2. Answer the 15 questions posted in the Switches/Bridges/ video submit your answers in one pdf file.

2.1 How does the FCS field in Ethernet provide error recovery?

Corrupted data frames typically occur during the transmission of data frames through a communication medium. FCS bits are added before the frame is transferred across the network. If the FCS codes match, transmission is regarded successful; otherwise, frames are erased. The FCS code is once again generated at the destination site and compared with the FCS bits of the frame. It is used in error detection as a result. FCS is just used for error detection; it doesn't offer any information on error recovery. The only basis for the error recovery technique is the transmission protocol.

When a message is sent to a recipient using the Ethernet protocol, it is divided into data frames with FCS bits attached to each frame, which are then sent via the medium. The FCS bits of any problematic frames will be changed during transmission. Each frame's FCS is determined at the destination and contrasted with the FCS bits; if the corrupted frame's FCS does not match the computed FCS, it is discarded. Data would be lost since Ethernet does not outline what should be done in the event of mistake detection, such as retransmitting a flawed frame.

2.2 When is CSMA/CD used?

Because numerous stations in a wireless network regularly use the same AP (Access Point), there is a danger of a network collision, which is why wireless networks use CSMA/CA (Carrier Sence Multiple Access/ Collision Avoidance).

Collision Avoidance (CSMA/CA) holds out on sending data until the transmission signal has been received in order to avoid collisions. If a signal is received, the transmitter starts a counter value with a random number and waits. If this counter is exhausted, the sender will attempt again. This process is repeated until all the data has to be communicated. When this counter expires or decreases, the sender can send the data.

2.3 What are the five primary functions that make bridges and switches intelligent?

Five primary functions that make bridges and switches intelligent are:

- Forwarding

- Learning

- Filtering

- Aging

- Flooding

2.4 What layers do switches and hubs operate at?

Long ago, hubs were used to connect various network devices in a Local Area Network (LAN), but network switches have since taken their place. These days, seeing a network hub active in a live local area network is rather challenging (LAN). Hubs serve as the primary Local Area Network connection point (LAN). Hubs were made to function in Ethernet networks using twisted pair cables and RJ45 jacks to link various network devices. Individual network cables are used to connect network devices (servers, workstations, printers, scanners, etc.) to the hub. Different designs and numbers of ports were offered for hubs.

A hub broadcasts (repeats) a packet of data (an Ethernet frame) that it receives from a network device at one of its ports to all of the other network devices. Hubs are thought to function at the Physical Layer (Layer 1) of the OSI model, which occurs when two network devices on the same network attempt to send packets at the same time. Below is a picture of an 8 port hub.

By evaluating the Data Link Layer (Layer 2) data packet (Ethernet Frame) and forwarding the packet to other network devices based on Layer 2 addresses, a bridge or switch accomplishes its function (MAC Addresses). In an Ethernet-based LAN, both switches and bridges use the Datalink Layer (Layer 2) addressing scheme, often known as MAC addresses, to forward Ethernet frames from one device to another (Local Area Network).

A network switch can partition a large collision domain into numerous smaller collision domains since each port is in its own collision domain. Only a few collision domains, or hosts, are connected by the bridge, which only has a few ports. Comparatively speaking, a bridge has fewer ports than a switch. In the market, network switches with 24 or 48 ports are frequently found. In terms of the OSI model, switches and brides are thought to function at the DataLink Layer (Layer 2).

2.5 What is the differences between switches and hubs?

The differences between switches and hubs are as follow:

Switches	Hubs
Given that a switch is an intelligent device that sends messages to certain destinations, it is expensive.	Because it is not an intelligent device that sends messages to all ports, the hub is relatively inexpensive.
Each port in a switch has its own collision domain.	In hubs, there is only one collision domain.
Can be used as repeater	Cannot be used as repeater.
Can have 24 to 48 ports.	Has 4/12 ports.
Uses full duplex transmission mode	Uses half duplex transmission mode
Operates on the data link layer	Operates on the physical layer.

2.6 How do switches learn the MAC addresses that they put in their MAC table?

By logging the MAC addresses of every device connected to each of its ports, a switch creates its MAC address database. The switch sends frames meant for a particular device out the port that has been designated for that device using information from the MAC address database.

A switch has two options for learning MAC addresses: statically or dynamically. The MAC addresses must be manually entered in the CAM (Content Addressable Memory) database for the static option. In the dynamic configuration, the switch automatically detects and adds the MAC addresses to the CAM table. The CAM table is kept by the switch in RAM.

2.7 Which MAC address ends up in the MAC table?

Both static and dynamic MAC address can end up into MAC table. Dynamic address which can be both manually added or dynamically learned may age out due to flood or other things. But static entries will never age out. The MAC address of the other Ethernet interfaces is stored in the MAC table.

2.8 How does a switch decide which port to send a frame on? How does this behavior change between a known and an unknown unicast frame?

The switch looks at the destination MAC address and compares it to addresses in the MAC address table before forwarding the packet. If the address is listed, the frame is sent to the port connected to the listed MAC address. A switch's primary objective is to forward frames as quickly as possible, and you can ensure that it succeeds in doing so. Before fully drawing the frame inside, a switch can begin the forwarding operation.

In unknown unicast, once the switch receives a frame from the destination which it doesnot know, it will insert the source MAC address into the CAM table (table that maps mac addresses to its port). After that it forwards the frame to all ports. The process of broadcasting this type of frame is called unknown unicast.

Switch forwards an unknown unicast frame from all of its ports besides the port on which it arrived, but it only forwards a known unicast frame from the port that is directly attached to the destination address of that frame.

2.9 Which type of switching waits until the entire frame has been received before it sent out?

Store-and-forward type of Store-and-forward Switching is a technique that waits until the entire frame is received.

When a switching device receives a data frame and then verifies it for defects before sending the packets, this process is known as "store-and-forward switching." It facilitates the effective transfer of undamaged frames. It typically finds use in telecommunication networks. The switching device in store-and-forward switching waits until it has received the complete frame before storing it in the buffer memory. The frame is next CRC (Cyclic Redundancy Check)-checked for errors; if any are discovered, the packet is discarded; otherwise, it is transmitted to the following device.

2.10 What command do you use to show this table?

show mac-address table.

2.11 How was 0e00. 4d67.cba1 learned?

It is a static Mac address that is added later in the lab.

It is added by using **mac address-table static 0e00. 4d67.cba1 vlan1 interface gi 1/1**

It can be seen later by using **show mac address-table address 0e00. 4d67.cba1**

2.12 True or False: 0e00.baa1.25a1 was sending traffic to 0e00.24fa.9c51, which is why they're both in the table?

False, 0e00.baa1.25a1 was not sending traffic to 0e00.24fa.9c51 but it was later on added in the table as a static Mac address.

2.13 How fast is the interface that 0e00.baa1.25a1 was learned on?

Initially mac address table aging time was 300 but was changed later to 900. And the speed was auto. It was a-full Duplex.

2.14 True or false: The device connected to port Gi0/1 definitely has a MAC address of 0e00.4d67.cba1

False, as it is static port and is created later and we cannot say that it definitely has port connected to it. The port where the static and dynamic MAC address is not the same as 0e00.4d67.cba1 was on port 1/1 and 0e00.4d67.cba1 is on port 0/1

2.15 Four frames with the destination MAC addresses below arrive at the switch. Which will be flooded?

0e00.4d67.cba1

Ffff.ffff.ffff

0e11.4675.ac12

0e00.24fa.9c51

As static MAC address**(0e00.4d67.cba1)** never wears out as it is manually added. From the following MAC address, **0e00.24fa.9c51** will be flooded as it is presented in the MAC address table and other two (**ffff.ffff.ffff, 0e11.4675.ac12**)are not presented in the table.

Watch the two videos for Cisco Switches and routers.

1. For each video, write a report of all the commands described in the videos

- **enable**

When using the console port, we can enter global configuration mode by executing this command.

Syntax: enable**,** show (clock, version, ?)

The router's status and configuration information can be viewed using the show command.

Syntax: show <commands>

configure terminal

Prior to being configured, a router needs to be in privileged mode. We must keep in mind that the two sublevels of exact modes are privileged and user. We can modify our authorization from user to just being allowed to carry out maintenance and monitoring duties by using the enable command. We must at the very least enter global configuration mode before configuring, which we may accomplish by entering configure terminal. The commands we can use moving forward will be different because that puts us in a different mode.

Command

- **configure terminal**

Everything you specify in global configuration mode, such as the host name, passwords, and banners, will frequently have an effect on the router as a whole. If you want to customize a single component, you must do so from global configuration.

- **hostname**

To change or set the host name of the network server, use the hostname global configuration command. The host name is used in both prompts and default configuration file names. Additionally, when the setup command facility first starts up, a host name is needed.

Examples

Display the hostname of the router: hostname

Change the device hostname to ciscolab: hostname ciscolab

- **show ip interface brief:** To check the usefulness of an interface when it is setup for several IP addresses, use the show ip interface brief command in privileged EXEC mode.
- **crypto key generate rsa: t**he Cisco router's SSH feature is enabled using this command. Before executing this command, the router's hostname, domain name, and one interface's static IP address must all be set up. After running the command, select a key size larger than the default size of 512 to ensure strong encryption.
- **show running-config:** This command, show running-config, is used to display the configuration that is currently active on the FWSM. It should be run in privileged EXEC mode.

- **copy running-config startup-config:** The show running-config command can be used to show the system's current running configuration. Use the following command to save the running configuration to the starting configuration file in NVRAM.
- **brief:** summarizes each interface's usability status data and displays it.

Execute the show ip interface short command to view a list of the router interfaces. This command displays further information, the IP address, and the state of the interface.

- **interface gigabit 0/1:** create a gigabit interface.
- **description corporate Network:** give description about the created interface
- **ip address ip subnet:** specify the ip address and subnet mask of the created interface gigabit.
- **Shutdown:** Shutdown command is used to disable the interface. To restart a disabled interface, we have to use no form of this command.

Syntax:

There are no arguments or keywords for this command. All of the features on the given interface were turned off by the shutdown command. This command drops the DTR signal on serial interfaces. The interfaces can also be marked as inaccessible with this command. Use the EXEC command display interfaces to see if the interfaces are accessible or not.

Example:

- **Turn off Ethernet interface 1**

interface Ethernet 1

shutdown

- **Turn on Ethernet interface 1**

interface Ethernet 1

no shutdown

- **show interface description:** Network interface statistics are displayed via the show interfaces command. If the parameter description is supplied, the command will show all of the interfaces that are available along with their status, protocol, and description.
- **enable secret:** By employing a nonreversible cryptographic function to store the enable secret password, the aforementioned command offers improved security. It offers an additional encryption layer for security.
- **write mem:** To modify the current configuration, use the write command. When the save-config overwrite command finds that this file can be overwritten, only then does it store the currently running configuration as the startup configuration.

Example

write memory

Overwrite previously saved configuration? Y