Notes made by

Name: Johan Milter Jakobsen

Profession: Software & Automation Programmer at Novo Nordisk

School: TEC Ballerup - Data and Communication, specializing in Programming

CCNA EXAM NOTES

TABLE OF CONTENTS

KEYWORD DEFINITIONS

DECIMAL BINARY CONVERSION

C# CONVERTER

Johan has provided a file called “Decimal2Binary”. This will let you type the Decimal value, and get a Binary output.

BY HAND

Every time there’s a ‘0’ don’t plus, but every time there’s a ‘1’ plus it. Remember count from the right!!! Like this:

Example: 0 0 1 1 1 0 0 0 => 8+16+32=56

1	256	65536	16777216
2	512	131072	33554432
4	1024	262144	67108864
8	2048	524288	134217728
16	4096	1048576	268435456
32	8192	2097152	536870912
64	16384	4194304	1073741824
128	32768	8388608	2147483648

NETWORK

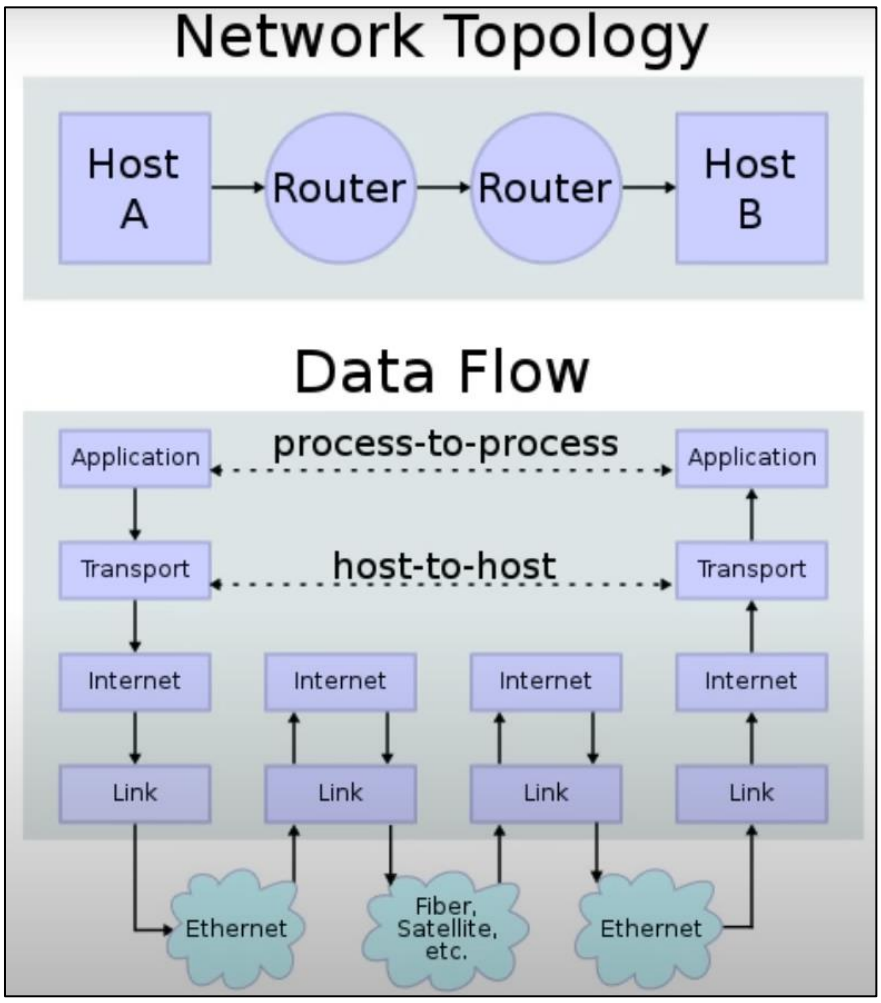
Network:

- Purpose
    - A computer network is a digital telecommunications network which allows nodes to share resources.

Network Models:

- Purpose
    - Networking models categorize and provide a structure for networking protocols and standards.
        - Protocols: A set of rules defining how network devices and software should work.
            - These rules are logical rules, and not physical rules!
- Models

- Example of TCP/IP between 2 PCs with 2 routers between them.



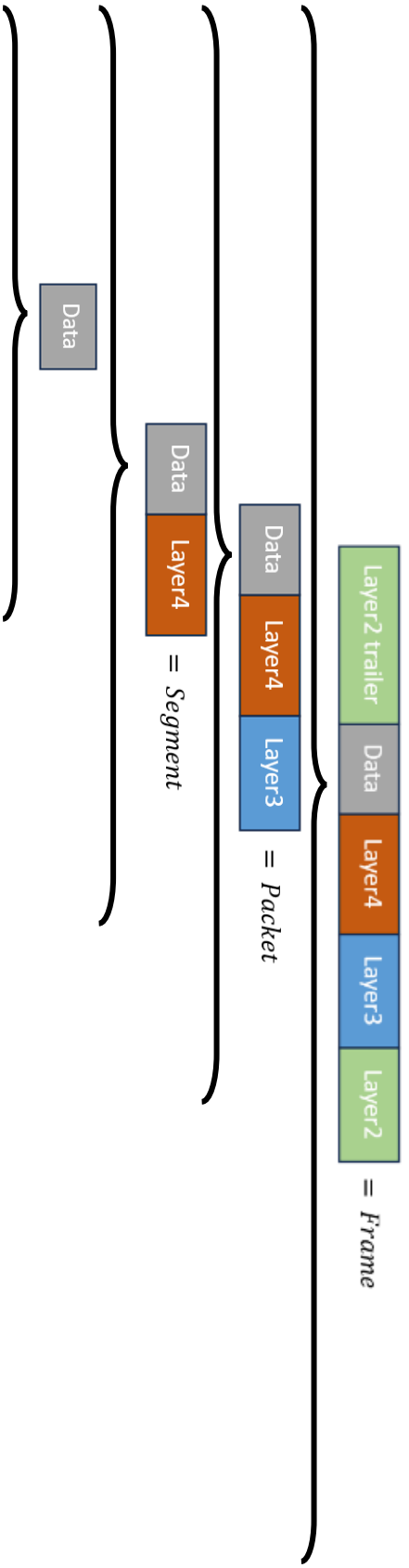
- The OSI Model is not used in modern networks, but it still influences how network engineers think and talk about networks. The TCP/IP is the model being used in modern networks.
  - Though, when network engineers refer to specific layers, they refer to the OSI models layers, not the TCP/IP layers. This is important to know, because the TCP/IP layers and the OSI model layers are not the same, and are called different things, which can lead to misunderstanding between network engineers.
- OSI Model
  - 'OSI' = 'Open Systems Interconnection'
  - Purpose
    - A conceptual model that categorizes and standardizes the different functions in a network.
    - Created by the 'International Organization for Standardization' (ISO).
    - Functions are divided into 7 'Layers'.
    - These layers work together to make the network.
  - Example
    - If 2 computers want to connect to each other, we can represent these 2 computers with OSI models. The first computer needs run through the layers from 7 to 1 each layer giving something to the next layer. When the message comes to the 'Physical' layer of the OSI-model, it has gone through a process called 'Encapsulation'. The message is then sent to the other computer (represented by an OSI-model). The message now needs to go through a process called 'De-encapsulation', which is the opposite process of 'Encapsulation'.
  - The different stages of Encapsulation are called a PDU (Protocol Data Unit). For example, is a 'Segment', 'Packet', 'Frame', etc. a PDU.
  - The Model in layers

7	Application	– *This layer is closest to the end user.*
		– *Interact with software applications, for example your web browser (Brave, Firefox, Chrome, etc.)*
		– *HTTP and HTTPS are layer 7 protocols*
		– *Functions of layer 7 include*
		  i *Identifying communication partners*
		  i *Synchronizing communication*

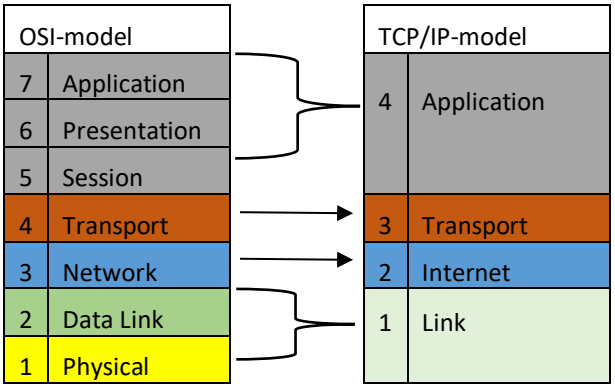
6	Presentation	– *Data in the application layer is in 'Application format'.* – *It needs to be 'translated' to a different format to be sent over the network.* – *The Presentation Layers job is to translate between application and network formats.* – *For example, encryption of data as it is sent, and decryption of data as it is received.* – *Also translates between different Application Layer formats. To make sure the receiving host, understands it.*
5	Session	– *Controls dialogues (sessions) between communicating hosts.* – *Establishes, manages, and terminates connections between the local application (for example, your web browser) and the remote application (for example, YouTube)*
4	Transport	– *Segments and reassembles data for communications between end hosts* – *Breaks large pieces of data into smaller segments which can be more easily sent over the network and are less likely to cause transmission problems if errors occur.* i *For example, if you're watching a video, and the and error occur, you wouldn't be able to watch the video if the data was sent in large pieces. By breaking the data into smaller pieces, you're only going to see a small skip in the video.* – *Provide 'host-to-host' or 'end-to-end' communication.*
3	Network	– *Provides connectivity between end hosts on different networks (Outside of the LAN).* – *Provides logical addressing (IP addresses).* – *Provides path selection between source and destination.* i *It figures out the best possible path* – *Routers operate at Layer 3.*

2	Data Link	– *Provides node-to-node connectivity and data transfer (for example, PC to switch, switch to router, router to router, etc.).*
		– *Defines how data is formatted for transmission over a physical medium (for example, copper UTP cables).*
		– *Detects and (possibly) corrects Physical Layer errors.*
		– *Uses Layer 2 addressing, separate from Layer 3 addressing.*
		– *Switches operate in Layer 2.*
		– *Sublayers*
		  1. *LLC (Logical Link Control)*
		  2. *MAC*
		– *Adds the FCS (Frame Check Sequence) in the trailer.*
		  i *It is 4 bytes (32 bits) in length*
		  i *Detects corrupted data by running a 'CRC' algorithm over the received data.*
		  ▤ *CRC is Cyclic Redundancy Check*

1	Physical	– *Defines physical characteristics of the medium used to transfer data between devices.* – *For example, voltage levels, maximum transmission distances, physical connectors, cable specifications, etc.* – *Digital bits are converted into electrical (for wired connections) or radio (for wireless connections) signals.*



- TCP/IP
  - Characteristics
    - Conceptual model and set of communications protocols used on the internet and other networks.
    - Known as TCP/IP because those are two of the foundational protocols in the suite.
    - Developed by the United States Department of Defense through DARPA (Defense Advanced Research Projects Agency).
    - Similar structure to the OSI-model, but with fewer layers.
    - This is the model in use in modern networks.
  - The TCP/IP-model VS the OSI-model



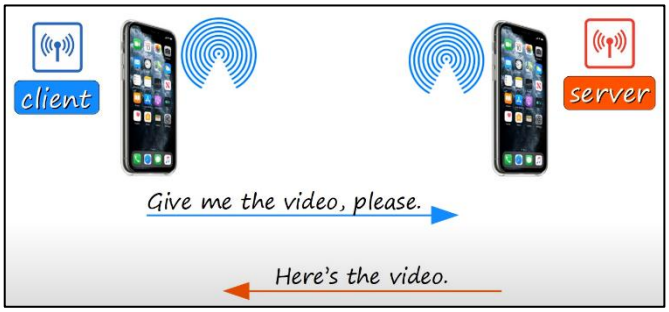
CLIENTS

Clients / End-devices:

- Purpose
  - A client is a device that accesses a service made available by a server.

Bonus facts:

- Clients can also be servers
  - Example
    - I want a video, located on my friend's phone. For me to get that video, my friend's phone needs to act like a server, so the video can be sent to me. My friend's phone therefore provides the service of sending the video to me over the internet. My phone requested the video, and his phone provided it.
  - Visual example



Possible questions and answers:

- **A client packet is received by a server. The packet has a destination port number of 110. What service is the client requesting?**
  - POP3
- **A client packet is received by a server. The packet has a destination port number of 53. What service is the client requesting?**
  - DNS
- **A client packet is received by a server. The packet has a destination port number of 80. What service is the client requesting?**
  - http
- **A client packet is received by a server. The packet has a destination port number of 67. What service is the client requesting?**

    - DHCP
- **A client packet is received by a server. The packet has a destination port number of 69. What service is the client requesting?**
    - TFTP
- **A client packet is received by a server. The packet has a destination port number of 143. What service is the client requesting?**
    - IMAP
- **A client packet is received by a server. The packet has a destination port number of 21. What service is the client requesting?**
    - FTP
- **A client packet is received by a server. The packet has a destination port number of 22. What service is the client requesting?**
    - SSH

SERVERS

Server:

- Purpose
    - A server is a device that provides functions or services for clients.

Bonus facts:

- Even though a client and a server are both end-devices, that does not mean a server is a client. A client is a device that uses the services or functions a server provides. End-devices are the last destination of the LAN.

Possible questions and answers:

- **A company has a file server that shares a folder named Public. The network security policy specifies that the Public folder is assigned Read-Only rights to anyone who can log into the server while the Edit rights are assigned only to the network admin group. Which component is addressed in the AAA network service framework?**
    - Authorization

HACKING

Possible questions and answers:

- **A disgruntled employee is using some free wireless networking tools to determine information about the enterprise wireless networks. This person is planning on using this information to hack the wireless network. What type of attack is this?**
    - Reconnaissance

SWITCHES

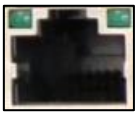
Switch:

- Purpose
    - A switch is used to forward traffic within a LAN (Local Area Network).
    - Characteristics
        - Switches have many network interfaces/ports for end hosts to connect to (usually 24+)
        - Switches provide connectivity to hosts within the same LAN (Local Area Network).
        - Switches do not provide connectivity between LANs/over the internet.
    - Switches can dynamically learn MAC-addresses as they get introduced to the Switch.
        - That MAC address is called dynamic MAC address
        - A switch uses the Source MAC-address field to populate its MAC address table. It associates the source MAC address with the interface on which the frame was received. This allows the switch to learn how to reach other devices on the network.
        - They then add the source MAC-addresses and which port they came from, to the MAC-address table on the switch

- When a Switch learns about MAC-addresses its “Floods” all the hosts connected to its ports. When the hosts get the flooded frames, it will send a frame back to switch, saying what the individual host’s source-address was. The switch then adds the source-address and the port in came in through, to the MAC-address table.
- When the Switch knows about the destination MAC-address, it will forward the frame to the destination. This is known as a “Known Unicast frame”.
- When the Switch doesn’t know about the destination it will flood the LAN and get to the destination and port. When this happens, it will ‘flood’ out all interfaces, except the one it was received on. This is known as an “Unknown Unicast frame”.

Switch Inputs:

- RJ-45 (RJ = Registered Jack)
  - Example
    -
  - Visual example



Bonus facts:

- Switched cannot be used to send packets/frames, directly over the internet. A switch is typically connected to a router, which job is to send these packets/frames over the internet.

ETHERNET STANDARDS/NETWORK PROTOCOLS & UTP & FIBER-OPTIC CABLES

Ethernet:

- Purpose:
  - Ethernet is a collection of network protocols/standards.

Why Network Protocols?

- If 2 people talk to each other, where one speaks English, and the other speaks German. How can they communicate? That’s why we need ‘Standard Network Protocols’, so that we can communicate in a ‘language’, that all understands. This is why standards like ‘Ethernet’ exists.
  - Example
    If you’re trying to connect to a network switch, but the maker of the cable and the maker of the switch, haven’t agreed upon the size and shape of the connector and port, you won’t be able to connect them. This is why ‘Network Protocols’ is so important.

Where and when were the Standards defined?

- Defined in the IEEE 802.3 standard in 1983
- IEEE = Institute of Electrical and Electronics Engineers

UTP vs Fiber-Optic Cabling:

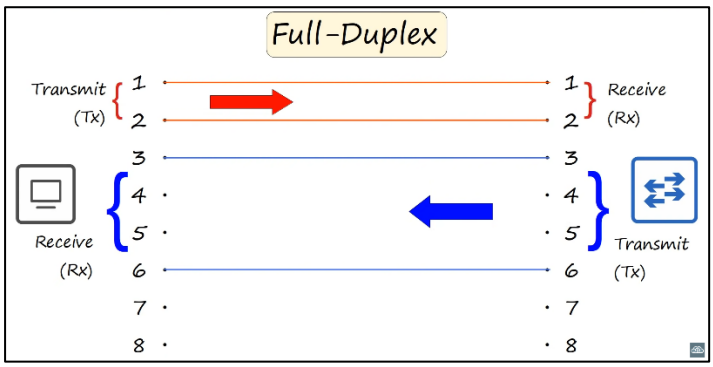
UTP	***Fiber-Optic***
Lower cost than fiber-optic	Higher cost than UTP
Shorter maximum distance than fiber-optic (~100m)	Longer maximum distance than UTP
Can be vulnerable to EMI (Electromagnetic interference)	No vulnerability to EMI
RJ45 ports used with UTP are cheaper than SFP Transceivers	SFP ports are more expensive than RJ45 ports (single-mode is more expensive than multi-mode)
Emit (leak) a faint signal outside of the cable, which can be copied (=security risk)	Does not emit any signal outside the cable (=no security risk)

Ethernet Copper cables - Typically UTP cables:

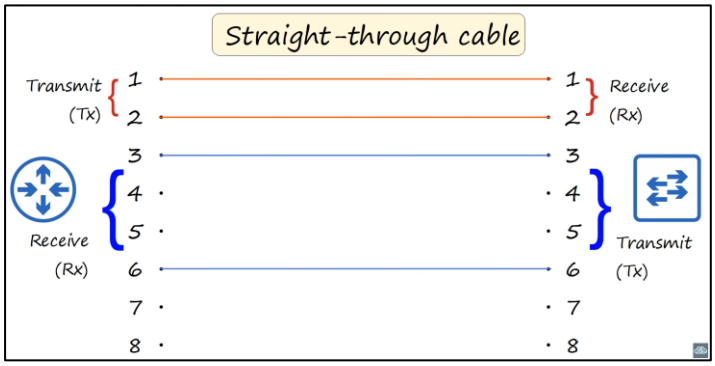
- Values of different copper cables and their standards.

Speed	Common Name	IEEE Standard	Informal Name	Maximum length
10 Mbps	Ethernet	802.3i	10BASE-T	100 m
100 Mbps	Fast Ethernet	802.3u	100BASE-T	100 m
1 Gbps	Gigabit Ethernet	802.3ab	1000BASE-T	100 m
10 Gbps	10 Gig Ethernet	802.3an	10GBASE-T	100 m

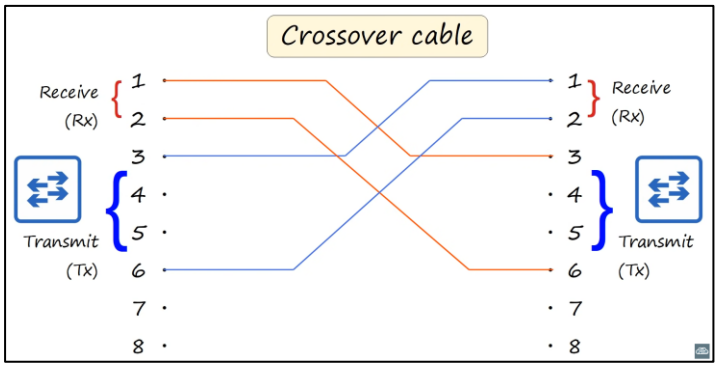
- UTP cables (Unshielded Twisted Pair):
  - Unshielded = No Metallic shield (Vulnerable to electric interference).
  - Twisted = The cables are twisted (Helps protect against electromagnetic interference).
  - Pair = 2.
  - Typically, there is 4 pair, which means $4 \cdot 2 = 8$ cables.
  - 'Auto MDI-X' is a way to automatically change the 'Receive pins' and 'Transmit pins', depending on the which wire the data comes from.
  - Examples of connections with low-speed cables: UTP cables (10BASE-T, 100BASE-T)
    - Connections between devices without 'Auto MDI-X'
      - Connecting a PC to a Switch
        - Full Duplex means that both devices can send and receive data at the same time, because they use separate pins to transmit and receive data.
        - Full Duplex is a bit different from Half Duplex
          - 🕮 In Half Duplex the device cannot send and receive data at the same time. Devices attached to hubs must operate in half duplex. If it's receiving a frame, it must wait before sending a frame.
        - In Full Duplex the device can send and receive data at the same time. It does not have to wait.



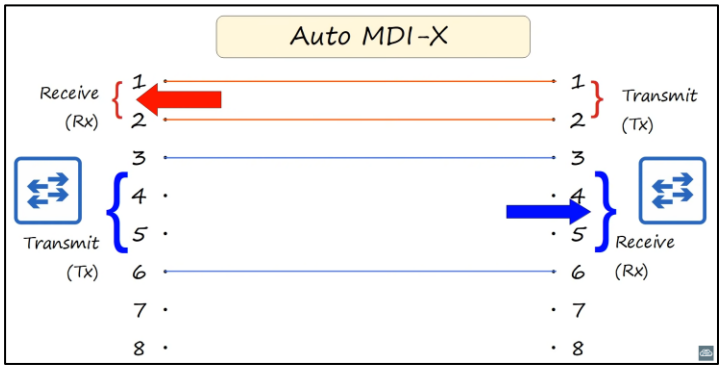
      - Connecting a Router to a Switch
        - Functions the same as connecting a PC to a Switch
        - Straight-though cable means that Pin 1 transmits to Pin 1, Pin 2 transmits to Pin 2, Pin 3 receives from Pin 3, etc.



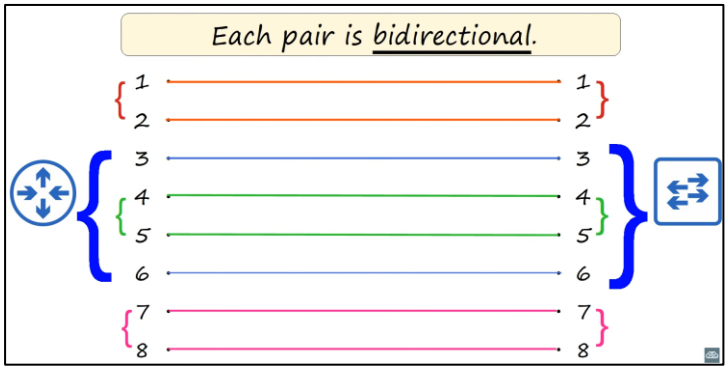
      - Connecting a Router to a Router
        - Crossover cable means that Pin 1 doesn't connect to Pin 1 but connects to Pin 3 and so on, like the picture below.
        - The wires cross over each other, hence the name "Crossover cable"



- Example of connections between devices with 'Auto MDI-X'
  - Connecting a Switch to a Switch
    - As you can see on the picture below, the 'Auto MDI-X' allows the switch to not be dependent on which pins does what. Instead, it just switches the function of the pins to match the way data comes in.
    - Therefor although switches by default receive data on pin 1 and 2, it can change it using 'Auto MDI-X'.



- Example of connections with high-speed cables: UTP cables (1000BASE-T, 10GBASE-T)
  - This is a newer method of connecting devices, which is primarily seen today.
    - Connecting Router to Switch
      - Instead of only using 4 pins in the lower-speed cables, we use all 8 pins, on high-speed cables. This makes it faster.
      - Another thing making it faster is the bidirectional pairs which means each pair isn't dedicated to either receiving or transmitting.



- Table of Devices with their default Transmit pins and Receive pins.

Device Type	*Transmit (Tx) Pins*	*Receive (Rx) Pins*
Router 	1 and 2	3 and 6
Firewall 	1 and 2	3 and 6

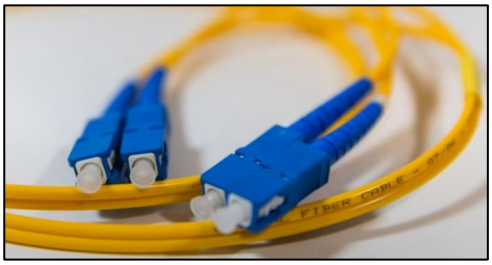
PC 	1 and 2	3 and 6
Switch 	3 and 6	1 and 2

Fiber-Optic Connections:

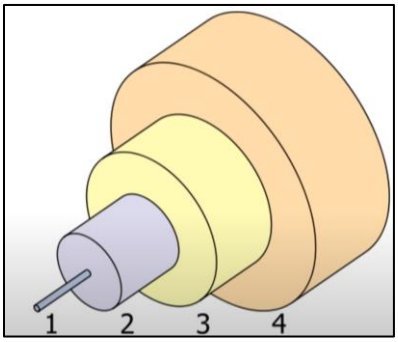
- Values of different copper cables and their standards.

Speed	***Cable Type***	***IEEE Standard***	***Informal Name***	***Maximum length***
1 Gbps	Multi-mode or Single-mode	802.3z	1000BASE-LX	550m (Multi-mode) 5km (Single-mode)
10 Gbps	Multi-mode	802.3ae	10GBASE-SR	400m
10 Gbps	Single-mode	802.3ae	10GBASE-LR	10km
10 Gbps	Single-mode	802.3ae	10GBASE-ER	30km

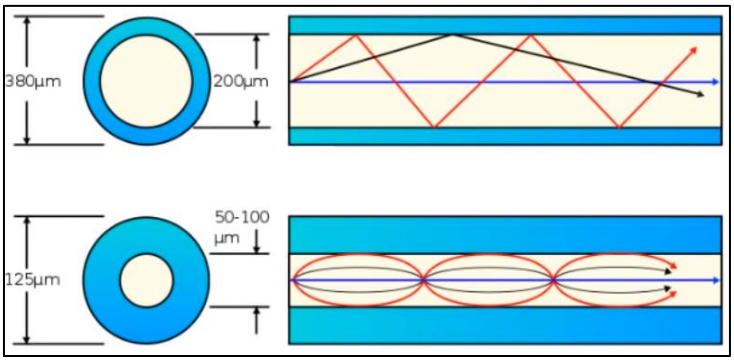
- Fiber-optic cables is fast and can be used for much longer distances than copper cables



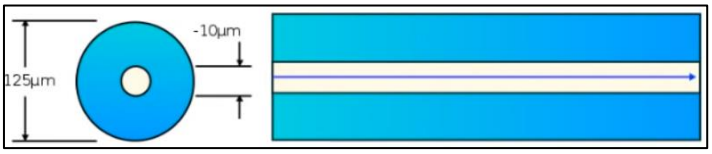
  - This cable has 2 inputs on both sides. One to transmit data and one to receive data.
  - A fiber optic cable therefor uses 2 different cables, where the UTP cables use different pins for transmitting and receive.
  - A fiber optic cable looks like this in layers
    1. The fiberglass core itself
    2. Cladding that reflects light
    3. A protective buffer
    4. The outer jacket of the cable



  - Multi-mode Fiber
    - Core diameter is wider than single-mode fiber.
    - Allows multiple angles (modes) of light waves to enter the fiberglass core.
    - Allows longer cables than UTP, but shorter cables than single-mode fiber.
    - Cheaper than single-mode fiber (due to cheaper LED-based SFP transmitters)



- Single-mode Fiber
  - Core diameter is narrower than multi-mode fiber
  - Light enters at a single angle (mode) from a laser-base transmitter
  - Allows longer cables than both UTP and multi-mode fiber
  - More expensive than multi-mode fiber (due to more expensive laser based SFP transmitters)



- SFP Transceiver (Small Formfactor Pluggable)
  - This is used inside of an ethernet port and can be used to transform light pulses into data.
  - The cables that connect to this Transceiver is a Fiber-Optic cable

Possible questions and answers:

- **A network technician is researching the use of fiber optic cabling in a new technology center. Which two issues should be considered before implementing fiber optic media? (Choose two.)**
  - Fiber optic cabling requires different termination and splicing expertise from what copper cabling requires.
  - Fiber optic provides higher data capacity but is more expensive than copper cabling.

BITS, BYTES & SPEED

Bit:

- A bit is a value represented by either 0 or 1. Therefor 1 bit = '0' or '1'
- This is called 'Binary Code' and is how computers and devices work and operates.
- Use cases
  - Binary Code
  - Speed of cables and devices

Byte:

- A byte is 8 bits. Therefor 1 byte = '00000000' or '00001000' or '10010001', ect.

Speed:

- Types
  - 'bps' = 'Bits Per Second'
  - 'Kbps' = 'Kilo Bits Per Second'
    - 'Kilo' is 1000
    - 'Kbps' = '(Bits/1000) Bits Per Second'
    - This means for every 1000 bits, we will have 1 'Kb' (Kilobit)
    - 1000 = One thousand
  - 'Mbps' = 'Mega Bits Per Second'
    - 'Mega' is 1000000
    - 'Mbps' = '(Bits/1000000) Bits Per Second'

        - This means for every 1000000 bits, we will have 1 ‘Mb’ (Megabit)
        - 1000000 = One million
    - ‘Gbps’ = ‘Giga Bits Per Second’
        - ‘Giga’ is 1000000000
        - ‘Gbps’ = ‘(Bits/1000000000) Bits Per Second’
        - This means for every 1000000000 bits, we will have 1 ‘Gb’ (Gigabit)
        - 1000000000 = One billion
    - ‘Tbps’ = ‘Tera Bits Per Second’
        - ‘Tera’ is 1000000000000
        - ‘Tbps’ = ‘(Bits/1000000000000) Bits Per Second’
        - This means for every 1000000000000 bits, we will have 1 ‘Tb’ (Terabit)
        - 1000000000000 = One trillion

Bonus facts:

- 1 bit = 0.125 bytes & 8 bits = 1 bytes
    - Bits to bytes formula: $bytes = \frac{bits}{8}$
    - Bytes to bits formula: $bits = bytes \cdot 8$

ROUTERS

Routers:

- Purpose
    - A router connects LANs over the internet.
    - Characteristics
        - Routers have fewer network interfaces than switches.
        - Routers are used to provide connectivity between LANs.
        - Routers are used to send data over the internet.

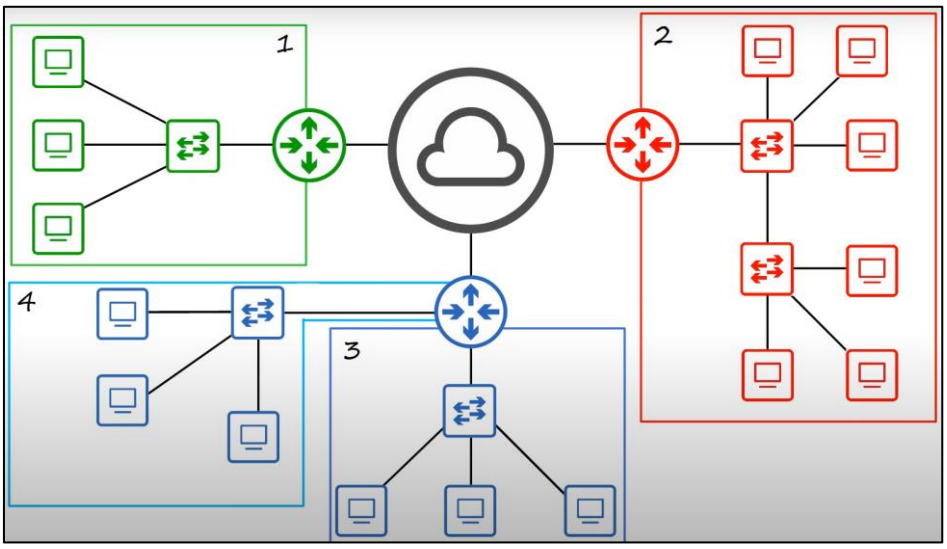
Bonus facts:

-

LANS (LOCAL AREA NETWORK’S)

End hosts within the same area. Like a bunch of computers on one floor of an office or perhaps an entire small office for your home network.

What is a LAN:



- Everything highlighted above is a LAN
    - LAN1 consists of 1 Router, 1 Switch and 3 PC’s
    - LAN2 consists of 1 Router, 2 Switches and 6 PC’s
    - LAN3 consists of 1 Router, 1 Switch and 3 PC’s
    - LAN4 consists of 1 Router, 1 Switch and 3 PC’s

- Important:
  - LAN3 and LAN4 use the same Router because each Switch, from both LANs, is connected to the same Router.
  - LAN2 have 2 Switches but is only 1 LAN because only 1 Switch is connected to the Router, and the other Switch is connected to the Switch going into the Router.

FIREWALLS

Network Firewalls:

- Purpose
  - Firewalls are specialty network security devices that control network traffic, entering and exiting your network.
  - Firewalls protect end hosts/devices inside of the LAN, like PC's or servers.
  - Firewalls must be configured with security rules to determine which network traffic should be allowed and which should be denied entering the LAN.
- Characteristics
  - Firewalls are hardware devices that filter traffic between networks.
  - Firewalls monitor and control network-traffic based on configured rules.
  - Firewalls can be placed 'inside' the network, or 'outside' the network. Meaning the firewall can filter the traffic before it reaches the router or after it has passed through the router.
  - When a firewall includes more modern and advanced filtering capabilities, they're known as 'Next-Generation Firewalls'.

Host-bases firewalls:

- Purpose
  - Host-bases firewalls are software applications that filter traffic entering and exiting a host machine, like a PC.

Bonus facts:

- Even though a network with a hardware firewall, each PC should include a software firewall as an extra line of defense.

LABS

"Labbing" / "Doing Labs":

- Refers to hands-on practice with the technology you're studying.

Bonus facts:

- Since you're studying for the CCNA, "labbing" means practicing configuring Cisco routers.

TTL (TIME TO LIVE)

What is it:

- When you ping, some frames are sent to another host. But what if the request was never received? Then the frame would just go around trying to find the receiving host. That is why we have something called TTL (Time to Live). It basically just tells the frame how much time it should be alive, while trying to find the receiving host, so that no data is repeated over an over again trying to find a host that isn't reachable.

SLAAC

Possible questions and answers:

- **A client is using SLAAC to obtain an IPv6 address for its interface. After an address has been generated and applied to the interface, what must the client do before it can begin to use this IPv6 address?**
  - It must send an ICMPv6 Neighbor Solicitation message to ensure that the address is not already in use on the network.

Possible questions and answers:

-
  -

STP (SPANNING TREE PROTOCOL)

Store Layer1 and Layer2 information.

OSPF ()

Store Layer1, Layer2 and Layer3 information.

DHCP

Layer7 protocol.

Automatically give devices IP addresses.

PUTTY (TERMINAL EMULATOR)

What is it?

- PuTTY is a Terminal Emulator. It emulates the functionalities of classic computer terminals. It assists a host computer to gain access to another computer in a different location via either a command-line interface or a graphical user interface.

How to use it?

- Click on the radiobutton called “Serial” and access the Terminal using that.
- To change the default configuration of “Serial”, click on the menu item to the left called “Serial”: Connection->Serial.

Serial Line Settings:

- Speed (baud):
  - Measured in ‘bits/s’
- Data bits:
  - Not in the exam :)
- Stop bits:
  - Not in the exam :)
- Parity:
  - Used to detect errors
- Flow Control:
  - Controlling the flow of data from transmitter to receiver

MESSAGE TIMING

Flow Control:

Manages the rate of data transmission and defines how much information can be sent and the speed at which it can be delivered.

Response timeout:

Manages how long a device waits when it does not hear a reply from the destination

Access method:

Determines when someone can send a message

- There may be various rules governing issues like collisions. This is when more than one device sends traffic at the same time, and the messages become corrupt.
- Some protocols are proactive and attempt to prevent collisions; other protocols are reactive and establish a recovery method after the collision occurs.

CLI (COMMAND LINE INTERFACE)

What is it?

- The CLI (Command Line Interface), is used to configure cisco devices.

Help in the CLI:

- When you don't know what to type in the CLI, type "?" and enter. This will give you all of the commands you can type in the current mode you're in.

When you enter the CLI:

- You will be greeted with some text and a question saying "Would you like to enter the initial configuration dialog? [yes/no]:"
  - Type "no"
- You will be EXEC mode will be "User EXEC mode", represented by the ">" sign at the end of the line.
  - The "User EXEC mode" only allows you to type in basic commands.
  - Users can look at things but can't change anything in the configuration.
- "Privileged EXEC mode"
  - This mode allows you to type commands more advanced than in the "User EXEC mode".
    - Provides complete access to view the devices configuration.
  - To enter the "Privileged EXEC mode", type enable, and press enter:
    - Example: `Router>enable`
- Config t:
  - "Config t" = "Configure Terminal"
    - This is also called the "Global Configuration Mode"
  - Commands in "Global Configuration Mode"
    - Passwords
      - `Router(config)# enable password any_password`
        - Only allows specific people knowing the password, to enter the "Global Configuration Mode"
        - Passwords are case sensitive!
        - Don't type special characters, as it may not work with some!
      - `Router(config)# enable secret any_password`
        - This is a secure way to encrypt the passwords, even more secure than typing: `Router(config)# service password-encryption`
        - This will give your passwords "MD5" encryption or "type 5" encryption
        - If you execute this command, any password configured by: `Router(config)# enable password any_password` will be ignored.
        - This is the most secure way to protect access to "Privileged EXEC mode"
    - Exiting modes
      - `Router# exit`
        - This command will exit the current mode you're in and go to the previous mode.
        - Example typing: `Router# exit` will exit "Privileged EXEC mode" and enter "User EXEC mode"
    - Saving configuration
      - `Router# copy running-config startup-config`
        - This saves the current configuration.
        - Remember to do this when you're done with your configuration of the device!
        - You will be asked to type in something. Just press enter!
        - Command structuring
          - `Router# copy (source-file) (destination-file)`
    - Showing configuration
      - `Router# show running-config`
        - Shows the current configuration
        - Command structuring
          - `Router# show (file)`
      - `Router# show startup-config`
        - If you haven't saved the running-config yet, then this command will output: "startup-config is not present"
        - Command structuring
          - `Router# show (file)`
    - Encryption of passwords
      - `Router(config)# service password-encryption`

- This will encrypt all passwords in a jumble of numbers and letters, so they cannot easily be read.
- For more secret passwords, use Router(config)# service password-encryption when typing your passwords.
- This will give you passwords “type 7” encryption.
- This command has no effect on the Router(config)# enable secret any_password
- Command structuring
  - Router# service (service)

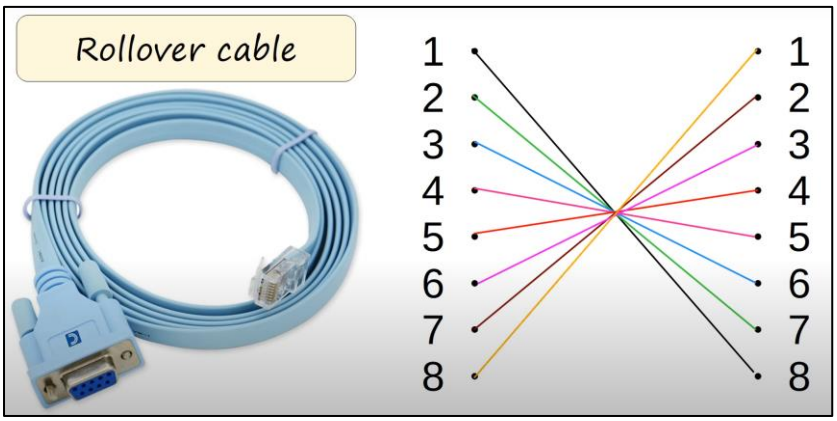
- Delete any configured command
  - Router(config)# no any_command
    - This will delete the command, for example if ‘any_command’ was “enable secret”, the secret password would be deleted from the running-config (running-configuration).
    - Command structuring
      - Router# no (command)
- Hostnames
  - Router(config)# hostname any_hostname
    - This will change the hostname for example “Router” in the command above, to “any_hostname”
    - “any_hostname” can be any name, but keep it simple and concise. So if you have multiple routers, then maybe make the hostname: “R1” or “Router1”
    - Command structuring
      - Router# hostname (name)

- running-config / startup-config
  - There are 2 separate configuration files kept on the device at once.
    - Running-config
      - The current, active configuration file on the device. As you enter commands in the CLI, you edit the active configuration.
    - Startup-config
      - The configuration file that will be loaded upon restart of the device.

DEVICE CONNECTION (CONSOLE PORT / REMOTELY)

How to connect a device to CLI?

- Console Port
  - Connecting to a device through the console port typically involves bringing the CLI to the device you want to configure.
  - When you first connect to a device, it needs to be through the console port.
  - Theres 2 types of console ports: USB Mini-B and the RJ45. Typically, we use the RJ45.
  - For RJ45 Port
    - Use a Rollover cable, which is a RJ45 to DB9 connector. It connects like this:



]

- Remotely
  -

MODES

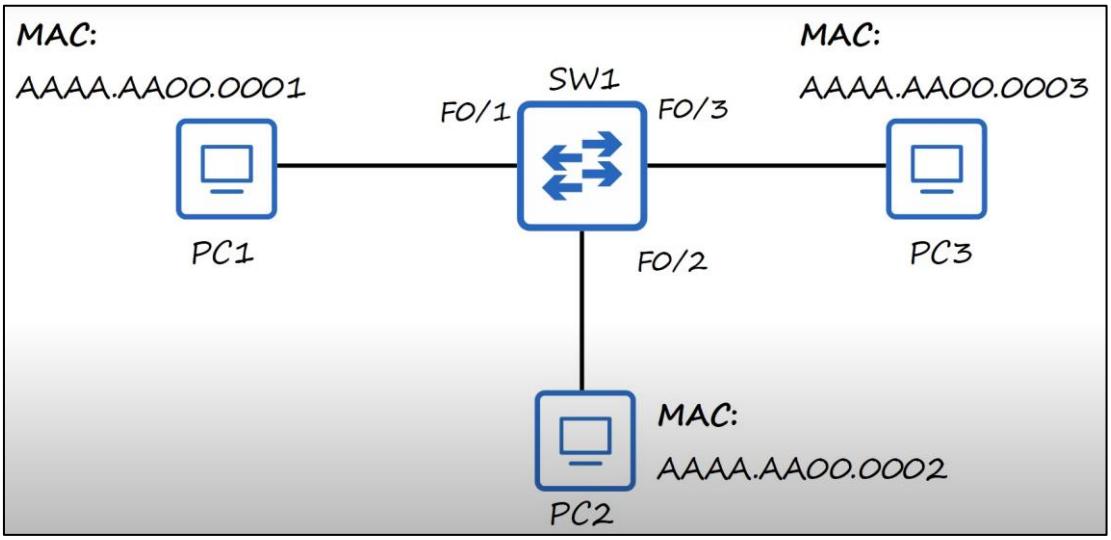
Possible questions and answers:

- A group of Windows PCs in a new subnet has been added to an Ethernet network. When testing the connectivity, a technician finds that these PCs can access local network resources but not the Internet resources. To troubleshoot the problem, the technician wants to initially confirm the IP address and DNS configurations on the PCs, and also verify connectivity to the local router. Which three Windows CLI commands and utilities will provide the necessary information? (Choose three.)
    - Ping
    - ipconfig
    - nslookup
- **A new network administrator has been asked to enter a banner message on a Cisco device. What is the fastest way a network administrator could test whether the banner is properly configured?**
    - Exit privileged EXEC mode and press Enter.

MAC-ADDRESS (MEDIA ACCESS CONTROL) - (PHYSICAL ADDRESS)

What is it:

- The MAC-address is 6 bytes (48 bits).
- It is the address assigned to the physical device when it's made.
- References
    - BIA (Burned-In Address)
        - This is just a name referring to the MAC-address because the MAC-address is burned into the device as it is made.
- The MAC-address is globally unique, which means that there no 2 devices in the world with the same MAC-address
    - Though there are MAC-addresses knows as "Locally Unique MAC-addresses", which don't have to be globally unique. But in almost all cases they are globally unique.
- Proportion of the MAC-address
    - The first 3 bytes or the first half of the MAC-address are the OUI (Organizationally Unique Identifier), which is assigned to the company making the device.
    - The last 3 bytes are unique to the device itself.
- It is written as 12 hexadecimal characters
- Example of network setup with MAC-addresses



    - In the example above there are 3 MAC-addresses. If you look at the first 3 characters AAAAAA they are all the same, indicating that the 3 hosts are from the same maker, for example Cisco or ASUS. The last characters are different though indicating their unique address of the host.
    - Keep in mind that the MAC-addresses above is probably not going to be in real life, but for simplicity, we use those values.

Possible questions and answers:

- **A host is trying to send a packet to a device on a remote LAN segment, but there are currently no mappings in its ARP cache. How will the device obtain a destination MAC address?**

- It will send an ARP request for the MAC address of the default gateway.

NETWORK MASK

Possible questions and answers:

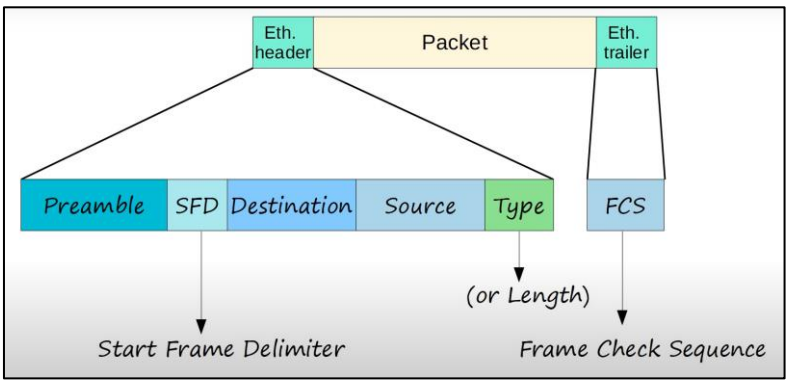
- **A network administrator is adding a new LAN to a branch office. The new LAN must support 25 connected devices. What is the smallest network mask that the network administrator can use for the new network?**
  - 255.255.255.224
- **A network administrator is adding a new LAN to a branch office. The new LAN must support 61 connected devices. What is the smallest network mask that the network administrator can use for the new network?**
  - 255.255.255.192
- **A network administrator is adding a new LAN to a branch office. The new LAN must support 90 connected devices. What is the smallest network mask that the network administrator can use for the new network?**
  - 255.255.255.128
- **A network administrator is adding a new LAN to a branch office. The new LAN must support 4 connected devices. What is the smallest network mask that the network administrator can use for the new network?**
  - 255.255.255.248
- **A network administrator is adding a new LAN to a branch office. The new LAN must support 200 connected devices. What is the smallest network mask that the network administrator can use for the new network?**
  - 255.255.255.0
- **A network administrator is adding a new LAN to a branch office. The new LAN must support 10 connected devices. What is the smallest network mask that the network administrator can use for the new network?**
  - 255.255.255.240
- **A network administrator is designing the layout of a new wireless network. Which three areas of concern should be accounted for when building a wireless network? (Choose three.)**
  - Interference
  - security
  - coverage area
- **A network administrator needs to keep the user ID, password, and session contents private when establishing remote CLI connectivity with a switch to manage it. Which access method should be chosen?**
  - SSH
- **A network administrator notices that some newly installed Ethernet cabling is carrying corrupt and distorted data signals. The new cabling was installed in the ceiling close to fluorescent lights and electrical equipment. Which two factors may interfere with the copper cabling and result in signal distortion and data corruption? (Choose two.)**
  - RFI
  - EMI
- **A network administrator wants to have the same network mask for all networks at a particular small site. The site has the following networks and number of devices:**
  IP phones – 22 addresses
  PCs – 20 addresses needed
  Printers – 2 addresses needed
  Scanners – 2 addresses needed
  The network administrator has deemed that 192.168.10.0/24 is to be the network used at this site. Which single subnet mask would make the most efficient use of the available addresses to use for the four subnetworks?
  - 255.255.255.224
- **A network administrator wants to have the same subnet mask for three subnetworks at a small site. The site has the following networks and numbers of devices: What single subnet mask would be appropriate to use for the three subnetworks?**
  - 255.255.255.240

FRAMES

What is it:

- A Frame is the second last step in the OSI-model, in the Data-Link Layer (Layer2).

- Different kinds of frames
  - Unicast frame
    - A frame destined for a single target
  - Broadcast frame
    - A frame destined for all targets on a LAN
  - Multicast frame
    - A frame destined for multiple targets, but not all!
- Ethernet Frame example



  - Preamble
    - Is 7 bytes (56 bits)
    - Used for synchronization and to allow the device to be prepared to receive the rest of the data in frame
  - SFD (Start Frame Delimiter)
    - Is 1 byte (8 bits)
    - Used for synchronization and to allow the device to be prepared to receive the rest of the data in frame
    - It marks the end of the preamble, and the beginning of the rest of the frame
  - Destination
    - Is 6 bytes (48 bits)
    - The Layer2 address to the device which the frame is being sent to
    - Indicating the device receiving the frame
    - Consists of the destination 'MAC-address'
  - Source
    - Is 6 bytes (48 bits)
    - The Layer2 address of the source device of the frame
    - Indicating the device transmitting the frame
    - Consists of the source 'MAC-address'
  - Type
    - Is 2 bytes (16 bits)
    - Indicates the Layer3 protocol used in the encapsulated packet, which is almost always Internet Protocol, IPv4 or IPv6
    - The type of field can also be a Length, indicating the length of the encapsulated data.
      - If the value of the type is 1500 or less, its indicating the Length of the encapsulated packet (in bytes)
      - If the value of the type is 1536 or greater, its indicating the Type of the encapsulated packet (usually IPv4 or IPv6), and the length is determined via other methods
  - FCS (Frame Check Sequence)
    - Used by the receiving device to detect any errors that might have occurred in the transmission
    - *It is 4 bytes (32 bits) in length*
    - *Detects corrupted data by running a 'CRC' algorithm over the received data.*
      - *CRC is Cyclic Redundancy Check*
  - *The hole frame is then* $7 + 1 + 6 + 6 + 2 + 4 = 26\ bytes$
    - *Though usually the Preamble and SFD are not considered a part of the Ethernet Header. So the value of the frame is* $6 + 6 + 2 + 4 = 18\ bytes$

- Runts: Frames that are too small
- Giants: Frames that are too big

DECIMAL

What is it:

- The decimal-system uses 10 possible digits: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9

HEXADECIMAL

What is it:

- The hexadecimal-system uses 16 possible digits: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F
- Letters and what they represent
    - A = 10
    - B = 11
    - C = 12
    - D = 13
    - E = 14
    - F = 15
- Example of decimals and their hexadecimal value

DEC.	HEX.	DEC.	HEX.	DEC.	HEX.	DEC.	HEX.
0	0	8	8	16	10	24	18
1	1	9	9	17	11	25	19
2	2	10	A	18	12	26	1A
3	3	11	B	19	13	27	1B
4	4	12	C	20	14	28	1C
5	5	13	D	21	15	29	1D
6	6	14	E	22	16	30	1E
7	7	15	F	23	17	31	1F

- Calculate hexadecimal value from decimal
    - Example of decimal 20 and 29
        - 20 in hexadecimal is 14, because the “1” in 14, means 16, and the “4” in 14, means there are 4 x “0”, so we basically just do: 16 + 4 = 20
        - 29 in hexadecimal is 1D, because “1” in 1D, means 16, and the “D” in 1D, means there are 13 x “0”, because D = 13, as shown above. Then we just do: 16 + 13 = 29

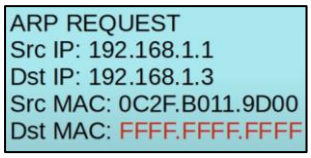
ARP (ADDRESS RESOLUTION PROTOCOL)

What is it:

- It is used to discover the Layer 2 address (MAC address) of a known Layer 3 address (IP address)
- What does the switch with the Dynamic MAC addresses
    - The Switch keeps these MAC addresses for 5 minutes. It does that because it needs to know where to sent the data, if someone is for example playing a game or something, where the game needs constant information about what to display, etc. But when the game is turned off and the Host doesn’t need information about the game, the Switch will just delete the MAC address from the Table, so that there’s space for new MAC addresses, from other or the same host.
- Consists of 2 messages
    - ARP request
        - The ARP request message is used to learn the Layer 2 address of a host. Because the Layer 2 address is not yet known, the message must be broadcast to all hosts on the local network.
        - Sent by the device that wants to know the MAC address of the other device
        - Sent as broadcast: Sent to all hosts on the network
            - The destination MAC address for broadcast is: FFFF.FFFF.FFFF

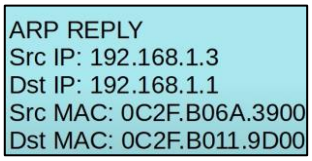
- When the broadcast is sent, the host that has the right MAC-address will then send back a message saying: "I'm the host you're searching for". The Switch will then take that MAC address and store it in the MAC-address table, which has the values of the port and the MAC-address. This way the Switch knows exactly where and how to get to the host!

- The ARP request contains for example



- What will the Switch do with the request
  - For the Switch the request is an "Unknown Unicast Frame" which means that the Switch will "flood" (you can read about that under here)
  - When a host device sends an ARP request, the Switch will learn which port the request came in as (the interface), and what the source MAC address is. When the Switch learns these values, it will store them in the MAC Address Table of the Switch, this type of MAC address is called a "Dynamic MAC Address".
  - Since the Destination MAC address (DST MAC) - Look at the image above - is FFFF.FFFF.FFFF the Switch will sent a Broadcast to all active ports, except the port the request came in through.
    - Since all active ports are connected to host devices, and the hosts devices have IP-addresses; the host devices that don't match the Destination IP, will just ignore the ARP request. The host device that does match the Destination IP of the request will send an ARP reply to the host device that sent the request.

- ARP reply
  - What will the Switch do with the reply
    - For the Switch the request is an "Known Unicast Frame" which means that the Switch will NOT "flood", it will just "forward" the frame to the receiver.
  - Sent to inform the requesting device of the MAC address
  - Sent as unicast: Sent only to one host (the host that sent the request)
  - The ARP reply contains for example



    - As you can see, the ARP reply knows all the values, because it has learnt it from the ARP request. The only value the ARP request didn't have was the DST MAC address, but the ARP reply adds that, so the host that sent the request knows which MAC address it is.

SHOW INFORMATION

YOUR PC

SHOW ALL ARPS

```
C:\Users\user>arp -a

Interface: 169.254.146.29 --- 0x9
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.0.167 --- 0xd
  Internet Address      Physical Address      Type
  192.168.0.1           98-da-c4-dd-a8-e4     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Explanation:

- Internet Address = IP address (Lager 3 address)
- Physical Address = MAC address (Lager 2 address)
- Type static = Default entry
- Type dynamic = Learned via ARP

PACKET TRACER

SHOW MAC ADDRESS-TABLE

```
SW1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0c2f.b011.9d00    DYNAMIC     Gi0/0
   1    0c2f.b06a.3900    DYNAMIC     Gi0/2
Total Mac Addresses for this criterion: 2
```

SHOW IP INTERFACES FOR DEVICE - EXAMPLE ROUTER

```
R1>en
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         unassigned      YES unset  administratively down down
GigabitEthernet0/2         unassigned      YES unset  administratively down down
GigabitEthernet0/3         unassigned      YES unset  administratively down down
R1#
```

- administratively down: Interface has been disabled with the 'shutdown' command.
- This is the default Status of Cisco router interfaces.
- Cisco switch interfaces are NOT administratively down by default.

SHOW INTERFACE INFO AND ERRORS

Keep in mind that f0/1 can be any interface

```
SW1#show interfaces f0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is Fast Ethernet, address is 000C.2110.5542 (bia 000C.2110.5542)
  Description: ## to R1 ##
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Full-duplex, 100Mb/s
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 02:29:44, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queuing strategy: fifo
```

REMOVE INFORMATION

YOUR PC

PACKET TRACER

REMOVE SPECIFIC MAC ADDRESS OR INTERFACE FROM MAC ADDRESS-TABLE

```
SW1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0c2f.b011.9d00    DYNAMIC     Gi0/0
   1    0c2f.b06a.3900    DYNAMIC     Gi0/2
Total Mac Addresses for this criterion: 2
SW1#clear mac address-table dynamic address 0c2f.b011.9d00
```

Or

```
SW1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0c2f.b011.9d00    DYNAMIC     Gi0/0
   1    0c2f.b06a.3900    DYNAMIC     Gi0/2
Total Mac Addresses for this criterion: 2
SW1#clear mac address-table dynamic interface Gi0/0
```

REMOVE ALL MAC ADDRESSES FROM MAC ADDRESS-TABLE

```
SW1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0c2f.b011.9d00    DYNAMIC     Gi0/0
   1    0c2f.b06a.3900    DYNAMIC     Gi0/2
Total Mac Addresses for this criterion: 2
SW1#clear mac address-table dynamic
```

PING - FOR CISCO AND ICMP

What is it:

- A network utility that is used to test reachability
- Measures round-trip time
- Each message is 100-bytes (800 bit)
- Uses two messages:
    - ICMP Echo Request
        - Is a unicast message used to test the reachability of another specific host.
        - By default, it sends 5 Echo's to the desired IP-address
    - ICMP Echo Reply
        - Is a unicast reply to the request
        - By default, it replies 5 Echo's
        - Errors messages
            - If you get a '.': It means that it didn't work.
            - If you get a '!': It means that it did work.
            - It can for example look like this: '.!!!!', meaning the first one didn't work but the next 4 did work.

How to use:

- ping (IP-address)

Example and explanation:

```
PC1#
PC1#ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 20/20/22 ms
PC1#
```

- As you can see above, we got '.!!!!' indicating the first request failed. The reason it failed was because of ARP. It didn't know the MAC address of the receiver, so it had to get it first, therefore the first one failed. The next ones didn't because it knew the MAC address of the receiver (192.168.1.3).
- Keep in mind that these demonstrations are from CISCO, and may look different for you, but the logic is the same.
- When you ping on a PC to another PC, it will also do the ARP, which will turn out the same, just looking different. But when you try pinging to the same IP address again, the Switch knows about the MAC address, because the 5 minute time period has not succeeded.

Possible questions and answers:

- **A technician can ping the IP address of the web server of a remote company but cannot successfully ping the URL address of the same web server. Which software utility can the technician use to diagnose the problem?**
  - Nslookup

DATA FLOW

Possible questions and answers:

- **A technician with a PC is using multiple applications while connected to the Internet. How is the PC able to keep track of the data flow between multiple application sessions and have each application receive the correct packet flows?**
  - The data flow is being tracked based on the source port number that is used by each application.

ACCESS DOMAIN

Possible questions and answers:

- **A user is attempting to access http://www.cisco.com/ without success. Which two configuration values must be set on the host to allow this access? (Choose two.)**
  - DNS server
  - default gateway

PROBLEM SOLVING

Possible questions and answers:

- **A user is complaining that an external web page is taking longer than normal to load. The web page does eventually load on the user machine. Which tool should the technician use with administrator privileges in order to locate where the issue is in the network?**
  - Tracert
- **A user is executing a tracert to a remote device. At what point would a router, which is in the path to the destination device, stop forwarding the packet?**
  - when the value in the TTL field reaches zero
- **A user sends an HTTP request to a web server on a remote network. During encapsulation for this request, what information is added to the address field of a frame to indicate the destination?**
  - the MAC address of the default gateway
-
  -
-
  -
-
  -
-
  -
-
  -
-
  -
-
  -

NETWORKING MODELS

Possible questions and answers:

- **A wired laser printer is attached to a home computer. That printer has been shared so that other computers on the home network can also use the printer. What networking model is in use?**
    - peer-to-peer (P2P)
-
    -
-
    -
-
    -
-
    -
-
    -

VLAN (VIRTUAL LOCAL AREA NETWORK)

PADDING BYTES

What is it:

- In some cases, padding bytes are added if the size of a frame is less than the minimum size required for a ping/ethernet payload. For example, if I send a ping, with a specific size, for example 36 bytes, but since the ping/ethernet payload requires at least 46 bytes, it's going to add padding portrayed as 0's, until the required length of 46 bytes is reached.

LAN HUB

What is it:

- A LAN Hub is kind of a stupid Switch… A switch can send frames to specific hosts because it knows where the individual hosts are located, and if not, it will do an ARP request (You can read about that elsewhere in this document). A Hub will send the frame to all connected hosts, it's simply a repeater, it repeats the signal. A Hub always broadcasts signals instead of unicasting them to the right host.
- A Hub can also send out frames at once, which will result in collision, which is not good! A Switch makes sure that each frame is sent with "space" over the medium, so almost no collisions can happen, and no data loss is happening. Though some collisions do still happen with Switches, but its very rare.

CSMA/CD (CARRIER SENCE MULTIPLE ACCESS WITH COLLISION DETECTION)

What is it:

- This is used on half-duplex interfaces to detect and avoid collisions.
    - Hubs use this
- This was used to solve the collision problem with Hubs.
- Before sending frames, devices 'listen' to the collision domain until they detect that other devices are not sending.
- If a collision does occur, the device sends a jamming signal to inform the other devices that a collision happened.
- Each device will then wait a random period before sending frames again.
- The process repeats.

SPEED/DUPLEX AUTO-NEGOTIATION

- Interface that can run at different speeds (10/100 or 10/100/1000) have default settings of speed auto and duplex auto.
- Interfaces 'advertise' their capabilities to the neighboring device, and they negotiate the best speed and duplex settings they are both capable of.
- If auto-negotiation is disabled SW1 will not sense SW's duplex setting and collisions will therefore occur.
- Rules when Auto-negotiation is disabled
    - If the speed is 10 or 100 megabits per second, half duplex will be used. Otherwise, full duplex will be used.

ADDRESSING

IPV4

Find the value you know down below, and then get the other values from the table or formulas below:

Hosts: $2^{(32-bits_{used})}$

Subnets: $\frac{256}{hosts}$

CIDR notation/used bits: $32 - bits_{borrowed}$

Subnet Mask: Numbers… $256 - hosts$

Hosts	Subnets:	CIDR notation:	Subnet Mask	Subnet Mask Binary
$2^1 = 2$	$\frac{256}{2} = 128$	$32 - 1 = 31$	255.255.255.254	11111111.11111111.11111111.11111110
$2^2 = 4$	$\frac{256}{4} = 64$	$32 - 2 = 30$	255.255.255.252	11111111.11111111.11111111.11111100
$2^3 = 8$	$\frac{256}{8} = 32$	$32 - 3 = 29$	255.255.255.248	11111111.11111111.11111111.11111000
$2^4 = 16$	$\frac{256}{16} = 16$	$32 - 4 = 28$	255.255.255.240	11111111.11111111.11111111.11110000
$2^5 = 32$	$\frac{256}{32} = 8$	$32 - 5 = 27$	255.255.255.224	11111111.11111111.11111111.11100000
$2^6 = 64$	$\frac{256}{64} = 4$	$32 - 6 = 26$	255.255.255.192	11111111.11111111.11111111.11000000
$2^7 = 128$	$\frac{256}{128} = 2$	$32 - 7 = 25$	255.255.255.128	11111111.11111111.11111111.10000000
$2^8 = 256$	$\frac{256}{256} = 1$	$32 - 8 = 24$	255.255.255.0	11111111.11111111.11111111.00000000

IPV6

SSH (SECURE SHELL)

Possible questions and answers:

- **An administrator defined a local user account with a secret password on router R1 for use with SSH. Which three additional steps are required to configure R1 to accept only encrypted SSH connections? (Choose three.)**
    - Configure the IP domain name on the router.
    - Generate the SSH keys.
    - Enable inbound vty SSH sessions.
-
    -
-
    -
-

-
-

NETWORK CHARACTERISTICS

Possible questions and answers:

- **An employee of a large corporation remotely logs into the company using the appropriate username and password. The employee is attending an important video conference with a customer concerning a large sale. It is important for the video quality to be excellent during the meeting. The employee is unaware that after a successful login, the connection to the company ISP failed. The secondary connection, however, activated within seconds. The disruption was not noticed by the employee or other employees.**
  What three network characteristics are described in this scenario? (Choose three.)
  - Security
  - quality of service
  - fault tolerance
-
-

OVERALL-KNOWLEDGE

GET INFORMATION FROM YOUR PC

IP-ADDRESSING

What is it:

- The IP-address is 4 bytes (32 bits).
- It is the logical address of the device.

SUBNETTING

IPV4

Example:

- IP = $X_1.X_2.X_3.X_4\ /n$
  - Values depending on X_1
    - If $X_1 \leq 127$ then it's a class 'A'.
      - Prefix length: /8
      - Leading bits: 0
      - Default Subnet Mask
        - Decimal: 255.0.0.0
        - Binary: 11111111.00000000.00000000.00000000
      - Size of network number bit field: 8
      - Size of rest bit field: 24
      - Number of networks: 128 (2^7)
      - Addresses per network: 16777216 (2^{24})
    - If $X_1 \leq 192$ then it's a class 'B'.
      - Prefix length: /16
      - Leading bits: 10
      - Default Subnet Mask
        - Decimal: 255.255.0.0
        - Binary: 11111111.11111111.00000000.00000000
      - Size of network number bit field: 16

- Size of rest bit field: 16
- Number of networks: 16384 (2^{14})
- Addresses per network: 65536 (2^{16})

▪ If $X_1 \leq 223$ then it's a class 'C'.
- Prefix length: /24
- Leading bits: 110
- Default Subnet Mask
  - Decimal: 255.255.255.0
  - Binary: 11111111.11111111.11111111.00000000
- Size of network number bit field: 24
- Size of rest bit field: 8
- Number of networks: 2097152 (2^{21})
- Addresses per network: 256 (2^8)

○ Values depending on X_4
▪ If X_4 is 0 in decimal or 00000000 in binary
- X_4 is the network address.

▪ If X_4 is not 0 in decimal nor 00000000 in binary
- X_4 is a host address

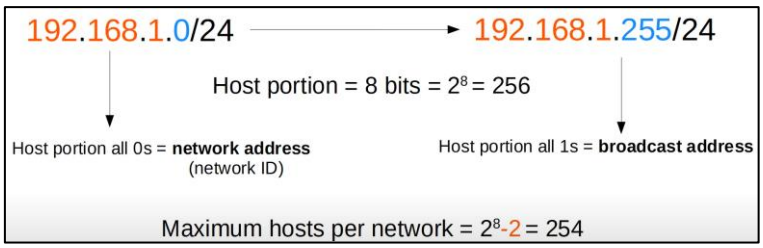
▪ If X_4 is 255 in decimal or 11111111 in binary
- X_4 broadcast address

IPV6

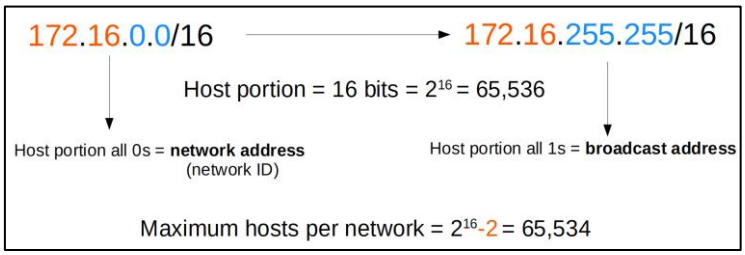
MAXIMUM USABLE HOSTS PER NETWORK

Formula: $2^n - 2$

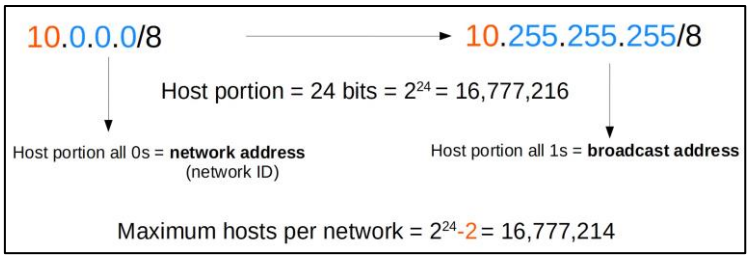
Class C:



Class B:



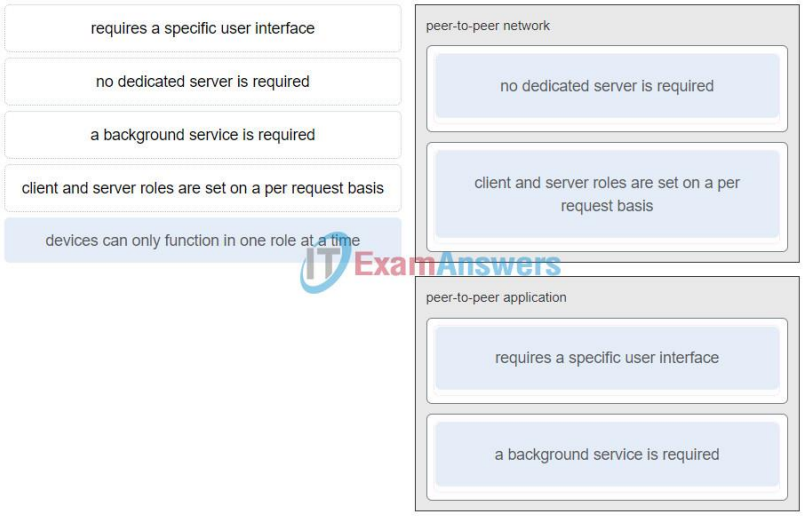
Class A:



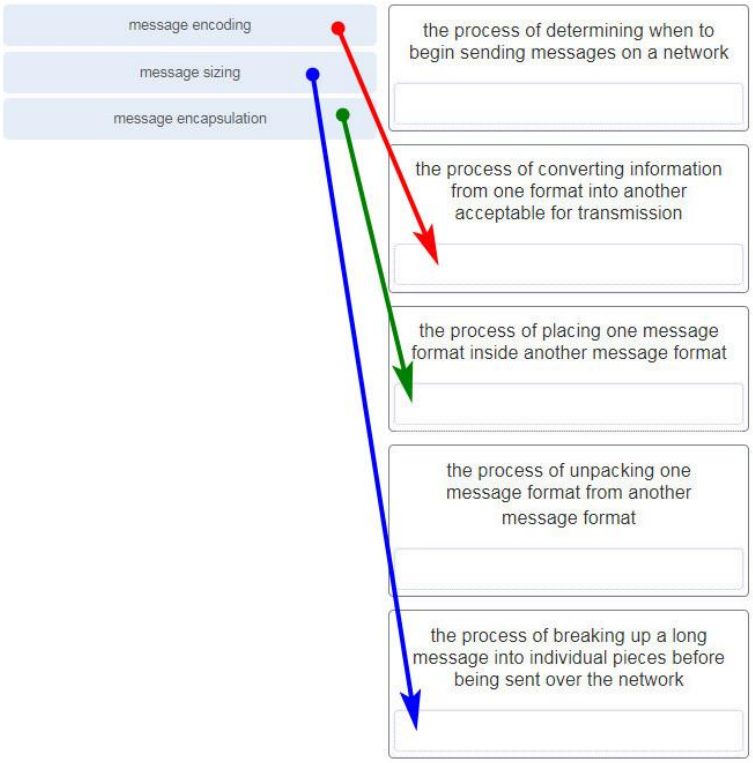
OTHER THINGS

Possible questions and answers:

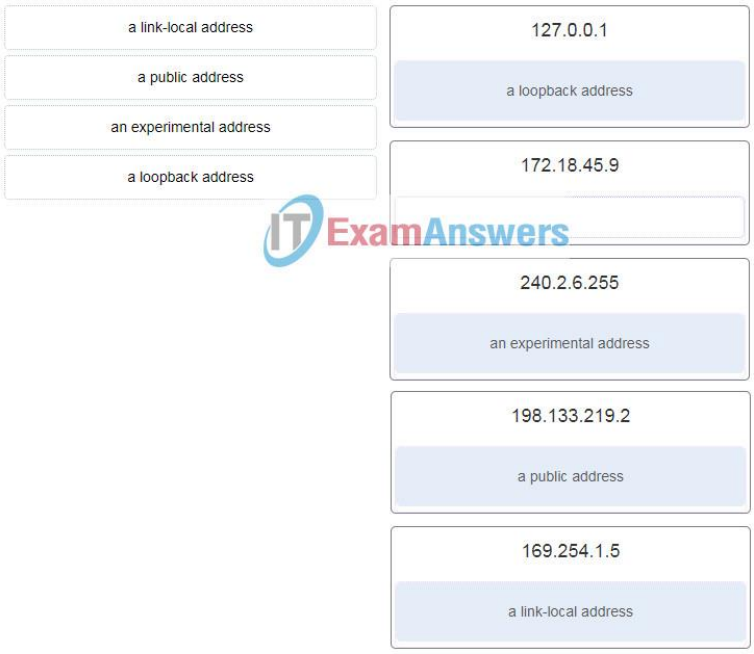
- **How does the service password-encryption command enhance password security on Cisco routers and switches?**
  - It encrypts passwords that are stored in router or switch configuration files.
- **Match a statement to the related network model. (Not all options are used.)**



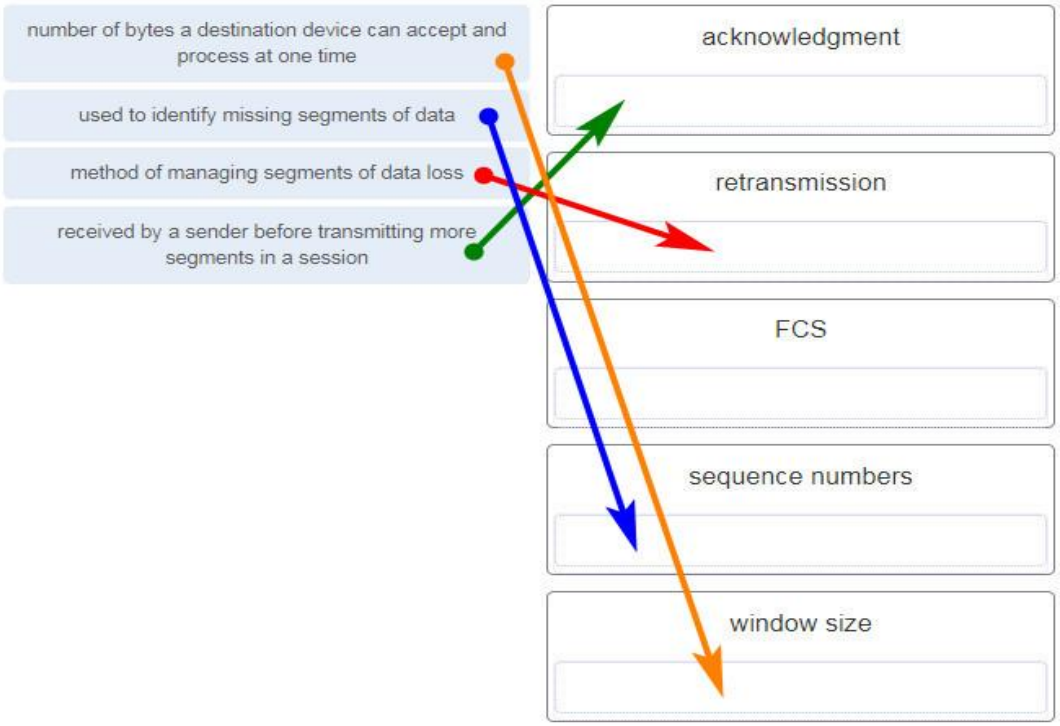
- **Match each description to its corresponding term. (Not all options are used.)**



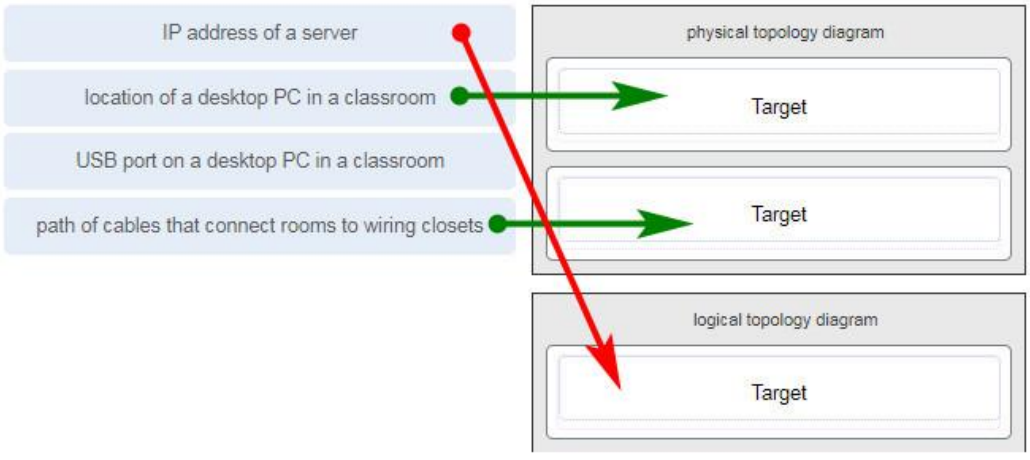
- **Match each description with an appropriate IP address. (Not all options are used.)**



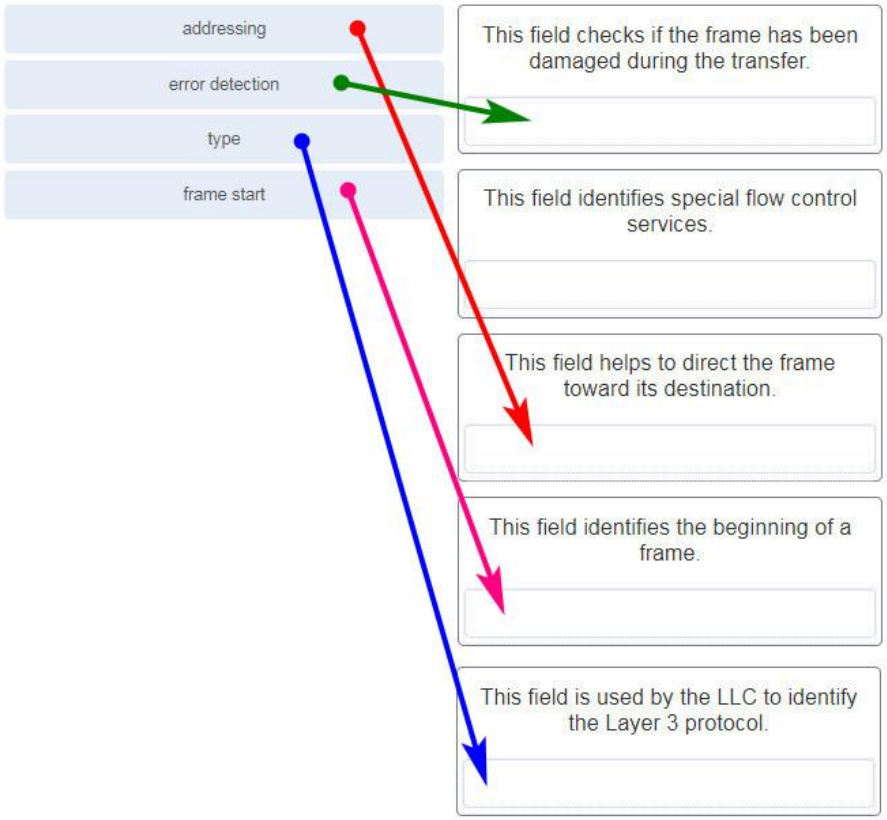
- **Match each description with the corresponding TCP mechanism. (Not all options are used.)**



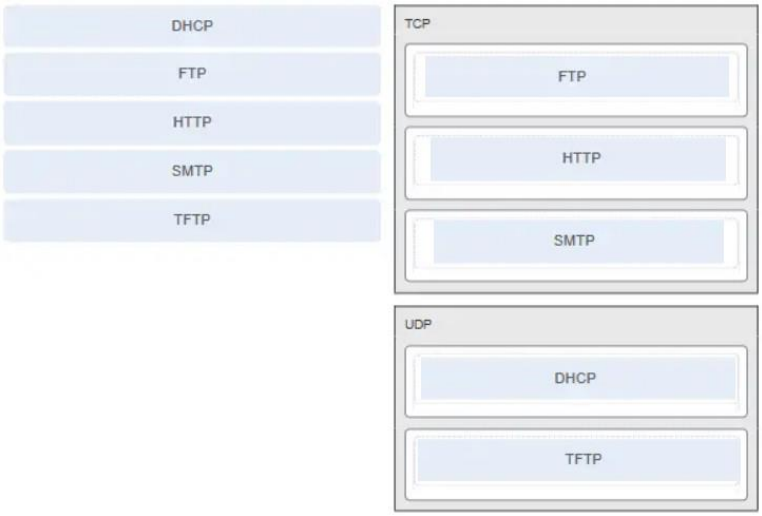
- **Match each item to the type of topology diagram on which it is typically identified. (Not all options are used.)**



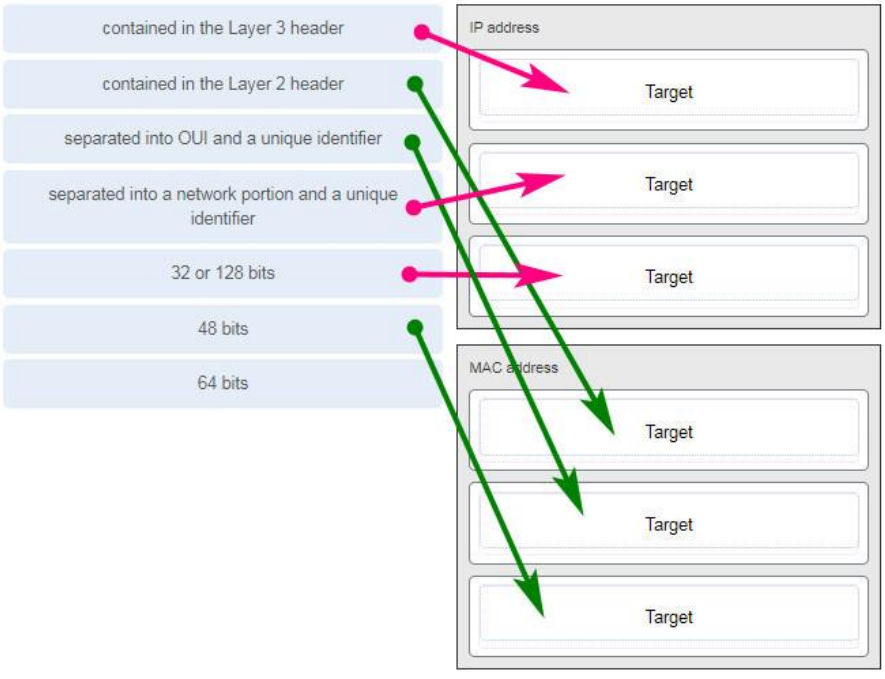
- **Match each type of frame field to its function. (Not all options are used.)**



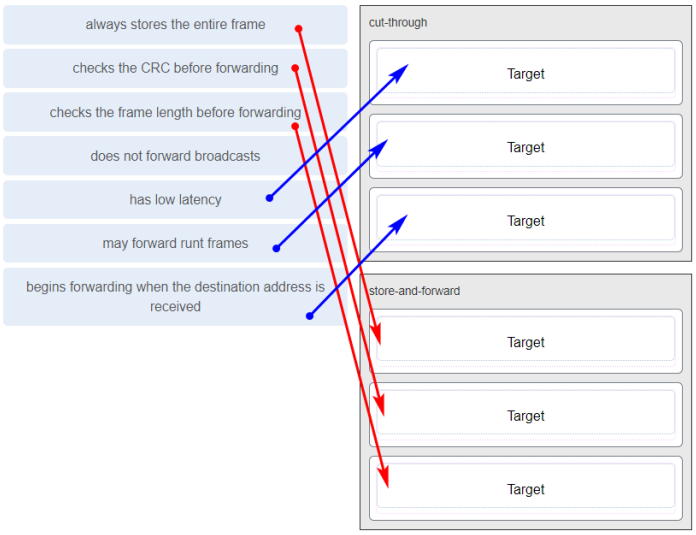
- **Match the application protocols to the correct transport protocols**



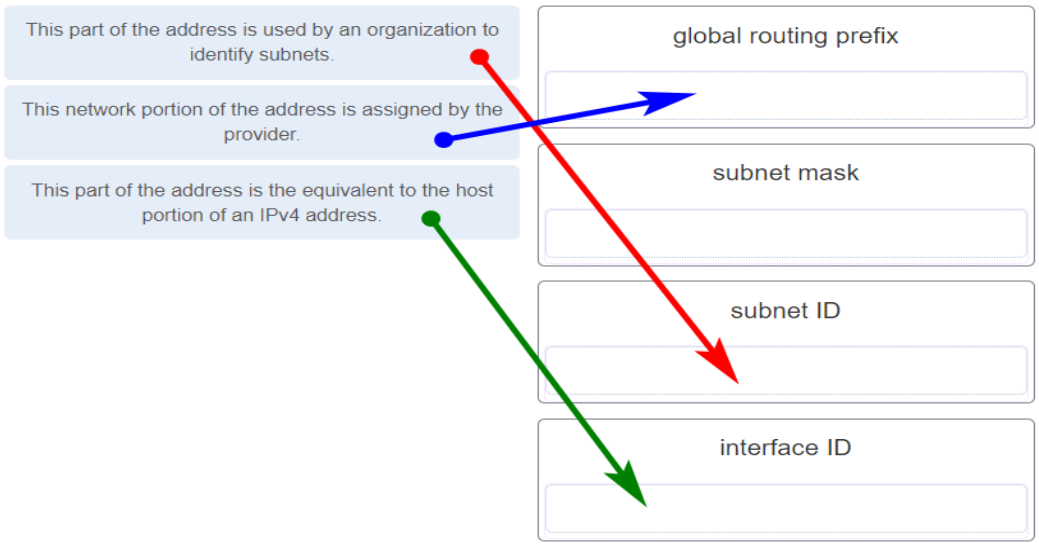
- **Match the characteristic to the category. (Not all options are used.)**



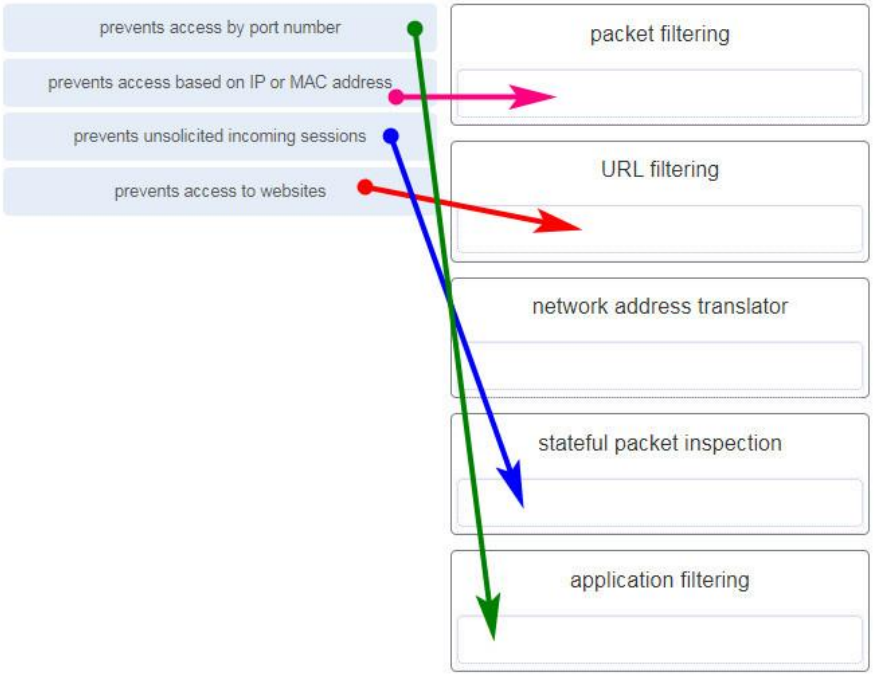
- **Match the characteristic to the forwarding method. (Not all options are used.)**



- **Match the description to the IPv6 addressing component. (Not all options are used.)**

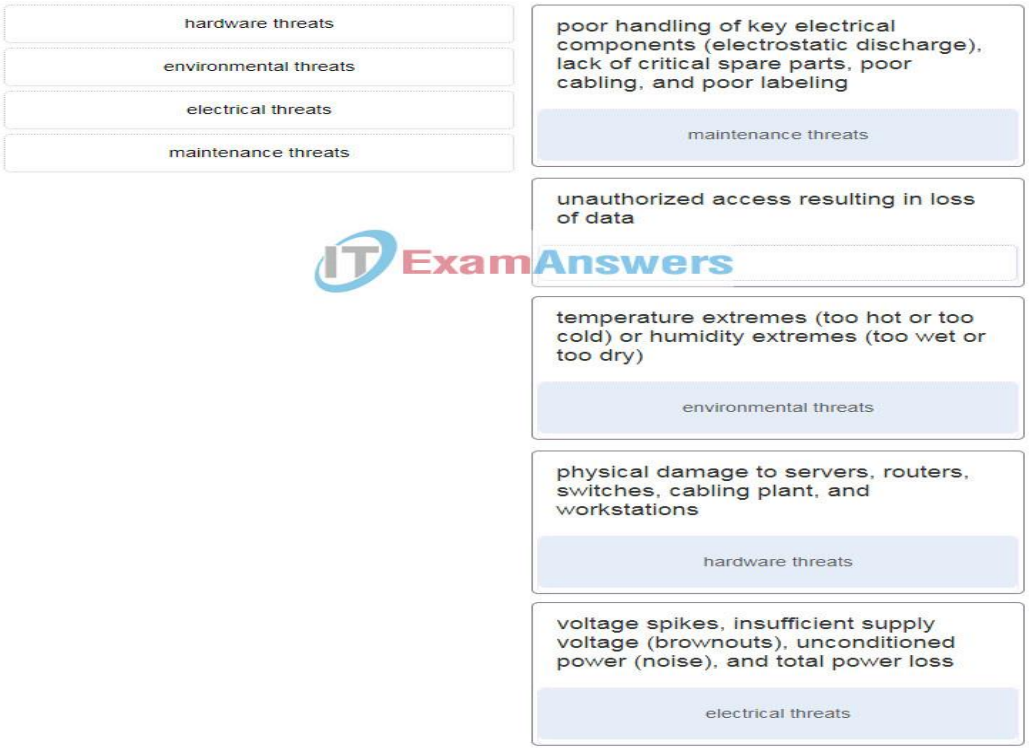


- **Match the firewall function to the type of threat protection it provides to the network. (Not all options are used.)**

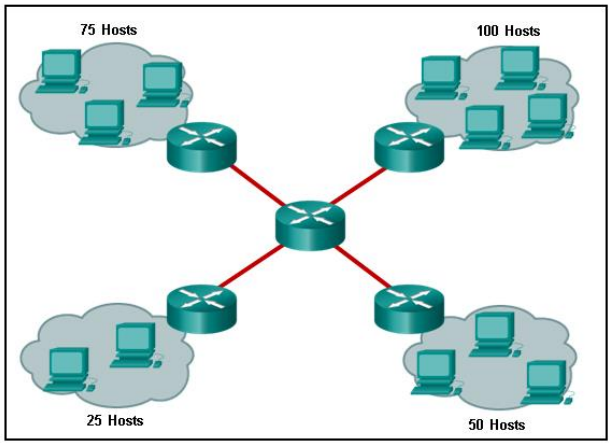


- **Match the header field with the appropriate layer of the OSI model. (Not all options are used.)**

- **Match the type of threat with the cause. (Not all options are used.)**

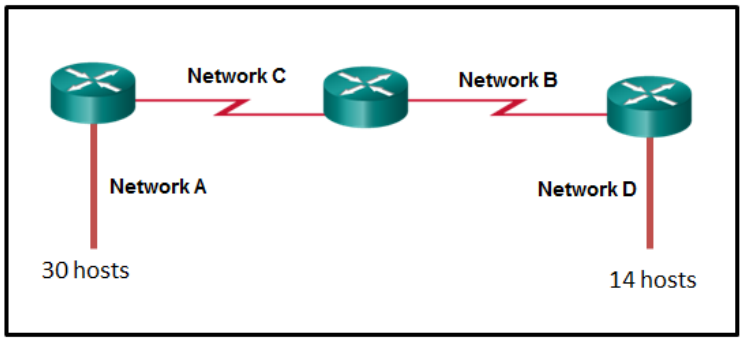


- **Refer to the exhibit. A company uses the address block of 128.107.0.0/16 for its network. What subnet mask would provide the maximum number of equal size subnets while providing enough host addresses for each subnet in the exhibit?**



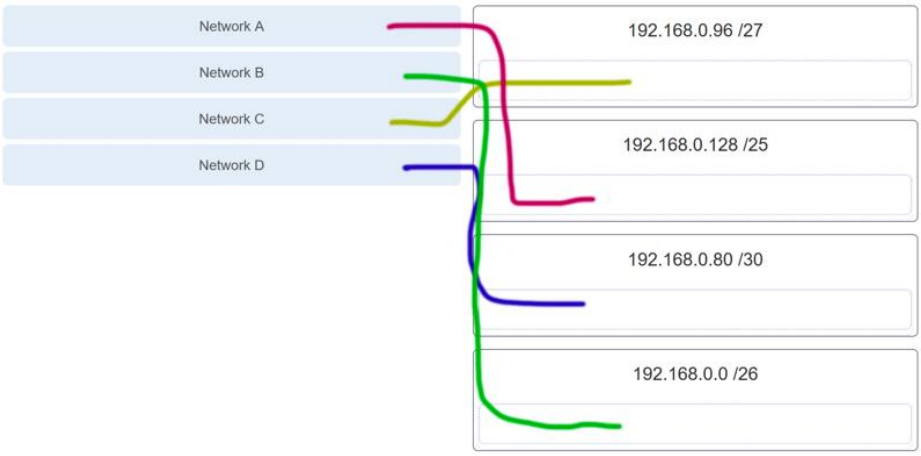
- 255.255.255.128

- **Refer to the exhibit. A network engineer has been given the network address of 192.168.99.0 and a subnet mask of 255.255.255.192 to subnet across the four networks shown. How many total host addresses are unused across all four subnets?**

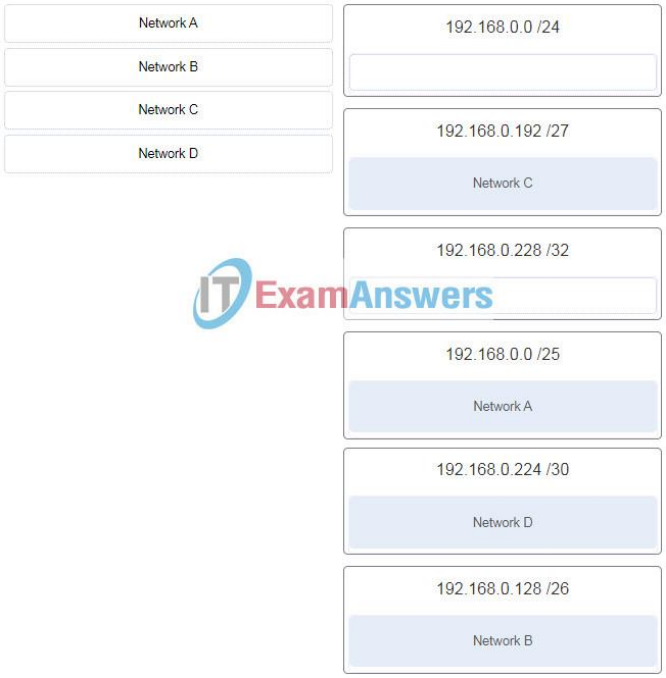


- 200

- **Which connector is used with twisted-pair cabling in an Ethernet LAN?**
  - RJ 45
- **Refer to the exhibit. An administrator is trying to configure the switch but receives the error message that is displayed in the exhibit. What is the problem?**
  - The administrator must first enter privileged EXEC mode before issuing the command.
- **Refer to the exhibit. Host B on subnet Teachers transmits a packet to host D on subnet Students. Which Layer 2 and Layer 3 addresses are contained in the PDUs that are transmitted from host B to the router?**
  - Layer 2 destination address = 00-00-0c-94-36-ab
    Layer 2 source address = 00-00-0c-94-36-bb
    Layer 3 destination address = 172.16.20.200
    Layer 3 source address = 172.16.10.200
- **Refer to the exhibit. If host A sends an IP packet to host B, what will the destination address be in the frame when it leaves host A?**
  - BB:BB:BB:BB:BB:BB
- **Refer to the exhibit. If Host1 were to transfer a file to the server, what layers of the TCP/IP model would be used?**
  - application, transport, Internet, and network access layers
- **Refer to the exhibit. If PC1 is sending a packet to PC2 and routing has been configured between the two routers, what will R1 do with the Ethernet frame header attached by PC1?**
  - remove the Ethernet header and configure a new Layer 2 header before sending it out S0/0/0
- **Refer to the exhibit. Match the network with the correct IP address and prefix that will satisfy the usable host addressing requirements for each network.**



- **Refer to the exhibit. Match the network with the correct IP address and prefix that will satisfy the usable host addressing requirements for each network. (Not all options are used.)**



- **Refer to the exhibit. On the basis of the output, which two statements about network connectivity are correct? (Choose two.)**
  - There are 4 hops between this device and the device at 192.168.100.1.
  - There is connectivity between this device and the device at 192.168.100.1.
- **Refer to the exhibit. PC1 issues an ARP request because it needs to send a packet to PC2. In this scenario, what will happen next?**
  - PC2 will send an ARP reply with the PC2 MAC address.
- **Refer to the exhibit. The IP address of which device interface should be used as the default gateway setting of host H1?**
  - R1: G0/0
- **Refer to the exhibit. The network administrator has assigned the LAN of LBMISS an address range of 192.168.10.0. This address range has been subnetted using a /29 prefix. In order to accommodate a new building, the technician has decided to use the fifth subnet for configuring the new network (subnet zero is the first subnet). By company policies, the router interface is always assigned the first usable host address and the workgroup server is given the last usable host address. Which configuration should be entered into the properties of the workgroup server to allow connectivity to the Internet?**
  - IP address: 192.168.10.38 subnet mask: 255.255.255.248, default gateway: 192.168.10.33
- **Refer to the exhibit. The switches are in their default configuration. Host A needs to communicate with host D, but host A does not have the MAC address for its default gateway. Which network hosts will receive the ARP request sent by host A?**
  - only hosts B, C, and router R1
- **Refer to the exhibit. What is wrong with the displayed termination?**
  - The untwisted length of each wire is too long.
- **Refer to the exhibit. What three facts can be determined from the viewable output of the show ip interface brief command? (Choose three.)**
  - The switch can be remotely managed.
  - One device is attached to a physical interface.

- The default SVI has been configured.

- **Refer to the exhibit. Which protocol was responsible for building the table that is shown?**
  - ARP
- **Refer to the exhibit. Which two network addresses can be assigned to the network containing 10 hosts? Your answers should waste the fewest addresses, not reuse addresses that are already assigned, and stay within the 10.18.10.0/24 range of addresses. (Choose two.)**
  - 10.18.10.208/28
  - 10.18.10.224/28
- **The global configuration command *ip default-gateway 172.16.100.1* is applied to a switch. What is the effect of this command?**
  - The switch can be remotely managed from a host on another network.
- **Three bank employees are using the corporate network. The first employee uses a web browser to view a company web page in order to read some announcements. The second employee accesses the corporate database to perform some financial transactions. The third employee participates in an important live audio conference with other corporate managers in branch offices. If QoS is implemented on this network, what will be the priorities from highest to lowest of the different data types?**
  - audio conference, financial transactions, web page
- **Two pings were issued from a host on a local network. The first ping was issued to the IP address of the default gateway of the host and it failed. The second ping was issued to the IP address of a host outside the local network and it was successful. What is a possible cause for the failed ping?**
  - Security rules are applied to the default gateway device, preventing it from processing ping requests.
- **Users are reporting longer delays in authentication and in accessing network resources during certain time periods of the week. What kind of information should network engineers check to find out if this situation is part of a normal network behavior?**
  - the network performance baseline
- **Users report that the network access is slow. After questioning the employees, the network administrator learned that one employee downloaded a third-party scanning program for the printer. What type of malware might be introduced that causes slow performance of the network?**
  - worm
- **What are proprietary protocols?**
  - protocols developed by organizations who have control over their definition and operation
- **What are the three parts of an IPv6 global unicast address? (Choose three.)**
  - subnet ID
  - global routing prefix
  - interface ID
- **What are the two most effective ways to defend against malware? (Choose two.)**
  - Update the operating system and other application software.
  - Install and update antivirus software.
- **What are three characteristics of the CSMA/CD process? (Choose three.)**
  - A device listens and waits until the media is not busy before transmitting.
  - After detecting a collision, hosts can attempt to resume transmission after a random time delay has expired.
  - All of the devices on a segment see data that passes on the network medium.
- **What are three commonly followed standards for constructing and installing cabling? (Choose three.)**
  - cable lengths
  - pinouts
  - connector types
- **What are two characteristics of IP? (Choose two.)**
  - does not require a dedicated end-to-end connection
  - operates independently of the network media
- **What are two characteristics shared by TCP and UDP? (Choose two.)**
  - port numbering
  - use of checksum
- **What are two common causes of signal degradation when using UTP cabling? (Choose two.)**
  - improper termination
  - low-quality cable or connectors
- **What are two features of ARP? (Choose two.)**
  - If a host is ready to send a packet to a local destination device and it has the IP address but not the MAC address of the destination, it generates an ARP broadcast.
  - If a device receiving an ARP request has the destination IPv4 address, it responds with an ARP reply.

- **What are two functions that are provided by the network layer? (Choose two.)**
  - directing data packets to destination hosts on other networks
  - providing end devices with a unique network identifier
- **What are two ICMPv6 messages that are not present in ICMP for IPv4? (Choose two.)**
  - Neighbor Solicitation
  - Router Advertisement
- **What are two primary responsibilities of the Ethernet MAC sublayer? (Choose two.)**
  - accessing the media
  - data encapsulation
- **What are two problems that can be caused by a large number of ARP request and reply messages? (Choose two.)**
  - The ARP request is sent as a broadcast, and will flood the entire subnet.
  - All ARP request messages must be processed by all nodes on the local network.
- **What attribute of a NIC would place it at the data link layer of the OSI model?**
  - MAC address
- **What characteristic describes a DoS attack?**
  - an attack that slows or crashes a device or network service
- **What characteristic describes a Trojan horse?**
  - malicious software or code running on an end device
- **What characteristic describes a virus?**
  - malicious software or code running on an end device
- **What characteristic describes a VPN?**
  - a tunneling protocol that provides remote users with secure access into the network of an organization
- **What characteristic describes adware?**
  - software that is installed on a user device and collects information about the user
- **What characteristic describes an IPS?**
  - a network device that filters access and traffic coming into a network
- **What characteristic describes antispyware?**
  - applications that protect end devices from becoming infected with malicious software
- **What characteristic describes identity theft?**
  - the use of stolen credentials to access private data
- **What characteristic describes spyware?**
  - software that is installed on a user device and collects information about the user
- **What command can be used on a Windows PC to see the IP configuration of that computer?**
  - Ipconfig
- **What does the term “attenuation” mean in data communication?**
  - loss of signal strength as distance increases
- **What happens when the *transport input ssh* command is entered on the switch vty lines?**
  - Communication between the switch and remote users is encrypted.
- **What is a benefit of using cloud computing in networking?**
  - Network capabilities are extended without requiring investment in new infrastructure, personnel, or software.
- **What is a function of the data link layer?**
  - provides for the exchange of frames over a common local media
- **What is an advantage for small organizations of adopting IMAP instead of POP?**
  - Messages are kept in the mail servers until they are manually deleted from the email client.
- **What is an advantage to using a protocol that is defined by an open standard?**
  - It encourages competition and promotes choices.
- **What is one main characteristic of the data link layer?**
  - It shields the upper layer protocol from being aware of the physical medium to be used in the communication.
- **What is the consequence of configuring a router with the *ipv6 unicast-routing* global configuration command?**
  - The IPv6 enabled router interfaces begin sending ICMPv6 Router Advertisement messages.
- **What is the purpose of the TCP sliding window?**
  - to request that a source decrease the rate at which it transmits data
- **What is the subnet ID associated with the IPv6 address**
  - 2001:DA48:FC5:A4:3D1B::1/64?2001:DA48:FC5:A4::/64
- **What mechanism is used by a router to prevent a received IPv4 packet from traveling endlessly on a network?**

- It decrements the value of the TTL field by 1 and if the result is 0, it discards the packet and sends a Time Exceeded message to the source host.

- **What method is used to manage contention-based access on a wireless network?**
  - CSMA/CA
- **What service is provided by BOOTP?**
  - Legacy application that enables a diskless workstation to discover its own IP address and find a BOOTP server on the network.
- **What service is provided by DHCP?**
  - Dynamically assigns IP addresses to end and intermediary devices.
- **What service is provided by DNS?**
  - Resolves domain names, such as cisco.com, into IP addresses.
- **What service is provided by FTP?**
  - Allows for data transfers between a client and a file server.
- **What service is provided by HTTP?**
  - A basic set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the web.
- **What service is provided by HTTPS?**
  - Uses encryption to secure the exchange of text, graphic images, sound, and video on the web.
- **What service is provided by Internet Messenger?**
  - An application that allows real-time chatting among remote users.
- **What service is provided by POP3?**
  - Retrieves email from the server by downloading the email to the local mail application of the client.
- **What service is provided by SMTP?**
  - Allows clients to send email to a mail server and the servers to send email to other servers.
- **What subnet mask is needed if an IPv4 network has 40 devices that need IP addresses and address space is not to be wasted?**
  - 255.255.255.192
- **What technique is used with UTP cable to help protect against signal interference from crosstalk?**
  - twisting the wires together into pairs
- **What three requirements are defined by the protocols used in network communcations to allow message transmission across a network? (Choose three.)**
  - message size
  - message encoding
  - delivery options
- **What two ICMPv6 message types must be permitted through IPv6 access control lists to allow resolution of Layer 3 addresses to Layer 2 MAC addresses? (Choose two.)**
  - neighbor solicitations
  - neighbor advertisements
- **What two pieces of information are displayed in the output of the show ip interface brief command? (Choose two.)**
  - IP addresses
  - Layer 1 statuses
- **What two security solutions are most likely to be used only in a corporate environment? (Choose two.)**
  - virtual private networks
  - intrusion prevention systems
- **What will happen if the default gateway address is incorrectly configured on a host?**
  - The host cannot communicate with hosts in other networks.
- **What would be the interface ID of an IPv6 enabled interface with a MAC address of 1C-6F-65-C2-BD-F8 when the interface ID is generated by using the EUI-64 process?**
  - 1E6F:65FF:FEC2:BDF8
- **When a switch configuration includes a user-defined error threshold on a per-port basis, to which switching method will the switch revert when the error threshold is reached?**
  - store-and-forward
- **Which frame field is created by a source node and used by a destination node to ensure that a transmitted data signal has not been altered by interference, distortion, or signal loss?**
  - frame check sequence field
- **Which information does the show startup-config command display?**
  - the contents of the saved configuration file in the NVRAM

- **Which layer of the TCP/IP model provides a route to forward messages through an internetwork?**
  - Internet
- **Which range of link-local addresses can be assigned to an IPv6-enabled interface?**
  - FE80::/10
- **Which scenario describes a function provided by the transport layer?**
  - A student has two web browser windows open in order to access two web sites. The transport layer ensures the correct web page is delivered to the correct browser window.
- **Which subnet would include the address 192.168.1.96 as a usable host address?**
  - 192.168.1.64/26
- **Which switching method drops frames that fail the FCS check?**
  - store-and-forward switching
- **Which three layers of the OSI model map to the application layer of the TCP/IP model? (Choose three.)**
  - Application
  - Session
  - Presentation
- **Which two commands can be used on a Windows host to display the routing table? (Choose two.)**
  - route print
  - netstat –r
- **Which two functions are performed at the LLC sublayer of the OSI Data Link Layer to facilitate Ethernet communication? (Choose two.)**
  - enables IPv4 and IPv6 to utilize the same physical medium
  - places information in the Ethernet frame that identifies which network layer protocol is being encapsulated by the frame

    Other case:
  - handles communication between upper layer networking software and Ethernet NIC hardware
  - adds Ethernet control information to network protocol data

    Other case:
  - places information in the Ethernet frame that identifies which network layer protocol is being encapsulated by the frame
  - adds Ethernet control information to network protocol data

    Other case:
  - enables IPv4 and IPv6 to utilize the same physical medium
  - adds Ethernet control information to network protocol data

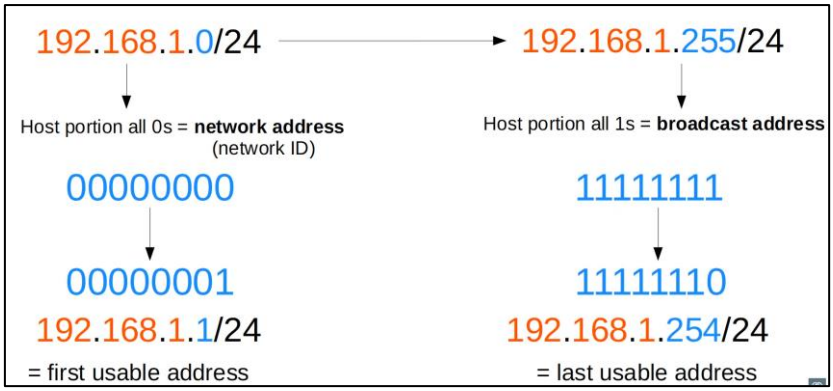
    Other case:
  - enables IPv4 and IPv6 to utilize the same physical medium
  - handles communication between upper layer networking software and Ethernet NIC hardware
- **Which two protocols operate at the top layer of the TCP/IP protocol suite? (Choose two.)**
  - POP
  - DNS
- **Which two statements accurately describe an advantage or a disadvantage when deploying NAT for IPv4 in a network? (Choose two.)**
  - NAT introduces problems for some applications that require end-to-end connectivity.
  - NAT provides a solution to slow down the IPv4 address depletion.
- **Which two statements are correct about MAC and IP addresses during data transmission if NAT is not involved? (Choose two.)**
  - Destination IP addresses in a packet header remain constant along the entire path to a target host.
  - Destination and source MAC addresses have local significance and change every time a frame goes from one LAN to another.
- **Which two statements are correct in a comparison of IPv4 and IPv6 packet headers? (Choose two.)**
  - The Source Address field name from IPv4 is kept in IPv6.
  - The Time-to-Live field from IPv4 has been replaced by the Hop Limit field in IPv6.
- **Which two statements describe features of an IPv4 routing table on a router? (Choose two.)**
  - It stores information about routes derived from the active router interfaces.
  - If a default static route is configured in the router, an entry will be included in the routing table with source code S.
- **Which two statements describe how to assess traffic flow patterns and network traffic types using a protocol analyzer? (Choose two.)**
  - Capture traffic during peak utilization times to get a good representation of the different traffic types.
  - Perform the capture on different network segments.
- **Which two traffic types use the Real-Time Transport Protocol (RTP)? (Choose two.)**

- Video
- Voice

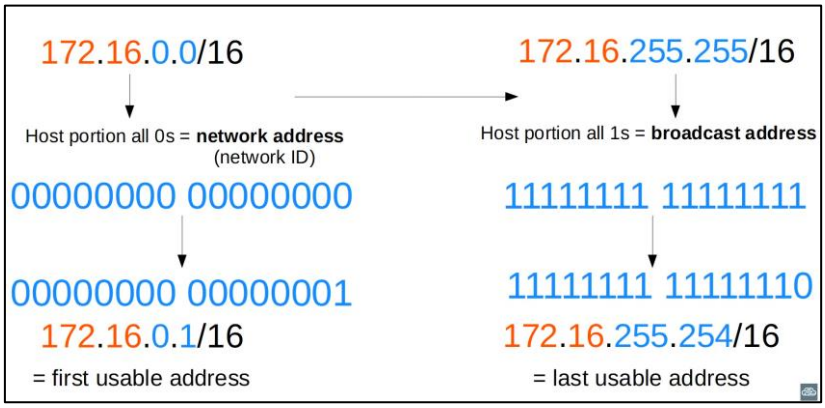
- **Which type of security threat would be responsible if a spreadsheet add-on disables the local software firewall?**
  - Trojan horse
- **Which type of server relies on record types such as A, NS, AAAA, and MX in order to provide services?**
  - DNS
- **Which value, that is contained in an IPv4 header field, is decremented by each router that receives a packet?**
  - Time-to-Live
- **Which wireless technology has low-power and data rate requirements making it popular in home automation applications?**
  - ZigBee
- **Which wireless technology has low-power and low-data rate requirements making it popular in IoT environments?**
  - Zigbee
- **Why would a Layer 2 switch need an IP address?**
  - to enable the switch to be managed remotely

FIRST/LAST USABLE ADDRESS

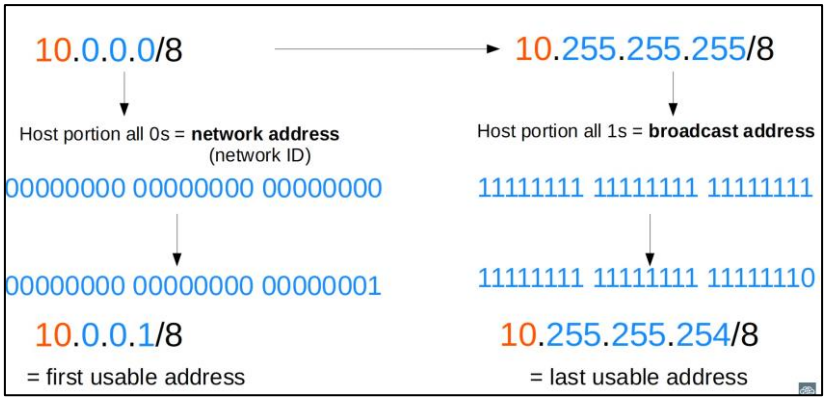
Class C:



Class B:



Class A:

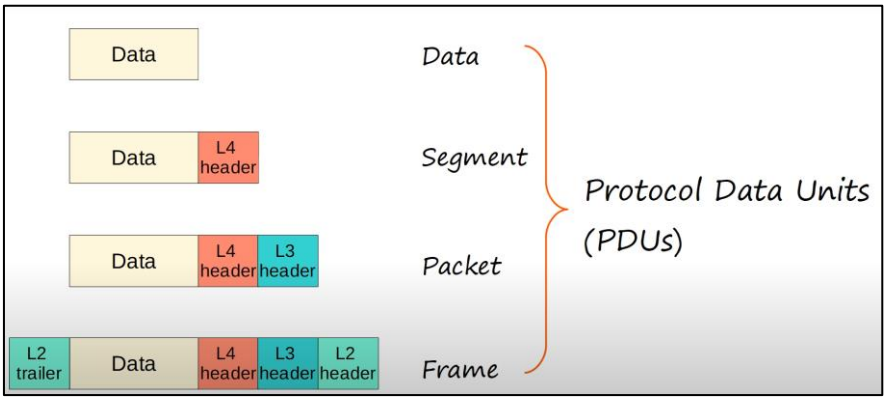


IP

IPV4

IPV4 HEADER

OSI Model and PDUs:



IPV6

Possible questions and answers:

- **An IPv6 enabled device sends a data packet with the destination address of FF02::2. What is the target of this packet?**
  - all IPv6 configured routers on the local link
- **An organization is assigned an IPv6 address block of 2001:db8:0:ca00::/56. How many subnets can be created without using bits in the interface ID space?**
  - 256
- **Data is being sent from a source PC to a destination server. Which three statements correctly describe the function of TCP or UDP in this situation? (Choose three.)**
  - The source port field identifies the running application or service that will handle data returning to the PC.
  - UDP segments are encapsulated within IP packets for transport across the network.
  - The UDP destination port number identifies the application or service on the server which will handle the data.
- **During the process of forwarding traffic, what will the router do immediately after matching the destination IP address to a network on a directly connected routing table entry?**
  - switch the packet to the directly connected interface
-
  -
-
  -
-
  -
-
  -
-
  -
-
  -

ROUTING

ROUTING FUNDAMENTALS

What is it:

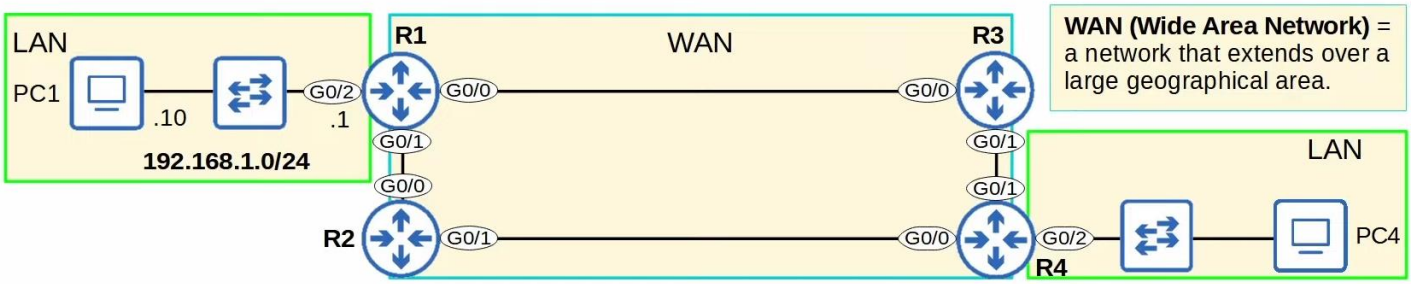
- Routing is the process that routers use to determine the path that IP packets should take over a network to reach their destination.
    - Routers store routes to all their known destinations in a routing table.
    - When routers receive packets, they look in the routing table to find the best route to forward that packet.
- There are two main routing methods (methods that routers use to learn routes):
  Dynamic Routing: Routers use dynamic routing protocols (ie. OSPF) to share routing information with each other automatically and build their routing tables.

The next slides is going to be pictures, since its very text and image based:

Static Routing: A network engineer/admin manually configures routes on the router.
→We will cover this in the next video.

next-hop = the next router in the path to the destination.

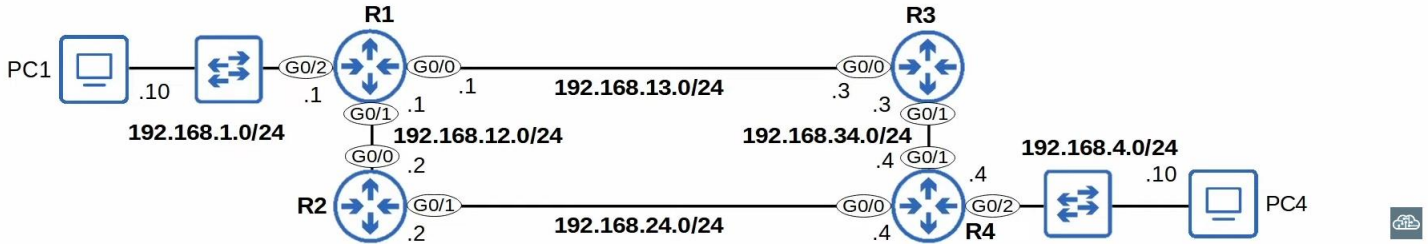
A **route** tells the router: *to send a packet to destination X, you should send the packet to* ***next-hop*** *Y.*
→or, if the destination is directly connected to the router, *send the packet directly to the destination.*
→or, if the destination is the router's own IP address, *receive the packet for yourself (don't forward it).*



The Routing table need to know where to send the packet, or else it is not going to be received. Commands like "Router Rip is used here to notify routers of other routers LANs, so each router know here each LAN is.

```
R1# conf t
R1(config)# interface g0/0
R1(config-if)# ip address 192.168.13.1 255.255.255.0
R1(config-if)# no shutdown

R1(config-if)# interface g0/1
R1(config-if)# ip address 192.168.12.1 255.255.255.0
R1(config-if)# no shutdown

R1(config-if)# interface g0/2
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown

R1# show ip int br
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         192.168.13.1    YES manual up                    up
GigabitEthernet0/1         192.168.12.1    YES manual up                    up
GigabitEthernet0/2         192.168.1.1     YES manual up                    up
GigabitEthernet0/3         unassigned      YES NVRAM  administratively down down
```

There is no need to use **`exit`** to return to global config mode before entering **`interface g0/1`**. You can use the **`interface g0/1`** command directly from interface config mode.



Show IP route:

```
R1# show ip route
```

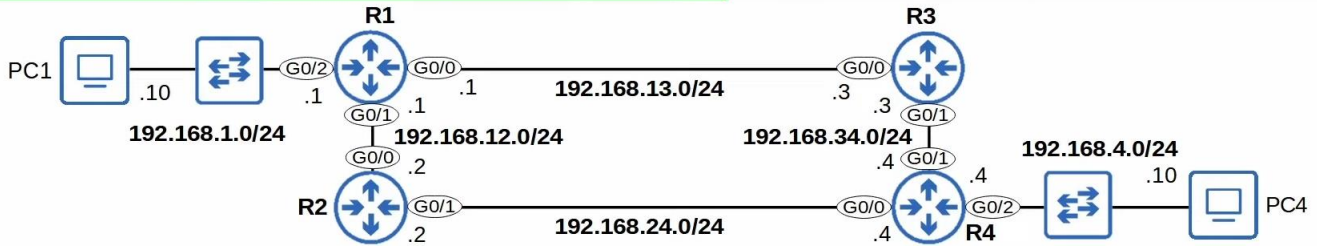
Use the command **`show ip route`** to view the routing table.

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/2
L        192.168.1.1/32 is directly connected, GigabitEthernet0/2
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, GigabitEthernet0/1
L        192.168.12.1/32 is directly connected, GigabitEthernet0/1
      192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.13.0/24 is directly connected, GigabitEthernet0/0
L        192.168.13.1/32 is directly connected, GigabitEthernet0/0
```

The Codes legend in the output of **`show ip route`** lists the different protocols which routers can use to learn routes.

- **L - local**
  → A route to the actual IP address configured on the interface. (with a /32 netmask)
- **C - connected**
  → A route to the network the interface is connected to. (with the actual netmask configured on the interface)

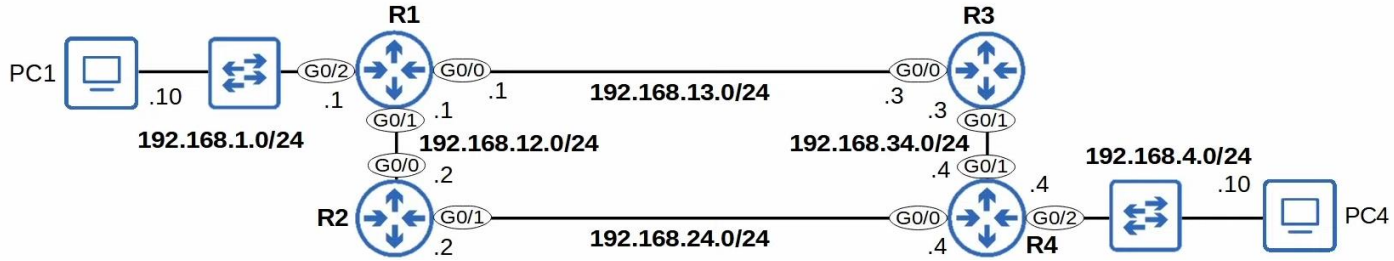
When you configure an IP address on an interface and enable it with **`no shutdown`**, 2 routes (per interface) will automatically be added to the routing table:
→ a **connected** route
→ a **local** route




```
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/2
L        192.168.1.1/32 is directly connected, GigabitEthernet0/2
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, GigabitEthernet0/1
L        192.168.12.1/32 is directly connected, GigabitEthernet0/1
      192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.13.0/24 is directly connected, GigabitEthernet0/0
L        192.168.13.1/32 is directly connected, GigabitEthernet0/0
```

- A **connected** route is a route to the network the interface is connected to.
- R1 G0/2 IP = 192.168.1.1/24
- Network Address = 192.168.1.0/24
- It provides a route to all hosts in that network (ie. 192.168.1.10, 192.168.1.100, 192.168.1.232, etc.)
- R1 knows: “If I need to send a packet to any host in the 192.168.1.0/24 network, I should send it out of G0/2”.

- A **local** route is a route to the exact IP address configured on the interface.
- A /32 netmask is used to specify the exact IP address of the interface.
  →/32 means all 32 bits are ‘fixed’, they can’t change.
- Even though R1’s G0/2 is configured as 192.168.1.1/24, the connected route is to 192.168.1.1/32.
- R1 knows: “If I receive a packet destined for this IP address, the message is for me”.



192 . 168 . 1 . 0 /24

255 . 255 . 255 . 0

=FIXED (can't change)

=not fixed

```
C        192.168.1.0/24 is directly connected, GigabitEthernet0/2
```

- **192.168.1.0/24** *matches* 192.168.1.0 ~ 192.168.1.255.
  →If R1 receives a packet with a destination in that range, it will send the packet out of G0/2.

A route **matches** a packet's destination if the packet's destination IP address is part of the network specified in the route.

192.168.1.2 = **match**
→Send packet out of G0/2
192.168.1.7 = **match**
→Send packet out of G0/2
192.168.1.89 = **match**
→Send packet out of G0/2
192.168.2.1 = **no match**
→Send the packet using a different route, or drop the packet if there is no matching route.

```
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/2
L        192.168.1.1/32 is directly connected, GigabitEthernet0/2
```

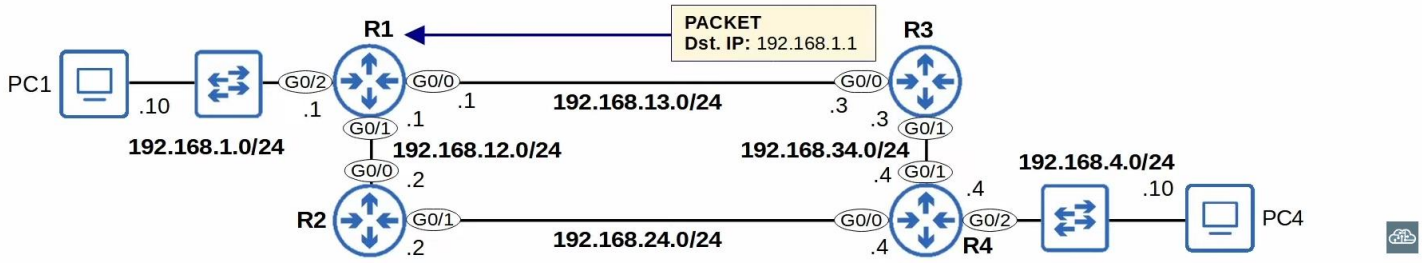
- A packet destined for **192.168.1.1** is matched by both routes:
  192.168.1.0/24
  192.168.1.1/32

When R1 receives a packet destined for 192.168.1.1, it will select the route to 192.168.1.1/32.
→R1 will receive the packet for itself, rather than forward it out of G0/2.
Local route = keep the packet, don't forward

- Which route will R1 use for a packet destined for 192.168.1.1?
  →It will choose the **most specific** matching route.

- The route to **192.168.1.0/24** includes 256 different IP addresses (192.168.1.0 – 192.168.1.255)
- The route to **192.168.1.1/32** includes only 1 IP address (192.168.1.1)
  →This route is more **specific**.

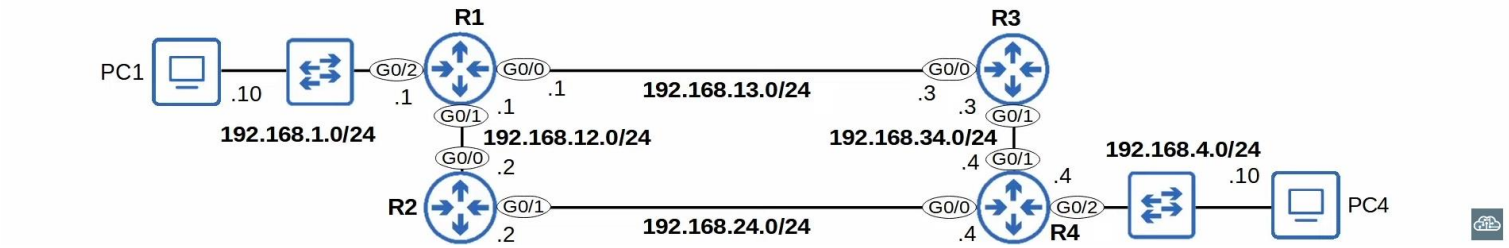
- **Most specific** matching route = the matching route with the **longest prefix length**.



```
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/2
L        192.168.1.1/32 is directly connected, GigabitEthernet0/2
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, GigabitEthernet0/1
L        192.168.12.1/32 is directly connected, GigabitEthernet0/1
      192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.13.0/24 is directly connected, GigabitEthernet0/0
L        192.168.13.1/32 is directly connected, GigabitEthernet0/0
```

- These three lines are not routes. They mean the following:
- `192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks`
  →In the routing table, there are two routes to *subnets* that fit within the 192.168.1.0/24 Class C network, with two different netmasks (/24 and /32).
- `192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks`
  →In the routing table, there are two routes to *subnets* that fit within the 192.168.12.0/24 Class C network, with two different netmasks (/24 and /32).
- `192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks`
  →In the routing table, there are two routes to *subnets* that fit within the 192.168.13.0/24 Class C network, with two different netmasks (/24 and /32).

- We will cover **subnetting** soon (in another video)! For now, I just wanted to point out that these three lines are not routes.



Summary:

- Routers store information about destinations they know in their **routing table**.
  → When they receive packets, the look in the routing table to find the best route to forward the packet.

- Each **route** in the routing table is an instruction:
  → To reach destinations in network X, send the packet to **next-hop** Y (the next router in the path to the destination).
  → If the destination is directly connected (**Connected** route) send the packet directly to the destination.
  → If the destination if your own IP address (**Local** route), receive the packet for yourself.
  *We will look at how **next-hops** work in the next video on **static routes**.

- When you configure an IP address on an interface and enable the interface, two routes are automatically added to the routing table:
  Connected route (code **C** in the routing table): A route to the network connected to the interface.
  → ie. if the interface's IP is **192.168.1.1/24**, the route will be to **192.168.1.0/24**.
  → Tells the router: "To send a packet to a destination in this network, send it out of the interface specified in the route".

  Local route (code **L** in the routing table): A route to the exact IP address configured on the interface.
  → ie. if the interface's IP is **192.168.1.1/24**, the route will be to **192.168.1.1/32**.
  → Tells the router: "Packets to this destination are for you. You should receive them for yourself (not forward them)".

- A route **matches** a destination if the packet's destination IP address is part of the network specified in the route.
  → ie. a packet to **192.168.1.60** is matched by a route to **192.168.1.0/24**, but not by a route to **192.168.0.0/24**.

- If a router receives a packet and it doesn't have a route that matches the packet's destination, it will **drop** the packet.
  → This is different than switches, which **flood** frames if they don't have a MAC table entry for the destination.

- If a router receives a packet and it has multiple routes that match the packet's destination, it will use the ***most specific*** *matching route* to forward the packet.
  → **Most specific** matching route = the matching route with the longest prefix length.
  → This is different than switches, which look for an **exact** match in the MAC address table to forward frames.

STATIC ROUTING

Default Gateway:

- The default gateway is used when hosts need to send packets to destinations outside their local network (LAN). The hosts do this by sending the packet to their default gateway. You can read more in-depth under here:

End hosts like PC1 and PC4 can send packets directly to destinations in their connected network.
→ PC1 is connected to 192.168.1.0/24, PC4 is connected to 192.168.4.0/24.

To send packets to destinations outside of their local network, they must send the packets to their **default gateway**.

PC1 (Linux) Config:

```
iface eth0 inet static
        address 192.168.1.10/24
        gateway 192.168.1.1
```

PC4 (Linux) Config:

```
iface eth0 inet static
        address 192.168.4.10/24
        gateway 192.168.4.4
```

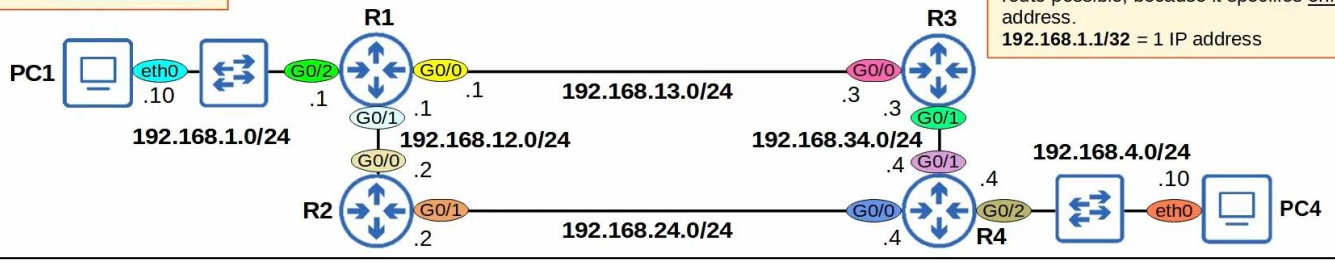
The **default gateway** configuration is also called a **default route**.
→ It is a route to 0.0.0.0/0 = all netmask bits set to 0. Includes all addresses from 0.0.0.0 to 255.255.255.255.

End hosts usually have no need for any more specific routes.
→ They just need to know: to send packets outside of my local network, I should send them to my default gateway.

Src. IP: 192.168.1.10
Dst. IP: 192.168.4.10
Dst. MAC: R1 **G0/2** MAC
Src. MAC: PC1 **eth0** MAC

*to learn R1 G0/2's MAC address, PC1 will first send an ARP request to 192.168.1.1.

The **default route** is the *least specific* route possible, because it includes all IP addresses.
0.0.0.0/0 = 4,294,967,296 IP addresses
A /32 route (ie. Local route) is the *most specific* route possible, because it specifies only one IP address.
192.168.1.1/32 = 1 IP address



When R1 receives the frame from PC1, it will de-encapsulate it (remove L2 header/trailer) and look at the inside packet.

It will check the routing table for the most-specific matching route:

```
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/2
L        192.168.1.1/32 is directly connected, GigabitEthernet0/2
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, GigabitEthernet0/1
L        192.168.12.1/32 is directly connected, GigabitEthernet0/1
      192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.13.0/24 is directly connected, GigabitEthernet0/0
L        192.168.13.1/32 is directly connected, GigabitEthernet0/0
```

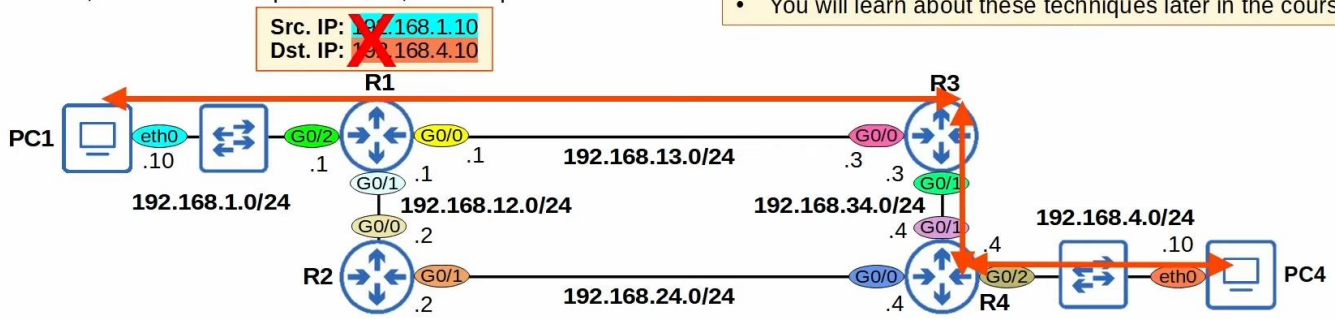
R1 has no matching routes in its routing table.
→It will drop the packet.

To properly forward the packet, R1 needs a route to the destination network (192.168.4.0/24).
→Routes are instructions: *To send a packet to destinations in network 192.168.4.0/24, forward the packet to next hop Y.*

There are two possible path packets from PC1 to PC4 can take:
1) PC1 → R1 → R3 → R4 →PC4
2) PC1 → R1 → R2 → R4 →PC4

In this video, we will use the path via R3, not the path via R2.

- It is possible to configure the routers to:
  → *load-balance* between path **1)** and **2)**
  → Use path **1)** as the main path and path **2)** as a backup path
- You will learn about these techniques later in the course.



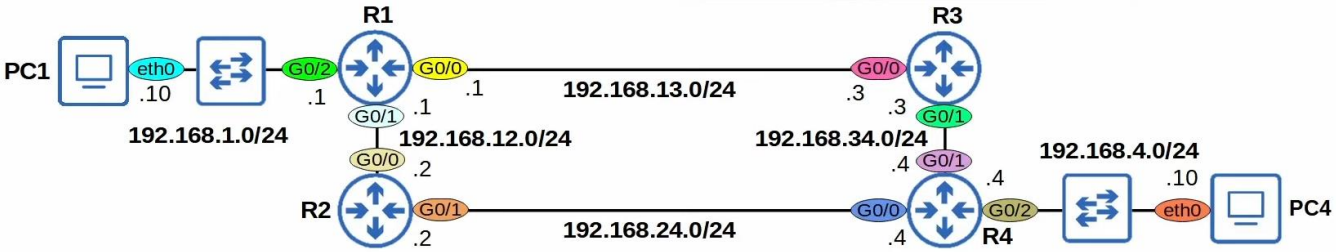
Each router in the path needs two routes: a route to 192.168.1.0/24 and a route to 192.168.4.0/24.
→This ensures **two-way reachability** (PC1 can send packets to PC4, PC4 can send packets to PC1).

R1 already has a **Connected route** to 192.168.1.0/24. R4 already has a **Connected route** to 192.168.4.0/24.
→The other routes must be manually configured (using **Static routes**).

*routers don't need routes to all networks in the path to the destination.
→R1 doesn't need a route to 192.168.34.0/24.
→R4 doesn't need a route to 192.168.13.0/24.

To allow PC1 and PC4 to communicate with each other over the network, let's configure these **Static routes** on R1, R3, and R4.

Router	Destination	Next-Hop
R1	192.168.1.0/24	Connected
	192.168.4.0/24	192.168.13.3
R3	192.168.1.0/24	192.168.13.1
	192.168.4.0/24	192.168.34.4
R4	192.168.1.0/24	192.168.34.3
	192.168.4.0/24	Connected



CISCO PACKET TRACER

WHAT IS IT?

Packet tracer:

- Packet tracer is free, quick, easy to set up, and lets you create simulated network labs without having to buy any hardware.

SETTINGS

"Show Device Model Labels":

- What does it do:

- Shows model-names for devices, in the 'Logical' menu, making it easier to see the devices used in the network.
- Find the setting:
  - 'Preferences' → 'Interface' → *Click* 'Show Device Model Labels'

"Show Device Name Labels":

- What does it do:
  - Shows the names you have created for the devices, placed in the 'Logical' menu, making it easier organize every component in the network.
- Find the setting:
  - 'Preferences' → 'Interface' → *Click* 'Show Device Name Labels'

"Font-size":

- What does it do:
  - Changes the font-size in the application, for example all the menu font sizes or the font-sizes in the devices 'CLI' (Command Line Interface).
- Find the setting:
  - 'Preferences' → 'Font' → *Look under* 'Application' → *Slide* 'Size'

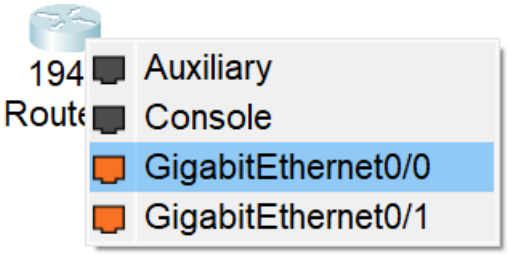
"Font-color":

- What does it do:
  - Changes the font-color in the application, for example all the menu font-color or the font-color in the devices 'CLI' (Command Line Interface).
- Find the setting:
  - 'Preferences' → 'Font' → *Look under* 'Colors' → *Select the color you want*

CABLES AND INPUTS

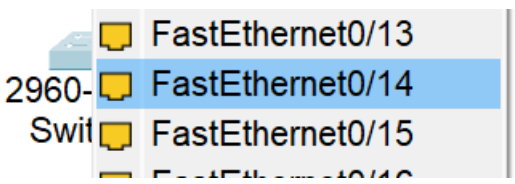
- Purpose
  - The purpose of cables and input is to connect devices in the network.
- Different cables to the right port
  - It's a good idea to use different cables depending on the network your connecting, since don't need to pay more for something you don't need. By using the right cables for different scenarios, we ensure that our network is connected in a way that is sufficient.
  - When the distance between a router or switch is more than the maximum length of UTP cables (100m), use Fiber-Optic cables and connect it to 'GigabitEthernet'.

Fiber



  - When the distance between a router or switch is less or equal to UTP cables, use UTP cables and connect it to 'FastEthernet'.

Copper Straight-Through



DEVICE SYMBOLS

Router:

Switch:

Firewall:

Cloud (Internet):

Server:

Printer:

Typical end-device (PC):

COMMANDS