No: SRT

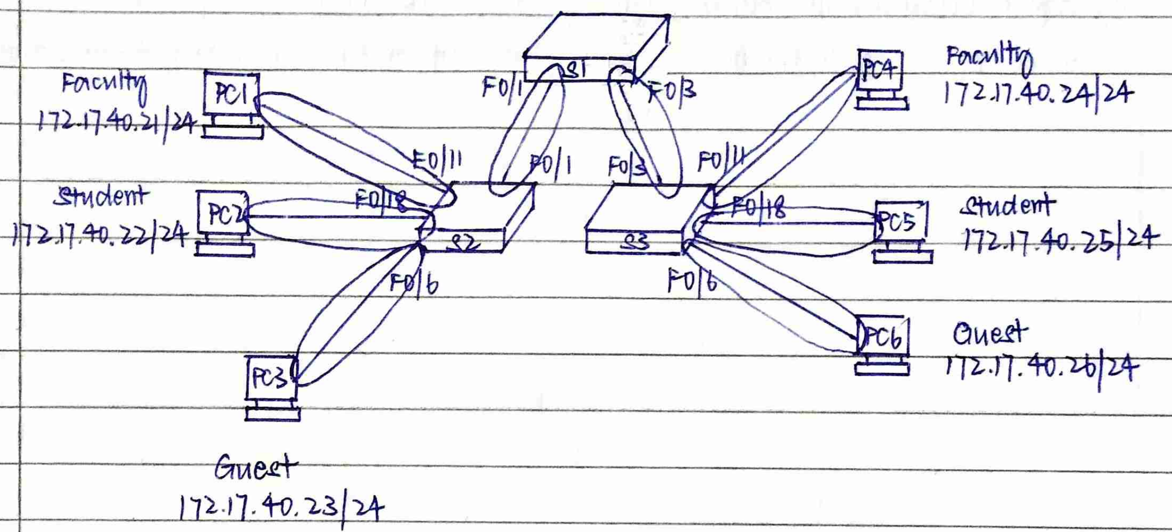
Date:

8 June 2023

Question 1

a) A collision domain is a network segment connected by a shared medium or through repeaters where simultaneous data transmission collides with one another.

8 collision domains



b) Disagree. Native VLAN supports untagged traffic whereas trunk VLAN support tagged traffic.

c) This statement is wrong.

When a layer 2 switch makes a forward decision, it is based on ingress interface of switch and destination MAC address of message.

No: .... Date: ....

d)(i) The switch will forward the frame to Fa3, Fa5, Fa7, Fa9.

(ii) The switch will receive the frame through Fa1 and it will add the source MAC address (0A) to the switch MAC table.

The switch will examine the destination MAC address (0B).

Since the destination MAC address doesn't exist in MAC table, it is flooded out all the interface except the one it was received (Fa3, Fa5, Fa7, Fa9).

(iii) Agree. Collision can occur in a hub-based network. A collision happens when two or more devices connected to the hub attempt to transmit and receive data at the same time.

No: ....

Date: ....

Question 2

a) It is because it is configured as trunk interfaces. The solution to remedy this problem is to convert interface Gi0/1 and Gi0/2 into access mode so that ports appear in the VLAN database.

b)(i) Switch 1

(ii) Switch 0: Gig0/1 Switch 2: Gig0/2 Switch 3: Gig0/2

(iii) Switch 0: Fa0/1, Gig0/2 Switch 2: Gig0/1

(iv) Switch 2: Fa0/1 Switch 3: Fa0/1, Gig0/1

c) STP is used to prevent loops from occuring by configuring a loop-free path through the network using strategically placed "blocking-state" ports.

d) (i) Default VLAN is the VLAN that cannot be deleted or renamed. Commonly, VLAN 1 is also known as default VLAN, default Native VLAN or default Management VLAN.

(ii) Router-on-a-Stick.

In this configuration, the router is connected to a single switchport on the switch. The router interface is configured with subinterfaces, each representing a separate VLAN. Each subinterface is tagged with a specific VLAN ID. The switchport connecting to the router is configured as trunk port, allowing multiple VLANs to pass through it. This method allows the router to act as the gateway for multiple VLANs without requiring a physical interface for each VLAN.

Question 3

a) (i) – For SWA, Fa0/8 has assigned to channel-group 8 which diffrent from the channel-group of Fa0/8 in SW3. Different channel group causes the failure to establish the EtherChannel link.

– For SW3, the channel-group 5 mode is desirable, but for SWA, the channel-group 5 mode is "ON". Since SW3 is using PAgP while SWA doesn't, switch SW3 and SW3 are failled to establish the EtherChannel link.

(ii) – Assign Fa0/8 of switch SWA to channel-group 5 mode active.

– Change the mode of channel-group 5 for Fa0/10 on both switch SW3 and SWA to "ACTIVE". (channel-group 5 mode active)

(iii) Change the mode of channel-group 5 for interface Fa0/10 from "ON" to "DESIRABLE". By changing the mode, switch SWA will establish a PAgP EtherChannel for interface Fa0/10.

(iv) – Interface types cannot be mixed. Fast Ethernet and Gigabit Ethernet cannot be mixed within a single EtherChannel.

– The individual EtherChannel group member port configuration must be consistent on both devices. If the physical ports of one side are configured as trunks, the physical ports of the other side must also be configured as trunks within the same native VLAN.

– Each EtherChannel has a logical port channel interface. A configuration applied to the port channel interface affects all physical interfaces that are assigned to that interface.

b) HSRP is a Cisco-proprietary FHRP that is designed to allow for transparent failover of a first-hop IP device.

HSRP ensures high network availability by providing first-hop routing redundancy for IP hosts on networks configured with an IP default gateway address.

HSRP is used in a group of routers for selecting an active device and a standby device.

c) The purpose of using a router includes determining the best path to forward packets based on the information in its routing table and also to forward packets towards their destination.

Question 4

a) Both DHCP starvation and DHCP spoofing are mitigated by implementing DHCP snooping.

DHCP Starvation Attack - The goal of this attack is to create a DoS for connecting clients. DHCP starvation attack requires an attack tool such as Gobbler. Gobbler has the ability to look at the entire scope of leasable IP addresses and tries to lease them all. Specifically, it creates DHCP discovery messages with bogus MAC addresses.

DHCP Spoofing Attack - This occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients. A rogue server can provide a variety of misleading information such as wrong default gateway, wrong DNS server and wrong IP address.

b)

Error Configurations	Solutions
The commands were entered in the wrong interface.	Enter all the commands above into interface F0/2.
The sticky command is not configured.	BMIT2164 (config-if)# switchport port-security mac-address sticky
The maximum address should be 5 instead of 4.	Change the maximum address to 5. BMIT2164 (config-if)# switchport port-security max 5
The violation mode was wrongly configured.	Replace BMIT2164 (config-if)# switchport port-security violation protect with BMIT2164 (config-if)# switchport port-security violation shutdown
VLAN 33 was not assigned to the port.	BMIT2164 (config-if)# switchport access vlan 33

No: .... Date: ....

c) In a man-in-the-middle (MITM) attack, the hacker is positioned in between two legitimate entities in order to read or modify the data that passes between the two parties. A popular wireless MITM attack is called the "evil twin AP" attack, where an attacker introduces a rogue AP and configures it with the same SSID as a legitimate AP.

Defeating a MITM attack begins with identifying legitimate devices on the WLAN. To do this, users must be authenticated. After all of the legitimate devices are known, the network can be monitored for abnormal devices or traffic.