets at full speed on all of its interfaces.

The two leading manufacturers of core routers are Cisco Systems and Juniper Networks.

The Juniper Networks T-series of routers (T320, T640, T1600, TX Matrix and TX Matrix Plus) provide throughput from 320 Gbps to 25.6 Tbps.

The Cisco Carrier Routing System (CRS) models CRS-1 and CRS-3 provide throughput from 320 Gbps to 322 Tbps.

Software Routing in Windows Server

So far in this lesson we have discussed hardware routers. It is also possible to perform *software routing*. Any host with more than one network interface card (NIC) is said to be *multihomed*. A multihomed device can have multiple connections to the same network, or connections to different networks. Any host that is connected to two networks can be configured to function as a router between those connected networks by installing and/or activating the necessary software. Using a computer as a router is called software routing.

Software-based routing solutions can be used for small networks with light traffic. Beginning with Windows Server 2003, all versions of Windows Server have offered Routing and Remote Access Service (RRAS).

RRAS consists of the following components:

Remote Access	By using RRAS, you can deploy VPN connections to provide end users with remote access to your organization's network. You can also create a site-to-site VPN connection between two servers at different locations.
Routing	RRAS is a software router and a platform for routing and networking. It offers routing services to businesses in local area network (LAN) and wide area network (WAN) environments or over the Internet by using secure VPN connections.

Transmission Types

In order for communications to flow through a network, the data must be transmitted across the transmission medium (whether it be air, copper or fiber). Transmission can take many forms, and it is helpful to understand various transmission concepts, including asynchronous and synchronous transmission modes, and baseband and broadband transmission.

Synchronous Transmission

When devices exchange data, the sender and receiver must have a way to extract individual characters or frames of information from the data stream. In synchronous transmission, the sending and receiving devices share a clock and transmission rate. The transmissions are synchronized.

Data is exchanged in character streams called message-framed data. A start-and-stop sequence is associated with each transmission. The sender and receiver need to be synchronized so that the entire message is received in the order it was transmitted. T1 lines use synchronous transmissions.

Asynchronous Transmission

In asynchronous transmission, there is no shared clock and the sender and receiver are not synchronized. (The transmission speeds between the sender and receiver must be the same, however.) Data is transmitted as individual characters, and each character includes a start bit and a stop bit so that both systems can identify where each character begins and ends. Dial-up modems use asynchronous transmissions.

Baseband and Broadband Transmissions

In networking, *bandwidth* is the amount of information (also called *traffic*) that can be carried on a given network connection at one time. In data networks, bandwidth is measured in bits per second (bps). A transmission medium's bandwidth can be divided into channels, and each channel is a portion of the total capacity available to transmit data. The two methods used to allocate bandwidth to channels are baseband and broadband.

Baseband

Baseband uses the entire media bandwidth for a single channel. Most LANs, such as Ethernet networks, use digital baseband signaling.

Baseband uses a transmission technology called *time division multiplexing (TDM)*. TDM sends multiple signals over one transmission path by interweaving the signals. For instance, three signals (X, Y and Z) can be sent as XXYYZZXXYYZZ. The receiving device separates this single stream into its original three signals.

Broadband

Broadband divides the media bandwidth into multiple channels, and each channel carries a separate signal. This method enables a single transmission medium to carry several communications simultaneously without interference.

Broadband uses a transmission technology called *frequency division multiplexing (FDM)*. Like TDM, FDM also transmits multiple signals over a single transmission path. However, each signal in FDM transmits within a unique frequency range, or carrier. FDM is used in cable modems and digital subscriber lines (DSL).

Transmission Media

Objective
2.3

Network transmission medium is usually a type of wire or cabling, although free space can also serve as a transmission medium in wireless networking. Wiring is the part of a network that is most vulnerable to interference and other performance problems which can be caused by improper handling or installation practices. The next several sections discuss transmission media.

Introducing the Cable Plant

A cable plant is another name for a network's cable implementation. In most networks, as many network connections as possible are made in one central location. However, restrictions in maximum cable length can sometime necessitate other layouts.

A backbone cable provides a path for communication between floors or between buildings. Central wiring locations are set up at strategic points to allow cables to fan out from the backbone to user locations within the building. Depending on how the network is configured, a bridge or router is typically used to connect to the backbone cable. In the past, coaxial cable has been used for backbones, but the use of fiber-optic is becoming more common.

When discussing cable distribution throughout a building or throughout a campus, you should understand the following terms:

Backbone cabling	Used to connect LANs together. Backbone cabling is found between internetworking devices such as routers and switches. Backbone cabling is usually used for high-speed connections that offer a large amount of bandwidth. Fiber optics, Gigabit Ethernet or ATM connections are often used. Within a building, the backbone runs between floors. *Note: ATM or Asynchronous Transfer Mode is a high-speed packet switching technology used for linking LANs.*
Campus distributor (CD)	Used between routers and switches to connect LANs in different buildings within one general location. Campus distributors use high-speed connections, such as fiber optics, Gigabit Ethernet or ATM.

Vertical cabling	Cabling that is considered part of the backbone and runs between floors in a multi-floor building.
Entrance facility	The point at which outside wiring enters a building (or where inside wiring leaves a building). This is also the termination point for the backbone cable.
Horizontal wiring	Wiring that connects individual users to the network.
Cross-connect	The point at which one type of wiring or cabling is connected with another.
Wiring closet	A room or closet that houses all equipment associated with network wiring systems. It includes the network's patch panels, cross-connects and access to the backbone. The connection for each user station terminates in the wiring closet. Networks that span multiple floors in a building typically have a wiring closet on each floor.
Intermediate distribution frame (IDF)	The cross-connection point between the horizontal wiring and the backbone cable. An IDF typically serves the needs of one floor. A building with several floors will have one IDF on each of the floors that is connected to the backbone cable.
Patch panel	A group of sockets (usually consisting of pin locations and ports) mounted on a rack. It is a central point where cables from different rooms or departments can be connected to one another (e.g., forming a LAN). It can then be used to connect a network to the Internet or some other WAN. A patch panel is a cross-connect.
Punchdown block	Also called a cross-connect block or a terminating block. The punchdown block is the predecessor of the patch panel. A device that connects one group of wires to another group of wires through a system of metal pins to which the wires are attached. Punchdown blocks come in 66-pin and 110-pin varieties.

Copper Cables and Interference

Before studying particular types of network cable, it is important to understand that copper network cable transmits information as electrical pulses through the wire. Metallic cable is susceptible to various types of interference that can disrupt data transmissions on the LAN. These types of interference include:

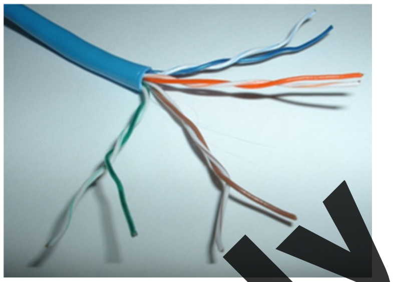
Electromagnetic interference (EMI)	Caused by the workings of electromechanical devices (for example, a device with a spinning motor), or by microprocessors, photocopiers, fluorescent lights and electrical power cords. EMI is also caused by natural atmospheric or solar activity.
Radio frequency interference (RFI)	Caused by radio and TV transmitters, communications equipment, cable television systems and other types of equipment that generate radio frequency energy as part of their operation. Both EMI and RFI can propagate through conduction over signal and power lines, and through radiation in free space.
Lightning and electricity	Sources of high voltage, such as power lines or lightning strikes can also interfere with data transmissions over metal cable.

Twisted-Pair Cable

Twisted-pair cable is perhaps the most widely used cabling system in Ethernet networks. A twisted-pair cable is composed of four pairs of copper wires. The wires in each pair are twisted around each other to protect against interference. The four pairs are then twisted together and bundled inside a covering.

Twisted-pair cable comes in two basic types—shielded twisted-pair (STP) and unshielded twisted-pair (UTP). Regardless of type, a twisted-pair segment cannot exceed 100 meters (328 feet).

Shielding is the selective use of metal to protect circuits from RFI and EMI. The metal shielding provides a conductive surface that directs potentially harmful EMI and RFI away from cabling. Shielded twisted-pair (STP) cable is simply twisted-pair cable that has a protective metal sheath wrapped around all of the twisted-pair wires. STP is more difficult to install than UTP because it is bulkier and more rigid. It was most commonly used on token-ring networks.



Unshielded twisted-pair is much more commonly used than STP because it is less expensive and it is easy to install. However, it is also less secure and is more susceptible to electromagnetic interference.

You should avoid passing UTP cables close to fluorescent lights. If the lights cannot be avoided, then the cables should cross the lights at right angles to limit the effects of EMI.

UTP cable is available in specific categories. Each category has a specific use, a specific number of twists per foot, and is capable of a specific bandwidth. The more twists there are per foot of cable, the less that interference affects the data traveling on the cable. This figure shows a section of UTP cable with the covering pulled back and the wire pairs separated for easy viewing.

The most commonly used grades today are Categories or "Cat" 5, 5e, 6 and 6a. A Cat7 cable exists, but it is still an emerging standard. The following table describes the most popular grades of twisted-pair, and lists both the data transfer rate (in Mbps) and the MHz value of the wire. Standard Ethernet requires a cable that supports at least 10 MHz; Fast Ethernet requires a cable that can support 100 MHz. The 100 meter maximum segment length applies to all categories of twisted-pair.

Cable Grade	Bandwidth	Uses
Cat 5	100 Mbps Rated at 100 MHz	Can be used for both standard Ethernet (10 Mbps) and Fast Ethernet (100 Mbps).
Cat 5e	1 Gbps Rated at up to 100 MHz	Can be used for Fast Ethernet and Gigabit Ethernet and other high-speed networks. Has largely replaced Cat 5.
Cat 6	2.5 Gbps Rated at up to 250 MHz	Supports Gigabit Ethernet. Unlike other categories of twisted pair, Cat 6 is not particularly durable and can cease to function if it is improperly bent.
Cat 6a	10 Gbps Rated at up to 500 MHz	Suitable for 10-Gigabit Ethernet.

Registered Jack-45 (RJ-45) connector

Twisted-pair cabling uses four types of connectors: RJ-11, RJ-14, RJ-25 and RJ-45. The "RJ" in each connector's name stands for "registered jack," and the number refers to the specific wiring pattern used for the jacks and connectors. Usually RJ-11, RJ-14 and RJ-25 are used for telephone connections.

MMM
Wiring an RJ-45 connector

Twisted-pair network cables use RJ-45 connectors. An RJ-45 connector (shown in the following figure) is slightly larger than the RJ-11 standard telephone connector. The RJ-45 connector holds up to eight wires, although only four of the wires are used for transmitting and receiving signals in a standard Ethernet or Fast Ethernet installation. Gigabit Ethernet and Power over Ethernet (PoE) installations use all four pairs of wires. A standard RJ-45 cable and connector is shown.

Twisted-pair cable is used for many types of network standards. For example, 10BaseT Ethernet networks use twisted pair; the name 10BaseT denotes a network running at 10 Mbps, using baseband transmission and twisted-pair cable. 1000BaseT runs at 1 Gbps on twisted-pair.

Understanding Ethernet wiring

Creating a cable is a simple matter of attaching the connectors. To attach an RJ-45 connector to a cable, the connector must be crimped using a tool called a *crimper*. The crimper pushes two plugs from the RJ-45 connector into the cable. One plug pushes into the cable jacket to attach the connector and cable. The other plug pushes eight pins through the cable jacket and into the respective wires.

An Ethernet cable can be wired using one of two sets of pin/pair assignments. These pin/pair assignments are named T568A and T568B.

The following table lists the standard wiring for an RJ-45 connector according T568B standard, with the tab facing down, and the wire entering the back of the connector. In the table, "tx" stands for "transmit" and "rx" stands for "receive." Note that only four wires in a standard Ethernet cable carry a signal.

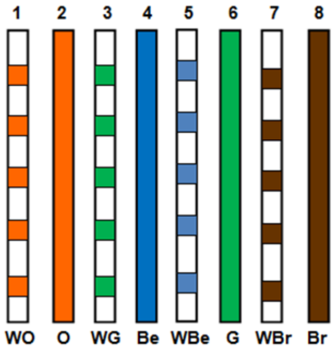
T568B Pin/Pair Assignments

Pin	Color	Input/Output
1	White with orange stripe (WO)	Output (+) tx
2	Orange (O)	Output (-) tx
3	White with green stripe (WG)	Input (+) rx
4	Blue (Be)	For telephone use, or Gigabit Ethernet standards
5	White with blue stripe (WBe)	For telephone use, or Gigabit Ethernet standards
6	Green (G)	Input (-) rx
7	White with brown stripe (WBr)	For telephone use, or Gigabit Ethernet standards
8	Brown (Br)	For telephone use, or Gigabit Ethernet standards

The T568A standard is older, and reverses the green and orange colors. The logical wiring is no different from that of T568B.

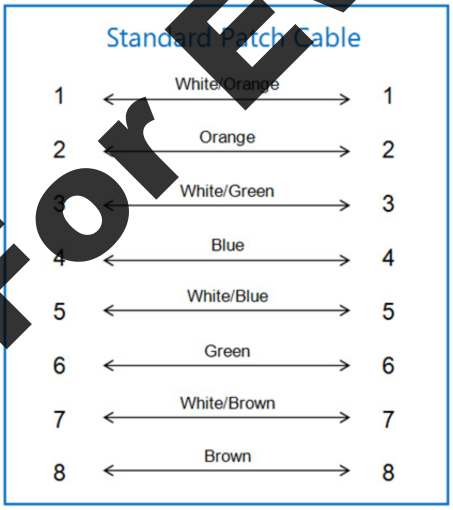
As shown in the table, Pins 1 and 2 are the transmit (tx) pair. Pins 3 and 6 are the receiving (rx) pair. Pins 4, 5, 7 and 8 do not carry a signal; they are reserved for telephony use or for additional Ethernet standards such as Gigabit Ethernet or Power over Ethernet, which use all eight pins.

This figure shows the standard wiring for an RJ-45 connector, with the tab (or clip) facing down, and the wire entering the back of the connector.



Straight-through cables

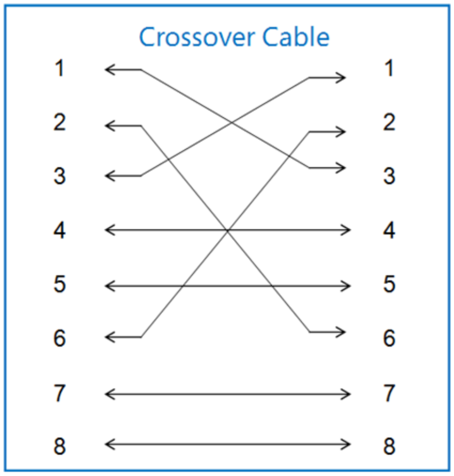
In twisted-pair wiring, two wires send data and two wires receive data. In a *straight-through cable*, both ends of the cable are wired into the connectors the same way. In other words, the same wires in the cable are connected to the same pins in the connectors at each end. Straight-through cables are used for Ethernet patch cables. You would use a patch cable to connect workstations to a hub or switch, for example.



You cannot use a straight-through cable to directly connect two computers. If Computer A is connected directly to Computer B with a straight-though cable (that is, a standard RJ-45 patch cable) and sends data to Computer B, then Computer B would receive the data on the wires intended for transmitting, not receiving. Hubs and switches translate these wiring sets. When a wire is plugged into a hub, the transmit wires are remapped to connect to the receiving wires on other cables connected to the hub.

Crossover cables

A *crossover cable* for Ethernet networks is a specialized cable that allows you to connect two computers directly without using an intermediary device such as a hub or switch. The crossover cable reverses, or crosses over, the respective PIN contacts. Whereas straight-through cables are wired the same way on both ends, crossover cables use the standard wiring on one end, and the reverse wiring for the transmit and receive pins on the other end.



Coaxial Cable

Coaxial cable, also called *coax* (pronounced "co-ax"), is a high-capacity cable used for video and communication networks. It provides higher bandwidth than twisted-pair cable. It contains a core of copper wire, surrounded by an external shield of woven copper braid or metallic foil. Flexible plastic insulation separates the inner and outer conductors, and another layer of insulation covers the outer braid.

The outer conductor shields the inner conductor from outside electrical interference and reduces the radiation of interior signals. This allows coax to be installed next to metal objects, such as rain gutters, without signal or power loss.

Several types of coaxial cable exist for different purposes. For instance, coaxial cable is designed for baseband, broadband and television (CATV) networks. A good quality video coaxial cable can transmit HD video at around 1.5 Gbps. In LAN environments, 10 Mbps was a common rate.

In LANs, coax has been superseded by UTP for desktop connections, and by fiber-optic cable for backbone cabling.

F-type connector

In cable TV and cable Internet installations, an F-type connector is used to attach coaxial cable to devices, such as television sets and cable modems. If you have cable TV, the coax cable that comes out of the wall uses an F-type connector to attach to your television. The F-type connector inserts the end of the coax signal wire into the port, then a threaded ring screws on to the threads on the port to keep the connection secure.

If you use a cable modem, you use one F-type connector to attach a coax cable to the wall, and another F-type connector to attach the other end of the cable to the appropriate port in your cable modem. The cable modem also has an RJ-45 port into which you insert an unshielded twisted-pair cable with an RJ-45 connector. The other end of the twisted-pair cable (with an RJ-45 connector) is connected to the RJ-45 port on the NIC in your computer.

Fiber-optic Cable

Fiber-optic cables consist of two small glass (or plastic) strands: one that sends signals and one that receives signals. These strands are called the core. Each core is surrounded by glass cladding. Each core and cladding element is wrapped with a plastic casing. Laser transmitters send light pulses through the core and optical receivers receive them.

Fiber-optic cable can accommodate data transmissions much faster than copper wire cable, transmitting data in the gigabits-per-second range. Because they send data as pulses of light over threads of glass, the transmissions can travel for miles without any signal degradation. No electrical signals are carried over the fiber-optic line, so the lines are free of electromagnetic interference as well. Fiber-optic transmissions are not generally susceptible to interception (that is, they are difficult to tap).

The two major types of fiber-optic cable are:

Single-mode fiber (SMF)	Supports a single transmission path. The cable's core diameter is 8 to 10 microns. It permits signal transmission at extremely high bandwidth and allows very long transmission distances (up to 70 km, or 43 miles). Single-mode fiber is often used for intercity telephone trunks and video applications.
Multi-mode fiber (MMF)	Uses a large number of frequencies (or modes). The cable's core is larger than that of single-mode fiber, usually 50 microns to 100 microns, and it allows for the use of inexpensive light sources. It is used for short to medium distances (less than 200 m, or 656 feet). Multi-mode fiber is the type usually specified for LANs and WANs.

Fiber-optic cable is also used as the backbone for networks. It had been predicted by experts in the optical networking industry that fiber-to-the-desktop (that is, a fiber-optic connection at the NIC) would become common. However, advances in copper cabling and the expensive nature of fiber-optic cable have at least delayed this occurrence.

Fiber-optic connectors

Optical fibers are joined to terminal equipment using fiber-optic connectors. Fibers may also be joined to one another using either fiber-optic connectors or splicing. The connectors couple and align the cores of the fibers so that light can pass through with minimal loss of light due to reflection or misalignment of the fibers.

Advantages

The advantages of fiber-optic cable are speed and distance. Fiber can carry signals over much longer distances than twisted pair.

Because fiber-optic cables send data as pulses of light, the signals are not distorted by any form of outside electronic, magnetic or radio interference. Fiber-optic cables are completely immune to lightning and high-voltage interference.

Disadvantages

Fiber-optic cable is expensive and difficult to install.

Fiber-optic networks and transmission speeds

Fiber-optic networks conform to one of two standards. These are *Synchronous Optical Network (SONET)* and *Synchronous Digital Hierarchy (SDH).*

SONET speeds are defined by the American National Standards Institute (ANSI). The basic unit of transmission for a SONET signal is the Synchronous Transport Signal (STS)-1 frame, which travels at 51.84 Mbps. SONET speed can be measured by STS designation (which refers to the frame format) or by the corresponding Optical Carrier (OC) levels. Although SONET is a North American standard, it is closely compatible with the equivalent international standard, Synchronous Digital Hierarchy (SDH).

The Synchronous Digital Hierarchy (SDH) standard is the international standard for fiber-ring networks. The basic unit for SDH is the Synchronous Transport Module (STM)-1 frame, which travels at 155.52 Mbps (three times the speed of an STS-1 frame).

The following table compares optical transmission speeds between the two standards.

SONET STS frame format	Optical Carrier Level (OC)	SDH Level STM frame	Speed
STS-1	OC-1		51.85 Mbps
STS-2	OC-2		103.68 Mbps
STS-3	OC-3	STM-1	155.52 Mbps
STS-6	OC-6	STM-2	311.04 Mbps
STS-9	OC-9	STM-3	466.56 Mbps
STS-12	OC-12	STM-4	622.08 Mbps
STS-18	OC-18		933.12 Mbps
STS-24	OC-24	STM-8	1.244 Gbps
STS-36	OC-36		1.866 Gbps
STS-48	OC-48	STM-16	2.488 Gbps
STS-96	OC-96	STM-32	4.976 Gbps
STS-192	OC-192	STM-64	9.952 Gbps
STS-768	OC-768	STM-256	40 Gbps
STS-3072	OC-3072	STM-1024	160 Gbps

Wireless Media

The four main free space transmission options are:

Infrared Signals are sent via light waves longer than those of the visible light spectrum. Infrared transmissions have a very limited range and require a clear path between the transmitter and the receiver. Infrared is susceptible to high levels of light and may not work in direct sunlight.

Microwave Signals are sent by line-of-sight transmission using parabolic (dish-shaped) antennas mounted on towers. Towers that are 100 meters (328 feet) high can transmit 100-km (62 miles) distances between towers. Microwave transmissions can support high data rates and quickly transfer large volumes of data. These transmissions can be affected by atmospheric conditions such as thunderstorms, and obstructions such as mountains or buildings.

Satellite Allows the transmission of signals between two stations that are not within the line of sight of one another. Satellites receive a transmission from one earth station, regenerate the signal (weakened by the distance), convert it (if necessary) to another frequency, and transmit it to another earth station.

Short-range wireless Used for networking PCs and for connecting PCs to peripherals. The common standard for peripheral devices communications is Bluetooth. The common standard for wireless LANs is 802.11 Ethernet. Short-range wireless does not require line-of-sight transmissions, allowing it to operate through office walls in most buildings.

Spread spectrum technologies

Wireless communications use spread spectrum technologies. In spread spectrum technologies, a signal is generated by a system, and then spread over a large number of frequencies to another system. The receiving system then reassembles the data. Types of spread spectrum transmissions include:

Frequency Hopping Spread Spectrum (FHSS) Involves changing the frequency of a transmission at regular intervals. Signals move from frequency to frequency, and each frequency change is called a hop. Both the sender and receiver must coordinate the hops between frequencies. That is, they retune at regular intervals during the transmission. FHSS offers speeds between 2 Mbps and 3 Mbps.

Direct Sequence Spread Spectrum (DSSS)	Rather than hopping from one frequency to another, a signal is spread over the entire band at once. DSSS is used by 802.11b and 802.11g networks. The 802.11b networks communicate as fast as 11 Mbps at 2.4 GHz. The 802.11g networks can operate at rates between 20 and 54 Mbps at 2.4 GHz.
Orthogonal Frequency Division Multiplexing (OFDM)	Splits a radio signal into smaller subsignals that are transmitted simultaneously on different frequencies. 802.11a, 802.11g and 802.11n networks can use OFDM. Speeds ranger from 54 Mbps to 300 Mbps.

Wireless signals and interference

Wireless signals are subject to interference from atmospheric conditions, environmental obstacles, and other devices operating on the same frequency.

Signal Interception

It should be understood that copper cables radiate signals which can be intercepted. It is also fairly easy to physically tap into a copper LAN cable without anyone knowing (unless all areas of the network are under constant monitoring and surveillance). Wireless signals are easily intercepted because they are radio transmissions. This is why encryption is so important in securing a wireless network.

When fiber-optic cables were first introduced, it was widely believed that they were inherently secure. In contrast to copper cables, fiber-optic cables do not radiate their signals in such a manner that they can be intercepted by an intruder who is not physically connected to the cable.

However, it is possible to physically tap a fiber-optic cable and leak a small amount of light through the cladding. High-speed fiber networks (such as those owned by telecom companies) employ encryption and intrusion detection and can easily detect a tap. The point is, that while public fiber networks are difficult to tap, this is true because of the security mechanisms put into place to prevent and detect signal interception.

Fiber is not inherently secure from tapping. Network managers need to keep this fact in mind when they are planning a budget for their fiber networks.

Exercise 2-6: Considering vulnerabilities

Exercise

In this exercise, you will watch a short video that shows how to tap a fiber-optic cable.

1. Instructor: Show the following video to the class:

   Hacking Fiber Optics http://www.youtube.com/watch?v=2fP-j4XCuFs&NR=1

2. The video shows how information was stolen from a fiber-optic line using a clip-on optic coupler and a packet sniffing program. Were you surprised at the simplicity of the steps involved to physically tap the fiber-optic cable?
3. What other factors made it easy to tap the line? ____________________
4. How did the investigators know where a line could be found? ____________________
5. Why do you think no one asked the investigators what they were doing in the man hole?____________________
6. What does this suggest to you about human nature? ____________________
7. What does this video suggest about the relative security or insecurity of fiber-optic lines? ____________________
8. What do you think would be an effective method of securing transmissions that cross fiber-optic lines?

   ____

In this exercise, you watched a video about tapping fiber-optic lines.

Transmission Media and Ethernet Standards

The IEEE creates standards for computers and communications. The IEEE 802 series of standards specifies various LAN technologies, including Ethernet, token ring and wireless technologies. The 802.3 group of standards defines Ethernet networks, as listed in the following table.

Standard	Name	Speed	Comments
802.3	Ethernet	10 Mbps	Can use coaxial cable, twisted-pair or fiber.
802.3u	Fast Ethernet	100 Mbps	Can use twisted-pair or fiber. Most NICs support speeds of 10 Mbps and 100 Mbps and are designated as 10/100 Mbps.
802.3z	Gigabit Ethernet	1 Gbps	This specification is for fiber.
802.3ab	Gigabit Ethernet	1 Gbps	This specification is for twisted-pair. This specification uses all four twisted pairs in the cable.
802.3ae	10-Gigabit Ethernet	10 Gbps	This specification is for fiber.
802.3an	10-Gigabit Ethernet	10 Gbps	This specification is for twisted-pair and requires Cat 6, Cat 6a or Cat 7 cable.

Exercise 2-7: Investigating transmission media *(Instructor-led)*

Exercise

In this exercise, your instructor will help you investigate the transmission media used in your classroom.

1. With your instructor, identify the transmission media used in your classroom network. ________________________

   If it is copper wire, what type is it? (STP, UTP, coax) ____

   If it is fiber, what type of fiber do you think is used? (single or multimode) ______________________________

   If your connection is wireless, what standard is used? ____

2. What speeds/Ethernet standards are supported by the classroom transmission media? ________________________

   What speed is your network connection? ____

   Approximately how long is the cable that attaches your computer to a network connection device? _____________

   What is the maximum length cable segment for your type of transmission media? ____________________________

3. If your transmission media is free space, how far is your station located from the access point? _________________

   How strong is the wireless signal? ____

   What is the maximum distance a station can be located from the access point and maintain a strong signal? ______

4. What factors (cost, ease of installation, speed, etc.) do you think influenced the choice of transmission media?

   ____

5. Would you change the transmission media for another type? Why or why not? ________________________________

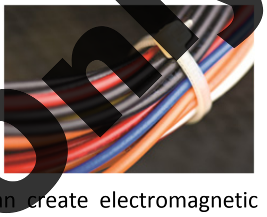
In this exercise, you investigated the transmission media used in your classroom.

Proper Cabling Procedures

You have learned about several types of transmission media. To keep a network running smoothly, the media must be installed correctly and maintained to ensure safety and performance.

Network cabling cannot be strung haphazardly throughout a computing environment. If you are involved in laying out network cabling, keep the following tips in mind:

- Clear a proper path for the cable before laying it or pulling it through walls.
- Do not allow network cabling to cross walkways.
- Do not allow cables to hang loosely behind a desk if there is any way those cables may come into contact with a user's foot, causing a tripping hazard. Tie cables neatly together and tuck them out of the way.
- Ensure that cabling does not interfere with mechanical equipment.
- Avoid passing network cable close to fluorescent lights if at all possible, as these can create electromagnetic interference (EMI) in unshielded twisted pair cable. If you cannot avoid these lights, the cables should cross the lights at right angles.



The *plenum* is the space above a dropped ceiling, or behind a wall. Plenum space is often empty, but can contain air ducts, wiring and other equipment. Network and telecommunications cabling is often run through the plenum in order to remain unobtrusive.

Any cable run through a plenum must adhere to stringent standards for fire safety. The jacket of a standard UTP or STP cable is made of polyvinyl chloride (PVC), a type of plastic. If PVC is burned, it creates toxic polyvinyl chloride gas, which is deadly to humans. If you need to install cabling in a plenum space, you must use plenum cabling. (Outside North America, plenum cabling is called *limited combustible cabling*.)

Instead of a PVC cover, plenum cable has a Teflon or Kevlar jacket, which allows the cable to emit fewer toxic fumes. These cables also slow the spread of a fire. North American performance requirements for plenum cable are defined in the National Fire Protection Association (NFPA) 90A standard and in article 760 of the National Electric Code (NEC). Types of plenum cable include:

- Class 2 plenum cable (CL2P) for use in ducts.
- Class 3 plenum cable (CL3P) for use in walls, as well as ducts.
- Fire power limited plenum (FPLP) for fire alarm use only.
- Fire power limited riser (FPLR) for use in a vertical shaft; designed to help stop a fire from rising from one floor to another.

Lesson Summary

In this lesson, you learned about networking devices and the transmission media that connects them. You are now able to:

☑ Identify the seven layers of the Open Systems Interconnection (OSI) reference model.

☑ Explain the process of data encapsulation and packet creation.

☑ Identify the four layers of the TCP model, and describe how they correspond to layers of the OSI model.

☑ Review concepts and terms related to network traffic.

☑ Understand the function and characteristics of network switches.

☑ Understand the function and benefits of virtual LANs (VLANs).

☑ Understand the function and characteristics of routers.

☑ Describe the routing function.

☑ Understand network address translation (NAT).

☑ Identify various transmission types, such as synchronous, asynchronous, baseband and broadband.

☑ Identify the characteristics of different types of transmission media such as twisted-pair, coaxial, and fiber-optic cable, including transmission speeds and susceptibility to interference and interception.

☑ Understand twisted-pair Ethernet wiring.

☑ Describe technologies for free-space transmission.

☑ Identify proper cabling procedures.

Review Questions

1. A data payload plus a layer-specific header is referred to as a(n)?
   a. bit
   b. protocol data unit (PDU)
   c. trailer or footer
   d. cyclic redundancy check (CRC)

2. A mode of communication in which the data can flow in two directions, but in only one direction at a time is called:
   a. Broadcast
   b. Simplex
   c. Half-duplex
   d. Full-duplex

3. Virtual LANs (VLANs) are implemented on:
   a. network interface cards
   b. hubs
   c. switches
   d. routers

4. Which of the following hides internal network systems from systems outside the LAN?
   a. hub
   b. network address translation (NAT)
   c. switch
   d. network interface card (NIC)

5. What is the maximum segment length for unshielded twisted-pair cable?
   a. 100 meters
   b. 70 kilometers
   c. 7 feet
   d. 7 inches