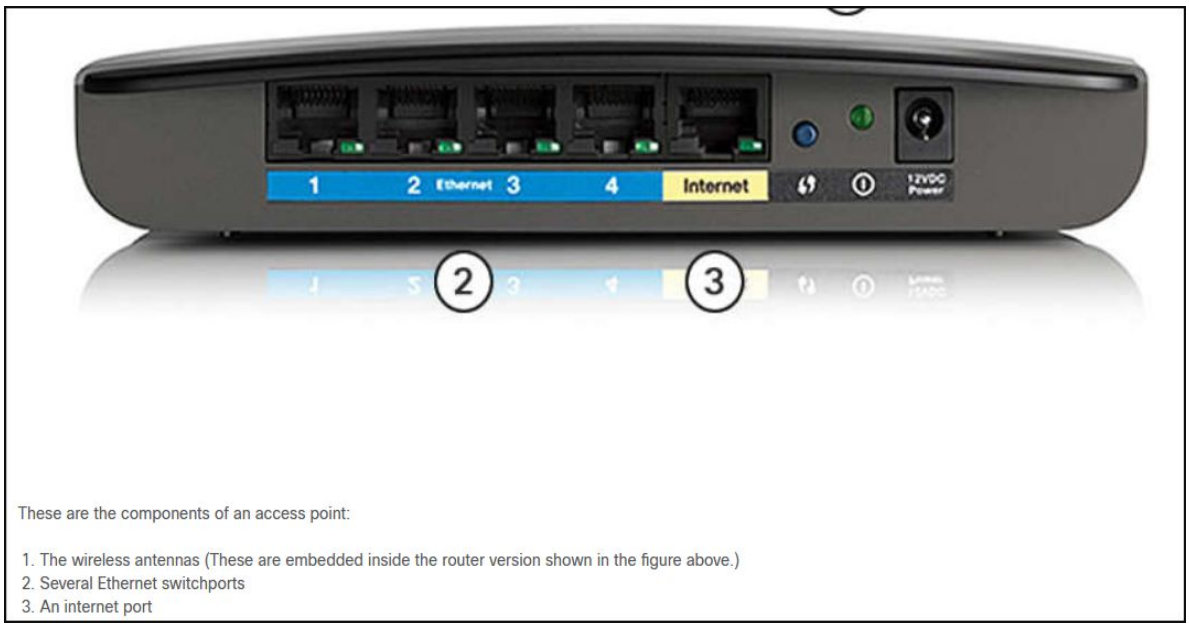
CHAPTER 4



These are the components of an access point:

1. The wireless antennas (These are embedded inside the router version shown in the figure above.)
2. Several Ethernet switchports
3. An internet port

The Physical Connection

- Before any network communications can occur, a physical connection to a local network must be established.
- This connection could be wired or wireless, depending on the setup of the network.
- This generally applies whether you are considering a corporate office or a home.
- A Network Interface Card (NIC) connects a device to the network.
- Some devices may have just one NIC, while others may have multiple NICs (Wired and/or Wireless, for example).
- Not all physical connections offer the same level of performance.

Network Interface Cards

Network interface cards (NICs) connect a device to the network. Ethernet NICs are used for a wired connection, as shown in the figure, whereas wireless local area network (WLAN) NICs are used for wireless. An end-user device may include one or both types of NICs. A network printer, for example, may only have an Ethernet NIC, and therefore, must connect to the network using

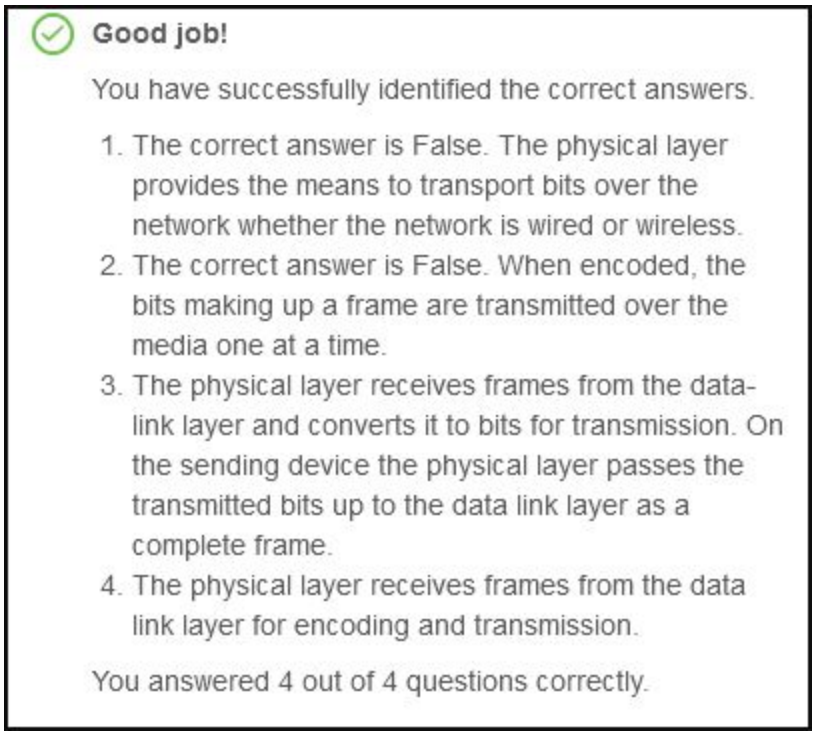
an Ethernet cable. Other devices, such as tablets and smartphones, might only contain a WLAN NIC and must use a wireless connection.

The Physical Layer

The OSI physical layer provides the means to transport the bits that make up a data link layer frame across the network media. This layer accepts a complete frame from the data link layer and encodes it as a series of signals that are transmitted to the local media. The encoded bits that comprise a frame are received by either an end device or an intermediate device.

The physical layer encodes the frames and creates the electrical, optical, or radio wave signals that represent the bits in each frame. These signals are then sent over the media, one at a time.

The destination node physical layer retrieves these individual signals from the media, restores them to their bit representations, and passes the bits up to the data link layer as a complete frame.

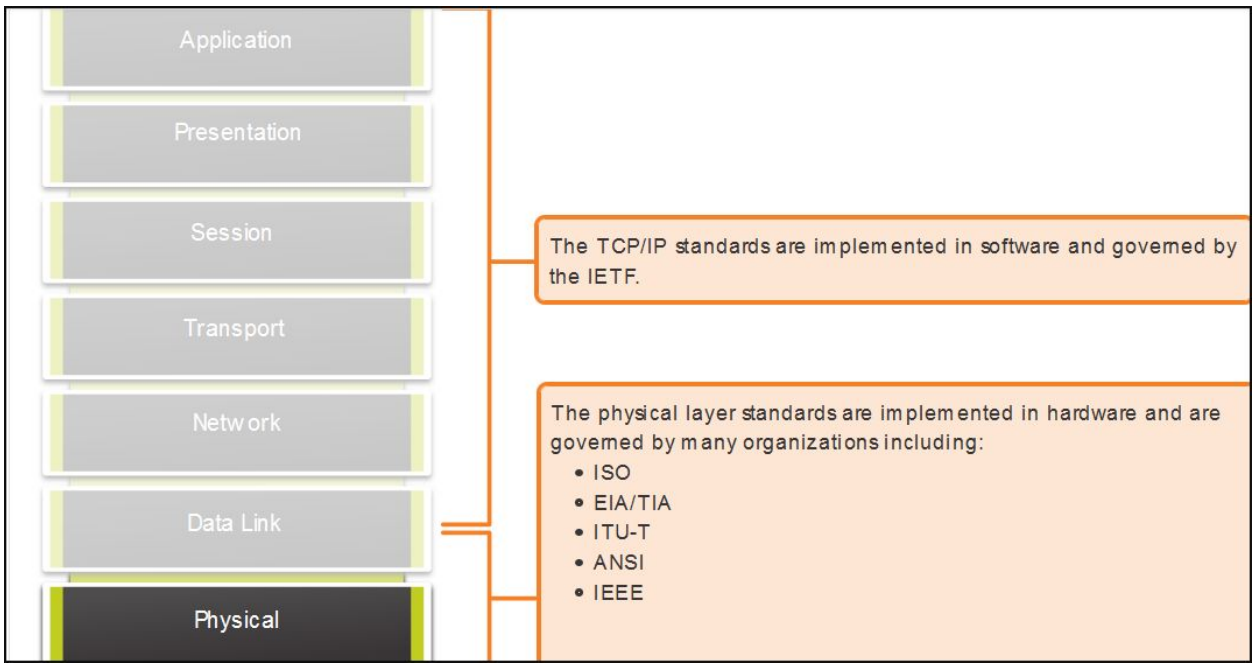


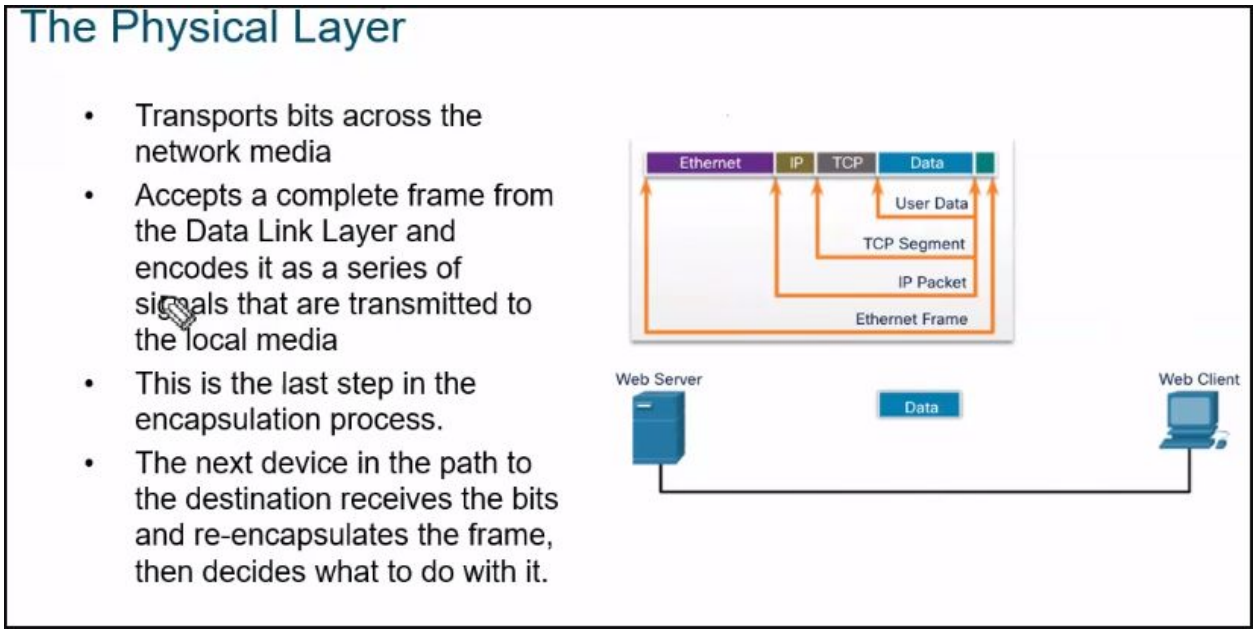
There are many different international and national organizations, regulatory government organizations, and private companies involved in establishing and maintaining physical layer standards. For instance, the physical layer hardware, media, encoding, and signaling standards are defined and governed by these standards organizations:

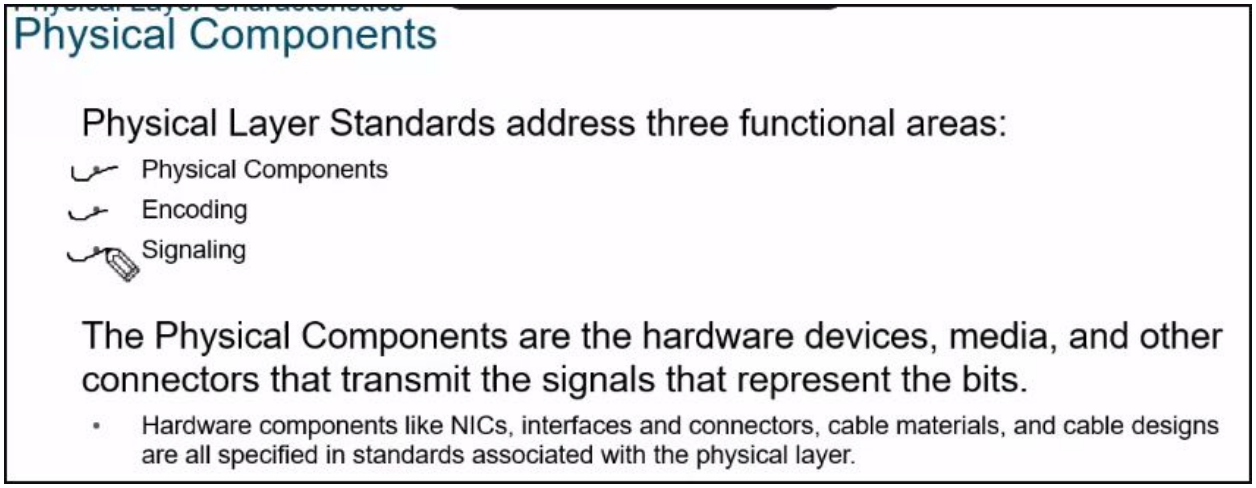
- International Organization for Standardization (ISO)
- Telecommunications Industry Association/Electronic Industries Association (TIA/EIA)
- International Telecommunication Union (ITU)

- American National Standards Institute (ANSI)
- Institute of Electrical and Electronics Engineers (IEEE)
- National telecommunications regulatory authorities including the Federal Communication Commission (FCC) in the USA and the European Telecommunications Standards Institute (ETSI)

In addition to these, there are often regional cabling standards groups such as CSA (Canadian Standards Association), CENELEC (European Committee for Electrotechnical Standardization), and JSA/JIS (Japanese Standards Association), which develop local specifications.







Encoding

Encoding or line encoding is a method of converting a stream of data bits into a predefined "code". Codes are groupings of bits used to provide a predictable pattern that can be recognized by both the sender and the receiver. In other words, encoding is the method or pattern used to represent digital information. This is similar to how Morse code encodes a message using a series of dots and dashes.

Manchester encoding represents a 0 bit by a high to low voltage transition, and a 1 bit is represented as a low to high voltage transition.

Signaling

The physical layer must generate the electrical, optical, or wireless signals that represent the "1" and "0" on the media. The way that bits are represented is called the signaling method.

Bandwidth

Different physical media support the transfer of bits at different rates. Data transfer is usually discussed in terms of bandwidth. Bandwidth is the capacity at which a medium can carry data. Digital bandwidth measures the amount of data that can flow from one place to another in a given amount of time. Bandwidth is typically measured in kilobits per second (kbps), megabits per second (Mbps), or gigabits per second (Gbps). Bandwidth is sometimes thought of as the speed that bits travel, however this is not accurate. For example, in both 10Mbps and 100Mbps Ethernet, the bits are sent at the speed of electricity. The difference is the number of bits that are transmitted per second.

A combination of factors determines the practical bandwidth of a network:

- The properties of the physical media

- The technologies chosen for signaling and detecting network signals

Physical media properties, current technologies, and the laws of physics all play a role in determining the available bandwidth.

Bandwidth Terminology

Terms used to measure the quality of bandwidth include:

- Latency
- Throughput
- Goodput

Latency

Latency refers to the amount of time, including delays, for data to travel from one given point to another.

In an internetwork, or a network with multiple segments, throughput cannot be faster than the slowest link in the path from source to destination. Even if all, or most, of the segments have high bandwidth, it will only take one segment in the path with low throughput to create a bottleneck in the throughput of the entire network.

Throughput

Throughput is the measure of the transfer of bits across the media over a given period of time.

Due to a number of factors, throughput usually does not match the specified bandwidth in physical layer implementations. Throughput is usually lower than the bandwidth. There are many factors that influence throughput:

- The amount of traffic
- The type of traffic
- The latency created by the number of network devices encountered between source and destination

There are many online speed tests that can reveal the throughput of an internet connection. The figure provides sample results from a speed test.

Goodput

There is a third measurement to assess the transfer of usable data; it is known as goodput. Goodput is the measure of usable data transferred over a given period of time. Goodput is throughput minus traffic overhead for establishing sessions, acknowledgments, encapsulation, and retransmitted bits. Goodput is always lower than throughput, which is generally lower than the bandwidth.

Good job!

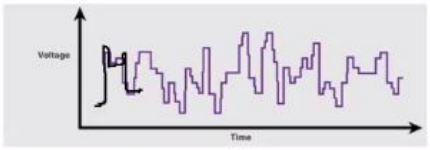
You have successfully identified the correct answers.

1. In wireless networks data is represented by patterns of microwave transmissions.
2. Fiber-optic cables use patterns of light to represent bits.
3. Electrical pulses are used to represent bits on networks using copper cable media.
4. Bandwidth is the capacity of a network medium to carry data.
5. The transfer of bits across the network media over a period of time is known as throughput.

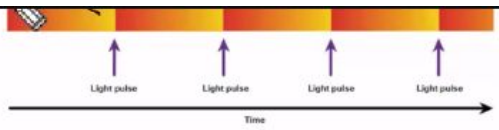
You answered 5 out of 5 questions correctly.

Signaling

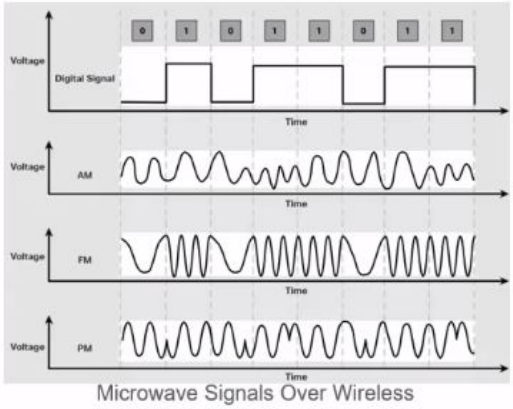
- The signaling method is how the bit values, "1" and "0" are represented on the physical medium.
- The method of signaling will vary based on the type of medium being used.



Electrical Signals Over Copper Cable



Light Pulses Over Fiber-Optic Cable



Microwave Signals Over Wireless

Bandwidth

- Bandwidth is the capacity at which a medium can carry data.
- Digital bandwidth measures the amount of data that can flow from one place to another in a given amount of time; how many bits can be transmitted in a second.
- Physical media properties, current technologies, and the laws of physics play a role in determining available bandwidth.

Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	bps	1 bps = fundamental unit of bandwidth
Kilobits per second	Kbps	1 Kbps = 1,000 bps = 10^3 bps
Megabits per second	Mbps	1 Mbps = 1,000,000 bps = 10^6 bps
Gigabits per second	Gbps	1 Gbps – 1,000,000,000 bps = 10^9 bps
Terabits per second	Tbps	1 Tbps = 1,000,000,000,000 bps = 10^{12} bps

Bandwidth Terminology

Latency

- Amount of time, including delays, for data to travel from one given point to another

Throughput

- The measure of the transfer of bits across the media over a given period of time

Goodput

- The measure of usable data transferred over a given period of time
- Goodput = Throughput - traffic overhead

Copper Cabling

Characteristics of Copper Cabling

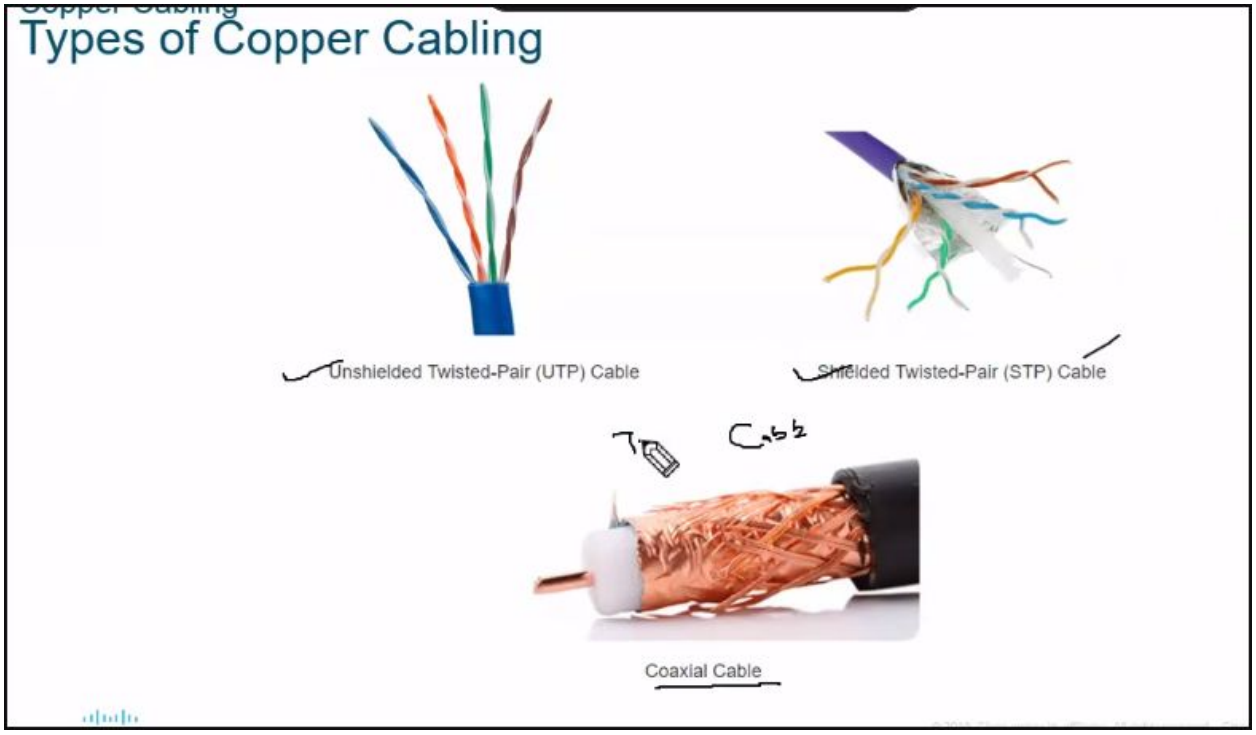
Copper cabling is the most common type of cabling used in networks today. It is inexpensive, easy to install, and has low resistance to electrical current flow.

Limitations:

- Attenuation – the longer the electrical signals have to travel, the weaker they get.
- The electrical signal is susceptible to interference from two sources, which can distort and corrupt the data signals (Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI) and Crosstalk).

Mitigation:

- Strict adherence to cable length limits will mitigate attenuation.
- Some kinds of copper cable mitigate EMI and RFI by using metallic shielding and grounding.
- Some kinds of copper cable mitigate crosstalk by twisting opposing circuit pair wires together.



Networks use copper media because it is inexpensive, easy to install, and has low resistance to electrical current. However, copper media is limited by distance and signal interference.
The timing and voltage values of the electrical pulses are also susceptible to interference from two sources:

- **Electromagnetic interference (EMI) or radio frequency interference (RFI) -** EMI and RFI signals can distort and corrupt the data signals being carried by copper media. Potential sources of EMI and RFI include radio waves and electromagnetic devices, such as fluorescent lights or electric motors.
- **Crosstalk** - Crosstalk is a disturbance caused by the electric or magnetic fields of a signal on one wire to the signal in an adjacent wire. In telephone circuits, crosstalk can result in hearing part of another voice conversation from an adjacent circuit. Specifically, when an electrical current flows through a wire, it creates a small, circular magnetic field around the wire, which can be picked up by an adjacent wire.

To counter the negative effects of EMI and RFI, some types of copper cables are wrapped in metallic shielding and require proper grounding connections.

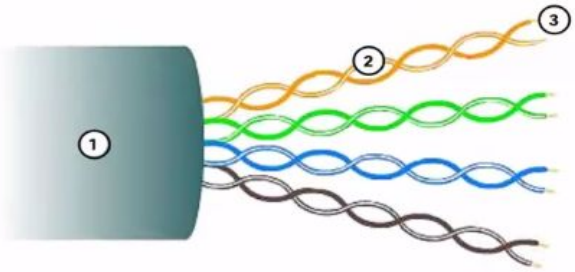
To counter the negative effects of crosstalk, some types of copper cables have opposing circuit wire pairs twisted together, which effectively cancels the crosstalk.

The susceptibility of copper cables to electronic noise can also be limited using these recommendations:

- Selecting the cable type or category most suited to a given networking environment

- Designing a cable infrastructure to avoid known and potential sources of interference in the building structure
- Using cabling techniques that include the proper handling and termination of the cables

Unshielded Twisted Pair (UTP)

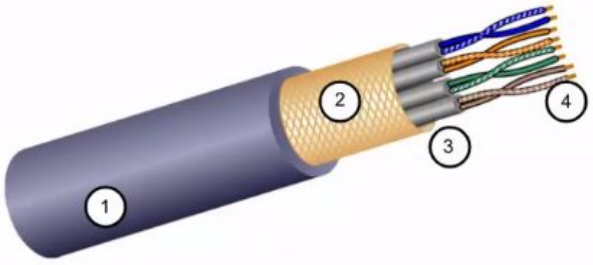


- UTP is the most common networking media.
- Terminated with RJ-45 connectors
- Interconnects hosts with intermediary network devices.

Key Characteristics of UTP

1. The outer jacket protects the copper wires from physical damage.
2. Twisted pairs protect the signal from interference.
3. Color-coded plastic insulation electrically isolates the wires from each other and identifies each pair.

Shielded Twisted Pair (STP)



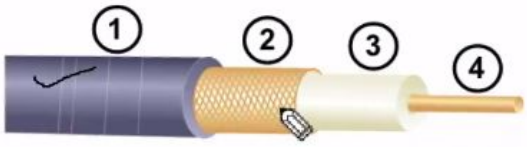
- Better noise protection than UTP
- More expensive than UTP
- Harder to install than UTP
- Terminated with RJ-45 connectors
- Interconnects hosts with intermediary network devices

Key Characteristics of STP

1. The outer jacket protects the copper wires from physical damage
2. Braided or foil shield provides EMI/RFI protection
3. Foil shield for each pair of wires provides EMI/RFI protection
4. Color-coded plastic insulation electrically isolates the wires from each other and identifies each pair

Consists of the following:

1. Outer cable jacket to prevent minor physical damage
2. A woven copper braid, or metallic foil, acts as the second wire in the circuit and as a shield for the inner conductor.
3. A layer of flexible plastic insulation
4. A copper conductor is used to transmit the electronic signals.



There are different types of connectors used with coax cable.

Commonly used in the following situations:

- Wireless installations - attach antennas to wireless devices
- Cable internet installations - customer premises wiring

Good job!

You have successfully identified the correct answers.

1. Coaxial cable, which is used for cable TV and internet service, is also used to attach antennas to wireless devices.
2. Shielded twisted pair cable (STP) incorporates shielding and special connectors to prevent signal interference from other wires, EMI, and RFI.
3. Unshielded twisted pair cable (UTP) is the most common type of wired network media.
4. Coaxial cable, which is used for cable TV and internet service and to attach antennas to wireless devices, uses several types of connectors to include BNC, N type, and F type connectors.

You answered 4 out of 4 questions correctly.

UTP cable does not use shielding to counter the effects of EMI and RFI. Instead, cable designers have discovered other ways that they can limit the negative effect of crosstalk:

- **Cancellation -** Designers now pair wires in a circuit. When two wires in an electrical circuit are placed close together, their magnetic fields are the exact opposite of each other. Therefore, the two magnetic fields cancel each other and also cancel out any outside EMI and RFI signals.
- **Varying the number of twists per wire pair -** To further enhance the cancellation effect of paired circuit wires, designers vary the number of twists of each wire pair in a cable. UTP cable must follow precise specifications governing how many twists or braids are

permitted per meter (3.28 feet) of cable. Notice in the figure that the orange/orange white pair is twisted less than the blue/blue white pair. Each colored pair is twisted a different number of times.

UTP cable relies solely on the cancellation effect produced by the twisted wire pairs to limit signal degradation and effectively provide self-shielding for wire pairs within the network media.

Cables are placed into categories based on their ability to carry higher bandwidth rates. For example, Category 5 cable is used commonly in 100BASE-TX Fast Ethernet installations.

Cables in higher categories are designed and constructed to support higher data rates. As new gigabit speed Ethernet technologies are being developed and adopted, Category 5e is now the minimally acceptable cable type, with Category 6 being the recommended type for new building installations.

- Category 3 was originally used for voice communication over voice lines, but later used for data transmission.
- Category 5 and 5e is used for data transmission. Category 5 supports 100Mbps and Category 5e supports 1000 Mbps
- Category 6 has an added separator between each wire pair to support higher speeds. Category 6 supports up to 10 Gbps.
- Category 7 also supports 10 Gbps.
- Category 8 supports 40 Gbps.

Different situations may require UTP cables to be wired according to different wiring conventions. This means that the individual wires in the cable have to be connected in different orders to different sets of pins in the RJ-45 connectors.

The following are the main cable types that are obtained by using specific wiring conventions:

- **Ethernet Straight-through -** The most common type of networking cable. It is commonly used to interconnect a host to a switch and a switch to a router.
- **Ethernet Crossover -** A cable used to interconnect similar devices. For example, to connect a switch to a switch, a host to a host, or a router to a router. However, crossover cables are now considered legacy as NICs use medium-dependent interface crossover (auto-MDIX) to automatically detect the cable type and make the internal connection.

Note: Another type of cable is a rollover cable, which is Cisco proprietary. It is used to connect a workstation to a router or switch console port.

Using a crossover or straight-through cable incorrectly between devices may not damage the devices, but connectivity and communication between the devices will not take place. This is a common error and checking that the device connections are correct should be the first troubleshooting action if connectivity is not achieved.

Cable Types and Standards

Cable Type	Standard	Application
Ethernet Straight-through	Both ends T568A or both ends T568B	Connects a network host to a network device such as a switch or hub
Ethernet Crossover	One end T568A, other end T568B	Connects two network hosts Connects two network intermediary devices (switch to switch or router to router)
Rollover	Cisco proprietary	Connects a workstation serial port to a router console port, using an adapter

Properties of UTP Cabling

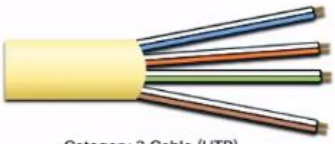
UTP has four pairs of color-coded copper wires twisted together and encased in a flexible plastic sheath. No shielding is used. UTP relies on the following properties to limit crosstalk:

- Cancellation - Each wire in a pair of wires uses opposite polarity. One wire is negative, the other wire is positive. They are twisted together and the magnetic fields effectively cancel each other and outside EMI/RFI.
- Variation in twists per foot in each wire - Each wire is twisted a different amount, which helps prevent crosstalk amongst the wires in the cable.

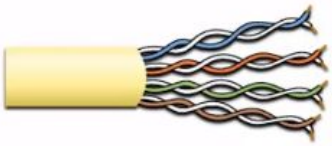
UTP Cabling Standards and Connectors

Standards for UTP are established by the TIA/EIA. TIA/EIA-568 standardizes elements like:

- Cable Types
- Cable Lengths
- Connectors
- Cable Termination
- Testing Methods



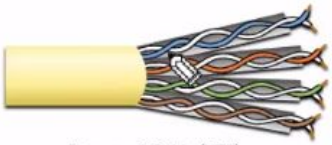
Category 3 Cable (UTP)



Category 5 and 5e Cable (UTP)

Electrical standards for copper cabling are established by the IEEE, which rates cable according to its performance. Examples include:

- Category 3
- Category 5 and 5e
- Category 6



Category 6 Cable (UTP)

UTP Cabling Standards and Connectors (Cont.)

RJ-45 Connector

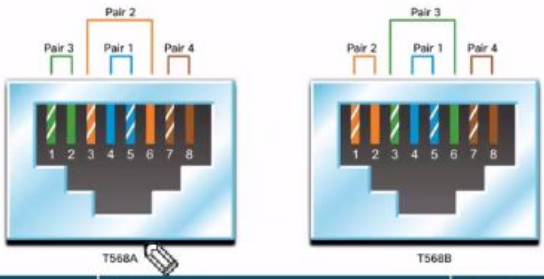
Poorly terminated UTP cable

RJ-45 Socket

Properly terminated UTP cable

UTP Cabling

Straight-through and Crossover UTP Cables



Cable Type	Standard	Application
Ethernet Straight-through	Both ends T568A or T568B	Host to Network Device
Ethernet Crossover *	One end T568A, other end T568B	Host-to-Host, Switch-to-Switch, Router-to-Router
* Considered Legacy due to most NICs using Auto-MDIX to sense cable type and complete connection		
Rollover	Cisco Proprietary	Host serial port to Router or Switch Console Port, using an adapter

Properties of Fiber-Optic Cabling

- Not as common as UTP because of the expense involved
- Ideal for some networking scenarios
- Transmits data over longer distances at higher bandwidth than any other networking media
- Less susceptible to attenuation, and completely immune to EMI/RFI
- Made of flexible, extremely thin strands of very pure glass
- Uses a laser or LED to encode bits as pulses of light
- The fiber-optic cable acts as a wave guide to transmit light between the two ends with minimal signal loss

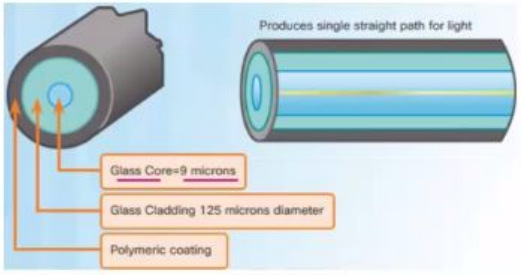
Optical fiber cable transmits data over longer distances and at higher bandwidths than any other networking media. Unlike copper wires, fiber-optic cable can transmit signals with less attenuation and is completely immune to EMI and RFI. Optical fiber is commonly used to interconnect network devices.

Fiber-optic cables are broadly classified into two types:

- Single-mode fiber (SMF)
- Multimode fiber (MMF)

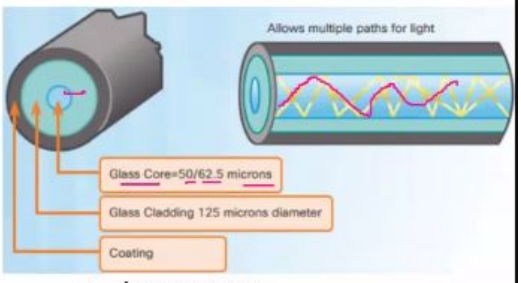
Types of Fiber Media

Single-Mode Fiber



- Very small core
- Uses expensive lasers
- Long-distance applications

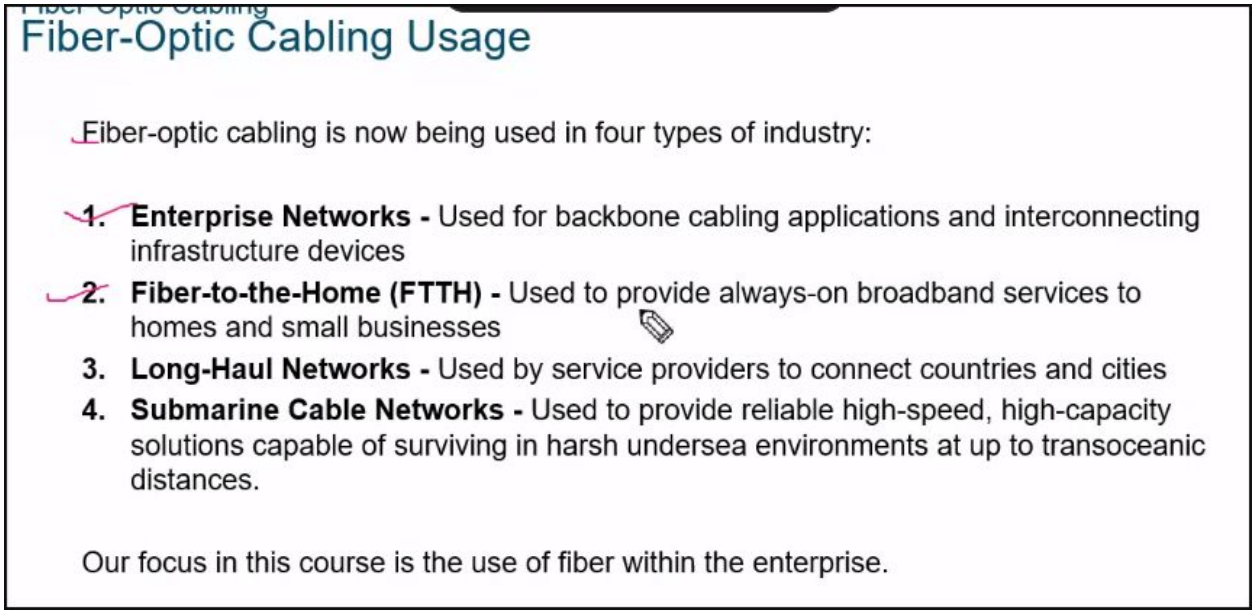
Multimode Fiber



- Larger core
- Uses less expensive LEDs
- LEDs transmit at different angles
- Up to 10 Gbps over 550 meters

Dispersion refers to the spreading out of a light pulse over time. Increased dispersion means increased loss of signal strength. MMF has greater dispersion than SMF, with a the maximum cable distance for MMF is 550 meters.

One of the highlighted differences between MMF and SMF is the amount of dispersion. Dispersion refers to the spreading out of a light pulse over time. Increased dispersion means increased loss of signal strength. MMF has a greater dispersion than SMF. That is why MMF can only travel up to 500 meters before signal loss.



Fiber-optic cabling is now being used in four types of industry:

- **Enterprise Networks -** Used for backbone cabling applications and interconnecting infrastructure devices
- **Fiber-to-the-Home (FTTH) -** Used to provide always-on broadband services to homes and small businesses
- **Long-Haul Networks -** Used by service providers to connect countries and cities
- **Submarine Cable Networks -** Used to provide reliable high-speed, high-capacity solutions capable of surviving in harsh undersea environments at up to transoceanic distances. Search the internet for “submarine cables telegeography map” to view various maps online.

Our focus in this course is the use of fiber within the enterprise.

The use of color distinguishes between single-mode and multimode patch cords. A yellow jacket is for single-mode fiber cables and orange (or aqua) for multimode fiber cables.

Fiber-Optic Connectors

Straight-Tip (ST) Connectors

Lucent Connector (LC) Simplex Connectors

Subscriber Connector (SC) Connectors

Duplex Multimode LC Connectors

Fiber Patch Cords

SC-SC MM Patch Cord | LC-LC SM Patch Cord | ST-LC MM Patch Cord | ST-SC SM Patch Cord

A yellow jacket is for single-mode fiber cables and orange (or aqua) for multimode fiber cables.

Fiber versus Copper

Optical fiber is primarily used as backbone cabling for high-traffic, point-to-point connections between data distribution facilities and for the interconnection of buildings in multi-building campuses.

Implementation Issues	UTP Cabling	Fiber-Optic Cabling
Bandwidth supported	10 Mb/s - 10 Gb/s	10 Mb/s - 100 Gb/s
Distance	Relatively short (1 - 100 meters)	Relatively long (1 - 100,000 meters)
Immunity to EMI and RFI	Low	High (Completely immune)
Immunity to electrical hazards	Low	High (Completely immune)
Media and connector costs	Lowest	Highest
Installation skills required	Lowest	Highest
Safety precautions	Lowest	Highest

Good job!

You have successfully identified the correct answers.

1. Multimode fiber has a shorter distance limitation than single-mode fiber. Commonly used on LANs with a distance of a few hundred meters but can be up to 2 km.
2. Multimode fiber used LEDs as the light source.
3. Single-mode fiber uses laser technology as the light source.
4. Single-mode fiber is commonly used for long haul TV and telephony applications.
5. Single-mode fiber is used for long haul applications up to 100 km.
6. Multimode fiber has a shorter distance limitation than single mode fiber. Commonly used on LANs within a campus network.

You answered 6 out of 6 questions correctly.

Properties of Wireless Media

It carries electromagnetic signals representing binary digits using radio or microwave frequencies. This provides the greatest mobility option. Wireless connection numbers continue to increase.

Some of the limitations of wireless:

- **Coverage area** - Effective coverage can be significantly impacted by the physical characteristics of the deployment location.
- **Interference** - Wireless is susceptible to interference and can be disrupted by many common devices.
- **Security** - Wireless communication coverage requires no access to a physical strand of media, so anyone can gain access to the transmission.
- **Shared medium** - WLANs operate in half-duplex, which means only one device can send or receive at a time. Many users accessing the WLAN simultaneously results in reduced bandwidth for each user.

Types of Wireless Media

The IEEE and telecommunications industry standards for wireless data communications cover both the data link and physical layers. In each of these standards, physical layer specifications dictate:

- Data to radio signal encoding methods
- Frequency and power of transmission
- Signal reception and decoding requirements
- Antenna design and construction

Wireless Standards:

- **Wi-Fi (IEEE 802.11)** - Wireless LAN (WLAN) technology
- **Bluetooth (IEEE 802.15)** - Wireless Personal Area network (WPAN) standard
- **WiMAX (IEEE 802.16)** - Uses a point-to-multipoint topology to provide broadband wireless access
- **Zigbee (IEEE 802.15.4)** - Low data-rate, low power-consumption communications, primarily for Internet of Things (IoT) applications

A common wireless data implementation is enabling devices to connect wirelessly via a LAN. In general, a WLAN requires the following network devices:

- **Wireless Access Point (AP)** - These concentrate the wireless signals from users and connect to the existing copper-based network infrastructure, such as Ethernet. Home and small business wireless routers integrate the functions of a router, switch, and access point into one device, as shown in the figure.
- **Wireless NIC adapters** - These provide wireless communication capability to network hosts.

Wireless LAN

In general, a Wireless LAN (WLAN) requires the following devices:

- **Wireless Access Point (AP) -** Concentrate wireless signals from users and connect to the existing copper-based network infrastructure
- **Wireless NIC Adapters -** Provide wireless communications capability to network hosts

There are a number of WLAN standards. When purchasing WLAN equipment, ensure compatibility, and interoperability.

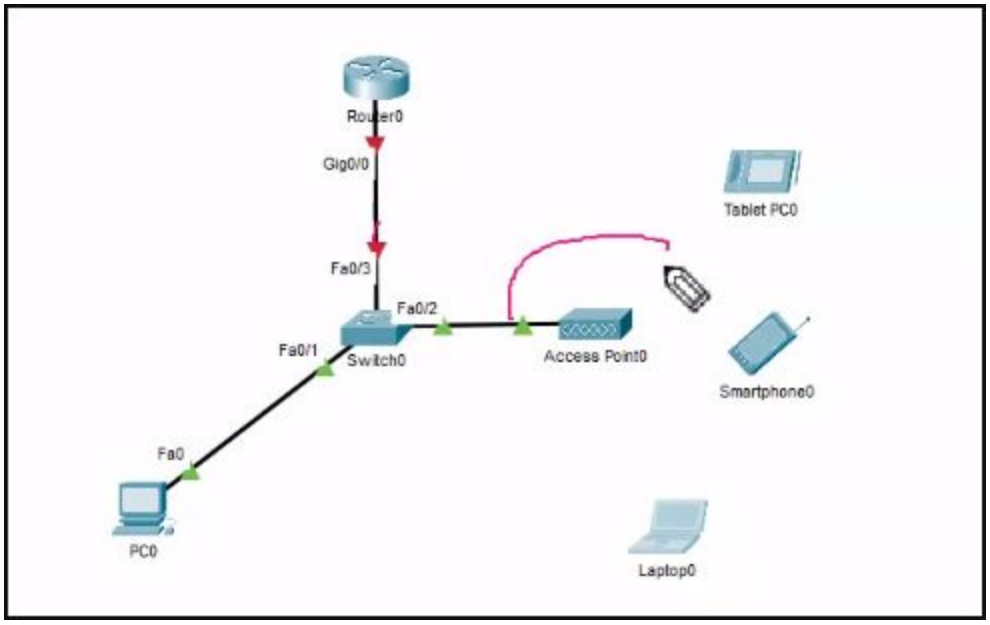
Network Administrators must develop and apply stringent security policies and processes to protect WLANs from unauthorized access and damage.

Good job!

You have successfully identified the correct answers.

1. The correct answer is False. Wireless provides the greatest mobility of all media and is gaining popularity in enterprise networks.
2. The correct answer is False. WLANs operate in half-duplex, which means only one device can send or receive at a time. This can impact network performance if there are many users accessing the WLAN at the same time.
3. Zigbee is intended for applications that require short-range, low data-rates, and long battery life, making it well suited for industrial and IoT applications.
4. This wireless standard is used for Personal Area Networks (PANs) and allows devices to communicate over distances of 1 to 100 meters.

You answered 4 out of 4 questions correctly.



Properties of Wireless Media

It carries electromagnetic signals representing binary digits using radio or microwave frequencies. This provides the greatest mobility option. Wireless connection numbers continue to increase.

Some of the limitations of wireless:

- **Coverage area** - Effective coverage can be significantly impacted by the physical characteristics of the deployment location.
- **Interference** - Wireless is susceptible to interference and can be disrupted by many common devices.
- **Security** - Wireless communication coverage requires no access to a physical strand of media, so anyone can gain access to the transmission.
- **Shared medium** - WLANs operate in half-duplex, which means only one device can send or receive at a time. Many users accessing the WLAN simultaneously results in reduced bandwidth for each user.

Types of Wireless Media

The IEEE and telecommunications industry standards for wireless data communications cover both the data link and physical layers. In each of these standards, physical layer specifications dictate:

- Data to radio signal encoding methods
- Frequency and power of transmission
- Signal reception and decoding requirements
- Antenna design and construction

Wireless Standards:

- **Wi-Fi (IEEE 802.11)** - Wireless LAN (WLAN) technology
- **Bluetooth (IEEE 802.15)** - Wireless Personal Area network (WPAN) standard
- **WiMAX (IEEE 802.16)** - Uses a point-to-multipoint topology to provide broadband wireless access
- **Zigbee (IEEE 802.15.4)** - Low data-rate, low power-consumption communications, primarily for Internet of Things (IoT) applications

What did I learn in this module?

- Before any network communications can occur, a physical connection to a local network, either wired or wireless, must be established.
- The physical layer consists of electronic circuitry, media, and connectors developed by engineers.
- The physical layer standards address three functional areas: physical components, encoding, and signaling.
- Three types of copper cabling are: UTP, STP, and coaxial cable (coax).
- UTP cabling conforms to the standards established jointly by the TIA/EIA. The electrical characteristics of copper cabling are defined by the Institute of Electrical and Electronics Engineers (IEEE).
- The main cable types that are obtained by using specific wiring conventions are Ethernet Straight-through and Ethernet Crossover.

What did I learn in this module?

Purpose of the Physical Layer

Before any network communications can occur, a physical connection to a local network must be established. A physical connection can be a wired connection using a cable or a wireless connection using radio waves. Network Interface Cards (NICs) connect a device to the network. Ethernet NICs are used for a wired connection, whereas WLAN (Wireless Local Area Network) NICs are used for wireless. The OSI physical layer provides the means to transport the bits that make up a data link layer frame across the network media. This layer accepts a complete frame

from the data link layer and encodes it as a series of signals that are transmitted onto the local media. The encoded bits that comprise a frame are received by either an end device or an intermediary device.

Physical Layer Characteristics

The physical layer consists of electronic circuitry, media, and connectors developed by engineers. The physical layer standards address three functional areas: physical components, encoding, and signaling. Bandwidth is the capacity at which a medium can carry data. Digital bandwidth measures the amount of data that can flow from one place to another in a given amount of time. Throughput is the measure of the transfer of bits across the media over a given period of time and is usually lower than bandwidth. Latency refers to the amount of time, including delays, for data to travel from one given point to another. Goodput is the measure of usable data transferred over a given period of time. The physical layer produces the representation and groupings of bits for each type of media as follows:

- **Copper cable** - The signals are patterns of electrical pulses.
- **Fiber-optic cable** - The signals are patterns of light.
- **Wireless** - The signals are patterns of microwave transmissions.

Copper Cabling

Networks use copper media because it is inexpensive, easy to install, and has low resistance to electrical current. However, copper media is limited by distance and signal interference. The timing and voltage values of the electrical pulses are also susceptible to interference from two sources: EMI and crosstalk. Three types of copper cabling are: UTP, STP, and coaxial cable (coax). UTP has an outer jacket to protect the copper wires from physical damage, twisted pairs to protect the signal from interference, and color-coded plastic insulation that electrically isolates wires from each other and identifies each pair. The STP cable uses four pairs of wires, each wrapped in a foil shield, which are then wrapped in an overall metallic braid or foil. Coaxial cable, or coax for short, gets its name from the fact that there are two conductors that share the same axis. Coax is used to attach antennas to wireless devices. Cable internet providers use coax inside their customers' premises.

UTP Cabling

UTP cabling consists of four pairs of color-coded copper wires that have been twisted together and then encased in a flexible plastic sheath. UTP cable does not use shielding to counter the effects of EMI and RFI. Instead, cable designers have discovered other ways that they can limit the negative effect of crosstalk: cancellation and varying the number of twists per wire pair. UTP cabling conforms to the standards established jointly by the TIA/EIA. The electrical characteristics of copper cabling are defined by the Institute of Electrical and Electronics Engineers (IEEE). UTP cable is usually terminated with an RJ-45 connector. The main cable types that are obtained by using specific wiring conventions are Ethernet Straight-through and

Ethernet Crossover. Cisco has a proprietary UTP cable called a rollover that connects a workstation to a router console port.

Fiber-Optic Cabling

Optical fiber cable transmits data over longer distances and at higher bandwidths than any other networking media. Fiber-optic cable can transmit signals with less attenuation than copper wire and is completely immune to EMI and RFI. Optical fiber is a flexible, but extremely thin, transparent strand of very pure glass, not much bigger than a human hair. Bits are encoded on the fiber as light impulses. Fiber-optic cabling is now being used in four types of industry: enterprise networks, FTTH, long-haul networks, and submarine cable networks. There are four types of fiber-optic connectors: ST, SC, LC, and duplex multimode LC. Fiber-optic patch cords include SC-SC multimode, LC-LC single-mode, ST-LC multimode, and SC-ST single-mode. In most enterprise environments, optical fiber is primarily used as backbone cabling for high-traffic point-to-point connections between data distribution facilities and for the interconnection of buildings in multi-building campuses.

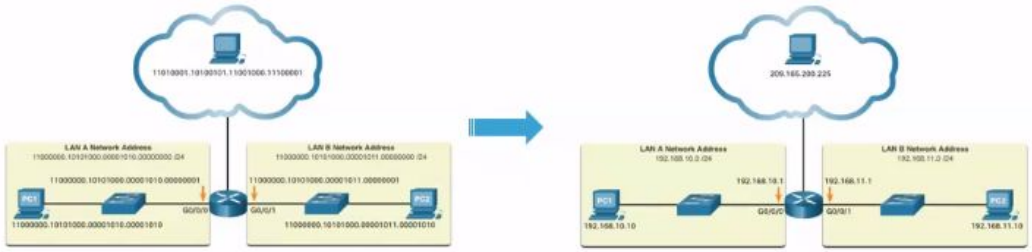
Wireless Media

Wireless media carry electromagnetic signals that represent the binary digits of data communications using radio or microwave frequencies. Wireless does have some limitations, including: coverage area, interference, security, and the problems that occur with any shared medium. Wireless standards include the following: Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15), WiMAX (IEEE 802.16), and Zigbee (IEEE 802.15.4). Wireless LAN (WLAN) requires a wireless AP and wireless NIC adapters.

CHAPTER 5

Binary and IPv4 Addresses

- Binary numbering system consists of 1s and 0s, called bits
- Decimal numbering system consists of digits 0 through 9
- Hosts, servers, and network equipment using binary addressing to identify each other.
- Each address is made up of a string of 32 bits, divided into four sections called octets.
- Each octet contains 8 bits (or 1 byte) separated by a dot.
- For ease of use by people, this dotted notation is converted to dotted decimal.

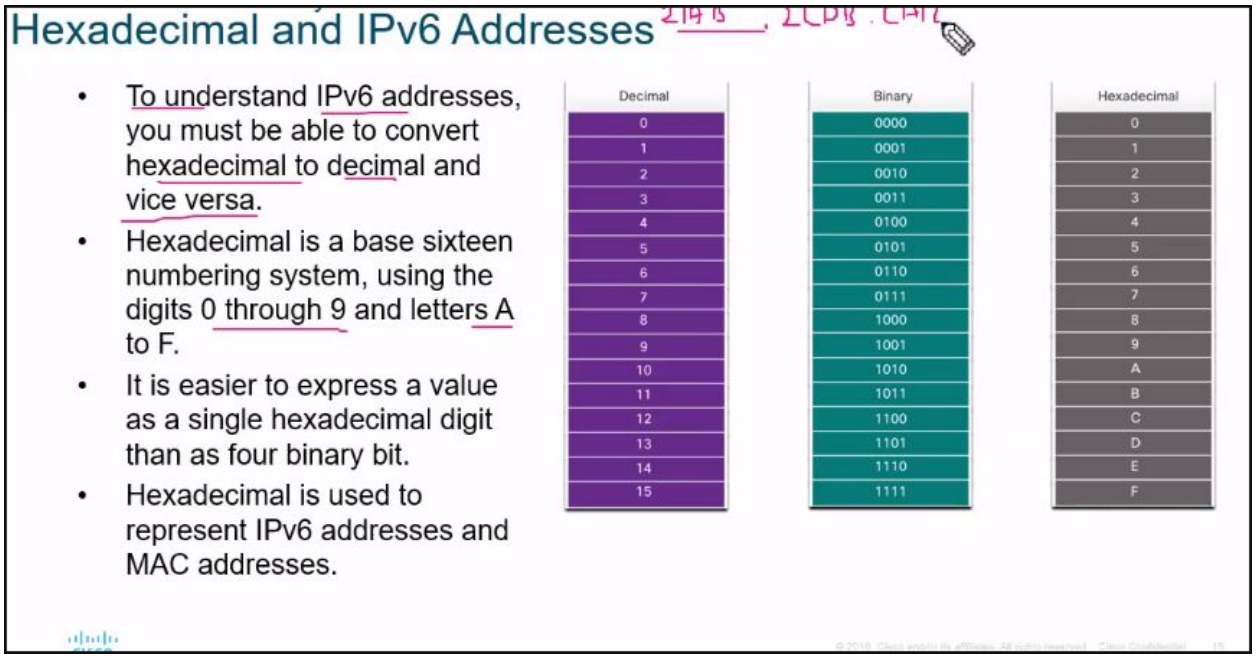


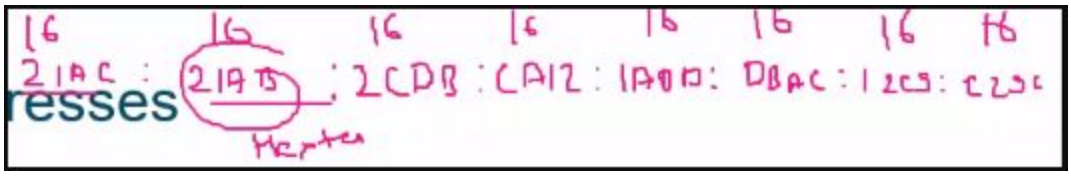
Viewing Mayank Jagota's screen

Binary – Base 2 (0,1)

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	0	1	0		

168 =





What did I learn in this module?

Binary Number System

Binary is a numbering system that consists of the numbers 0 and 1 called bits. In contrast, the decimal numbering system consists of 10 digits consisting of the numbers 0 – 9. Binary is important for us to understand because hosts, servers, and network devices use binary addressing, specifically, binary IPv4 addresses, to identify each other. You must know binary addressing and how to convert between binary and dotted decimal IPv4 addresses. This topic presented a few ways to convert decimal to binary and binary to decimal.

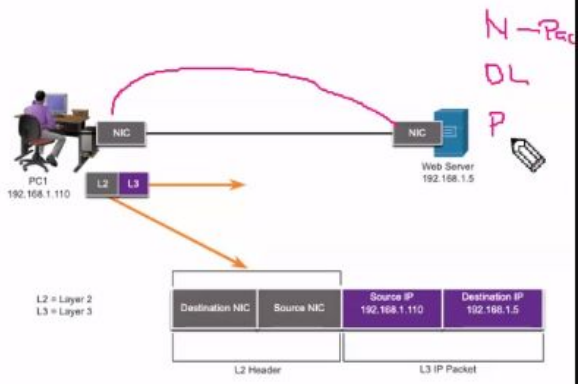
Hexadecimal Number System

Just as decimal is a base ten number system, hexadecimal is a base sixteen system. The base sixteen number system uses the numbers 0 to 9 and the letters A to F. The hexadecimal numbering system is used in networking to represent IPv6 addresses and Ethernet MAC addresses. IPv6 addresses are 128 bits in length and every 4 bits is represented by a single hexadecimal digit; for a total of 32 hexadecimal values. To convert hexadecimal to decimal, you must first convert the hexadecimal to binary, then convert the binary to decimal. To convert decimal to hexadecimal, you must also first convert the decimal to binary.

CHAPTER 6

The Data Link Layer

- The Data Link layer is responsible for communications between end-device network interface cards.
- It allows upper layer protocols to access the physical layer media and encapsulates Layer 3 packets (IPv4 and IPv6) into Layer 2 Frames.
- It also performs error detection and rejects corrupts frames.

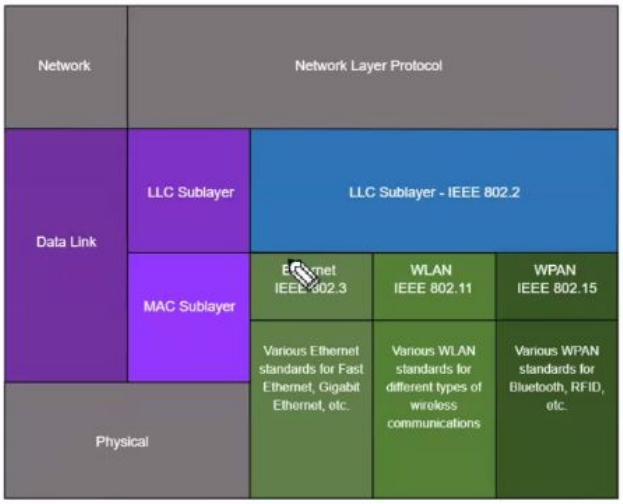


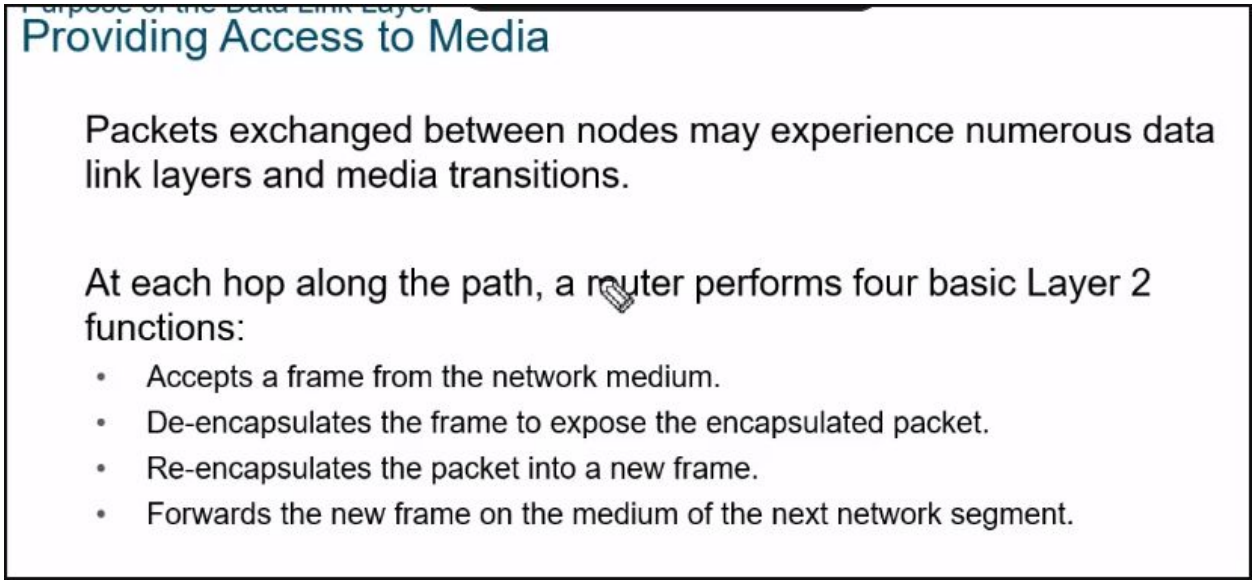
IEEE 802 LAN/MAN Data Link Sublayers

IEEE 802 LAN/MAN standards are specific to the type of network (Ethernet, WLAN, WPAN, etc).

The Data Link Layer consists of two sublayers. **Logical Link Control (LLC)** and **Media Access Control (MAC).**

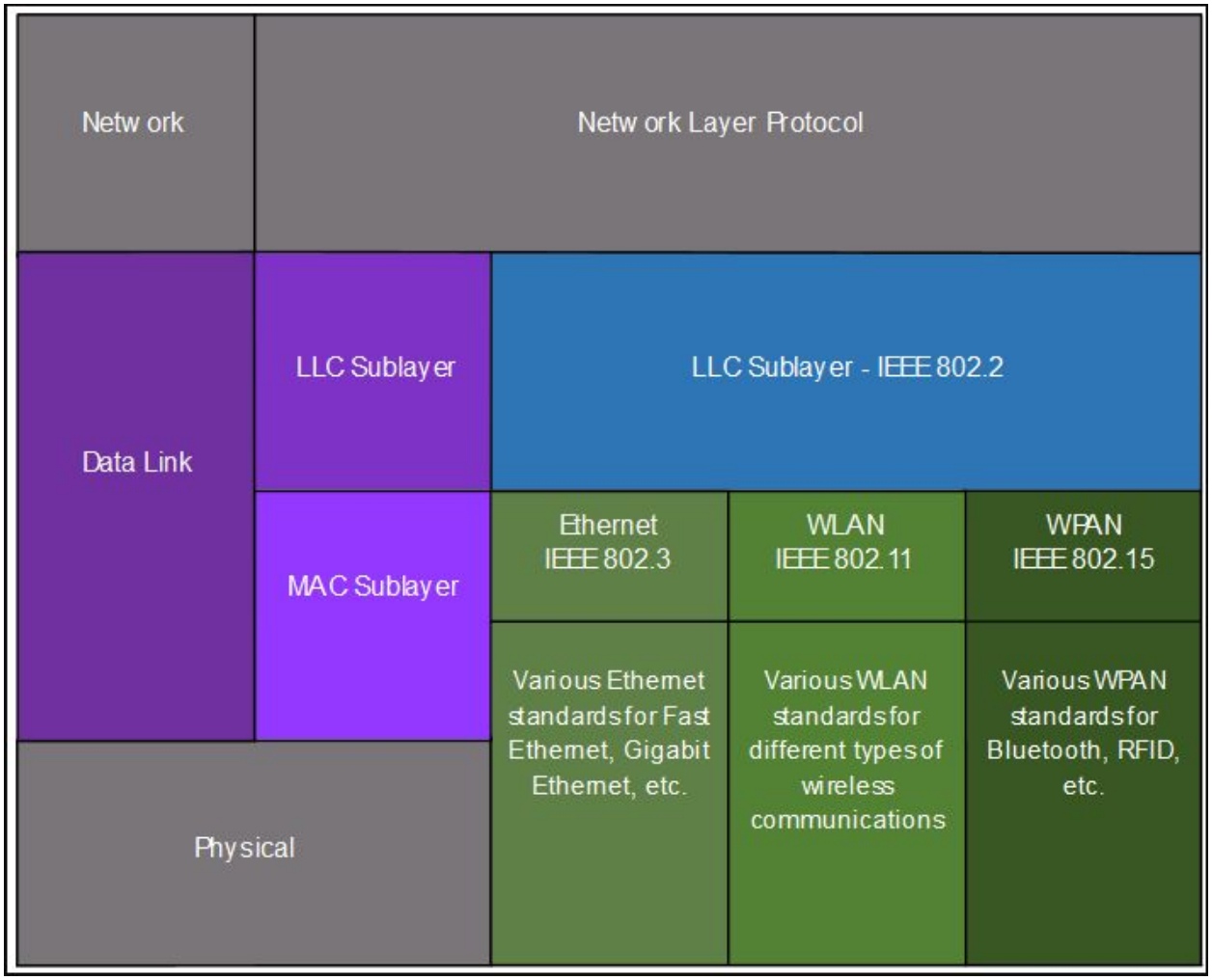
- The LLC sublayer communicates between the networking software at the upper layers and the device hardware at the lower layers.
- The MAC sublayer is responsible for data encapsulation and media access control.

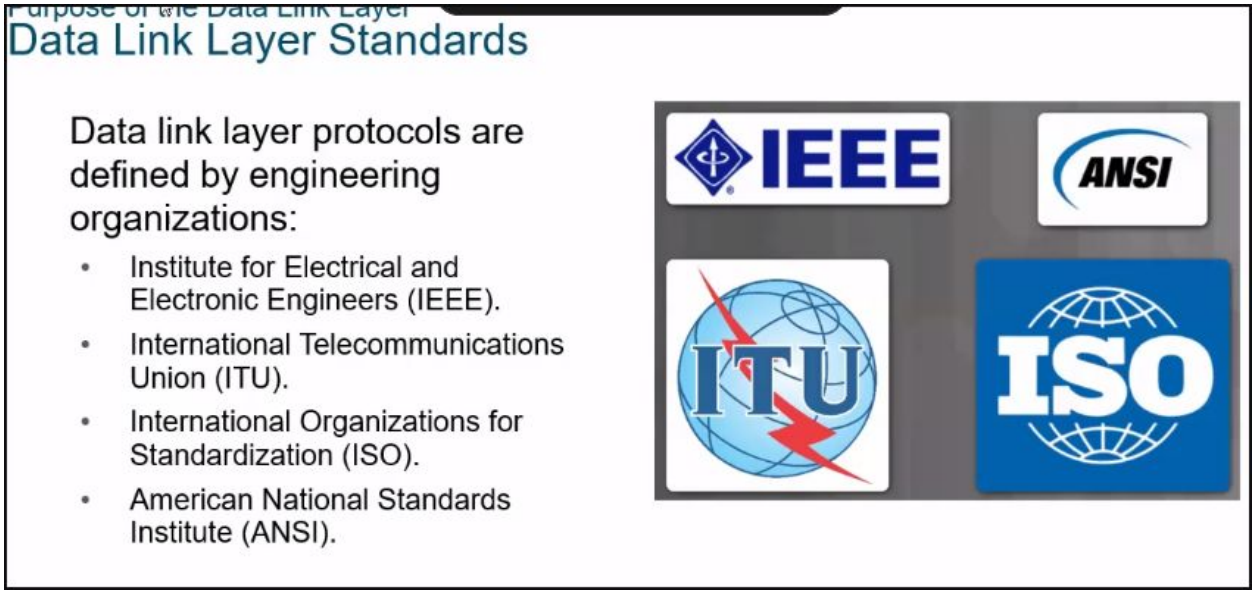




The data link layer does the following:

- Enables upper layers to access the media. The upper layer protocol is completely unaware of the type of media that is used to forward the data.
- Accepts data, usually Layer 3 packets (i.e., IPv4 or IPv6), and encapsulates them into Layer 2 frames.
- Controls how data is placed and received on the media.
- Exchanges frames between endpoints over the network media.
- Receives encapsulated data, usually Layer 3 packets, and directs them to the proper upper-layer protocol.
- Performs error detection and rejects any corrupt frame.

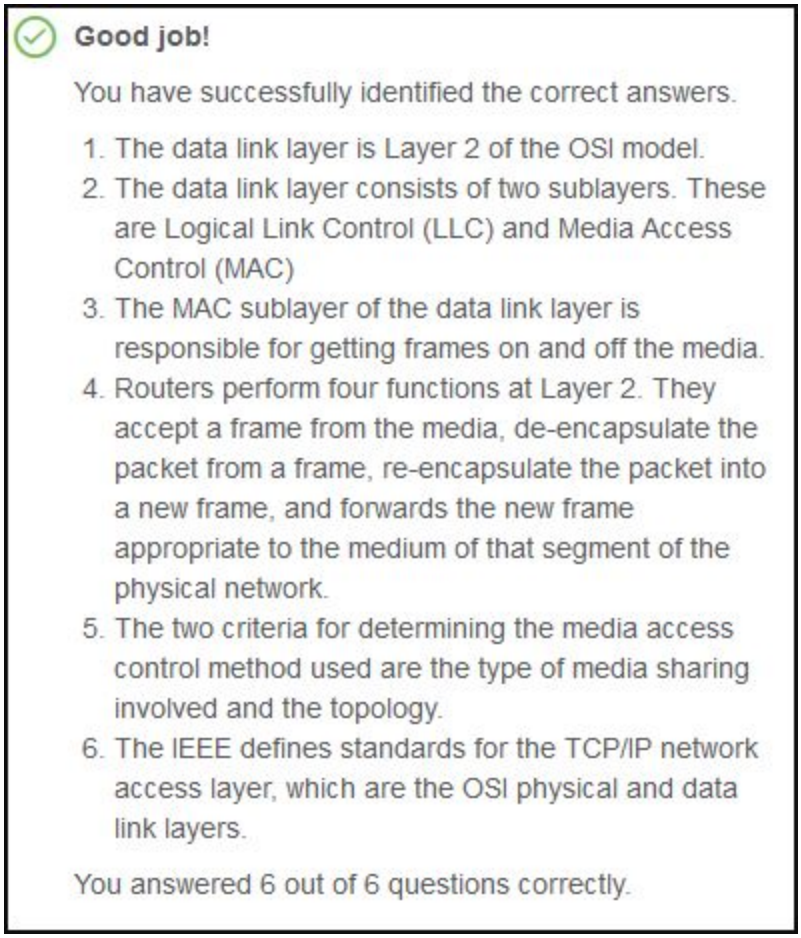


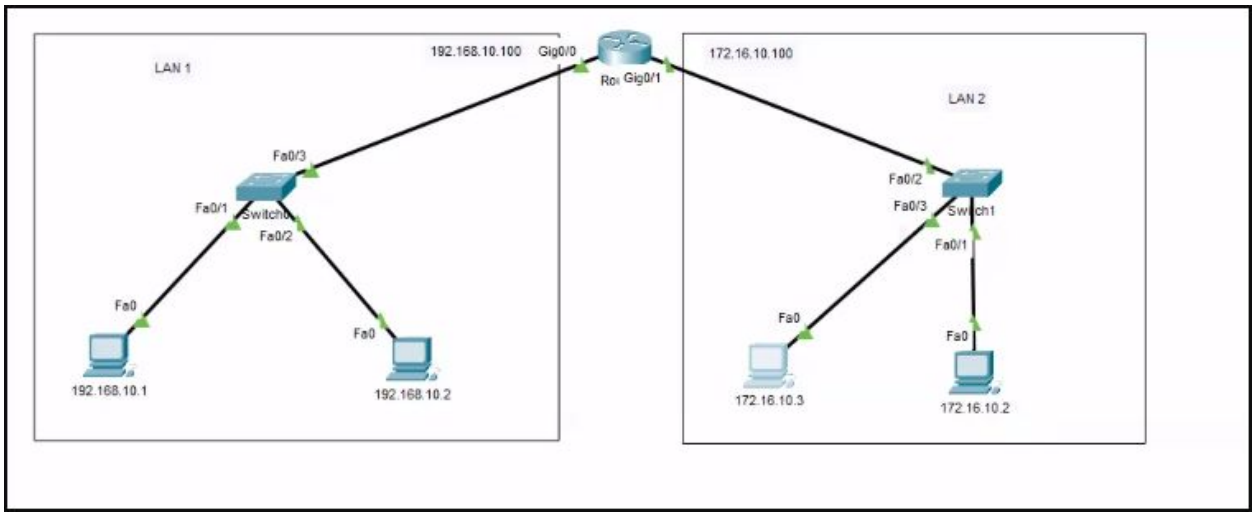


The MAC sublayer provides data encapsulation:

- **Frame delimiting** - The framing process provides important delimiters to identify fields within a frame. These delimiting bits provide synchronization between the transmitting and receiving nodes.
- **Addressing** - Provides source and destination addressing for transporting the Layer 2 frame between devices on the same shared medium.
- **Error detection** - Includes a trailer used to detect transmission errors.

The MAC sublayer also provides media access control, allowing multiple devices to communicate over a shared (half-duplex) medium. Full-duplex communications do not require access control.





Physical and Logical Topologies

The topology of a network is the arrangement and relationship of the network devices and the interconnections between them.

There are two types of topologies used when describing networks:

- **Physical topology** – shows physical connections and how devices are interconnected.
- **Logical topology** – identifies the virtual connections between devices using device interfaces and IP addressing schemes.

The topology of a network is the arrangement, or the relationship, of the network devices and the interconnections between them.

There are two types of topologies used when describing LAN and WAN networks:

- **Physical topology** – Identifies the physical connections and how end devices and intermediary devices (i.e, routers, switches, and wireless access points) are interconnected. The topology may also include specific device location such as room number and location on the equipment rack. Physical topologies are usually point-to-point or star.
- **Logical topology** - Refers to the way a network transfers frames from one node to the next. This topology identifies virtual connections using device interfaces and Layer 3 IP addressing schemes.

Early Ethernet and legacy Token Ring LAN technologies included two other types of topologies:

- **Bus** - All end systems are chained to each other and terminated in some form on each end. Infrastructure devices such as switches are not required to interconnect the end devices. Legacy Ethernet networks were often bus topologies using coax cables because it was inexpensive and easy to set up.
- **Ring** - End systems are connected to their respective neighbor forming a ring. The ring does not need to be terminated, unlike in the bus topology. Legacy Fiber Distributed Data Interface (FDDI) and Token Ring networks used ring topologies.

Half-duplex communication

Both devices can transmit and receive on the media but cannot do so simultaneously. WLANs and legacy bus topologies with Ethernet hubs use the half-duplex mode. Half-duplex allows only one device to send or receive at a time on the shared medium.
Ethernet switches operate in full-duplex mode by default, but they can operate in half-duplex if connecting to a device such as an Ethernet hub.
There are two basic access control methods for shared media:

- Contention-based access
- Controlled access

Contention-based access

In contention-based multiaccess networks, all nodes are operating in half-duplex, competing for the use of the medium. However, only one device can send at a time. Therefore, there is a process if more than one device transmits at the same time. Examples of contention-based access methods include the following:

- Carrier sense multiple access with collision detection (CSMA/CD) used on legacy bus-topology Ethernet LANs
- Carrier sense multiple access with collision avoidance (CSMA/CA) used on Wireless LANs

Controlled access

In a controlled-based multiaccess network, each node has its own time to use the medium. These deterministic types of legacy networks are inefficient because a device must wait its turn to access the medium. Examples of multiaccess networks that use controlled access include the following:

- Legacy Token Ring
- Legacy ARCNET

Contention-Based Access - CSMA/CD

Examples of contention-based access networks include the following:

- Wireless LAN (uses CSMA/CA)
- Legacy bus-topology Ethernet LAN (uses CSMA/CD)
- Legacy Ethernet LAN using a hub (uses CSMA/CD)

These networks operate in half-duplex mode, meaning only one device can send or receive at a time. This requires a process to govern when a device can send and what happens when multiple devices send at the same time.

If two devices transmit at the same time, a collision will occur. For legacy Ethernet LANs, both devices will detect the collision on the network. This is the collision detection (CD) portion of CSMA/CD. The NIC compares data transmitted with data received, or by recognizing that the signal amplitude is higher than normal on the media. The data sent by both devices will be corrupted and will need to be resent.

Contention-Based Access - CSMA/CA

Another form of CSMA used by IEEE 802.11 WLANs is carrier sense multiple access/collision avoidance (CSMA/CA).

CMSA/CA uses a method similar to CSMA/CD to detect if the media is clear. CMSA/CA uses additional techniques. In wireless environments it may not be possible for a device to detect a collision. CMSA/CA does not detect collisions but attempts to avoid them by waiting before transmitting. Each device that transmits includes the time duration that it needs for the transmission. All other wireless devices receive this information and know how long the medium will be unavailable.

Ethernet LANs using switches do not use a contention-based system because the switch and the host NIC operate in full-duplex mode.
6.2.9

Good job!

You have successfully identified the correct answers.

1. The logical topology shows the IP addresses assigned to device interfaces.
2. Wide Area Networks (WANs) come in many topologies, to include point-to-point, hub-and-spoke, and mesh.
3. The extended star topology is considered a hybrid topology because it combines multiple star topologies.
4. Wireless LANs (WLANs) only support half-duplex because only one device can access the media at a time.
5. Carrier sense multiple access /collision detection (CSMA/CD) is the media access control method used in legacy Ethernet LANs.

You answered 5 out of 5 questions correctly.

WAN Topologies

There are three common physical WAN topologies:

- **Point-to-point** – the simplest and most common WAN topology. Consists of a permanent link between two endpoints.
- **Hub and spoke** – similar to a star topology where a central site interconnects branch sites through point-to-point links.
- **Mesh** – provides high availability but requires every end system to be connected to every other end system.

Point-to-Point WAN Topology

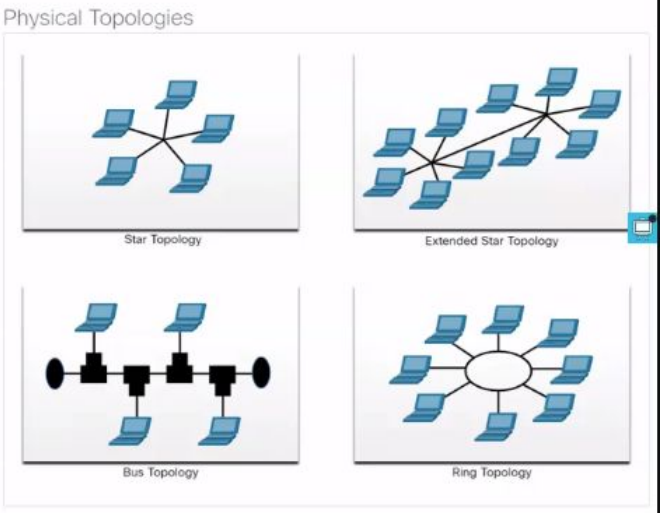
- Physical point-to-point topologies directly connect two nodes.
- The nodes may not share the media with other hosts.
- Because all frames on the media can only travel to or from the two nodes, Point-to-Point WAN protocols can be very simple.

LAN Topologies

End devices on LANs are typically interconnected using a star or extended star topology. Star and extended star topologies are easy to install, very scalable and easy to troubleshoot.

Early Ethernet and Legacy Token Ring technologies provide two additional topologies:

- **Bus** – All end systems chained together and terminated on each end.
- **Ring** – Each end system is connected to its respective neighbors to form a ring.



Half and Full Duplex Communication

Half-duplex communication

- Only allows one device to send or receive at a time on a shared medium.
- Used on WLANs and legacy bus topologies with Ethernet hubs.

Full-duplex communication

- Allows both devices to simultaneously transmit and receive on a shared medium.
- Ethernet switches operate in full-duplex mode.

Access Control Methods

Contention-based access

All nodes operating in half-duplex, competing for use of the medium. Examples are:

- Carrier sense multiple access with collision detection (CSMA/CD) as used on legacy bus-topology Ethernet.
- Carrier sense multiple access with collision avoidance (CSMA/CA) as used on Wireless LANs.

Controlled access

- Deterministic access where each node has its own time on the medium.
- Used on legacy networks such as Token Ring and ARCNET.

Contention-Based Access – CSMA/CD

CSMA/CD

- Used by legacy Ethernet LANs.
- Operates in half-duplex mode where only one device sends or receives at a time.
- Uses a collision detection process to govern when a device can send and what happens if multiple devices send at the same time.

CSMA/CD collision detection process:

- Devices transmitting simultaneously will result in a signal collision on the shared media.
- Devices detect the collision.
- Devices wait a random period of time and retransmit data.

Contention-Based Access – CSMA/CA

CSMA/CA

- Used by IEEE 802.11 WLANs.
- Operates in half-duplex mode where only one device sends or receives at a time.
- Uses a collision avoidance process to govern when a device can send and what happens if multiple devices send at the same time.

CSMA/CA collision avoidance process:

- When transmitting, devices also include the time duration needed for the transmission.
- Other devices on the shared medium receive the time duration information and know how long the medium will be unavailable.

The information appended to a frame is determined by the protocol being used.

The data link layer prepares the encapsulated data (usually an IPv4 or IPv6 packet) for transport across the local media by encapsulating it with a header and a trailer to create a frame.

The data link protocol is responsible for NIC-to-NIC communications within the same network. Although there are many different data link layer protocols that describe data link layer frames, each frame type has three basic parts:

- Header
- Data
- Trailer

Data Link Frame

The Frame

Data is encapsulated by the data link layer with a header and a trailer to form a frame.

A data link frame has three parts:

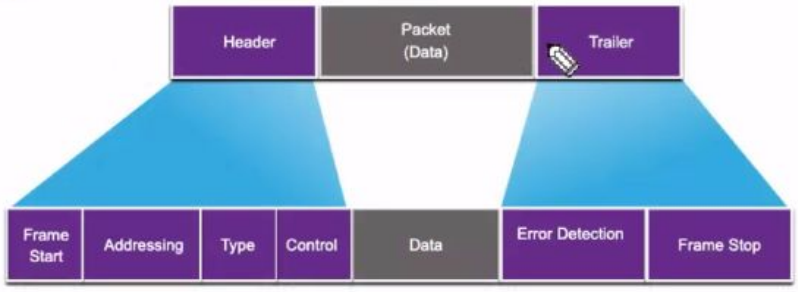
- Header
- Data
- Trailer

The fields of the header and trailer vary according to data link layer protocol.

The amount of control information carried with in the frame varies according to access control information and logical topology.

Data Link Frame

Frame Fields

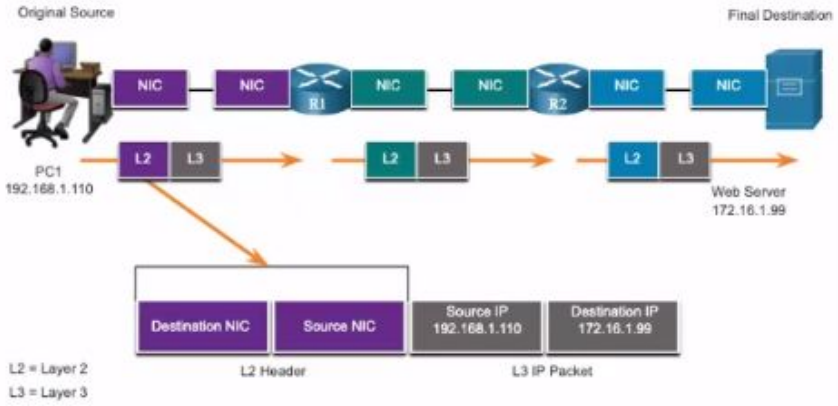


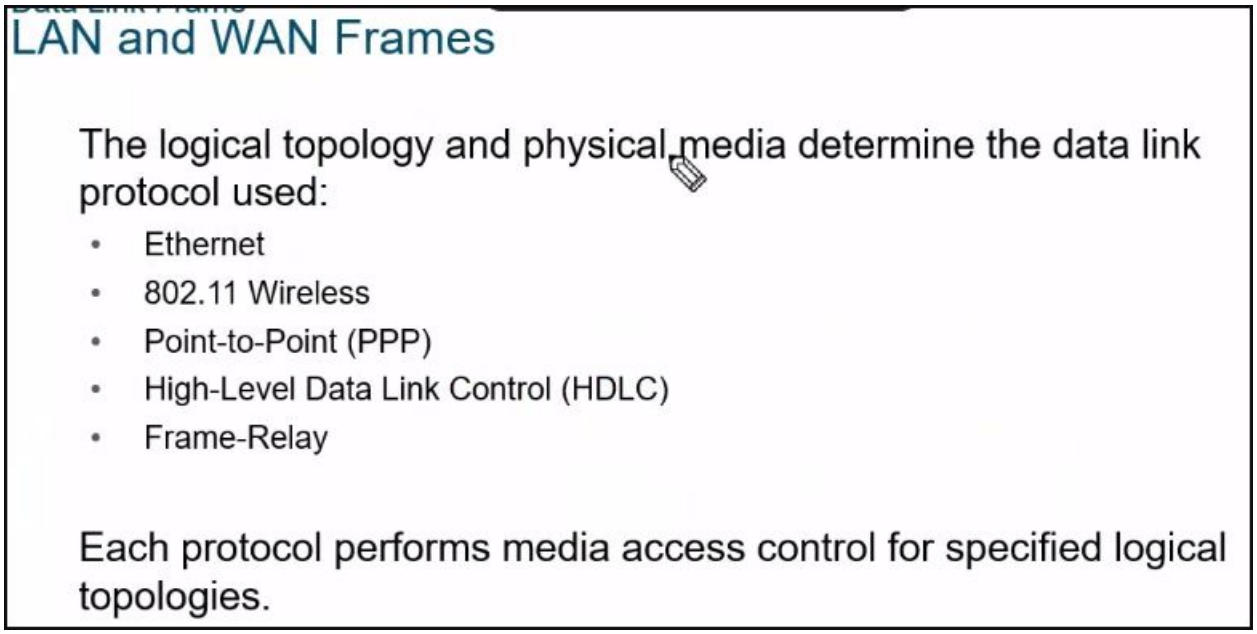
Field	Description
Frame Start and Stop	Identifies beginning and end of frame
Addressing	Indicates source and destination nodes
Type	Identifies encapsulated Layer 3 protocol
Control	Identifies flow control services
Data	Contains the frame payload
Error Detection	Used for determine transmission errors

Data Link Frame

Layer 2 Addresses

- Also referred to as a physical address.
- Contained in the frame header.
- Used only for local delivery of a frame on the link.
- Updated by each device that forwards the frame.





Some of the common WAN protocols over the years have included:

- Point-to-Point Protocol (PPP)
- High-Level Data Link Control (HDLC)
- Frame Relay
- Asynchronous Transfer Mode (ATM)
- X.25

These Layer 2 protocols are now being replaced in the WAN by Ethernet.

In a TCP/IP network, all OSI Layer 2 protocols work with IP at OSI Layer 3. However, the Layer 2 protocol used depends on the logical topology and the physical media.

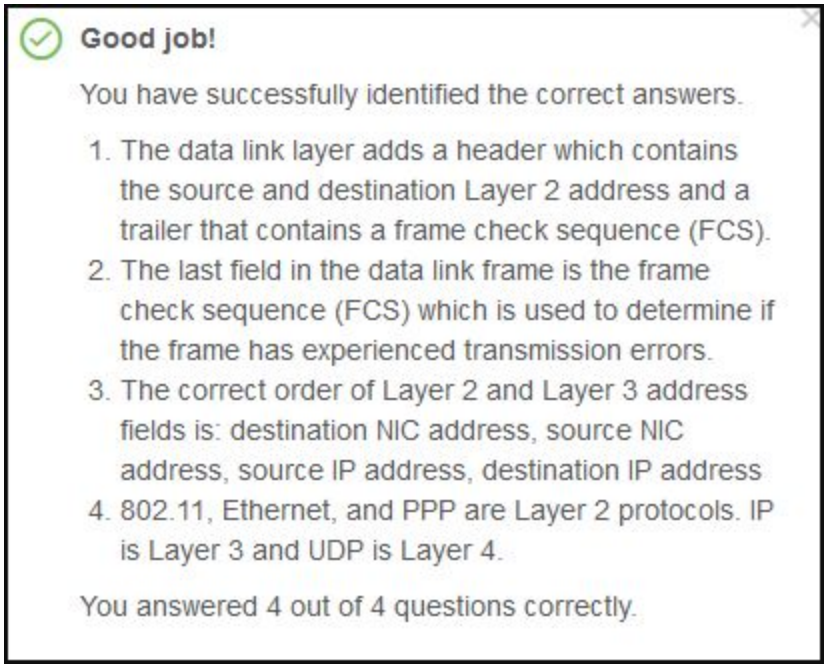
Each protocol performs media access control for specified Layer 2 logical topologies. This means that a number of different network devices can act as nodes that operate at the data link layer when implementing these protocols. These devices include the NICs on computers as well as the interfaces on routers and Layer 2 switches.

The Layer 2 protocol that is used for a particular network topology is determined by the technology used to implement that topology. The technology used is determined by the size of the network, in terms of the number of hosts and the geographic scope, and the services to be provided over the network.

A LAN typically uses a high bandwidth technology capable of supporting large numbers of hosts. The relatively small geographic area of a LAN (a single building or a multi-building campus) and its high density of users make this technology cost-effective.

Data link layer protocols include:

- Ethernet
- 802.11 Wireless
- Point-to-Point Protocol (PPP)
- High-Level Data Link Control (HDLC)
- Frame Relay



What did I learn in this module?

Purpose of the Data Link Layer

The data link layer of the OSI model (Layer 2) prepares network data for the physical network. The data link layer is responsible for network interface card (NIC) to network interface card communications. Without the data link layer, network layer protocols such as IP, would have to make provisions for connecting to every type of media that could exist along a delivery path. The IEEE 802 LAN/MAN data link layer consists of the following two sublayers: LLC and MAC. The MAC sublayer provides data encapsulation through frame delimiting, addressing, and error detection. Router interfaces encapsulate the packet into the appropriate frame. A suitable media access control method is used to access each link. Engineering organizations that define open standards and protocols that apply to the network access layer include: IEEE, ITU, ISO, and ANSI.

Topologies

The two types of topologies used in LAN and WAN networks are physical and logical. The data link layer "sees" the logical topology of a network when controlling data access to the media. The logical topology influences the type of network framing and media access control used.

Three common types of physical WAN topologies are: point-to-point, hub and spoke, and mesh. Physical point-to-point topologies directly connect two end devices (nodes). Adding intermediate physical connections may not change the logical topology. In multi-access LANs, nodes are interconnected using star or extended star topologies. In this type of topology, nodes are connected to a central intermediary device. Physical LAN topologies include: star, extended star, bus, and ring. Half-duplex communications exchange data in one direction at a time. Full-duplex sends and receives data simultaneously. Two interconnected interfaces must use the same duplex mode or there will be a duplex mismatch creating inefficiency and latency on the link. Ethernet LANs and WLANs are examples of multi-access networks. A multi-access network is a network that can have multiple nodes accessing the network simultaneously. Some multi-access networks require rules to govern how devices share the physical media. There are two basic access control methods for shared media: contention-based access and controlled access. In contention-based multi-access networks, all nodes are operating in half-duplex. There is a process if more than one device transmits at the same time. Examples of contention-based access methods include: CSMA/CD for bus-topology Ethernet LANs and CSMA/CA for WLANs.

Data Link Frame

The data link layer prepares the encapsulated data (usually an IPv4 or IPv6 packet) for transport across the local media by encapsulating it with a header and a trailer to create a frame. The data link protocol is responsible for NIC-to-NIC communications within the same network. There are many different data link layer protocols that describe data link layer frames, each frame type has three basic parts: header, data, and trailer. Unlike other encapsulation protocols, the data link layer appends information in the trailer. There is no one frame structure that meets the needs of all data transportation across all types of media. Depending on the environment, the amount of control information needed in the frame varies to match the access control requirements of the media and logical topology. Frame fields include: frame start and stop indicator flags, addressing, type, control, data, and error detection. The data link layer provides addressing used to transport a frame across shared local media. Device addresses at this layer are physical addresses. Data link layer addressing is contained within the frame header and specifies the frame destination node on the local network. The data link layer address is only used for local delivery. In a TCP/IP network, all OSI Layer 2 protocols work with IP at OSI Layer 3. However, the Layer 2 protocol used depends on the logical topology and the physical media. Each protocol performs media access control for specified Layer 2 logical topologies. The Layer 2 protocol that is used for a particular network topology is determined by the technology used to implement that topology. Data link layer protocols include: Ethernet, 802.11 Wireless, PPP, HDLC, and Frame Relay.

CHAPTER 7

Ethernet Encapsulation

This module starts with a discussion of Ethernet technology including an explanation of MAC sublayer and the Ethernet frame fields.

Ethernet is one of two LAN technologies used today, with the other being wireless LANs (WLANs). Ethernet uses wired communications, including twisted pair, fiber-optic links, and coaxial cables.

Ethernet operates in the data link layer and the physical layer. It is a family of networking technologies defined in the IEEE 802.2 and 802.3 standards. Ethernet supports data bandwidths of the following:

- 10 Mbps
- 100 Mbps
- 1000 Mbps (1 Gbps)
- 10,000 Mbps (10 Gbps)
- 40,000 Mbps (40 Gbps)
- 100,000 Mbps (100 Gbps)

As shown in the figure, Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies.

Ethernet and the OSI Model

ApplicationPresentationSessionTransportNetworkData
LinkPhysicalLLCMAC802.2802.3Ethernet

Ethernet is defined by data link layer and physical layer protocols.

7.1.2

Data Link Sublayers

IEEE 802 LAN/MAN protocols, including Ethernet, use the following two separate sublayers of the data link layer to operate. They are the Logical Link Control (LLC) and the Media Access Control (MAC), as shown in the figure.

Recall that LLC and MAC have the following roles in the data link layer:

- **LLC Sublayer** - This IEEE 802.2 sublayer communicates between the networking software at the upper layers and the device hardware at the lower layers. It places information in the frame that identifies which network layer protocol is being used for the frame. This information allows multiple Layer 3 protocols, such as IPv4 and IPv6, to use the same network interface and media.
- **MAC Sublayer** - This sublayer (IEEE 802.3, 802.11, or 802.15 for example) is implemented in hardware and is responsible for data encapsulation and media access control. It provides data link layer addressing and is integrated with various physical layer technologies.

The diagram shows the OSI network, data link, and physical layers. It also shows the data link layer LLC and MAC sublayers and various LAN/WAN protocols. At the top of the diagram is the network layer and the network layer protocol. Below that is the data link layer and its sublayers. The top sublayer is the LLC sublayer as specified in IEEE 802.2. Next is the MAC sublayer with three columns representing different types of network technologies. The first column is Ethernet IEEE 802.3 at the upper part of the MAC sublayer. Below this are various Ethernet standards for Fast Ethernet, Gigabit Ethernet, etc. that span across the lower part of the MAC sublayer and the entire OSI physical layer. The next column is WLAN IEEE 802.11 at the upper part of the MAC sublayer. Below this are the various WLAN standards for different types of wireless communications that span across the lower part of the MAC sublayer and the entire OSI physical layer. The last column is WPAN IEEE 802.15 at the upper part of the MAC sublayer. Below this are various WPAN standards for Bluetooth, RFID, etc. that span across the lower part of the MAC sublayer and the entire OSI physical layer.

Network Layer ProtocolNetworkData LinkLLC Sublayer - IEEE 802.2LLC SublayerMAC SublayerEthernet
IEEE 802.3WLAN
IEEE 802.11WPAN
IEEE 802.15Various Ethernet standards for Fast Ethernet, Gigabit Ethernet, etc.Various WLAN standards for different types of wireless communicationsVarious WPAN standards for Bluetooth, RFID, etc.Physical
7.1.3

MAC Sublayer

The MAC sublayer is responsible for data encapsulation and accessing the media.

Data Encapsulation

IEEE 802.3 data encapsulation includes the following:

- **Ethernet frame** - This is the internal structure of the Ethernet frame.
- **Ethernet Addressing** - The Ethernet frame includes both a source and destination MAC address to deliver the Ethernet frame from Ethernet NIC to Ethernet NIC on the same LAN.
- **Ethernet Error detection** - The Ethernet frame includes a frame check sequence (FCS) trailer used for error detection.

Accessing the Media

As shown in the figure, the IEEE 802.3 MAC sublayer includes the specifications for different Ethernet communications standards over various types of media including copper and fiber.

The diagram is showing various Ethernet standards in the MAC sublayer. At the top of the diagram is the network layer and the network layer protocol. Below that is the data link layer and its sublayers. The top sublayer is the IEEE 802.2 LLC sublayer. Next is the Ethernet IEEE 802.3 MAC sublayer. Below that are five columns with various Ethernet standards and media types that span the lower part of the MAC sublayer and the entire OSI physical layer. From left to right the columns are: IEEE 802.3u Fast Ethernet; IEEE 802.3z Gigabit Ethernet over Fiber; IEEE 802.ab Gigabit Ethernet over Copper; IEEE 802.3ae 10 Gigabit Ethernet over Fiber; and Etc.

Ethernet Standards in the MAC Sublayer

Ethernet-IEEE 802.3IEEE 802.3z
Gigabit Ethernet
over FiberIEEE 802.3ab
Gigabit Ethernet
over CopperIEEE 802.3u
Fast EthernetNetwork Layered ProtocolNetworkData LinkLLC Sublayer-IEEE 802.2LLC SublayerPhysicalMAC SublayerEtc.IEEE 802.3ae
10 Gigabit Ethernet
over Fiber

Recall that legacy Ethernet using a bus topology or hubs, is a shared, half-duplex medium. Ethernet over a half-duplex medium uses a contention-based access method, carrier sense multiple access/collision detection (CSMA/CD) This ensures that only one device is transmitting at a time. CSMA/CD allows multiple devices to share the same half-duplex medium, detecting a collision when more than one device attempts to transmit simultaneously. It also provides a back-off algorithm for retransmission.

Ethernet LANs of today use switches that operate in full-duplex. Full-duplex communications with Ethernet switches do not require access control through CSMA/CD.

7.1.4

Ethernet Frame Fields

The minimum Ethernet frame size is 64 bytes and the expected maximum is 1518 bytes. This includes all bytes from the destination MAC address field through the frame check sequence (FCS) field. The preamble field is not included when describing the size of the frame.

Note: The frame size may be larger if additional requirements are included, such as VLAN tagging. VLAN tagging is beyond the scope of this course.

Any frame less than 64 bytes in length is considered a “collision fragment” or “runt frame” and is automatically discarded by receiving stations. Frames with more than 1500 bytes of data are considered “jumbo” or “baby giant frames”.

If the size of a transmitted frame is less than the minimum, or greater than the maximum, the receiving device drops the frame. Dropped frames are likely to be the result of collisions or other unwanted signals. They are considered invalid. Jumbo frames are usually supported by most Fast Ethernet and Gigabit Ethernet switches and NICs.

The figure shows each field in the Ethernet frame. Refer to the table for more information about the function of each field.

The diagram shows the fields of an Ethernet frame. From left to right the fields and their length are: Preamble and SFD, 8 bytes; destination MAC address, 6 bytes; source MAC address, 6 bytes; type / length, 2 bytes; data, 46 - 1500 bytes; and F C S, 4 bytes. Excluding the first field, the total number of bytes in the remaining fields is between 64 – 1518 bytes.

Ethernet Frame Fields

FCSDataType / LengthSource MAC AddressPreamble and SFDDestination MAC Address8 bytes6 bytes6 bytes2 bytes46-1500 bytes4 bytes64-1518 bytes

Ethernet Frame Fields Detail

Field	Description

Preamble and Start Frame Delimiter Fields	The Preamble (7 bytes) and Start Frame Delimiter (SFD), also called the Start of Frame (1 byte), fields are used for synchronization between the sending and receiving devices. These first eight bytes of the frame are used to get the attention of the receiving nodes. Essentially, the first few bytes tell the receivers to get ready to receive a new frame.
Destination MAC Address Field	This 6-byte field is the identifier for the intended recipient. As you will recall, this address is used by Layer 2 to assist devices in determining if a frame is addressed to them. The address in the frame is compared to the MAC address in the device. If there is a match, the device accepts the frame. Can be a unicast, multicast or broadcast address.
Source MAC Address Field	This 6-byte field identifies the originating NIC or interface of the frame.
Type / Length	This 2-byte field identifies the upper layer protocol encapsulated in the Ethernet frame. Common values are, in hexadecimal, 0x800 for IPv4, 0x86DD for IPv6 and 0x806 for ARP. **Note**: You may also see this field referred to as EtherType, Type, or Length.
Data Field	This field (46 - 1500 bytes) contains the encapsulated data from a higher layer, which is a generic Layer 3 PDU, or more commonly, an IPv4 packet. All frames must be at least 64 bytes long. If a small packet is encapsulated, additional bits called a pad are used to increase the size of the frame to this minimum size.
Frame Check Sequence Field	The Frame Check Sequence (FCS) field (4 bytes) is used to detect errors in a frame. It uses a cyclic redundancy check (CRC). The sending device includes the results of a CRC in the FCS field of the frame. The receiving device receives the frame and generates a CRC to look for errors. If the calculations match, no error occurred. Calculations that do not match are an indication that the data has changed; therefore, the

frame is dropped. A change in the data could be the result of a disruption of the electrical signals that represent the bits.

Good job!

You have successfully identified the correct answers.

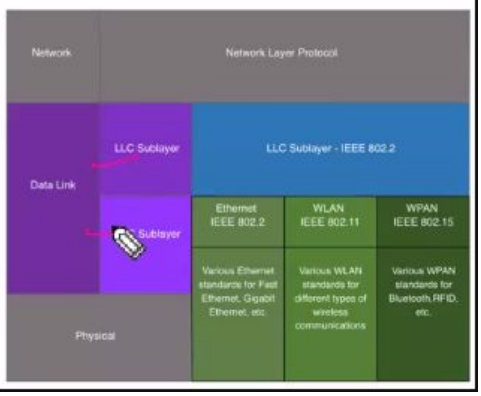
1. All frames must be at least 64 bytes long. Additional bits called a "pad" are used to increase the size of small frames to the minimum size.
2. The FCS field uses a CRC to detect errors in a frame.
3. The EtherType field identifies the upper layer protocol that is encapsulated in the Ethernet Frame.
4. The first few bytes of the preamble inform the receiver of a new frame.
5. The LLC sublayer is responsible for controlling the network interface card through software drivers
6. The LLC works with upper layers to support higher level protocols.
7. The MAC sublayer checks for bit errors, supports Ethernet technologies, and controls access to the media.

You answered 7 out of 7 questions correctly.

Data Link Sublayers

The 802 LAN/MAN standards, including Ethernet, use two separate sublayers of the data link layer to operate:

- **LLC Sublayer**: (IEEE 802.2) Places information in the frame to identify which network layer protocol is used for the frame.
- **MAC Sublayer**: (IEEE 802.3, 802.11, or 802.15) Responsible for data encapsulation and media access control, and provides data link layer addressing.



MAC Sublayer

The MAC sublayer is responsible for data encapsulation and accessing the media.

Data Encapsulation

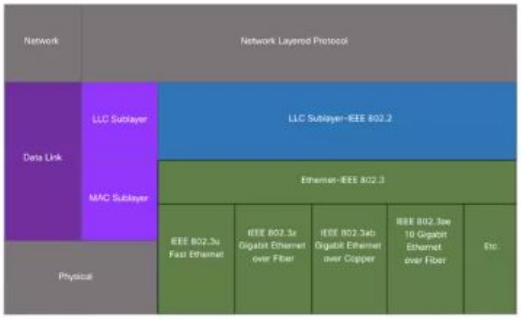
IEEE 802.3 data encapsulation includes the following:

1. **Ethernet frame** - This is the internal structure of the Ethernet frame.
2. **Ethernet Addressing** - The Ethernet frame includes both a source and destination MAC addres to deliver the Ethernet frame from Ethernet NIC to Ethernet NIC on the same LAN.
3. **Ethernet Error detection** - The Ethernet frame includes a frame check sequence (FCS) trailer used for error detection.

MAC Sublayer

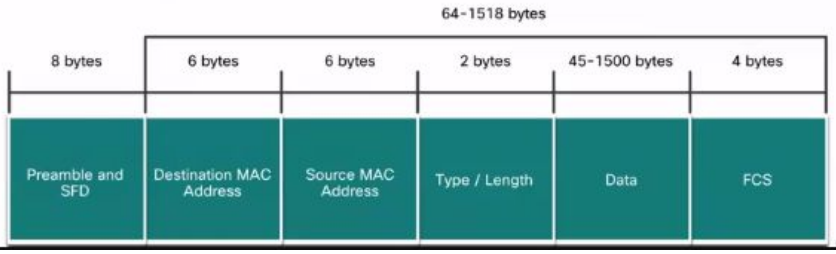
Media Access

- The IEEE 802.3 MAC sublayer includes the specifications for different Ethernet communication standards over various types of media including copper and fiber.
- Legacy Ethernet using a bus topology or hubs, is a shared, half-duplex medium. Ethernet over a half-duplex medium uses a contention-based access method, carrier sense multiple access/collision detection (CSMA/CD).
- Ethernet LANs of today use switches that operate in full-duplex. Full-duplex communications with Ethernet switches do not require access control through CSMA/CD.



Ethernet Frame Fields

- The minimum Ethernet frame size is 64 bytes and the maximum is 1518 bytes. The preamble field is not included when describing the size of the frame.
- Any frame less than 64 bytes in length is considered a “collision fragment” or “runt frame” and is automatically discarded. Frames with more than 1500 bytes of data are considered “jumbo” or “baby giant frames”.
- If the size of a transmitted frame is less than the minimum, or greater than the maximum, the receiving device drops the frame. Dropped frames are likely to be the result of collisions or other unwanted signals. They are considered invalid. Jumbo frames are usually supported by most Fast Ethernet and Gigabit Ethernet switches and NICs.



MAC Address and Hexadecimal

- An Ethernet MAC address consists of a 48-bit binary value, expressed using 12 hexadecimal values.
- Given that 8 bits (one byte) is a common binary grouping, binary 00000000 to 11111111 can be represented in hexadecimal as the range 00 to FF,
- When using hexadecimal, leading zeroes are always displayed to complete the 8-bit representation. For example the binary value 0000 1010 is represented in hexadecimal as 0A.
- Hexadecimal numbers are often represented by the value preceded by **0x** (e.g., 0x73) to distinguish between decimal and hexadecimal values in documentation.
- Hexadecimal may also be represented by a subscript 16, or the hex number followed by an H (e.g., 73H).

An Ethernet MAC address is a 48-bit address expressed using 12 hexadecimal digits, as shown in the figure. Because a byte equals 8 bits, we can also say that a MAC address is 6 bytes in length.

All MAC addresses must be unique to the Ethernet device or Ethernet interface. To ensure this, all vendors that sell Ethernet devices must register with the IEEE to obtain a unique 6 hexadecimal (i.e., 24-bit or 3-byte) code called the organizationally unique identifier (OUI).

When a vendor assigns a MAC address to a device or Ethernet interface, the vendor must do as follows:

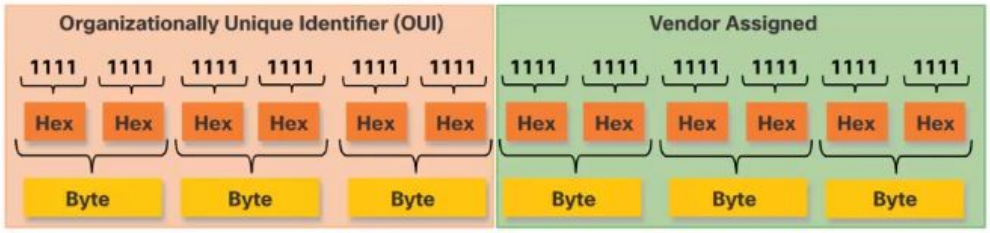
- Use its assigned OUI as the first 6 hexadecimal digits.

- Assign a unique value in the last 6 hexadecimal digits.

Therefore, an Ethernet MAC address consists of a 6 hexadecimal vendor OUI code followed by a 6 hexadecimal vendor-assigned value

Ethernet MAC Address

- In an Ethernet LAN, every network device is connected to the same, shared media. MAC addressing provides a method for device identification at the data link layer of the OSI model.
- An Ethernet MAC address is a 48-bit address expressed using 12 hexadecimal digits. Because a byte equals 8 bits, we can also say that a MAC address is 6 bytes in length.
- All MAC addresses must be unique to the Ethernet device or Ethernet interface. To ensure this, all vendors that sell Ethernet devices must register with the IEEE to obtain a unique 6 hexadecimal (i.e., 24-bit or 3-byte) code called the organizationally unique identifier (OUI).
- An Ethernet MAC address consists of a 6 hexadecimal vendor OUI code followed by a 6 hexadecimal vendor-assigned value.

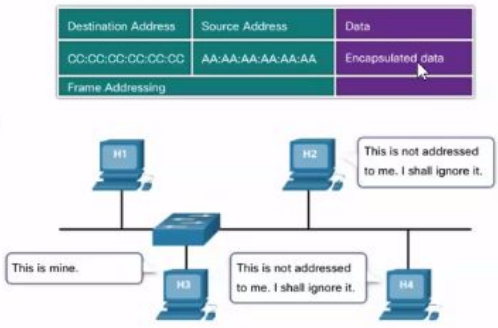


Frame Processing

- When a device is forwarding a message to an Ethernet network, the Ethernet header include a Source MAC address and a Destination MAC address.
- When a NIC receives an Ethernet frame, it examines the destination MAC address to see if it matches the physical MAC address that is stored in RAM. If there is no match, the device discards the frame. If there is a match, it passes the frame up the OSI layers, where the de-encapsulation process takes place.

Note: Ethernet NICs will also accept frames if the destination MAC address is a broadcast or a multicast group of which the host is a member.

- Any device that is the source or destination of an Ethernet frame, will have an Ethernet NIC and therefore, a MAC address. This includes workstations, servers, printers, mobile devices, and routers.



Sometimes the MAC address is referred to as a burned-in address (BIA) because the address is hard coded into read-only memory (ROM) on the NIC. This means that the address is encoded into the ROM chip permanently.

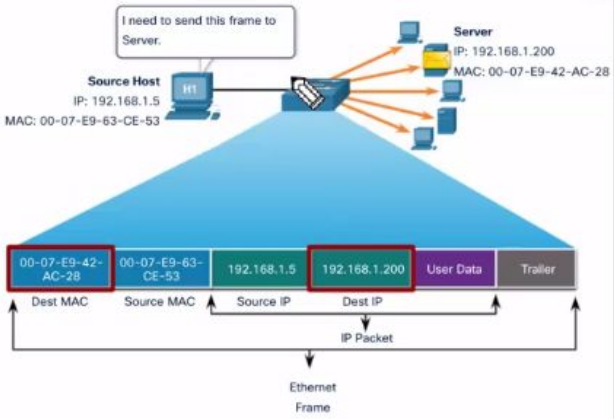
he process that a source host uses to determine the destination MAC address associated with an IPv4 address is known as Address Resolution Protocol (ARP). The process that a source host uses to determine the destination MAC address associated with an IPv6 address is known as Neighbor Discovery (ND).

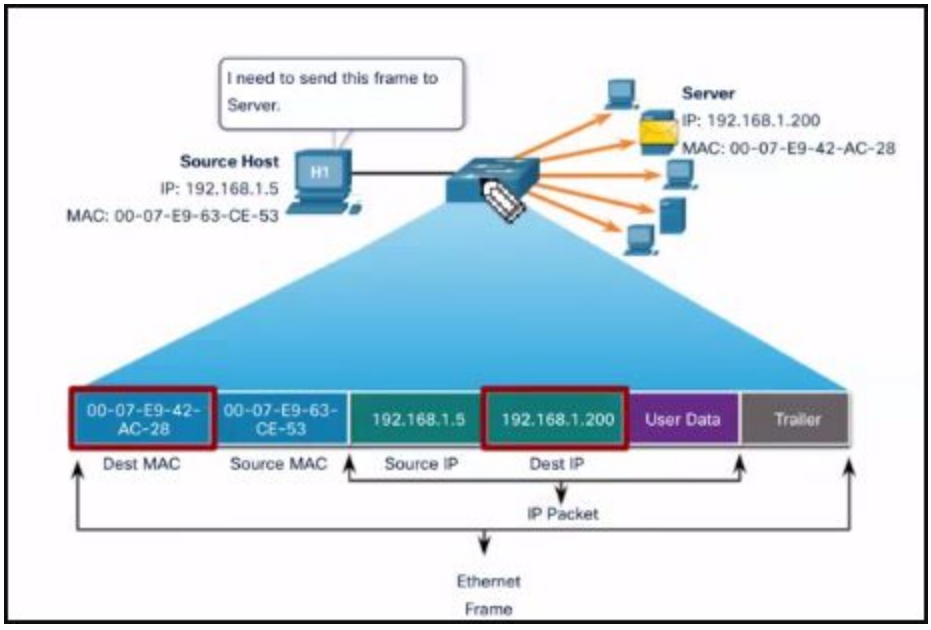
Unicast MAC Address

In Ethernet, different MAC addresses are used for Layer 2 unicast, broadcast, and multicast communications.

- A unicast MAC address is the unique address that is used when a frame is sent from a single transmitting device to a single destination device.
- The process that a source host uses to determine the destination MAC address associated with an IPv4 address is known as Address Resolution Protocol (ARP). The process that a source host uses to determine the destination MAC address associated with an IPv6 address is known as Neighbor Discovery (ND).

Note: The source MAC address must always be a unicast.



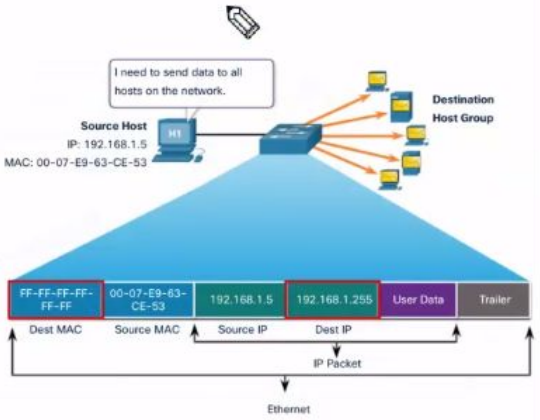


- There is a destination MAC address of 01-00-5E when the encapsulated data is an IPv4 multicast packet and a destination MAC address of 33-33 when the encapsulated data is an IPv6 multicast packet.
- There are other reserved multicast destination MAC addresses for when the encapsulated data is not IP, such as Spanning Tree Protocol (STP) and Link Layer Discovery Protocol (LLDP).
- It is flooded out all Ethernet switch ports except the incoming port, unless the switch is configured for multicast snooping.
- It is not forwarded by a router, unless the router is configured to route multicast packets.

Broadcast MAC Address

An Ethernet broadcast frame is received and processed by every device on the Ethernet LAN. The features of an Ethernet broadcast are as follows:

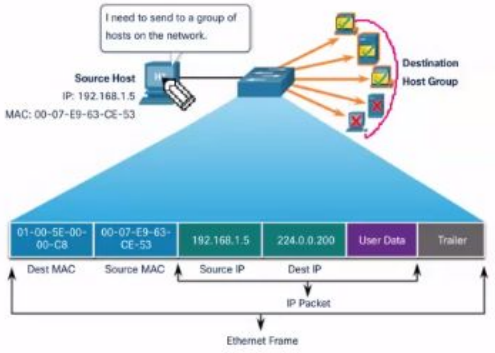
- It has a destination MAC address of FF-FF-FF-FF-FF-FF in hexadecimal (48 ones in binary).
- It is flooded out all Ethernet switch ports except the incoming port. It is not forwarded by a router.
- If the encapsulated data is an IPv4 broadcast packet, this means the packet contains a destination IPv4 address that has all ones (1s) in the host portion. This numbering in the address means that all hosts on that local network (broadcast domain) will receive and process the packet.



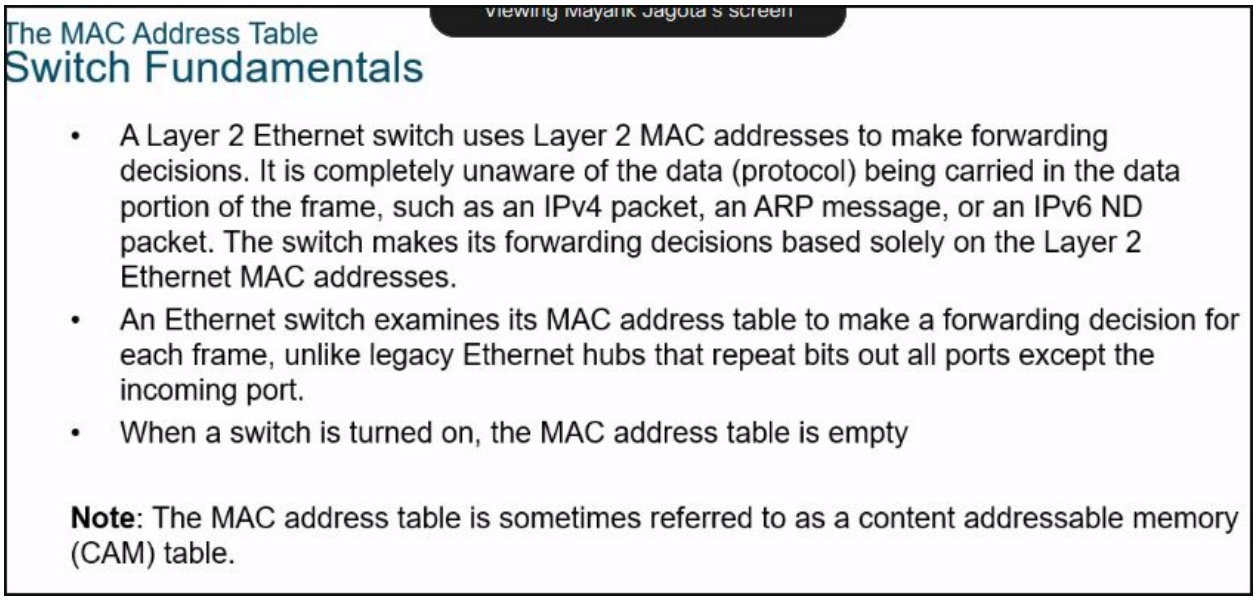
Multicast MAC Address

An Ethernet multicast frame is received and processed by a group of devices that belong to the same multicast group.

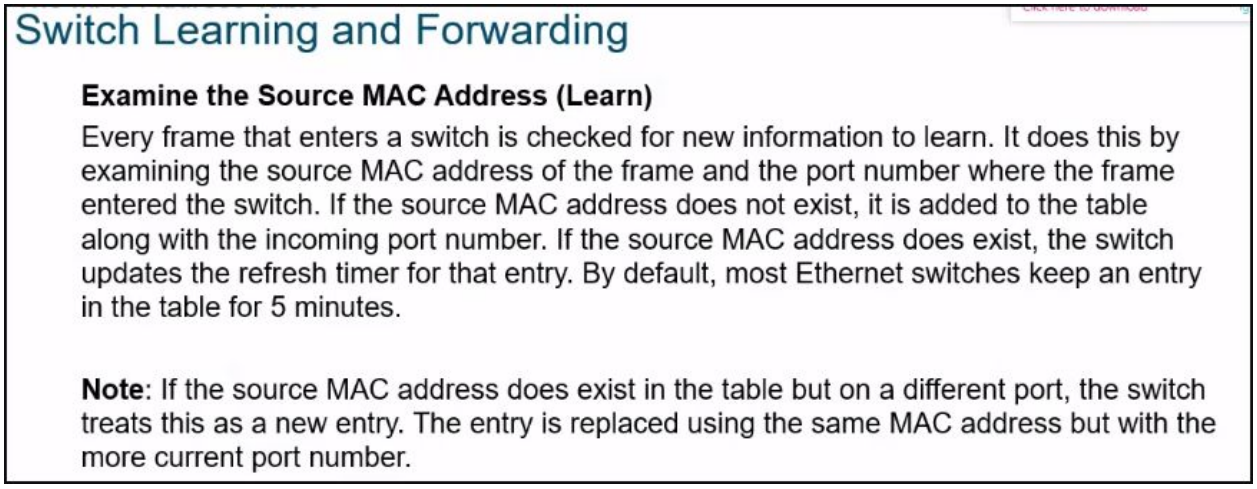
- There is a destination MAC address of 01-00-5E when the encapsulated data is an IPv4 multicast packet and a destination MAC address of 33-33 when the encapsulated data is an IPv6 multicast packet.
- There are other reserved multicast destination MAC addresses for when the encapsulated data is not IP, such as Spanning Tree Protocol (STP).
- It is flooded out all Ethernet switch ports except the incoming port, unless the switch is configured for multicast snooping. It is not forwarded by a router, unless the router is configured to route multicast packets.
- Because multicast addresses represent a group of addresses (sometimes called a host group), they can only be used as the destination of a packet. The source will always be a unicast address.
- As with the unicast and broadcast addresses, the multicast IP address requires a corresponding multicast MAC address.



The range of IPv4 multicast addresses is 224.0.0.0 to 239.255.255.255. The range of IPv6 multicast addresses begins with ff00::/8. Because multicast addresses represent a group of addresses (sometimes called a host group), they can only be used as the destination of a packet. The source will always be a unicast address.



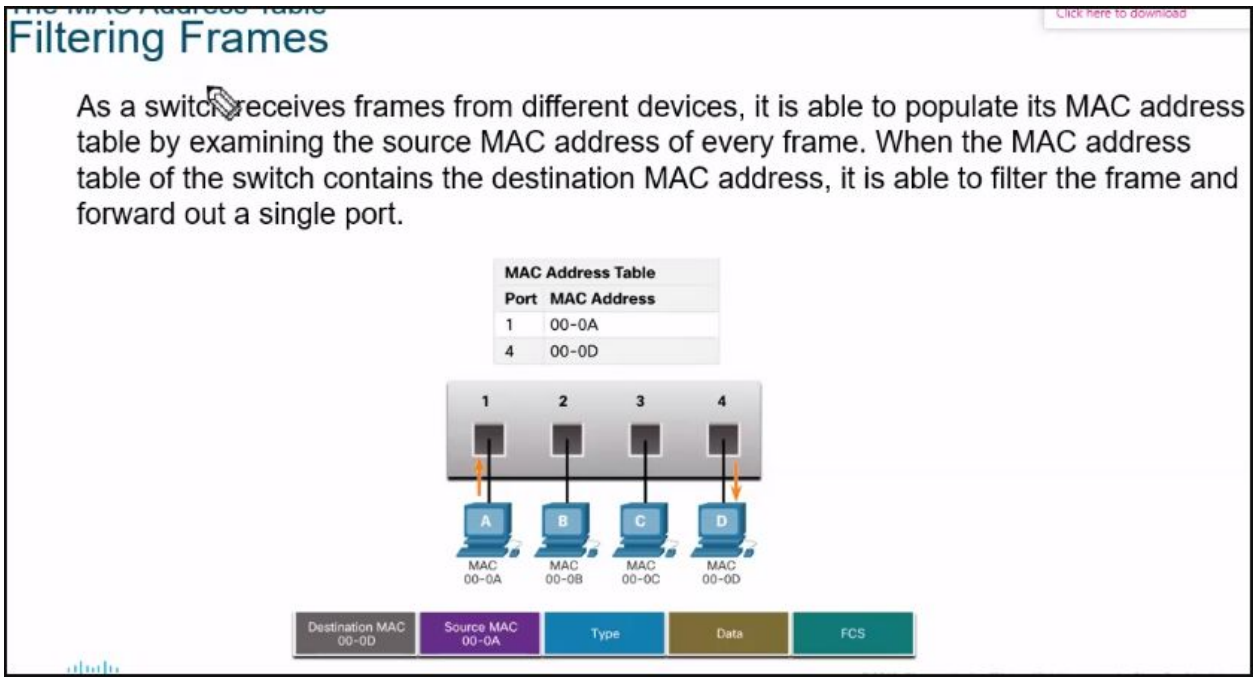
The MAC address table is sometimes referred to as a content addressable memory (CAM) table. While the term CAM table is fairly common, for the purposes of this course, we will refer to it as a MAC address table.
By default, most Ethernet switches keep an entry in the table for 5 minutes.
If the destination MAC address is not in the table, the switch will forward the frame out all ports except the incoming port. This is called an unknown unicast.

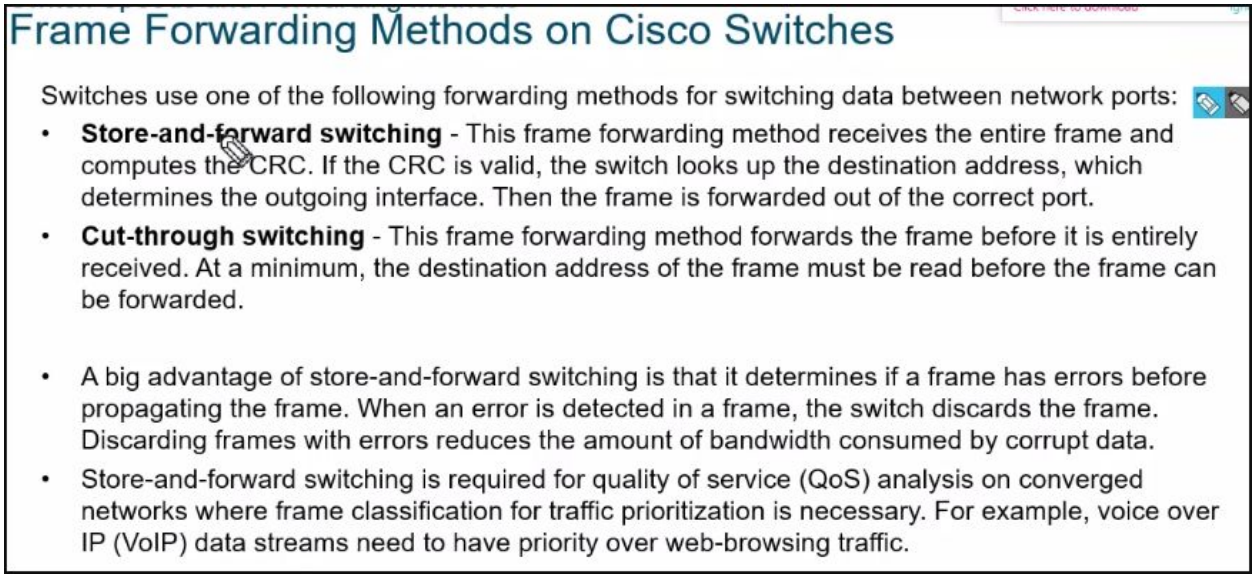


A switch can have multiple MAC addresses associated with a single port. This is common when the switch is connected to another switch. The switch will have a separate MAC address table entry for each frame received with a different source MAC address.
Switches use one of the following forwarding methods for switching data between network ports:

- **Store-and-forward switching** - This frame forwarding method receives the entire frame and computes the CRC. CRC uses a mathematical formula, based on the number of bits (1s) in the frame, to determine whether the received frame has an error. If the CRC is valid, the switch looks up the destination address, which determines the outgoing interface. Then the frame is forwarded out of the correct port.

- **Cut-through switching** - This frame forwarding method forwards the frame before it is entirely received. At a minimum, the destination address of the frame must be read before the frame can be forwarded.

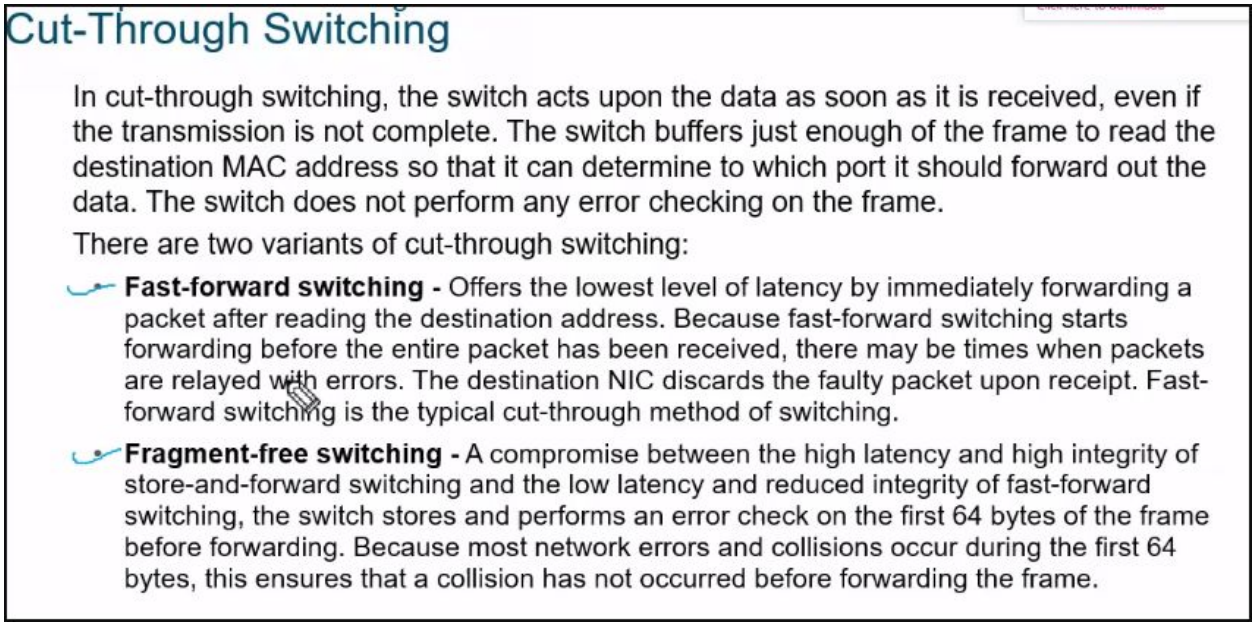




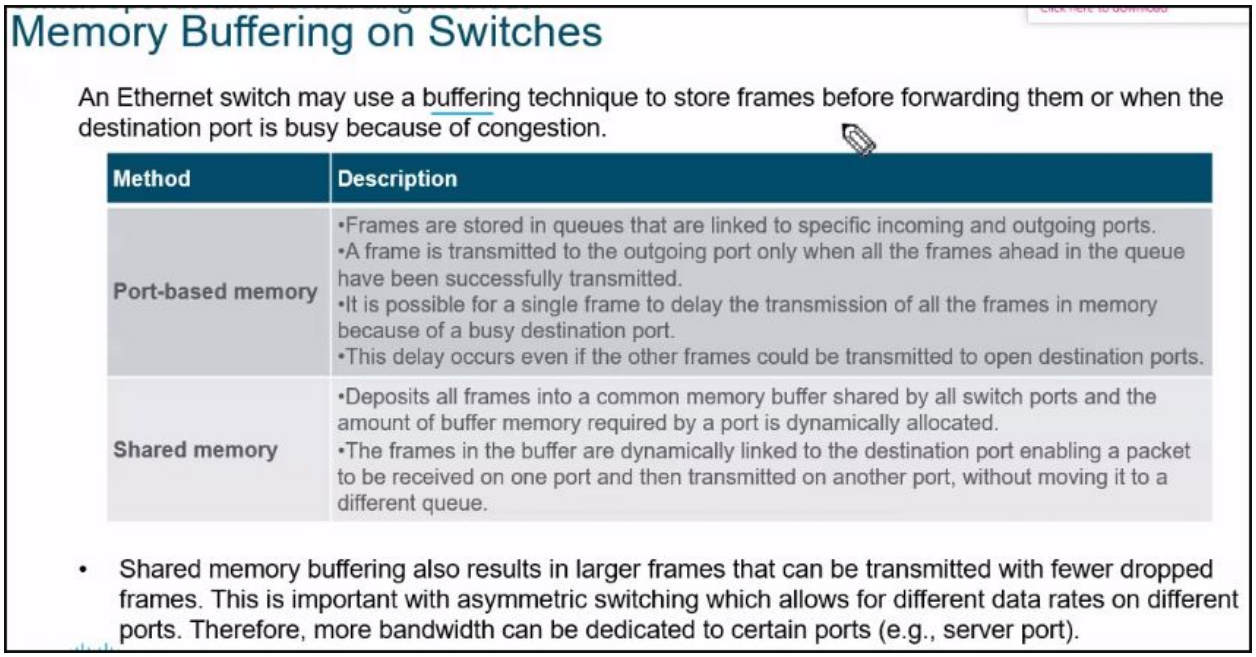
A big advantage of store-and-forward switching is that it determines if a frame has errors before propagating the frame. When an error is detected in a frame, the switch discards the frame. Discarding frames with errors reduces the amount of bandwidth consumed by corrupt data.
Store-and-forward switching is required for quality of service (QoS) analysis on converged networks where frame classification for traffic prioritization is necessary. For example, voice over IP (VoIP) data streams need to have priority over web-browsing traffic.

There are two variants of cut-through switching:

- **Fast-forward switching -** Fast-forward switching offers the lowest level of latency. Fast-forward switching immediately forwards a packet after reading the destination address. Because fast-forward switching starts forwarding before the entire packet has been received, there may be times when packets are relayed with errors. This occurs infrequently, and the destination NIC discards the faulty packet upon receipt. In fast-forward mode, latency is measured from the first bit received to the first bit transmitted. Fast-forward switching is the typical cut-through method of switching.
- **Fragment-free switching -** In fragment-free switching, the switch stores the first 64 bytes of the frame before forwarding. Fragment-free switching can be viewed as a compromise between store-and-forward switching and fast-forward switching. The reason fragment-free switching stores only the first 64 bytes of the frame is that most network errors and collisions occur during the first 64 bytes. Fragment-free switching tries to enhance fast-forward switching by performing a small error check on the first 64 bytes of the frame to ensure that a collision has not occurred before forwarding the frame. Fragment-free switching is a compromise between the high latency and high integrity of store-and-forward switching, and the low latency and reduced integrity of fast-forward switching.



Port-based memory	● Frames are stored in queues that are linked to specific incoming and outgoing ports. ● A frame is transmitted to the outgoing port only when all the frames ahead in the queue have been successfully transmitted. ● It is possible for a single frame to delay the transmission of all the frames in memory because of a busy destination port. ● This delay occurs even if the other frames could be transmitted to open destination ports.
Shared memory	● Deposits all frames into a common memory buffer shared by all switch ports and the amount of buffer memory required by a port is dynamically allocated. ● The frames in the buffer are dynamically linked to the destination port enabling a packet to be received on one port and then transmitted on another port, without moving it to a different queue.



Two of the most basic settings on a switch are the bandwidth (sometimes referred to as “speed”) and duplex settings for each individual switch port. It is critical that the duplex and bandwidth settings match between the switch port and the connected devices, such as a computer or another switch.

There are two types of duplex settings used for communications on an Ethernet network:

- **Full-duplex** - Both ends of the connection can send and receive simultaneously.
- **Half-duplex** - Only one end of the connection can send at a time.

Autonegotiation is an optional function found on most Ethernet switches and NICs. It enables two devices to automatically negotiate the best speed and duplex capabilities. Full-duplex is chosen if both devices have the capability along with their highest common bandwidth.

Duplex and Speed Settings

Two of the most basic settings on a switch are the bandwidth ("speed") and duplex settings for each individual switch port. It is critical that the duplex and bandwidth settings match between the switch port and the connected devices.

There are two types of duplex settings used for communications on an Ethernet network:

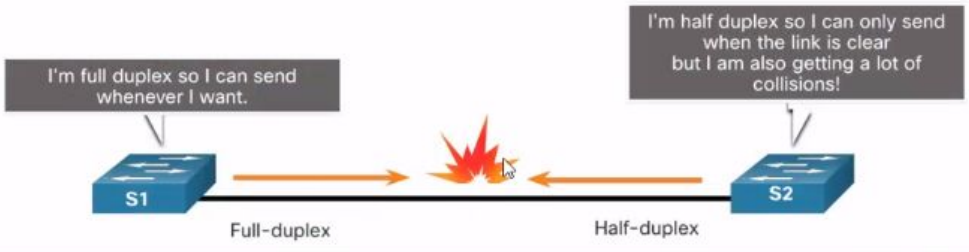
- **Full-duplex** - Both ends of the connection can send and receive simultaneously.
- **Half-duplex** - Only one end of the connection can send at a time.

Autonegotiation is an optional function found on most Ethernet switches and NICs. It enables two devices to automatically negotiate the best speed and duplex capabilities.

Note: Gigabit Ethernet ports only operate in full-duplex.

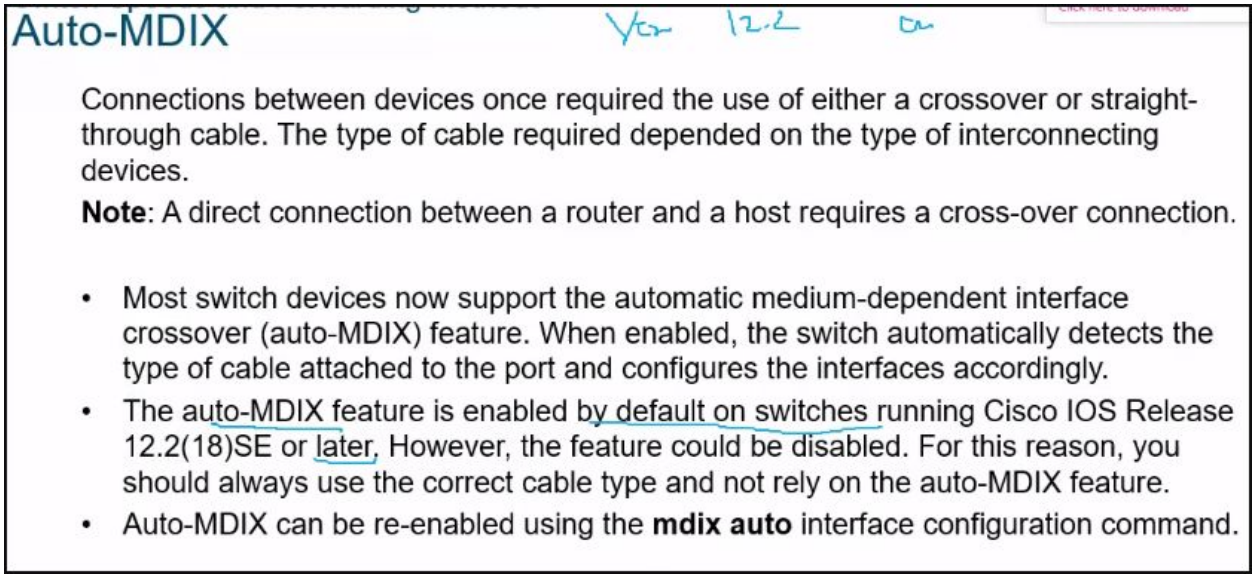
Duplex and Speed Settings

- Duplex mismatch is one of the most common causes of performance issues on 10/100 Mbps Ethernet links. It occurs when one port on the link operates at half-duplex while the other port operates at full-duplex.
- This can occur when one or both ports on a link are reset, and the autonegotiation process does not result in both link partners having the same configuration.
- It also can occur when users reconfigure one side of a link and forget to reconfigure the other. Both sides of a link should have autonegotiation on, or both sides should have it off. Best practice is to configure both Ethernet switch ports as full-duplex.



Most switch devices now support the automatic medium-dependent interface crossover (auto-MDIX) feature. When enabled, the switch automatically detects the type of cable attached to the port and configures the interfaces accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a copper 10/100/1000 port on the switch, regardless of the type of device on the other end of the connection.

The auto-MDIX feature is enabled by default on switches running Cisco IOS Release 12.2(18)SE or later. However, the feature could be disabled. For this reason, you should always use the correct cable type and not rely on the auto-MDIX feature. Auto-MDIX can be re-enabled using the **mdix auto** interface configuration command.

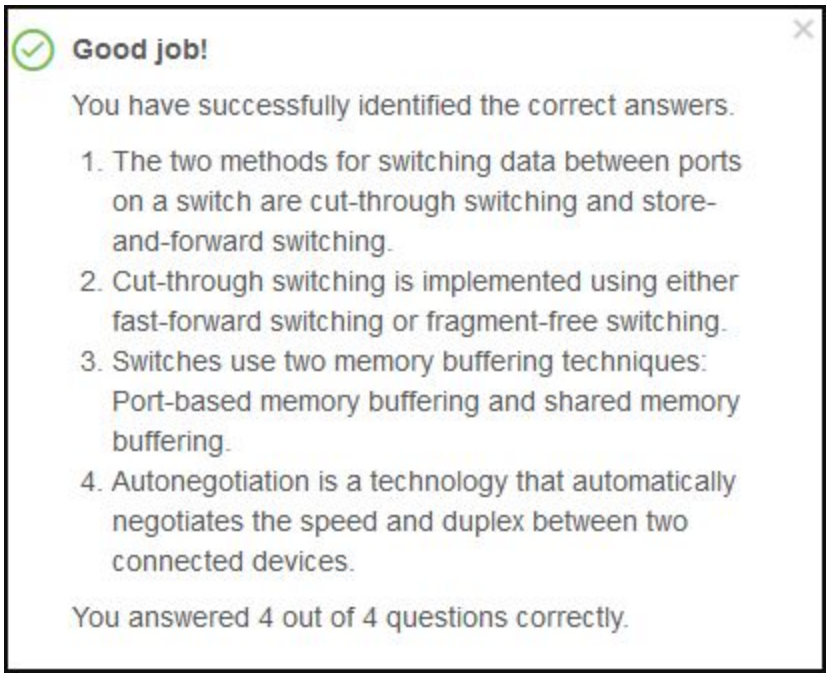


Auto-MDIX

Connections between devices once required the use of either a crossover or straight-through cable. The type of cable required depended on the type of interconnecting devices.

Note: A direct connection between a router and a host requires a cross-over connection.

- Most switch devices now support the automatic medium-dependent interface crossover (auto-MDIX) feature. When enabled, the switch automatically detects the type of cable attached to the port and configures the interfaces accordingly.
- The auto-MDIX feature is enabled by default on switches running Cisco IOS Release 12.2(18)SE or later, However, the feature could be disabled. For this reason, you should always use the correct cable type and not rely on the auto-MDIX feature.
- Auto-MDIX can be re-enabled using the **mdix auto** interface configuration command.



Good job!

You have successfully identified the correct answers.

1. The two methods for switching data between ports on a switch are cut-through switching and store-and-forward switching.
2. Cut-through switching is implemented using either fast-forward switching or fragment-free switching.
3. Switches use two memory buffering techniques: Port-based memory buffering and shared memory buffering.
4. Autonegotiation is a technology that automatically negotiates the speed and duplex between two connected devices.

You answered 4 out of 4 questions correctly.

What did I learn in this module?

Ethernet Frame

Ethernet operates in the data link layer and the physical layer. Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies. Ethernet uses the LLC and MAC sublayers of the data link layer to operate. Data encapsulation includes the following: Ethernet frame, Ethernet addressing, and Ethernet error detection. Ethernet LANs use switches that operate in full-duplex. The Ethernet frame fields are: preamble and start frame delimiter, destination MAC address, source MAC address, EtherType, data, and FCS.

Ethernet MAC Address

Binary number system uses the digits 0 and 1. Decimal uses 0 through 9. Hexadecimal uses 0 through 9 and the letters A through F. The MAC address is used to identify the physical source and destination devices (NICs) on the local network segment. MAC addressing provides a method for device identification at the data link layer of the OSI model. An Ethernet MAC address is a 48-bit address expressed using 12 hexadecimal digits, or 6 bytes. An Ethernet MAC address consists of a 6 hexadecimal vendor OUI code followed by a 6 hexadecimal vendor assigned value. When a device is forwarding a message to an Ethernet network, the Ethernet header includes the source and destination MAC addresses. In Ethernet, different MAC addresses are used for Layer 2 unicast, broadcast, and multicast communications.

The MAC Address Table

A Layer 2 Ethernet switch makes its forwarding decisions based solely on the Layer 2 Ethernet MAC addresses. The switch dynamically builds the MAC address table by examining the source MAC address of the frames received on a port. The switch forwards frames by searching for a match between the destination MAC address in the frame and an entry in the MAC address table. As a switch receives frames from different devices, it is able to populate its MAC address table by examining the source MAC address of every frame. When the MAC address table of the switch contains the destination MAC address, it is able to filter the frame and forward out a single port.

Switch Speeds and Forwarding Methods

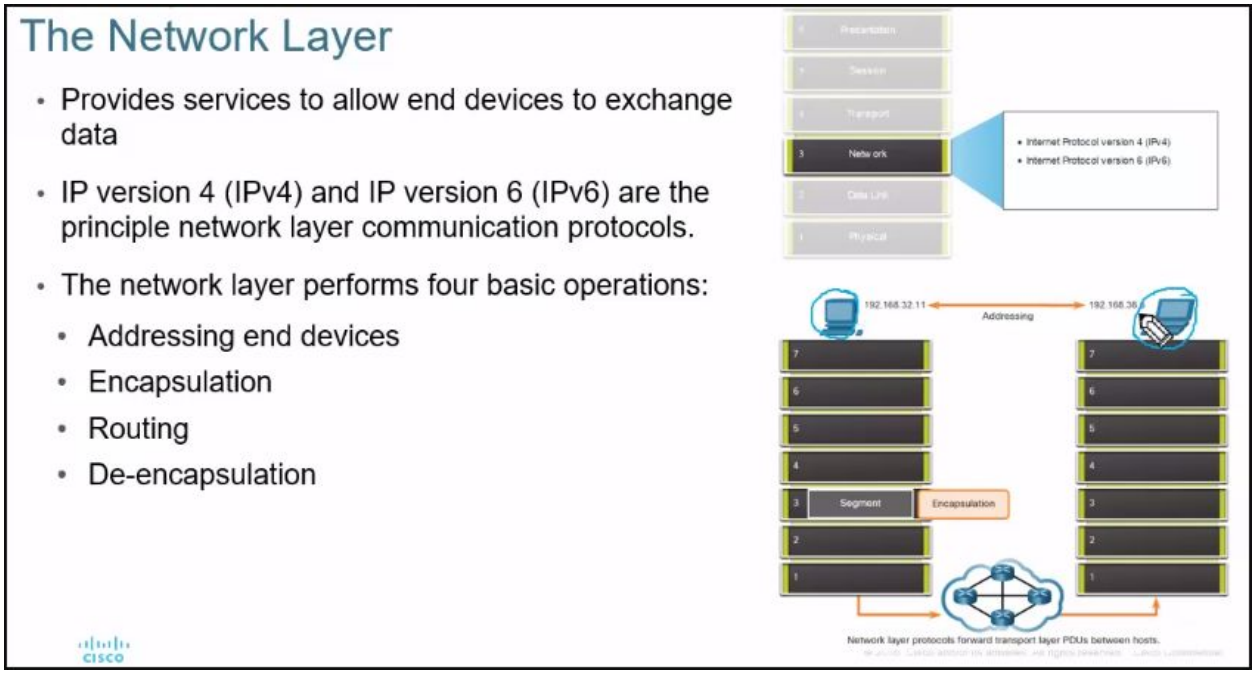
Switches use one of the following forwarding methods for switching data between network ports: store-and-forward switching or cut-through switching. Two variants of cut-through switching are fast-forward and fragment-free. Two methods of memory buffering are port-based memory and shared memory. There are two types of duplex settings used for communications on an Ethernet network: full-duplex and half-duplex. Autonegotiation is an optional function found on most Ethernet switches and NICs. It enables two devices to automatically negotiate the best speed and duplex capabilities. Full-duplex is chosen if both devices have the capability along with their highest common bandwidth. Most switch devices now support the automatic medium-dependent interface crossover (auto-MDIX) feature. When enabled, the switch automatically detects the type of cable attached to the port and configures the interfaces accordingly.

What did I learn in this module?

- Ethernet operates in the data link layer and the physical layer. Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies.
- Ethernet uses the LLC and MAC sublayers of the data link layer to operate.
- The Ethernet frame fields are: preamble and start frame delimiter, destination MAC address, source MAC address, EtherType, data, and FCS.
- MAC addressing provides a method for device identification at the data link layer of the OSI model.
- An Ethernet MAC address is a 48-bit address expressed using 12 hexadecimal digits, or 6 bytes.
- When a device is forwarding a message to an Ethernet network, the Ethernet header includes the source and destination MAC addresses. In Ethernet, different MAC addresses are used for Layer 2 unicast, broadcast, and multicast communications.

CHAPTER 8

Other network layer protocols include routing protocols such as Open Shortest Path First (OSPF) and messaging protocols such as Internet Control Message Protocol (ICMP).



To accomplish end-to-end communications across network boundaries, network layer protocols perform four basic operations:

- **Addressing end devices** - End devices must be configured with a unique IP address for identification on the network.

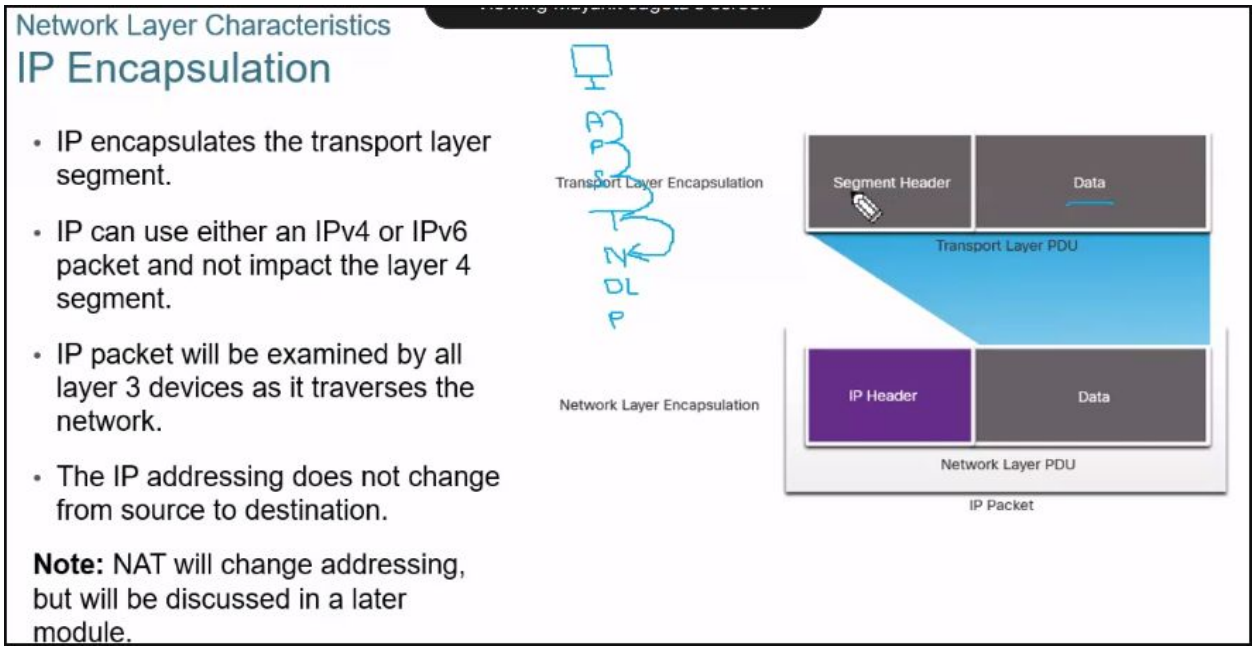
- **Encapsulation -** The network layer encapsulates the protocol data unit (PDU) from the transport layer into a packet. The encapsulation process adds IP header information, such as the IP address of the source (sending) and destination (receiving) hosts. The encapsulation process is performed by the source of the IP packet.
- **Routing -** The network layer provides services to direct the packets to a destination host on another network. To travel to other networks, the packet must be processed by a router. The role of the router is to select the best path and direct packets toward the destination host in a process known as routing. A packet may cross many routers before reaching the destination host. Each router a packet crosses to reach the destination host is called a hop.
- **De-encapsulation -** When the packet arrives at the network layer of the destination host, the host checks the IP header of the packet. If the destination IP address within the header matches its own IP address, the IP header is removed from the packet. After the packet is de-encapsulated by the network layer, the resulting Layer 4 PDU is passed up to the appropriate service at the transport layer. The de-encapsulation process is performed by the destination host of the IP packet.

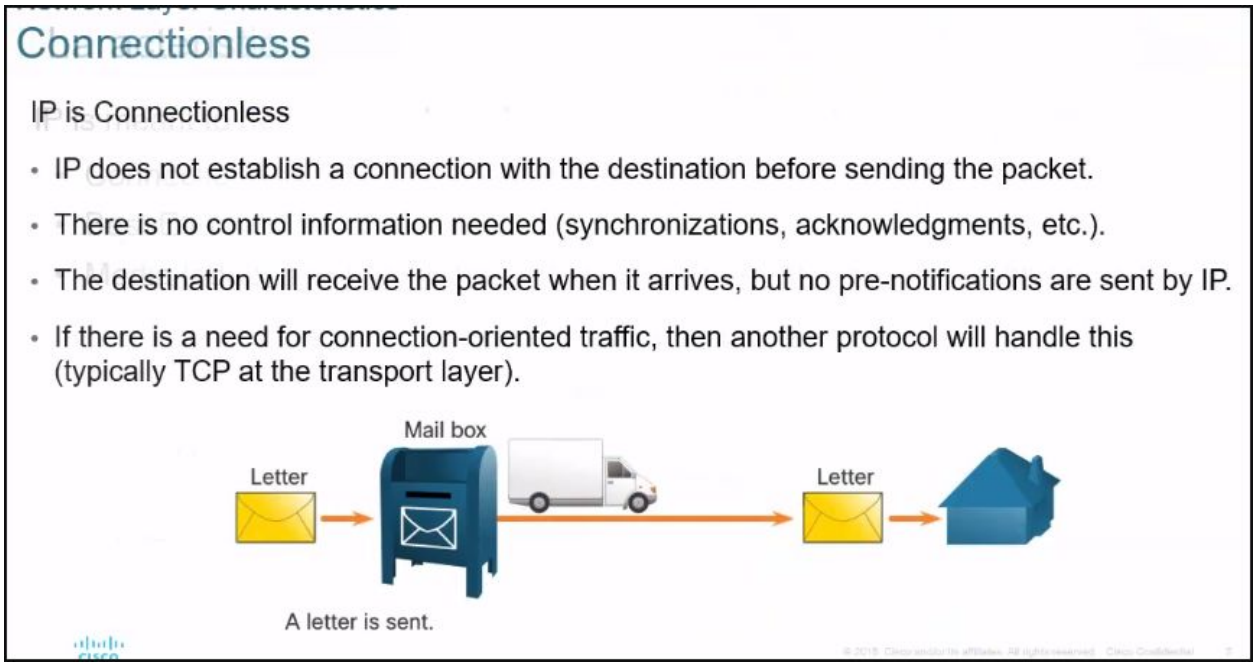
Unlike the transport layer (OSI Layer 4), which manages the data transport between the processes running on each host, network layer communication protocols (i.e., IPv4 and IPv6) specify the packet structure and processing used to carry the data from one host to another host. Operating without regard to the data carried in each packet allows the network layer to carry packets for multiple types of communications between multiple hosts.

These are the basic characteristics of IP:

- **Connectionless** - There is no connection with the destination established before sending data packets.
- **Best Effort** - IP is inherently unreliable because packet delivery is not guaranteed.
- **Media Independent** - Operation is independent of the medium (i.e., copper, fiber-optic, or wireless) carrying the data.

In the TCP/IP protocol suite, reliability is the role of the TCP protocol at the transport layer.





one major characteristic of the media that the network layer considers: the maximum size of the PDU that each medium can transport. This characteristic is referred to as the maximum transmission unit (MTU). Part of the control communication between the data link layer and the network layer is the establishment of a maximum size for the packet. The data link layer passes the MTU value up to the network layer. The network layer then determines how large packets can be.

In some cases, an intermediate device, usually a router, must split up an IPv4 packet when forwarding it from one medium to another medium with a smaller MTU. This process is called

fragmenting the packet, or fragmentation. Fragmentation causes latency. IPv6 packets cannot be fragmented by the router.

You have successfully identified the correct answers.

1. **Transport layer** PDUs, called segments, are encapsulated at the network layer by IPv4 and IPv6 into packets.
2. The **data link layer** receives IP packets from the network layer and encapsulates them for transmission over the medium.
3. **Fragmentation** is the process of splitting up IP packets to travel over a medium with a smaller MTU.
4. **Best effort** delivery does not guarantee packets will be delivered to the destination.

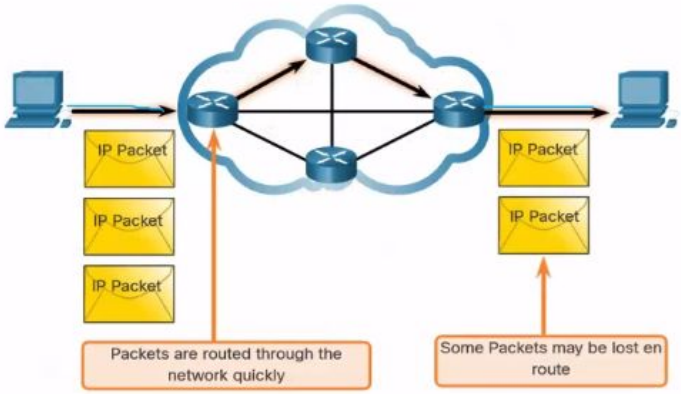
You answered 4 out of 4 questions correctly.

Network Layer Characteristics

Best Effort

IP is Best Effort

- IP will not guarantee delivery of the packet.
- IP has reduced overhead since there is no mechanism to resend data that is not received.
- IP does not expect acknowledgments.
- IP does not know if the other device is operational or if it received the packet.



Good job!

You have successfully identified the correct answers.

1. The IP header fields that identify where the packet originated and where it is going are **Source IP Address** and **Destination IP Address**.
2. **The source and destination IP addresses in the IP packet do not change** in route from source to destination.
3. The **Header Checksum** field in an IPv4 header is used to detect corrupt packets.
4. The **protocol** field identifies the upper layer protocol that is carried inside the IP packet. Common protocols are TCP, UDP, and ICMP.

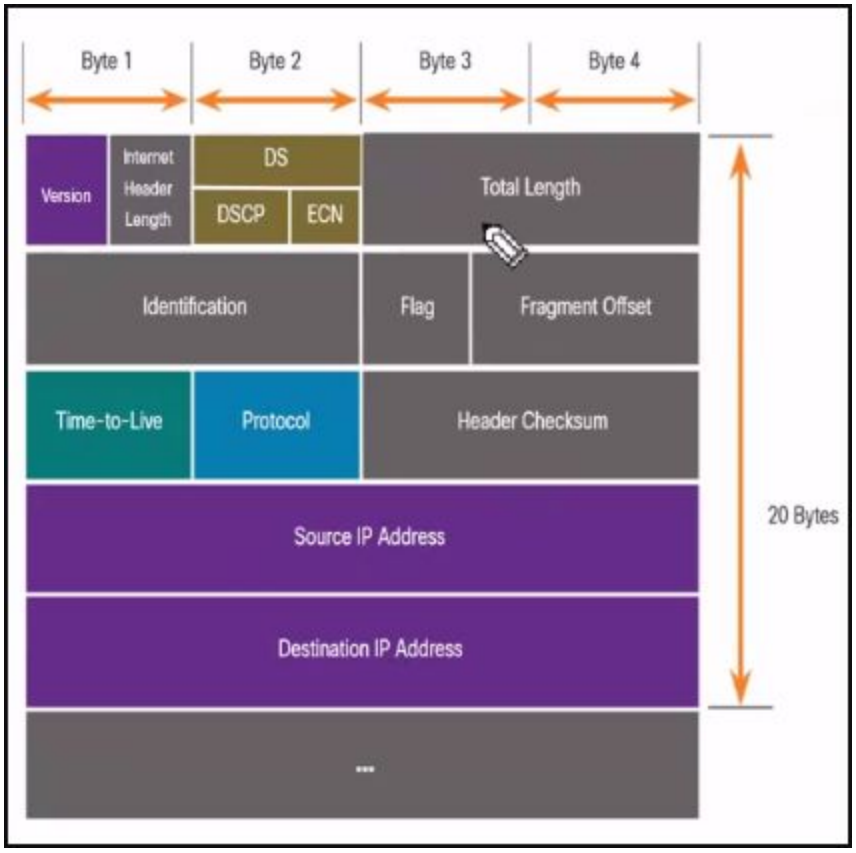
You answered 4 out of 4 questions correctly.

IPv4 Packet Header Fields

The IPv4 network header characteristics:

- It is in binary.
- Contains several fields of information
- Diagram is read from left to right, 4 bytes per line
- The two most important fields are the source and destination.

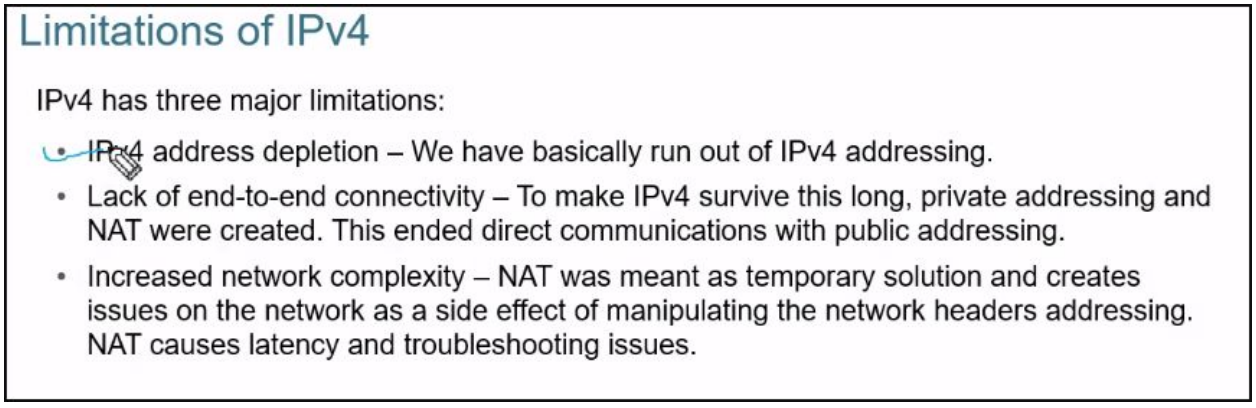
Protocols may have may have one or more functions.



IPv4 Packet Header Fields

Significant fields in the IPv4 header:

Function	Description
Version	This will be for v4, as opposed to v6, a 4 bit field= 0100
Differentiated Services	Used for QoS: DiffServ – DS field or the older IntServ – ToS or Type of Service
Header Checksum	Detect corruption in the IPv4 header
Time to Live (TTL)	Layer 3 hop count. When it becomes zero the router will discard the packet.
Protocol	I.D.s next level protocol: ICMP, TCP, UDP, etc.
Source IPv4 Address	32 bit source address
Destination IPV4 Address	32 bit destination address



IPv4 still has three major issues:

- **IPv4 address depletion -** IPv4 has a limited number of unique public addresses available. Although there are approximately 4 billion IPv4 addresses, the increasing number of new IP-enabled devices, always-on connections, and the potential growth of less-developed regions have increased the need for more addresses.
- **Lack of end-to-end connectivity -** Network Address Translation (NAT) is a technology commonly implemented within IPv4 networks. NAT provides a way for multiple devices to share a single public IPv4 address. However, because the public IPv4 address is shared, the IPv4 address of an internal network host is hidden. This can be problematic for technologies that require end-to-end connectivity.
- **Increased network complexity** – While NAT has extended the lifespan of IPv4 it was only meant as a transition mechanism to IPv6. NAT in its various implementation creates additional complexity in the network, creating latency and making troubleshooting more difficult.

Improvements that IPv6 provides include the following:

- **Increased address space** - IPv6 addresses are based on 128-bit hierarchical addressing as opposed to IPv4 with 32 bits.
- **Improved packet handling** - The IPv6 header has been simplified with fewer fields.
- **Eliminates the need for NAT** - With such a large number of public IPv6 addresses, NAT between a private IPv4 address and a public IPv4 is not needed. This avoids some of the NAT-induced problems experienced by applications that require end-to-end connectivity.

The 32-bit IPv4 address space provides approximately 4,294,967,296 unique addresses. IPv6 address space provides 340,282,366,920,938,463,463,374,607,431,768,211,456, or 340 undecillion addresses. This is roughly equivalent to every grain of sand on Earth.

An IPv6 packet may also contain extension headers (EH), which provide optional network layer information. Extension headers are optional and are placed between the IPv6 header and the payload. EHs are used for fragmentation, security, to support mobility and more.

Unlike IPv4, routers do not fragment routed IPv6 packets.

Click here to download

IPv6 Overview

- IPv6 was developed by Internet Engineering Task Force (IETF).
- IPv6 overcomes the limitations of IPv4.
- Improvements that IPv6 provides:
  - **Increased address space** – based on 128 bit address, not 32 bits
  - **Improved packet handling** – simplified header with fewer fields
  - **Eliminates the need for NAT** – since there is a huge amount of addressing, there is no need to use private addressing internally and be mapped to a shared public address

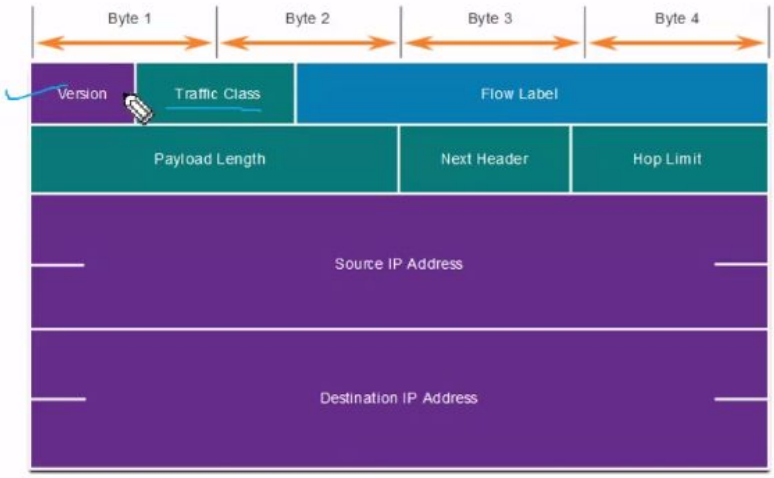
IPv4 and IPv6 Address Space Comparison

Number Name	Scientific Notation	Number of Zeros
1 Thousand	10^3	1,000
1 Million	10^6	1,000,000
1 Billion	10^9	1,000,000,000
1 Trillion	10^12	1,000,000,000,000
1 Quadrillion	10^15	1,000,000,000,000,000
1 Quintillion	10^18	1,000,000,000,000,000,000
1 Sextillion	10^21	1,000,000,000,000,000,000,000
1 Septillion	10^24	1,000,000,000,000,000,000,000,000
1 Octillion	10^27	1,000,000,000,000,000,000,000,000,000
1 Nonillion	10^30	1,000,000,000,000,000,000,000,000,000,000
1 Decillion	10^33	1,000,000,000,000,000,000,000,000,000,000,000
1 Undecillion	10^36	1,000,000,000,000,000,000,000,000,000,000,000,000

Legend
There are 4 billion IPv4 addresses
There are 340 undecillion IPv6 addresses

IPv4 Packet Header Fields in the IPv6 Packet Header

- The IPv6 header is simplified, but not smaller.
- The header is fixed at 40 Bytes or octets long.
- Several IPv4 fields were removed to improve performance.
- Some IPv4 fields were removed to improve performance:
  - Flag
  - Fragment Offset
  - Header Checksum



IPv6 Packet Header

Significant fields in the IPv6 header:

Function	Description
Version	This will be for v6, as opposed to v4, a 4 bit field= 0110
Traffic Class	Used for QoS: Equivalent to DiffServ – DS field
Flow Label	Informs device to handle identical flow labels the same way, 20 bit field
Payload Length	This 16-bit field indicates the length of the data portion or payload of the IPv6 packet
Next Header	I.D.s next level protocol: ICMP, TCP, UDP, etc.
Hop Limit	Replaces TTL field Layer 3 hop count
Source IPv4 Address	128 bit source address
Destination IPV4 Address	128 bit destination address

cisco

You have successfully identified the correct answers.

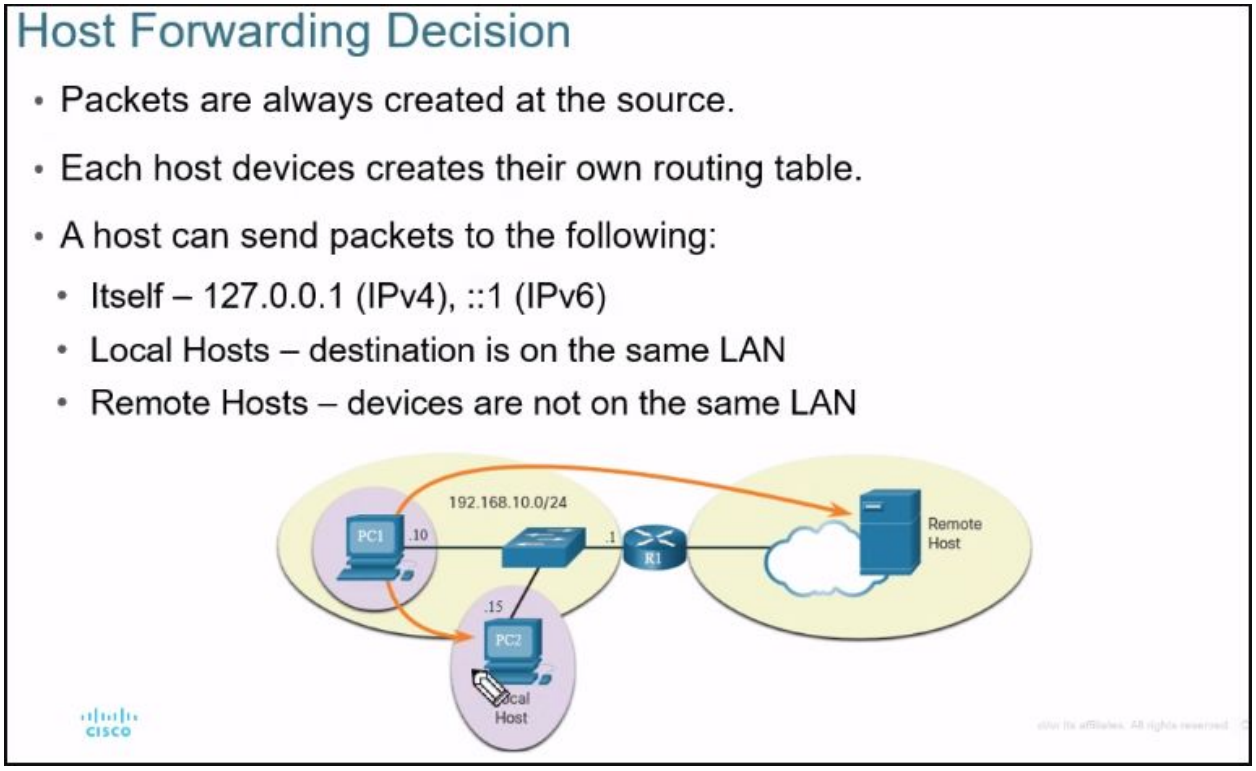
1. IPv4 was standardized in the 1980s and has several technological limitations, such as lack of end-to-end connectivity and a depleted address space.
2. There are several technical improvements made to IPv6, two of which are a vastly larger IP address pool and a simplified protocol header.
3. The IPv6 header is a fixed length of 40 octets and contains 8 header fields.
4. Several fields in the IPv6 header replaced fields in the IPv4 header. For example, the Hop Limit field replaced the IPv4 header Time to Live field.

You answered 4 out of 4 questions correctly.

Another role of the network layer is to direct packets between hosts. A host can send a packet to the following:

- **Itself** - A host can ping itself by sending a packet to a special IPv4 address of 127.0.0.1 or an IPv6 address ::1, which is referred to as the loopback interface. Pinging the loopback interface tests the TCP/IP protocol stack on the host.
- **Local host** - This is a destination host that is on the same local network as the sending host. The source and destination hosts share the same network address.
- **Remote host** - This is a destination host on a remote network. The source and destination hosts do not share the same network address.

The router connected to the local network segment is referred to as the default gateway.
A host routing table will typically include a default gateway. In IPv4, the host receives the IPv4 address of the default gateway either dynamically from Dynamic Host Configuration Protocol (DHCP) or configured manually. In IPv6, the router advertises the default gateway address or the host can be configured manually.
On a Windows host, the **route print** or **netstat -r** command can be used to display the host routing table

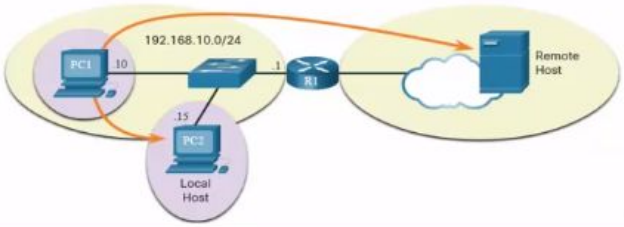


Entering the **netstat -r** command or the equivalent **route print** command displays three sections related to the current TCP/IP network connections:

- **Interface List -** Lists the Media Access Control (MAC) address and assigned interface number of every network-capable interface on the host, including Ethernet, Wi-Fi, and Bluetooth adapters.
- **IPv4 Route Table -** Lists all known IPv4 routes, including direct connections, local network, and local default routes.
- **IPv6 Route Table -** Lists all known IPv6 routes, including direct connections, local network, and local default routes.

Host Forwarding Decision (Cont.)

- The Source device determines whether the destination is local or remote
- Method of determination:
  - IPv4 – Source uses its own IP address and Subnet mask, along with the destination IP address
  - IPv6 – Source uses the network address and prefix advertised by the local router
- Local traffic is dumped out the host interface to be handled by an intermediary device.
- Remote traffic is forwarded directly to the default gateway on the LAN.



Default Gateway

A router or layer 3 switch can be a default-gateway.

Features of a default gateway (DGW):

- It must have an IP address in the same range as the rest of the LAN.
- It can accept data from the LAN and is capable of forwarding traffic off of the LAN.
- It can route to other networks.

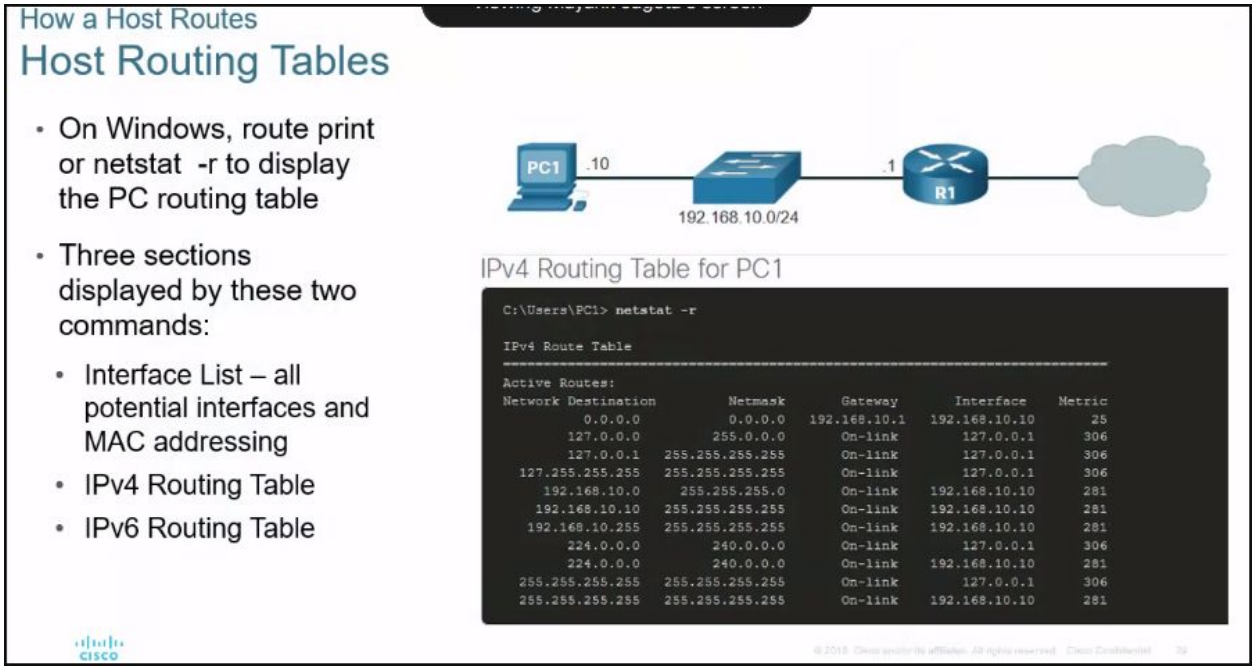
If a device has no default gateway or a bad default gateway, its traffic will not be able to leave the LAN.

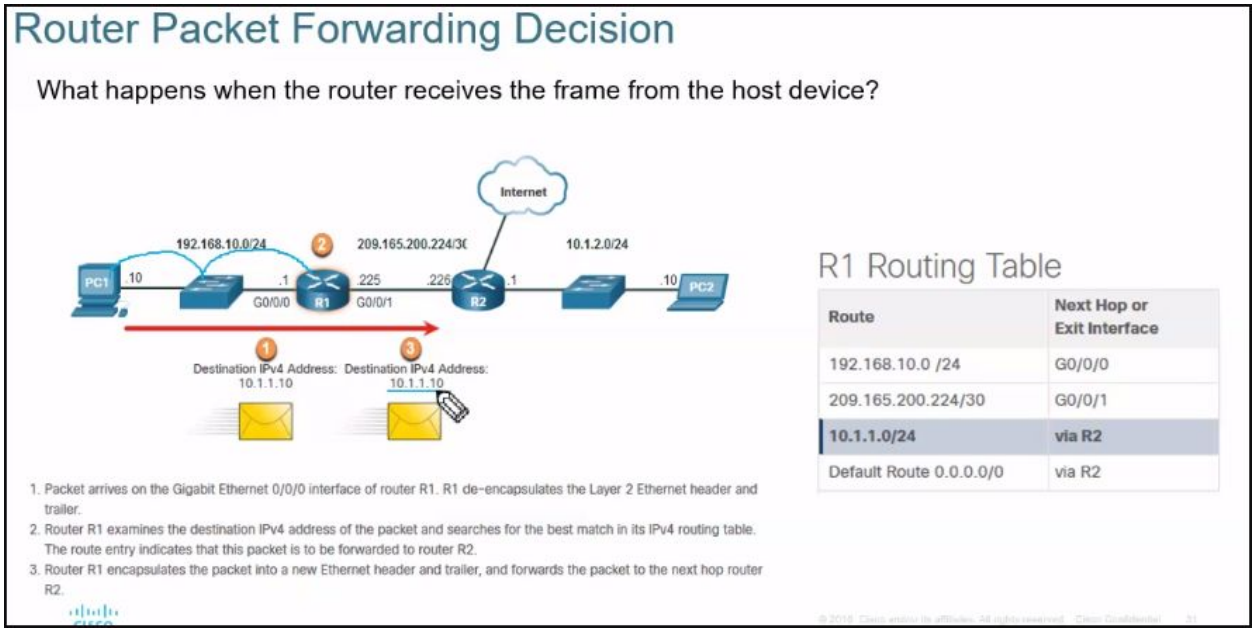
Good job!

You have successfully identified the correct answers.

1. A router is not needed to forward packets between local hosts on the network.
2. The default gateway is the IP address of a router on the local network.
3. The commands **netstat -r** and **route print** will display the routing table of a Windows host.

You answered 3 out of 3 questions correctly.





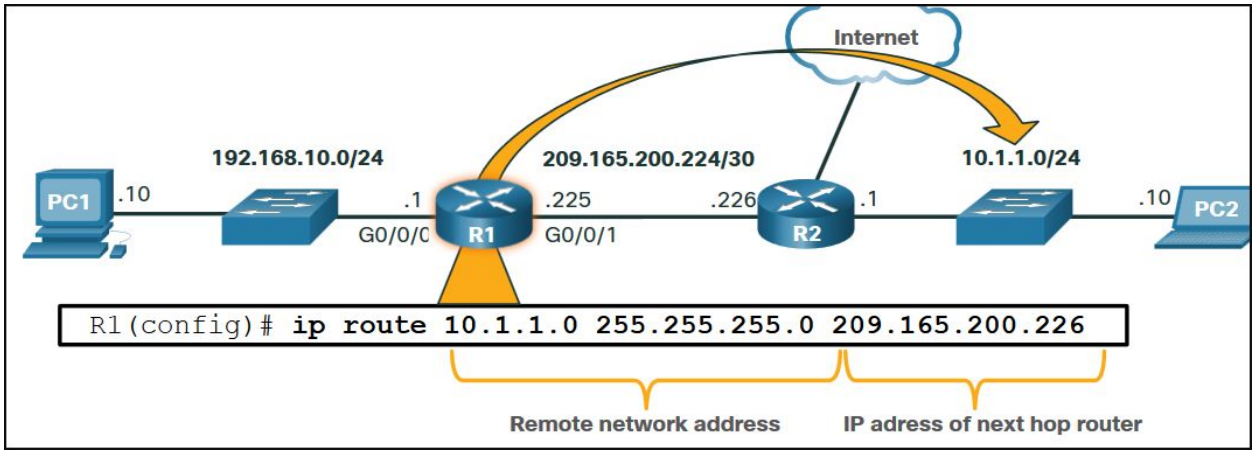
The routing table stores three types of route entries:

Directly-connected networks - These network route entries are active router interfaces. Routers add a directly connected route when an interface is configured with an IP address and is activated

Remote networks - These network route entries are connected to other routers. Routers learn about remote networks either by being explicitly configured by an administrator or by exchanging route information using a dynamic routing protocol

Default route – Like a host, most routers also include a default route entry, a gateway of last resort. The default route is used when there is no better (longer) match in the IP routing table

Static routes are route entries that are manually configured



Static routing has the following characteristics:

- A static route must be configured manually.
- The administrator needs to reconfigure a static route if there is a change in the topology and the static route is no longer viable.
- A static route is appropriate for a small network and when there are few or no redundant links.
- A static route is commonly used with a dynamic routing protocol for configuring a default route.

Routers that use dynamic routing protocols automatically share routing information with other routers and compensate for any topology changes without involving the network administrator. If there is a change in the network topology, routers share this information using the dynamic routing protocol and automatically update their routing tables.Dynamic routing protocols include OSPF and Enhanced Interior Gateway Routing Protocol (EIGRP)

The dynamic routing protocol will automatically do as follows:

- Discover remote networks
- Maintain up-to-date routing information
- Choose the best path to destination networks
- Attempt to find a new best path if the current path is no longer available

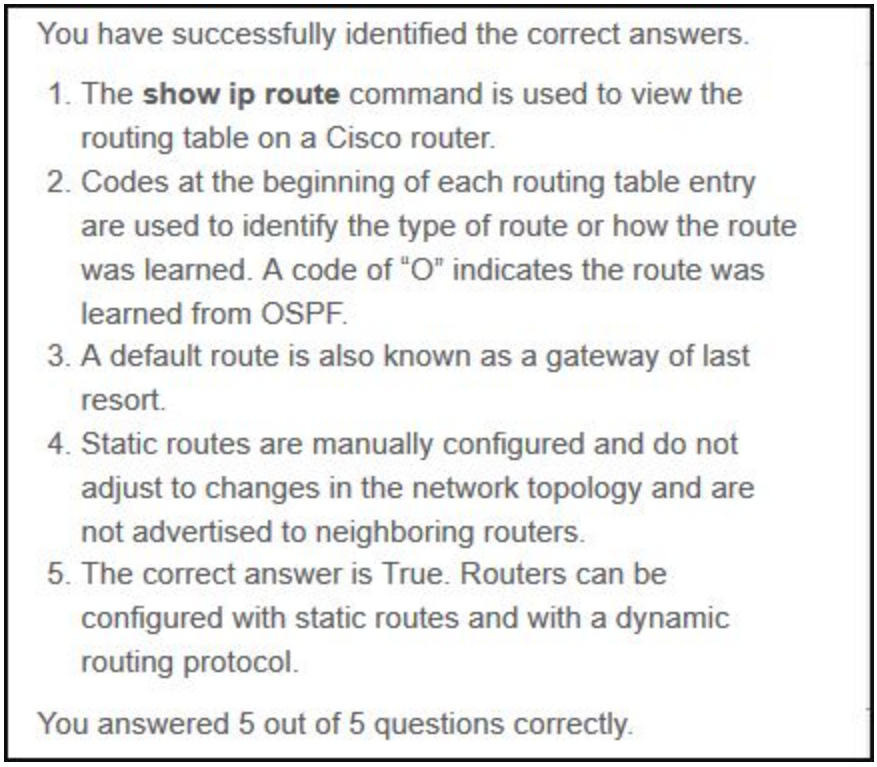
The **show ip route** privileged EXEC mode command is used to view the IPv4 routing table on a Cisco IOS router.
At the beginning of each routing table entry is a code that is used to identify the type of route or how the route was learned. Common route sources (codes) include these:

- **L** - Directly connected local interface IP address
- **C** – Directly connected network
- **S** – Static route was manually configured by an administrator

- **O** - OSPF
- **D** - EIGRP

A directly connected route is automatically created when a router interface is configured with IP address information and is activated. The router adds two route entries with the codes **C** (i.e., the connected network) and **L** (i.e., the local interface IP address of the connected network). The route entries also identify the exit interface to use to reach the network.

A default route has a network address of all zeroes. For example, the IPv4 network address is 0.0.0.0. A static route entry in the routing table begins with a code of **S***



What did I learn in this module?

Network Layer Characteristics

The network layer (OSI Layer 3) provides services to allow end devices to exchange data across networks. IPv4 and IPv6 are the principle network layer communication protocols. The network layer also includes the routing protocol OSPF and messaging protocols such as ICMP. Network layer protocols perform four basic operations: addressing end devices, encapsulation, routing, and de-encapsulation. IPv4 and IPv6 specify the packet structure and processing used to carry the data from one host to another host. IP encapsulates the transport layer segment by adding an IP header, which is used to deliver the packet to the destination host. The IP header

is examined by Layer 3 devices (i.e., routers) as it travels across a network to its destination. The characteristics of IP are that it is connectionless, best effort, and media independent. IP is connectionless, meaning that no dedicated end-to-end connection is created by IP before data is sent. The IP protocol does not guarantee that all packets that are delivered are, in fact, received. This is the definition of the unreliable, or best effort characteristic. IP operates independently of the media that carry the data at lower layers of the protocol stack.

IPv4 Packet

An IPv4 packet header consists of fields containing information about the packet. These fields contain binary numbers which are examined by the Layer 3 process. The binary values of each field identify various settings of the IP packet. Significant fields in the IPv4 packet header include: version, DS, header checksum, TTL, protocol, and the source and destination IPv4 addresses.

IPv6 Packet

IPv6 is designed to overcome the limitations of IPv4 including: IPv4 address depletion, lack of end-to-end connectivity, and increased network complexity. IPv6 increases the available address space, improves packet handling, and eliminates the need for NAT. The fields in the IPv6 packet header include: version, traffic class, flow label, payload length, next header, hop limit, and the source and destination IPv6 addresses.

How a Host Routes

A host can send a packet to itself, another local host, and a remote host. In IPv4, the source device uses its own subnet mask along with its own IPv4 address and the destination IPv4 address to determine whether the destination host is on the same network. In IPv6, the local router advertises the local network address (prefix) to all devices on the network, to make this determination. The default gateway is the network device (i.e., router) that can route traffic to other networks. On a network, a default gateway is usually a router that has a local IP address in the same address range as other hosts on the local network, can accept data into the local network and forward data out of the local network, and route traffic to other networks. A host routing table will typically include a default gateway. In IPv4, the host receives the IPv4 address of the default gateway either dynamically via DHCP or it is configured manually. In IPv6, the router advertises the default gateway address, or the host can be configured manually. On a Windows host, the route print or netstat -r command can be used to display the host routing table.

Introduction to Routing

When a host sends a packet to another host, it consults its routing table to determine where to send the packet. If the destination host is on a remote network, the packet is forwarded to the default gateway which is usually the local router. What happens when a packet arrives on a router interface? The router examines the packet’s destination IP address and searches its routing table to determine where to forward the packet. The routing table contains a list of all

known network addresses (prefixes) and where to forward the packet. These entries are known as route entries or routes. The router will forward the packet using the best (longest) matching route entry. The routing table of a router stores three types of route entries: directly connected networks, remote networks, and a default route. Routers learn about remote networks manually, or dynamically using a dynamic routing protocol. Static routes are route entries that are manually configured. Static routes include the remote network address and the IP address of the next hop router. OSPF and EIGRP are two dynamic routing protocols. The show ip route privileged EXEC mode command is used to view the IPv4 routing table on a Cisco IOS router. At the beginning of an IPv4 routing table is a code that is used to identify the type of route or how the route was learned. Common route sources (codes) include:

L - Directly connected local interface IP address

C - Directly connected network

S - Static route was manually configured by an administrator

O - Open Shortest Path First (OSPF)

D - Enhanced Interior Gateway Routing Protocol (EIGRP)