Tutorial 1 : Switching Concepts

1.

a. Ingress interface is the interface where a frame enters the interface of a switch. (**True**/False)

b. Egress interface is the interface where a frame leaves the interface of a switch. (**True**/False)

c. A switch uses its MAC address table and routing table to make forwarding decisions. (True/**False**)
Comment: A switch only uses MAC address tables (destination MAC address and ingress port) to make forwarding decisions whereas the routing table is only used by the router.

d. A switch builds a MAC address table, also known as a Content Addressable Memory (CAM) table. (**True**/False)

e. Switches use the MAC address table and full-duplex to eliminate broadcast domains and avoid congestion. (True/**False**)
Comment: Switches use the MAC address table and full-duplex to eliminate collisions and avoid congestion but not broadcast domains.

f. Only a layer 3 device (router) will break the broadcast domain. (**True**/False)

2. "When a layer 2 switch makes a forwarding decision, it is based on the egress port and the destination IP address of the message." Comment on the above statement.
   - This statement is false.
   - This is because the layer 2 switch makes a forwarding decision based on the ingress port (entry port) and destination MAC address of the message but not egress port (exit port) and destination IP address of the message.

   Sample Answer:

   - When a layer 2 switch makes a forwarding decision, it is based on the ingress port and the destination MAC address of the message.

3. Explain how a switch builds its MAC address tables.
    - A switch builds its MAC address table by examining the source MAC address of the frame and port number where the frame entered the switch.
    - If the source MAC address does not exist, it will then be added into the MAC table along with its port number.
    - If the source MAC address does exist, the switch resets the timeout setting for that entry back to 5 minutes.

4. Explain how switches forward frames based on the content of their MAC address tables.
    - The switches forward the frame by examining the destination MAC address and comparing it to the addresses that are found in the MAC address table.
    - If the destination MAC address is in the MAC address table, it is forwarded out to the specified port.
    - If the destination MAC address is not in the MAC address table, it forwards the frame out of all ports (flooding) except for the ingress port of the frame.

5. Answer the questions below by using the information provided in Figure 1.

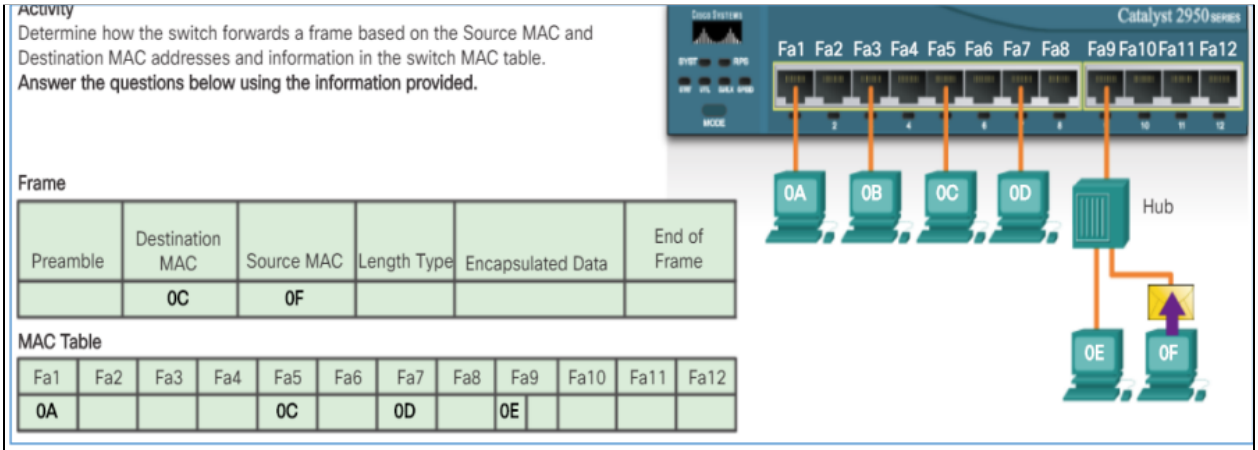


Figure 1: A switch forwarding diagram

    a. Where will the switch forward the frame? Circle the answer(s).
    Fa1 Fa2 Fa3 Fa4 **Fa5** Fa6 Fa7 Fa8 Fa9 Fa10 Fa11 Fa12

    b. Explain the how the switch forwards the frame to the destination device(s) by using Figure 1
        - Switch adds the source MAC address of PC “OF” and its incoming port (Fa9) which is currently not in the MAC address table.
        - The switch makes forwarding decisions based on the destination MAC address of PC “OC” to its associated port which is fa5.

- Frame is a unicast frame and will be sent to a specific port only which is Fa5.

Sample answer:

- The switch received the frame through Fa9 and it will **add** the source MAC address (OF) to the switch MAC table. (1 mark)
- The switch will make forwarding decision based on Destination MAC address – OC (2 marks)
- The Destination MAC address is inside the switch MAC table and the associated port is Fa5. The switch forwards out the frame through Fa5 as a unicast frame (2 marks)

6. Answer the questions below by using the information provided in Figure 2.

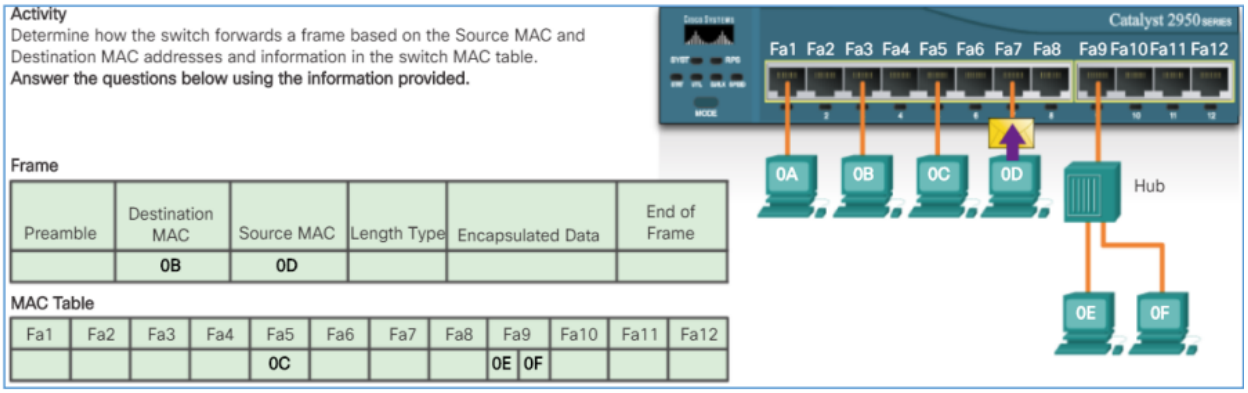


Figure 2: A switch forwarding diagram

a. Where will the switch forward the frame? Circle the answer(s).
Fa1 Fa2 **Fa3** Fa4 **Fa5** Fa6 Fa7 Fa8 **Fa9** Fa10 Fa11 Fa12

b. Explain the how the switch forwards the frame to the destination device(s) by using Figure 2
   - Switch adds the source MAC address of PC "OD" and its incoming port (Fa7) which is currently not in the MAC address table.
   - Since the destination MAC address of PC "OB" is not presented in the MAC address table, the switch will forward the unicast frame (flood) to all ports (Fa1, Fa3, Fa5, Fa9) except the ingress port which is Fa7.

Sample Answer:

- The switch received the frame through Fa7 and it will **add** the source MAC address (OD) to the switch MAC table. (1 mark)
- The switch will make forwarding decision based on Destination MAC address (OB) but it is **not available** in the switch MAC table. (1 mark)
- The frame is a unicast frame and will be **flooded** to all connected ports except the ingress port. (2 marks)

7. Contrast and compare the TWO (2) switch forwarding methods.

Store-and-Forward switching method	Cut-through switching method
Receives entire frame to ensure it is valid before forward the frame	Forward the frame immediately after determining the destination MAC address of an incoming frame and the egress port
Error-free forwarding as the bad frame will be discarded before forwarding	Bad frames will be forward too, which will cause amounts of error frames.
Waiting time (switch latency) is a little long as It takes time to store the entire frame in the switch.	Wait time (switch latency) is very low as the switch will not store the entire frames or packets.

Sample Answer:

Store-and-forward
- Receive entire frame and computes the CRC.
- If CRC is valid, the switch looks up the destination address which determines the outgoing interface.
- The frame is forwarded out the correct port.
- Slower forwarding but no invalid frames

Cut-through
- Forward the frame before it is entirely received.
- Destination address must be read before the frame can be forwarded
- Does not drop invalid frames and if high error rate, it may clog up bandwidth with damaged and invalid frames

8. When there is one or more devices in half-duplex, there will now be a collision domain. Why will this happen?
    - In half duplex mode, two or more devices can transmit and receive frames but cannot do it simultaneously.
    - Hence, ethernet ports in half-duplex will be part of a collision domain when there are two or more devices attempting to send the frame at the same time on the shared network segment.
    - The more devices in a collision domain, the higher probability of collision.

Sample Answer:

- When there is one or more devices in half-duplex there will now be a collision domain.
- Half-duplex is unidirectional and sending and receiving does not happen at the same time.
- There will now be contention for the bandwidth.
- Collisions are now possible.

9. What is the duplex setting of the switches whereby the collision domains are eliminated and congestion is reduced?
    - Most of the devices use auto-negotiation to reduce congestion and eliminate collision domains.
    - When there is full duplex on the link, the collision domains can be eliminated and congestion is reduced.

    Sample Answer:

- When there is full duplex on the link the collision domains are eliminated and congestion is reduced.

10. Differentiate collision domain for a hub and for a switch.

Collision domain for a hub	Collision domain for a switch
• There will be only one collision domain in the hub. • Whenever a frame is transmitted to a hub, the hub will spread the frame to all of its connected hosts.	• The number of collision domains on the switch is determined by the number of ports it has. • Whenever a frame is transmitted to a switch, the switch will search the mac address of the host in order to forward it thus isolating a one on one host connectivity.

Sample Answer:

- Collision domain is the segment where devices must compete to communicate
- All ports of a hub belongs to the same collision domain
- Every port of a switch is a collision domain on its own

11. What is a broadcast domain?
    - A broadcast domain is a logical division of a computer network in which all devices can reach each other by broadcast at the data link layer.
    - A broadcast domain extends across all Layer 1 or Layer 2 devices on a LAN.
    - Only a layer 3 device (router) will break the broadcast domain (aka MAC broadcast domain).
    - The broadcast domain consists of all devices on the LAN that receive the broadcast traffic.

    Sample Answer:

- A broadcast domain extends across all Layer 1 or Layer 2 devices on a LAN.

12. What are the consequences of connecting many switches together?

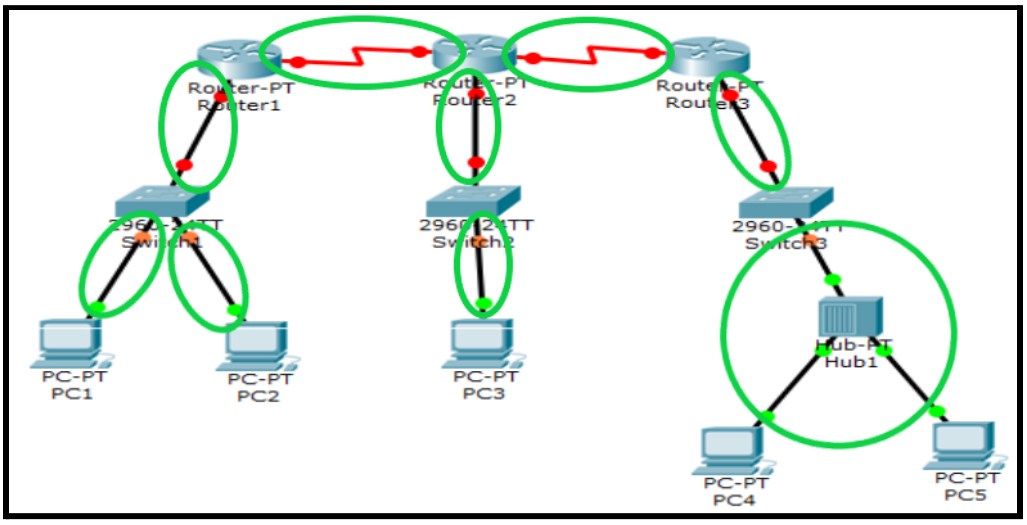
- The consequences of connecting many switches together causing the broadcast domain to be expanded. Subsequently, too many broadcasts will lead to congestion and poor network performance.

Sample Answer:

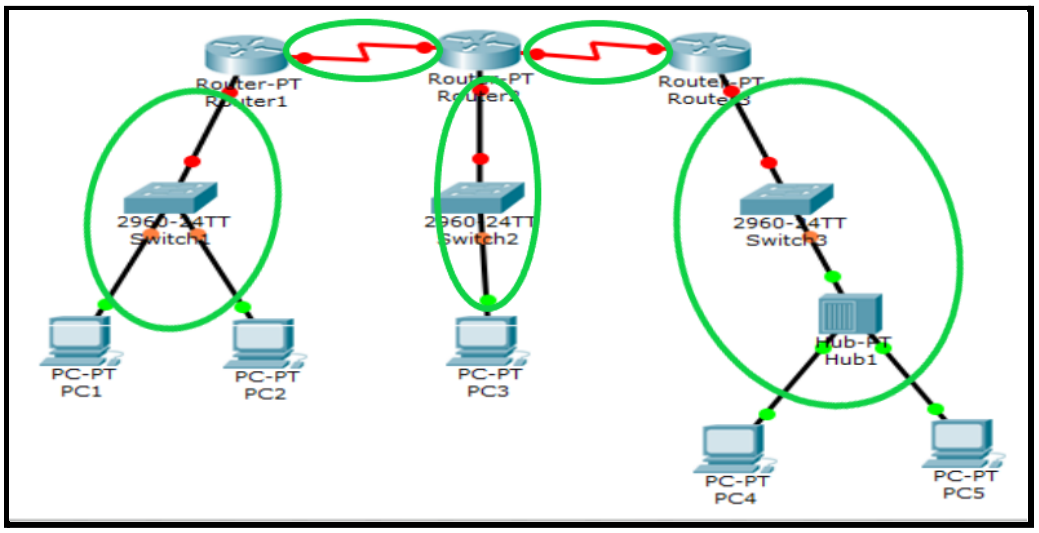
- When two switches or more switches are connected together, the size of broadcast domain is increased because the broadcast is propagated from switch to switch.
- Too many broadcasts can cause network congestion.

13.

a. Collision domains (switch and router) = 9

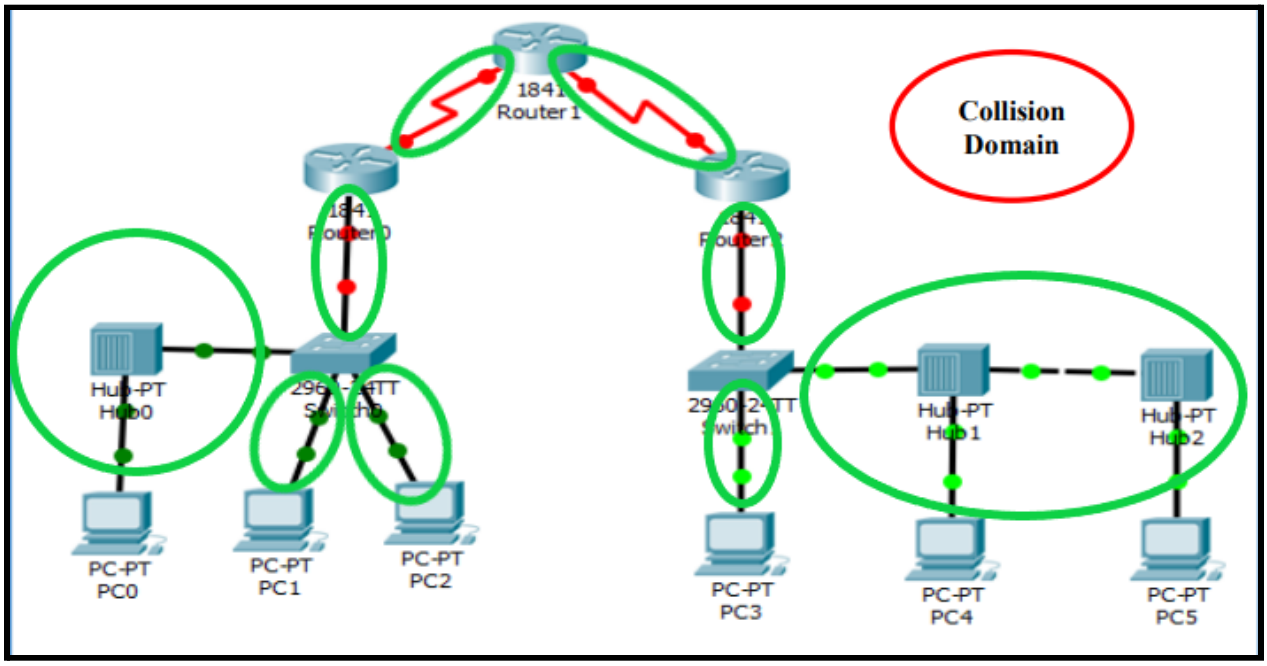


b. Broadcast domain (router) = 5

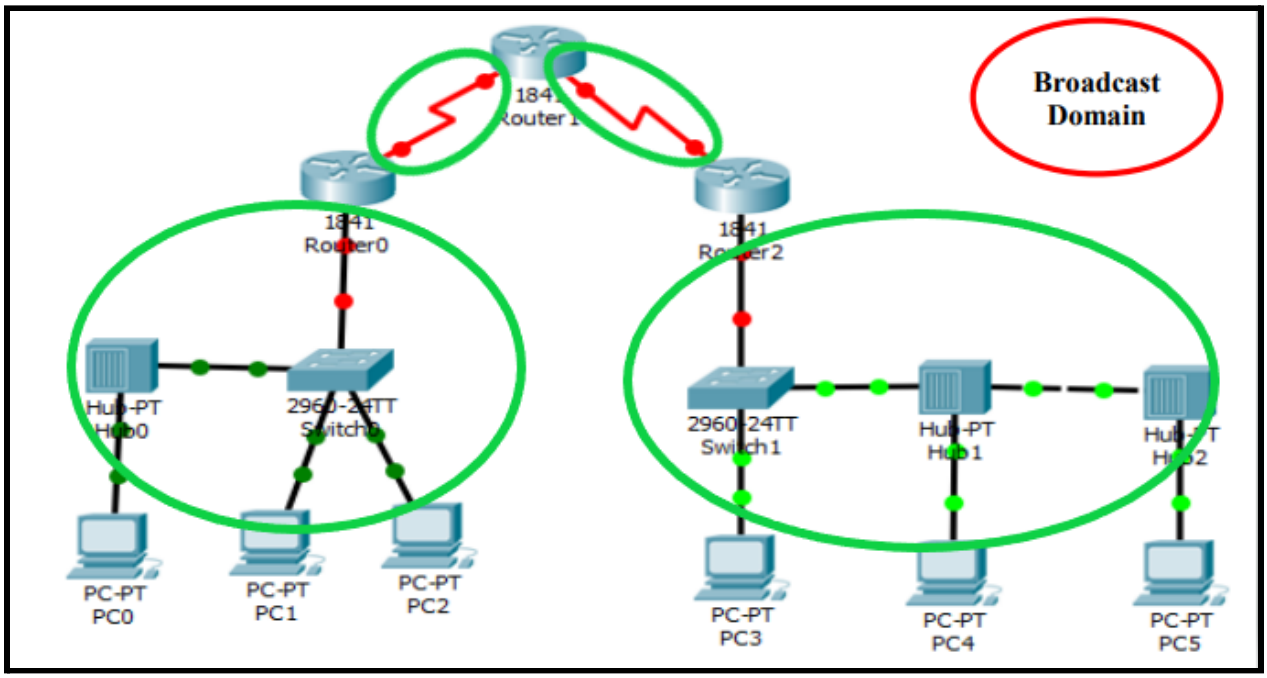


14. Based on the following figures, identify the collision domains and broadcast domains by circling the network symbols in the diagrams. In addition, indicate how many collision domains and broadcast domains show in the following topology.

a. Collision domains = 9



b. Broadcast Domains = 4



Notes for network devices and their role regarding to the broadcast and collision domains

Switch : Expands Broadcast domains and breaks up Collision domains.

Bridge : Expands Broadcast domains and breaks up Collision Domains.

Hub : Expands both Broadcast and Collision domains.

Router : Breaks up both Broadcast and Collision domains.

Reference:
https://broadcaststormblog.wordpress.com/2016/03/28/broadcast-and-collision-domains/

Tutorial 2

1. What is a Virtual Local Area Network (VLAN)?
    - VLANs are logical connections instead of physical connection with other similar devices.
    - Placing devices into various VLANs have the following characteristics:
        - Provide segmentation and organization flexibility in a switched network
        - Provide organization that is easier to manage
            - Broadcasts, multicasts and unicasts are isolated in the individual VLAN.
            - Each VLAN will have its own unique range of IP addressing.
            - Improve network performance by separating large broadcast domains into smaller ones.

    Sample answer

    - A VLAN is a logical connection or logical partition of a Layer 2 network.
        - Multiple partitions can be created and multiple VLANs can co-exist.
        - The partitioning of the Layer 2 network takes place inside a Layer 2 device, usually via a switch.
        - Each VLAN is a broadcast domain that can span multiple physical LAN segments.
        - Hosts on the same VLAN are unaware of the VLAN's existence.

2. List the benefits of using VLANs.

Benefit	Description
Smaller broadcast domains	• Dividing a network into VLANs reduces the number of devices in the broadcast domain.
Improved security	• Only users in the same VLAN can communicate together.
Improved IT efficiency	• VLANs simplify network management because users can group devices with similar requirements. • VLANs can be named to be easily identify
Reduced cost	• VLANs reduce the need for expensive network upgrades and use the existing bandwidth and uplinks more efficiently
Better performance	• Smaller broadcast domains reduce traffic and improve performance
Simpler project and application management	• VLANs aggregate users and network devices to support business or geographic requirements.

	• Having separate functions makes managing a project or working with a specialized application easier (i.e e-learning development platform for faculty).

3. Introduce a default VLAN.
    - A default VLAN on a CISCO switch is VLAN 1.
    - All ports are assigned to VLAN 1 by default.
    - The native VLAN is VLAN 1 by default.
    - The management VLAN is VLAN 1 by default.
    - VLAN 1 cannot be renamed or deleted.

    Sample Answer:

- VLAN 1 is the following:
    - All switch ports become a part of the default VLAN after the initial boot up of a switch loading the default configuration.
    - The default VLAN for Cisco switches is VLAN 1.
    - The default Native VLAN
    - The default Management VLAN
    - Cannot be deleted or renamed

4. Explain the following types of VLANs.
    a. Data VLAN
        - VLAN that is dedicated to user-generated traffic (i.e email and web traffic).
        - It can be referred to as user VLAN because they separate the network into groups of users or devices.
        - VLAN 1 is the default data VLAN as all interfaces are assigned to it.

    b. Native VLAN
        - This VLAN is solely used for trunk links
        - All frames are tagged on an 802.1Q trunk link except for those on the native VLAN.

    c. Management VLAN
        - A data VLAN configured specifically for network management traffic such as SSH, Telnet, HTTPS, HTTP, and SNMP.
        - VLAN 1 is the default management VLAN on a layer 2 switch.

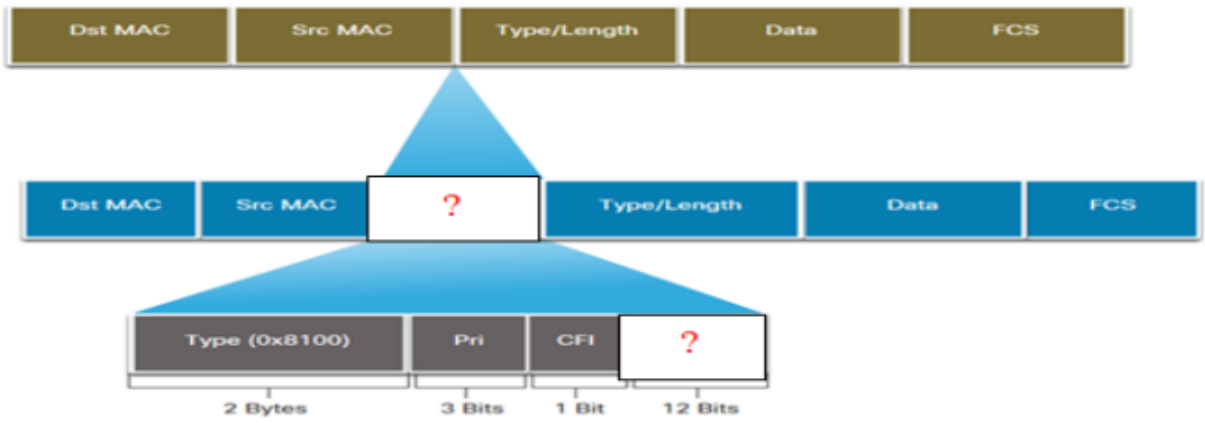
Sample Answer:

- Data VLAN
  - A data VLAN is a VLAN that is configured to carry user-generated traffic.
  - VLAN 1 is the default data VLAN
  - Network admin can create data VLAN, example, VLAN 2, 3, 10, etc.
  - VLAN numbers 1 – 1005
  - 1002 – 1005 reserved for Token Ring & FDDI (not data VLAN)

- Native VLAN
  - This is used for trunk links only.
  - All frames are tagged on an 802.1Q trunk link except for those on the native VLAN.
  - A native VLAN is assigned to an 802.1Q trunk port.
  - Trunk ports are the links between switches that support the transmission of traffic associated with more than one VLAN.
  - The use of a native VLAN was designed for legacy use, like the hub in the example.
  - Unless changed, VLAN1 is the native VLAN.

- A management VLAN is any VLAN configured to access the management capabilities of a switch.
- VLAN 1 is the management VLAN by default.
- This is used for SSH/Telnet VTY traffic and should not be carried with end user traffic.
- Typically, the VLAN that is the SVI for the Layer 2 switch.

5. Fill in the blank.



- Tag (blue diagram)
- VLAN ID (VID) (gray diagram)

6. Compare a Normal range VLAN to an Extended VLAN.

Normal range VLANs	Extended Range VLANs
They are used in all small- and medium-sized business and enterprise networks.	They are used by service providers to service multiple customers and by global enterprises large enough to need extended range VLAN IDs.
They are identified by a VLAN ID between 1 and 1005.	They are identified by a VLAN ID between 1006 and 4094.
IDs 1002 through 1005 are reserved for legacy network technologies (i.e., Token Ring and Fiber Distributed Data Interface).	Configurations are saved, by default, in the running configuration.
Ds 1 and 1002 to 1005 are automatically created and cannot be removed.	They support fewer VLAN features than normal range VLANs.
Configurations are stored in the switch flash memory in a VLAN database file called vlan.dat.	Requires VTP transparent mode configuration to support extended range VLANs.
When configured, VLAN trunking protocol (VTP), helps synchronize the VLAN database between switches.	

Sample Answer:

Normal Range VLAN	Extended Range VLAN
1 – 1005	**1006 - 4095**
Used in Small to Medium sized businesses	Used by Service Providers
1002 – 1005 are reserved for legacy VLANs	Are in Running-Config
1, 1002 – 1005 are auto created and cannot be deleted	Supports fewer VLAN features
Stored in the vlan.dat file in flash	Requires VTP configurations
VTP can synchronize between switches	

7. During the configuration of a fixed form factor switch with 24 Fast Ethernet and 2 Gigabit Ethernet ports, you noticed the VLAN table of this switch shows the following listing.

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Figure 1-2 A VLAN table

Illustrate TWO (2) possible conclusions that you can obtain from the listing of the VLAN table shown in Figure 1-2.

- Fa0/1 and Gig0/1 are missing.

Sample Answer:

Answer: (3 marks each; total 6 marks)

- Port Fa0/1 and Gig0/1 are not shown in the VLAN table.
- 1st possibility: These ports may be configured as trunk ports. This is because trunked ports are not listed in the VLAN table
- 2nd possibility: A VLAN where these 2 ports have been assigned to has been removed from the VLAN database before reassign these ports to another VLAN

```
S1(config)#int range f0/1,g0/1
S1(config-if-range)#sw m a
S1(config-if-range)#sw access vlan 2
S1(config-if-range)#exit
```

```
S1#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/2
2    VLAN0002                         active    Fa0/1, Gig0/1
10   R&D                              active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

8. A switch port has been configured with commands as shown in Figure 1-3. How to reset a trunk port to default state?

```
Switch(config-if)#int f0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 88
Switch(config-if)#switchport trunk allowed vlan 88,100,110,120
Switch(config-if)#end
```

```
S2#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/3       on           802.1q         trunking      88

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/3       88,100,110,120

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20
Fa0/3       none

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20
Fa0/3       none
```

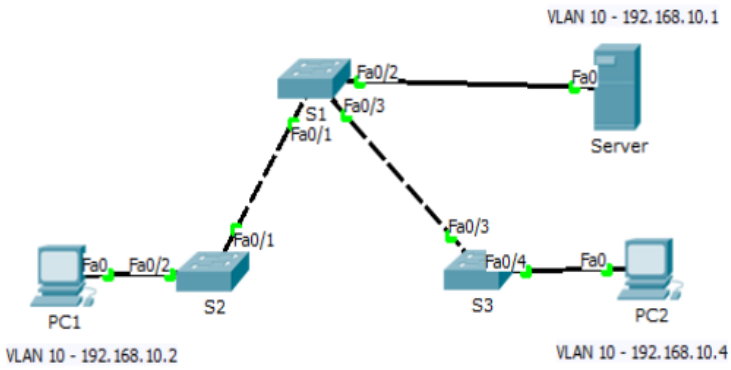
- We can reset the trunk port to default settings by issuing “no” command:

Sample Answer:

```
Switch1(config-if)#int f0/3
Switch1(config-if)#no switchport trunk native vlan 88
Switch1(config-if)#no switchport trunk allowed vlan 88,100,110,120
Switch1(config-if)end
Switch1(config)config t
Switch1(config-if)#int f0/3
Switch1(config-if)#switchport mode dynamic auto// return port to dynamic
auto mode or no sw mode trunk
Switch1(config-if)end
```

9. Based on the following topology and configuration files, identify the reason why PC1 cannot ping to the server.

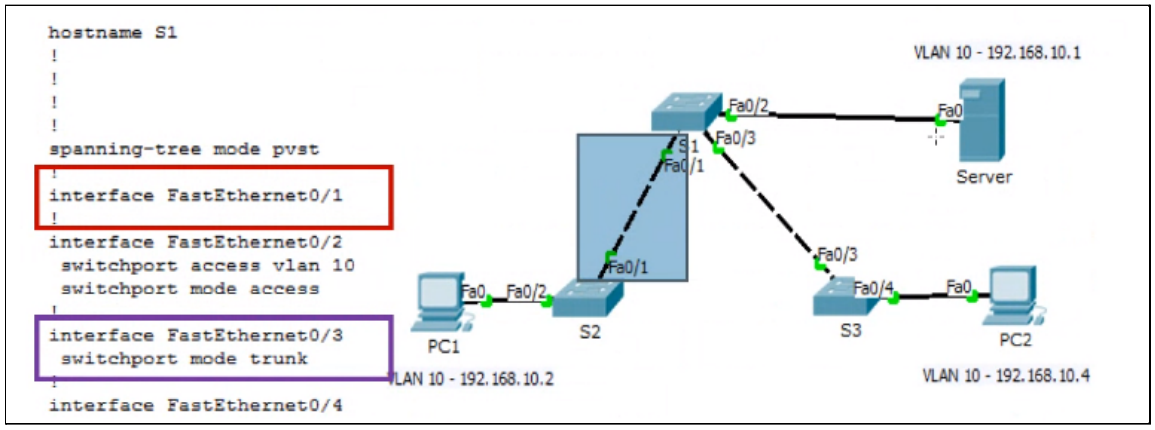
```
hostname S1
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
```




```
hostname S2
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
```

```
!
hostname S3
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/5
!
```

Sample Answer:



```
hostname S2
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
```

```
!
hostname S3
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/5
!
```

- **Interface FastEthernet 0/1 on S1 and S2 are not configured as trunk port**
- **Frame from PC1 cannot transmit from S2 to S1 to reach the server**
- **A trunk connection is needed to transfer traffic for all VLANs from one switch to another.**

	S1 int f0/1	S2 int f0/1
1	sw mode trunk	sw mode trunk
2	sw mode dynamic desirable	sw mode dynamic auto
3	sw mode dynamic auto	sw mode dynamic desirable
4	sw mode dynamic desirable	sw mode dynamic desirable

10. As a network associate, you have been assigned to troubleshoot a misconfigured VLAN network. The topology and the configurations of the VLAN network are shown in Figure 2-1 and Table 2-1 respectively. Your objectives are to locate and correct errors in the configurations and establish end-to-end connectivity between PCA and PCB which are in VLAN 10. Document the problems discovered and potential solutions using the template shown in Table 2-2.

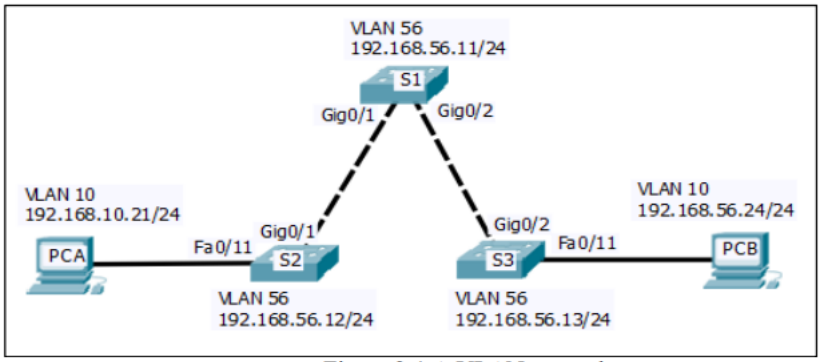


Figure 2-1 A VLAN network

S2	S1	S3
interface GigabitEthernet0/1 **switchport trunk native vlan 56** **switchport mode trunk** **!** **interface FastEthernet0/11** **switchport mode access** **switchport access vlan 10** **!** **VLAN created:** **VLAN 10, VLAN 56**	**interface GigabitEthernet0/1** **switchport mode trunk** **!** **!** **interface GigabitEthernet0/2** **switchport trunk native vlan 56** **switchport mode access** **!** **VLAN created:** **VLAN 56**	**interface GigabitEthernet0/2** **switchport trunk native vlan 56** **switchport mode access** **!** **interface FastEthernet0/11** **switchport mode access** **!** **VLAN created:** **VLAN 10, VLAN 56**

Table 2-1 Configurations on switches S1, S2 and S3

Sample Answer:

Device and ports	Problems Discovered	Solutions	Marks
S1, g0/1	Native VLAN mismatches between S2 and S1. Native VLAN on S2 is VLAN 56 but on S1 is the default VLAN (or VLAN 1)	On S1: Native VLAN on both end of the inter-switch link must be the same. Configure native VLAN 56 on Gig0/1 of S1 OR On S1: interface GigabitEthernet0/1 switchport trunk native vlan 56 [VLAN1 as native VLAN is not acceptable]	2+2

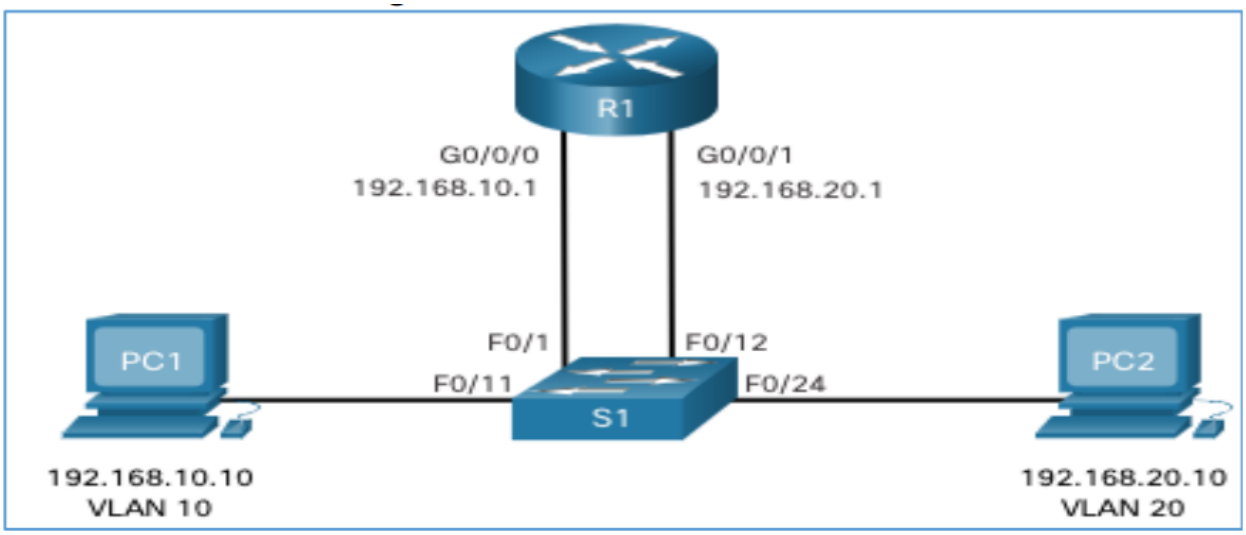
S1,S3, g0/2	Switch port modes on Gig0/2 of S1 and Gig0/2 of S3 are both configured as access mode. Therefore the inter-switch link between S1 and S3 will only support the default VLAN and no other VLANs	On S1& S3: configure trunk mode on both the Gig0/2 ports of S1 and S3 so that inter-switch link can transmit all VLANs' frames OR On S1& S3: interface GigabitEthernet0/2 switchport mode trunk	2 + 2
S1	Only VLAN 56 has been created in S1.	On S1: VLAN 10 must be created in all switches to make communication successful. In this scenario, VLAN 10 needs to be created in S1 OR On S1: Vlan 10	2 + 1
S3, f0/11	Port Fa0/11 on S3 is accessing the default VLAN (VLAN 1)	On S3: Assign the Fa0/11 on S3 access to VLAN 10 OR On S3: int fa0/11 Switchport access vlan 10	1 + 1
PCB	PCB is configured with an IP address from 192.168.56.0/24 network.	On PCB: Configure PCB with an IP address 192.168.10.24/24 from 192.168.10.0/24	1+1

Conclusion

1. Native VLAN must be the same; else it will be mismatch
2. Trunk port must be configured to support all the VLAN or VLAN that specified by ourselves
3. All the VLAN must be created in order to make the communication become successful
4. Have to be careful about the IP address of a PC (whether it's IP address is within the VLAN)
5. Assign the interface to correct VLAN

Tutorial 3: Inter VLAN-Routing

1. With reference to the following diagram, identify the type of inter-vlan routing and explain the limitation of this inter-vlan routing



- **Type** - Legacy Inter-VLAN Routing
- Legacy Inter-VLAN Routing using physical interfaces works, but it has a significant limitation.
- It is not reasonably scalable because routers have a limited number of physical interfaces. Requiring one physical router interface per VLAN quickly exhausts the physical interface capacity of a router.

2. A junior network associate had set up router-on-a-stick inter-vlan configuration as depicted in Figure 2-1, Figure 2-2 and Figure 2-3. The basic requirement is to set up two VLANs which are VLAN 301 and VLAN 303. PCA and PCB are in VLAN 301 whereas PrinterC is in VLAN 303. VLAN 301 is assigned to the first subnet and VLAN 303 is assigned to the second subnet of 192.168.10.0.

   Identify SIX (6) configuration errors in Figure 2-1, Figure 2-2 and Figure 2-3. Document the configuration errors and give correct solutions using Table 2-1 in your answer booklet.

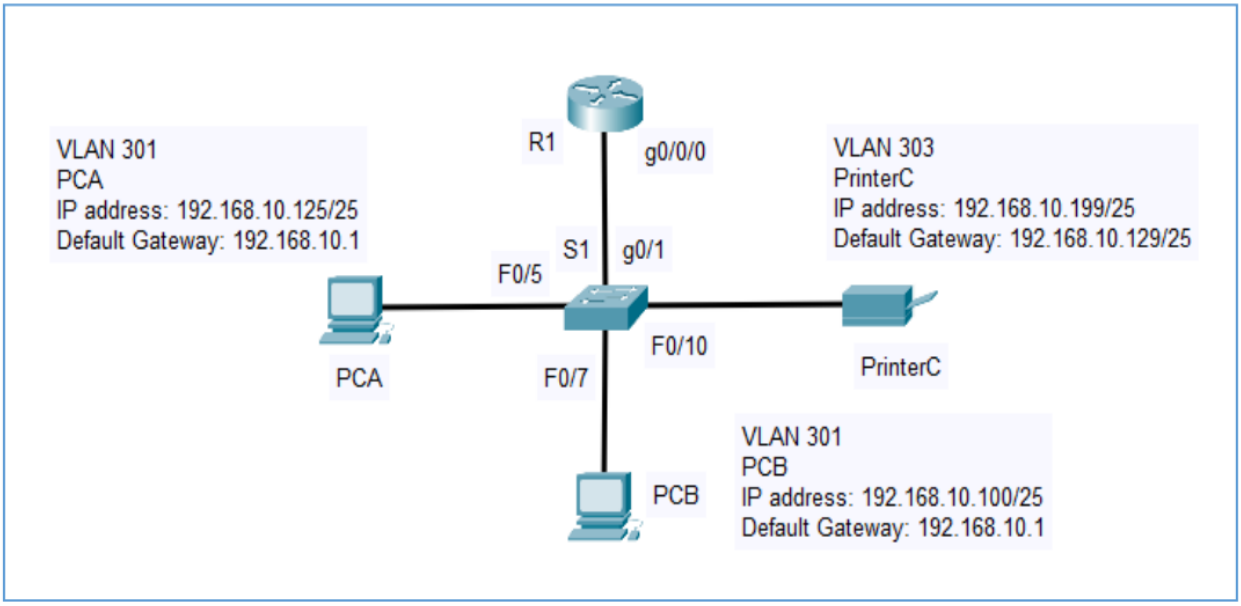


Figure 2-1: A network topology diagram

```
S1(config)#int g0/1
S1(config-if)#switchport mode access
S1(config-if)#exit
```

Figure 2-2: S1 configurations

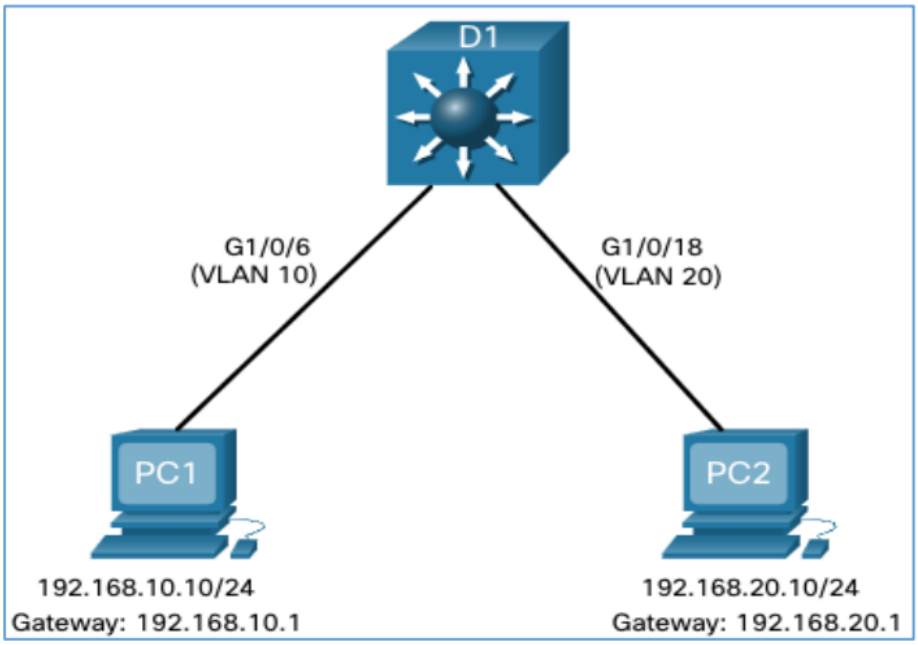
```
R1(config)#int g0/0/0.301
R1(config-subif)#encapsulation dot1Q 301
R1(config-subif)#ip address 192.168.10.1 255.255.255.0
R1(config-subif)#int g0/0/1.303
R1(config-subif)# encapsulation dot1Q 33
R1(config-subif)#ip address 192.168.10.126 255.255.255.128
R1(config-subif)#int g0/0/0
R1(config-if)# shutdown
```

Figure 2-3: R1 configurations

Items	Configuration Errors	Solutions
1	S1(config-if)#switchport mode access	S1(config-if)#switchport mode trunk
2	R1(config-subif)# encapsulation dot1Q 33	R1(config-subif)# encapsulation dot1Q 303

3	R1(config-subif)#ip address 192.168.10.1 255.255.255.0	R1(config-subif)#ip address 192.168.10.1 255.255.255.128
4	R1(config-subif)#int g0/0/1.303	R1(config-subif)#int g0/0/0.303
5	R1(config-subif)#ip address 192.168.10.126 255.255.255.128	R1(config-subif)#ip address 192.168.10.129 255.255.255.128
6	R1(config-if)# shutdown	R1(config-if)# no shutdown

3. Identify the type of inter-vlan routing and explain the steps to configure this type of inter-vlan routing.



Layer 3 switch using switched virtual interfaces (SVIs)

Step 1 - Create the VLANs. In the example, VLANs 10 and 20 are used.

Step 2 - Create the SVI VLAN interfaces. The IP address configured will serve as the default gateway for hosts in the respective VLAN.

Step 3 - Configure access ports. Assign the appropriate port to the required VLAN.

Step 4 - Enable IP routing. Issue the ip routing global configuration command to allow traffic to be exchanged between VLANs 10 and 20. This command must be configured to enable inter-VLAN routing on a Layer 3 switch for IPv4.

4. A network administrator has received a complaint that PC10 on VLAN 10 and PC20 on VLAN 20 cannot communicate. Based on the information and configurations shown in Figure 2-1, identify the configuration errors and suggest the corresponding solutions. Explain your answers.

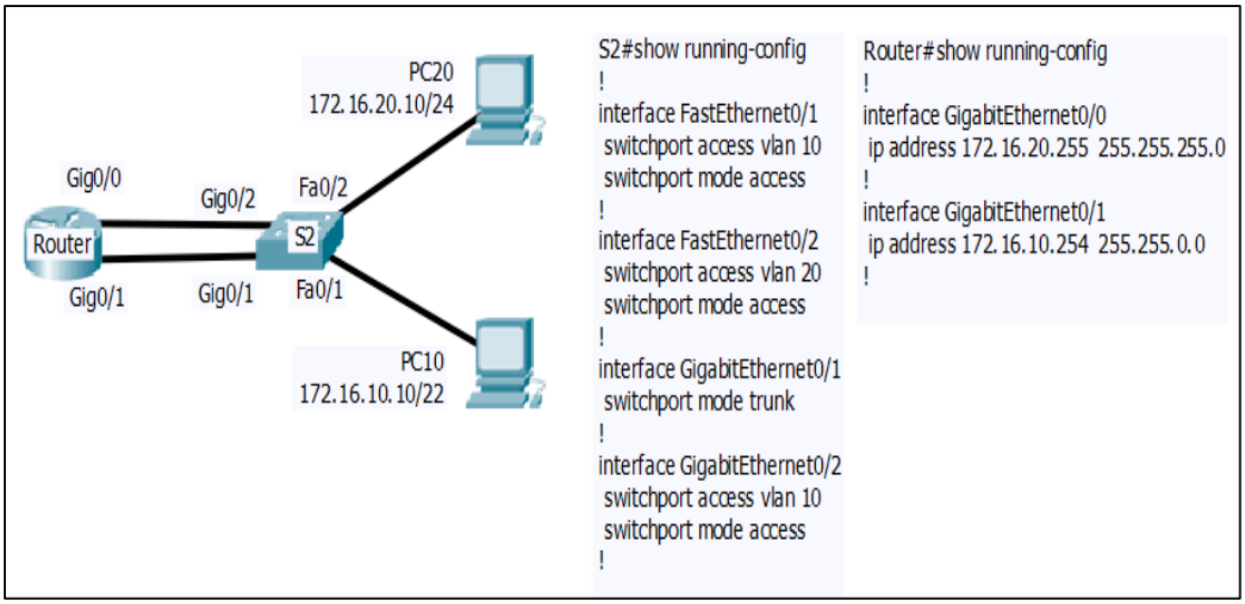


Figure 2-1 A Legacy Inter-VLAN routing network

(10 marks)

No.	Configuration Errors	Solutions	Mark
1	Interface Gig0/1 on S2 is configured as trunk mode	There is a Legacy Inter-VLAN routing network where the physical interface on the Router will be assigned to an individual VLAN. Therefore, the interface Gig0/1 on S2 has to be configured as access mode and access to VLAN 10 S2: interface Gig0/1 switchport mode access switchport access vlan 10	2+2
2	The interface Gig0/2 on S2 is accessed to wrong VLAN	The interface Gig0/2 on S2 should access to VLAN 20 S2: interface Gig0/2 switchport mode access switchport access vlan 20	1+1

3	The IP address of Gig0/0 on the router is incorrect. It is a broadcast address.	Re-configure the Router's Gig0/0 IP address to 172.16.20.254 (or any available IP address except 172.16.20.10)	1+1
4	The subnet mask of PC10 and interface Gig0/1 on Router are not tally	Re-configure either PC10 subnet mask to /16 or interface Gig0/1 on Router to /22 **OR** PC 10: ip address for PC10 is 172.16.10.10 /16 **OR** On router: interface Gig0/1 ip address 172.16.10.254 255.255.252.0	1+1

Tutorial 4: STP

1. The spanning tree algorithm (STA) uses three simple steps to achieve a logical loop-free topology.

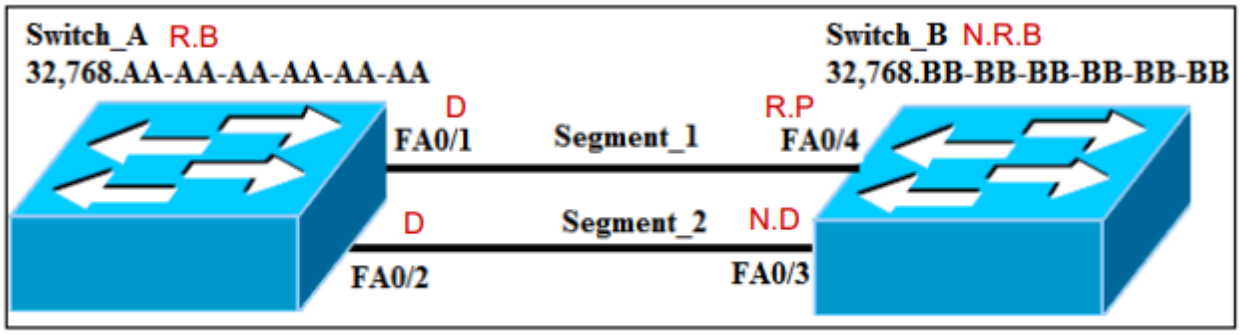


Figure 1 Network Topology

With reference to Figure 1, determine the following:

I. **Root bridge**
Switch A as it has the lowest BID 32,768 with mac address AA-AA-AA-AA-AA-AA

II. **Non-root bridge**
Switch B as it has higher BID 32,768 with mac address BB-BB-BB-BB-BB-BB

III. **Root port on the non-root bridge**
FA0/4 on Switch B. Lowest sender port ID, FA0/1 compare to FA0/2

IV. **Designated port on Segment_1**
FA0/1. Root path cost = 0 compare to root path cost of 19 from FA0/4

V. **Designated port on Segment_2**
FA0/2. Root path cost = 0 compare to root path cost of 19 from FA0/3

VI. **Non-designated port on Segment_2 segment**
FA0/3 on Switch B. Root path cost = 19

VII. **The port is in blocking state**
FA0/3. All non-designated ports are in a blocking state.

2. Spanning Tree Protocol (STP) is a Layer 2 protocol that runs on switches

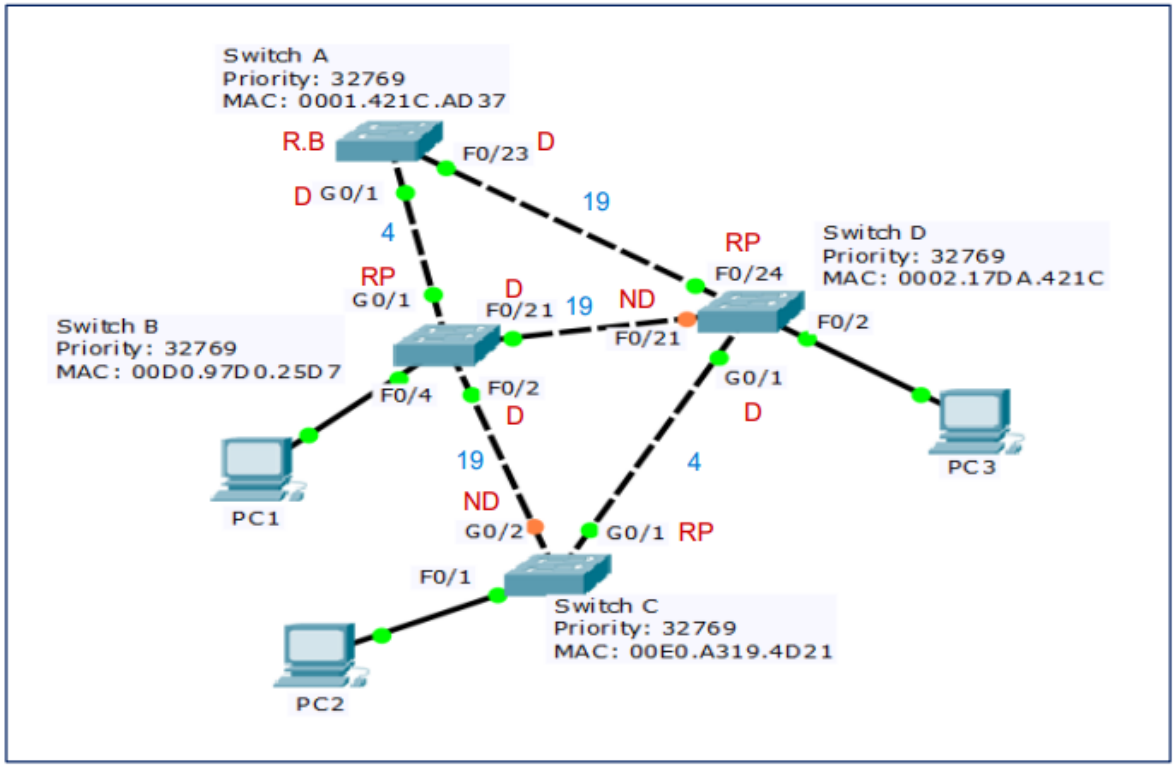


Figure 1-1: Network Topology

Network Topology

(i) Root bridge

- Switch A has the lowest MAC address 0001.421C.AD37 compared to Switch B, C, D meanwhile they all have the same priority.

(ii) Root port on the non-root bridge

- Switch B - G0/1
- Switch C - G0/1 (lower sender BID on Switch D)
- Switch D - F0/24

(iii) Designated ports on the non-root bridge

- Switch A - G0/1, F0/23
- Switch B - F0/2, F0/21
- Switch D - G0/1

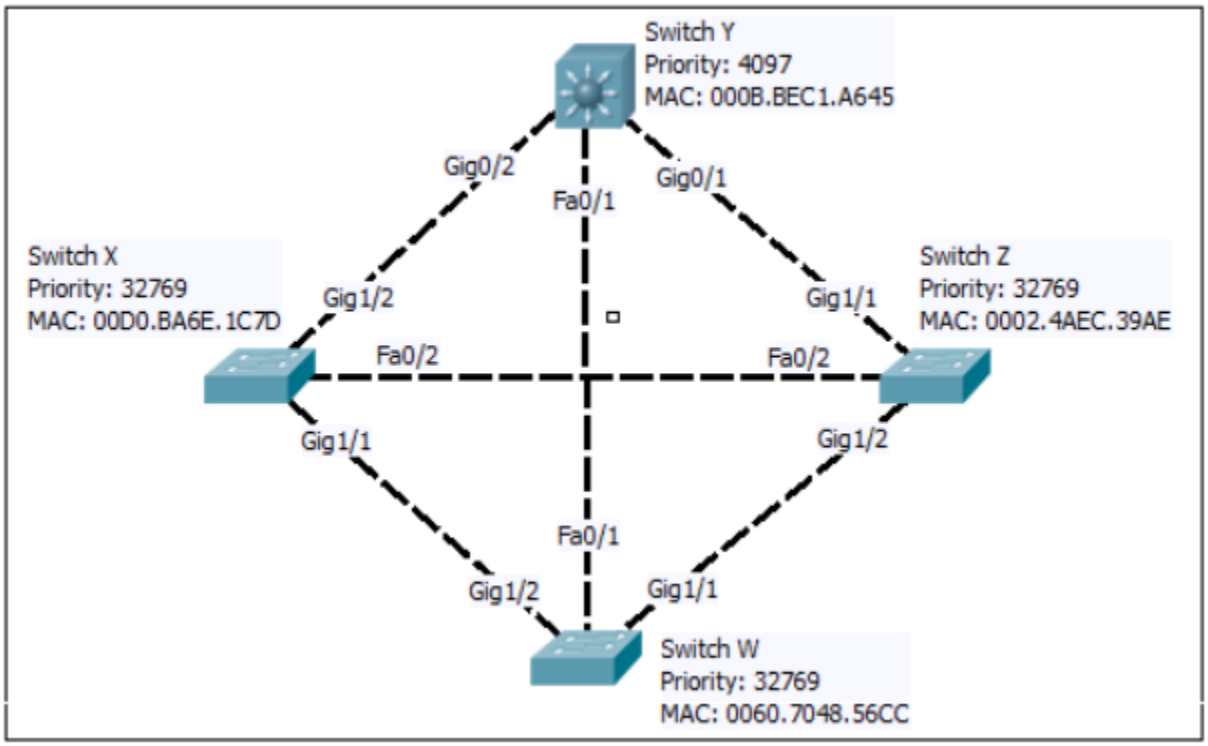
(iv) Non-designated port on the non-root bridge

- Switch C - G0/2
- Switch D - F0/21

(v) Referring to Figure 1-1, suggest which of the switch(es) interfaces that need to be configured with Port fast and BPDU guard command? Justify your answers.

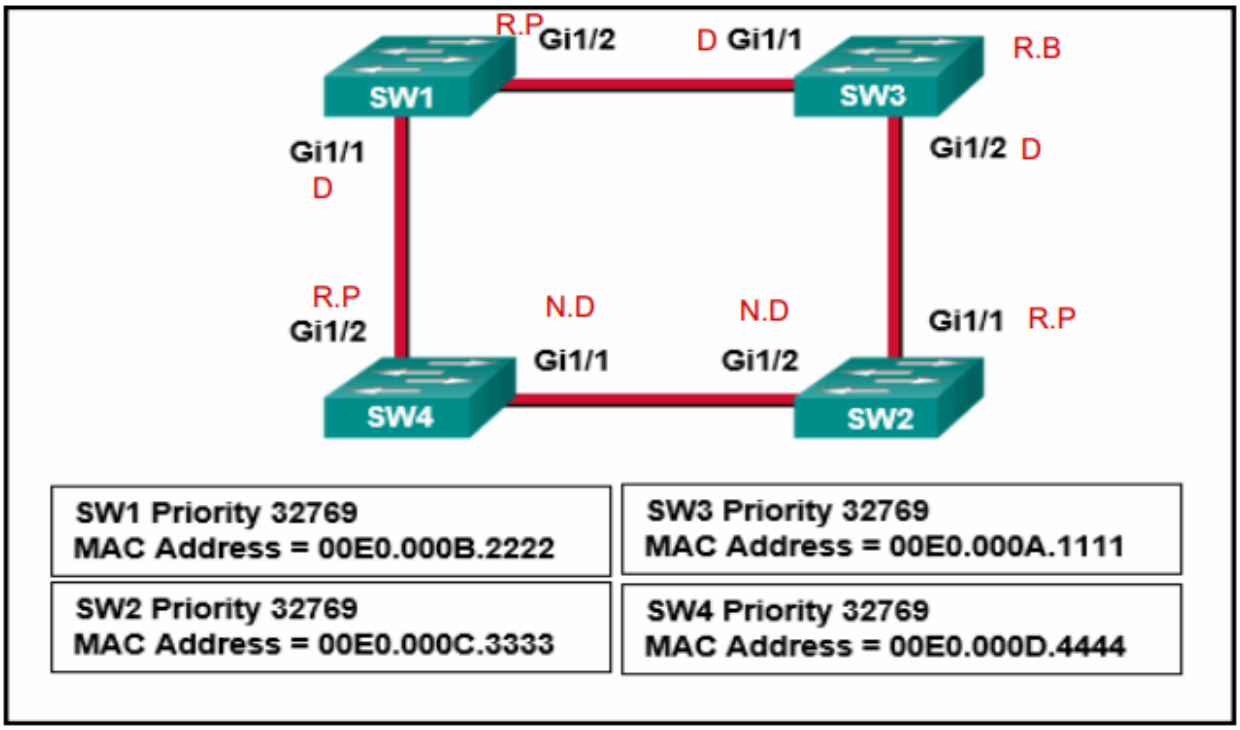
- Edge ports: Switch B F0/4, Switch C F0/1, Switch D F0/2
- Edge ports will never have the switch connected to it but end devices such as PCs
- PortFast will immediately transition from blocking to forwarding state
- When configured on a PortFast-enabled port, the BPDU guard shuts down the ports that receive a BPDU. This is to avoid attacks from unauthorized users.
- BPDU guard puts the port in an err-disabled on the receipt of a BPDU.

3. A converged switch-based network with spanning tree protocol is pictured below. Which port is the root port for Switch W? Explain the derivation of your answer in detail.



- G1/1 is the root port for Switch W.
- Switch Y is the root bridge because it has the lowest priority value.
- There are 2 equal LOWEST root path costs to reach the root bridge, i.e path via Switch X and path via Switch Z.
- In this case, the tiebreaker is the lowest sender BID, step-3 in the 5-step decision sequence. Switch Z's BID is lower than Switch X's. This is because Switch Z's BID is 0002.4AEC.39AE while Switch X's BID is 00D0.BA6E.1C7D
- Therefore, port Gig1/1 is the root port.

4. Analyze the following diagram and illustrate which switch will be elected as the root bridge and which switch's port will place a port in blocking mode. Justify your answers.



- SW3 will be the root bridge because BID (MAC address) is the lowest since the priority in all switches are the same.
- G1/1 on SW4 and G1/2 on SW2 segment: root path cost via SW1 is 8 whereas root path cost via SW2 is 4. Since the root path cost of G1/1 of SW4 via SW1 is higher therefore the port will be blocked.

5. STP has five ports states, list down the five ports states.

- Blocking
- Listening
- Learning
- Forwarding
- Disabled

6. When an interface is configured with PortFast and BPDU guard, illustrate these features and how the interface will respond when it receives a BPDU?

- PortFast: Cause a layer 2 LAN interface configured as an access port to enter the forwarding state immediately, bypassing the listening and learning states. Use PortFast only when connecting a single end station to a Layer 2 access port.

- BPDU guard prevents a port in Portfast mode from accepting BPDUs. If any BPDU comes in on a port that’s running BPDU Guard, the port will be shut down and placed into the error-disabled state, shown on the switch as err-disabled.

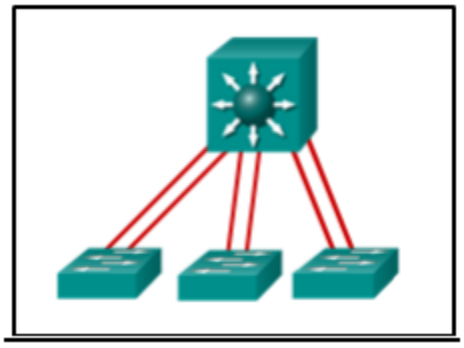
Tutorial 5: EtherChannel

1. A network administrator configured an EtherChannel link with three interfaces between two switches. What is the result if one of the three interfaces is down?
    - The remaining two interfaces continue to load balance traffic.

2. When EtherChannel is implemented, multiple physical interfaces are bundled into which type of logical connection?
    - Port Channel

3. Which mode configuration setting would allow the formation of an EtherChannel link between switches SW1 and SW2 without sending negotiation traffic?
    - SW1 - on
    - SW2 - on

4. Refer to the diagram. Which switching technology would allow data to be transmitted over each access layer switch link and prevent the port from being blocked by the spanning tree due to the redundant link?



    - EtherChannel

5. (i) Refer to Figure 1-2 and Figure 1-3, illustrating why PAgP EtherChannel is not created.

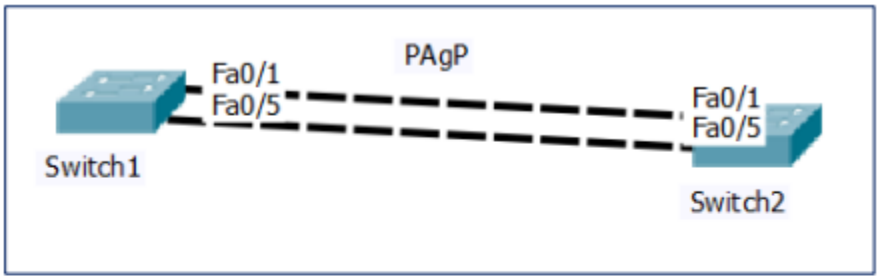


Figure 1-2: Etherchannel network

```
Switch2#show run
:
<omitted ouput>
:
interface FastEthernet0/1
channel-group 3 mode on

interface FastEthernet0/5
channel-group 3 mode auto
```

Figure 1-3: "show run" command

- Wrong modes are being used. The "on" mode bundles the links unconditionally and no negotiation protocol is used. In this mode, PAgp packets are sent or received.
- PAgp is using auto and desirable mode. All ports in an EtherChannel must use the same protocol. F0/1 and F0/5 in Switch 2 must use auto and desirable mode or desirable and desirable mode on each port.

(ii) Suggest TWO (2) settings that must be identical on both ends of the connections for the Etherchannel network to be successfully formed as shown in Figure 1-2.

- EtherChannel must be supported
- Speed and duplex must match
- VLAN match - All interfaces are in the same VLAN
- Range of VLAN - Same range on all interfaces

6. (i) Explain why the EtherChannel between S1 and S2 is down

```
S1# show etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
------+-------------+-----------+-----------------------------------------------
1 Po1(SD) - Fa0/1(D) Fa0/2(D)
-----------------------------------------------------------------------------------------------
S1# show run | begin interface Port-channel
interface Port-channel1
switchport mode trunk
!
interface FastEthernet0/1
switchport mode trunk
channel-group 1 mode auto
!
interface FastEthernet0/2
switchport mode trunk
channel-group 1 mode auto
!
<output omitted>
-----------------------------------------------------------------------------------------------
S2# show run | begin interface Port-channel
interface Port-channel1
switchport mode trunk
!
interface FastEthernet0/1
switchport mode trunk
channel-group 1 mode auto
!
interface FastEthernet0/2
switchport mode trunk
channel-group 1 mode auto
!
```

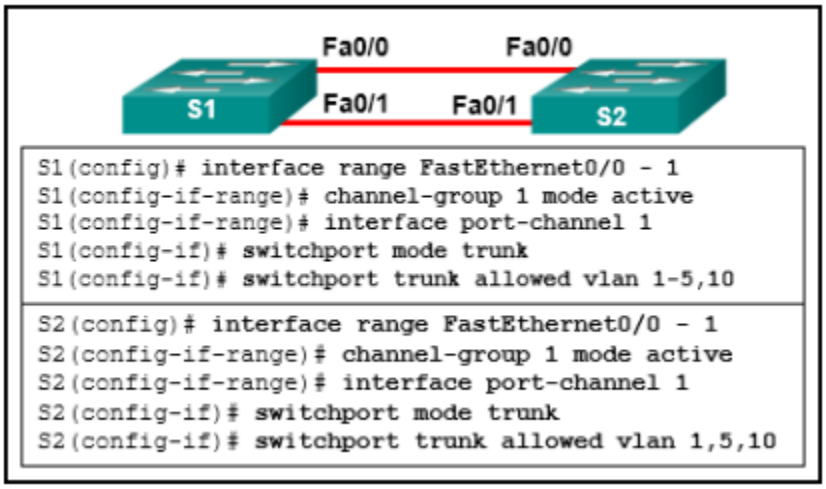
- Both sides of the link are set to the PAgP auto mode, which means that the interface will listen for PAgP packets but will not initiate negotiations.
- Neither side initiates negotiation, so the channel is down

(ii) What would you suggest to correct the issue shown in Q6(a) if the requirement is to use PAgP?

- EtherChannel and spanning tree must interoperate. For this reason, the order in which EtherChannel-related commands are entered is important. To correct this issue, you must first remove the port channel. Otherwise, spanning-tree errors cause the associate ports to go into a blocking or err-disabled state.
- Remove the port-channel 1 interface, and then configure the interfaces to use desirable mode. This can be done on one or both switches.
- Commands:

```
S1(config)# no interface Port-channel 1
S1(config)# interface range f0/1 - 2
S1(config-if-range)# channel-group 1 mode desirable
S1(config-if-range)# interface Port-channel 1
S1(config-if)# switchport mode trunk
```

7. An EtherChannel was configured between switches S1 and S2, but the interfaces do not form an EtherChannel. Identify and rectify the problem. Justify your answers.



- **Problem** - The EtherChannel was not configured with the same allowed range of VLANs on each interface
  - VLAN 1-5, 10 is not the same as VLAN 1, 5, 10
- **Solution** - The allowed range of VLANs must be the same on both switches. Example: VLAN 1-5, 10 are configured on both switches.

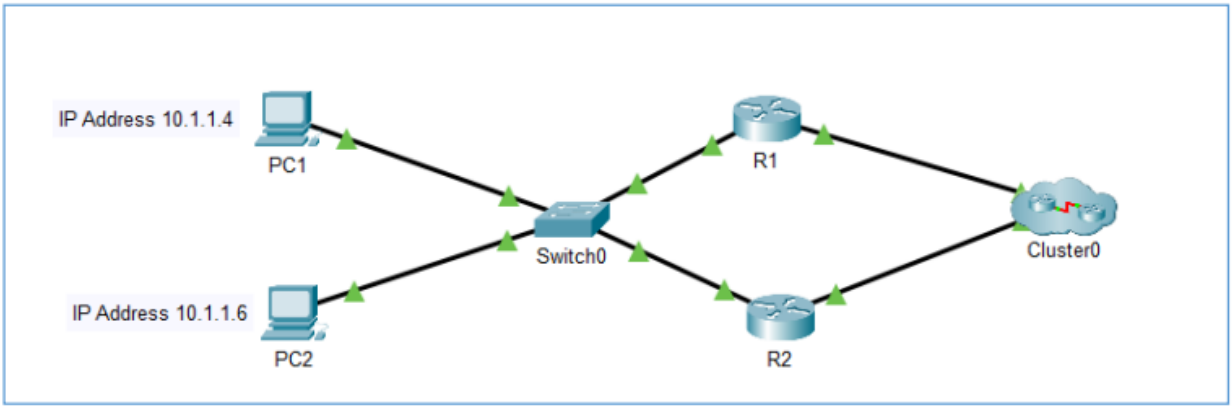
Tutorial 6: FHRP Concepts

1. What is the limitation of default gateway?
    - End devices are typically configured with a single default gateway IPv4. If the default gateway router interface fails, LAN hosts outside LAN connectivity.

2. What is the mechanism to overcome a single point of failure at the default gateway?
    - First hop redundancy protocols (FHRPs) are mechanisms that provide alternate default gateways in switched networks where two or more routers are connected to the same VLANs.
    - To prevent a single point of failure at the default gateway is to implement a virtual router. To implement this type of router redundancy, multiple routers are configured to work together to present the illusion of a single router to the hosts on the LAN. By sharing an IP address and a MAC address,two or more routers can act as a single virtual router.

3. List the options available for FHRP.
    - These are the options available for FHRPs:
        - HSRP and HSRP for IPv6
        - VRRPv2 and VRRPv3
        - GLBP and GLBP for IPv6
        - IRDP

4. With reference to Figure 6-1, answer the following questions



R1	R2
R1#configure terminal R1(config)#interface gi0/1 R1(config-if)#ip address 10.1.1.2 255.255.255.0 R1(config-if)#standby 1 ip 10.1.1.1 R1(config-if)#standby 1 priority 150 R1(config-if)#standby 1 preempt R1(config-if)#standby 2 ip 10.1.1.5 R1(config-if)#standby 2 priority 110 R1(config-if)#exit R1(config)#exit R1#	R2#configure terminal R2(config)#interface gi0/1 R2(config-if)#ip address 10.1.1.3 255.255.255.0 R2(config-if)#standby 1 ip 10.1.1.1 R2(config-if)#standby 1 priority 110 R2(config-if)#standby 2 ip 10.1.1.5 R2(config-if)#standby 2 priority 150 R2(config-if)#standby 2 preempt R2(config-if)#exit R2(config)#exit R2#

Table 6-1: HSPR configuration

a. What is the IP address assigned to R1 g0/1?
   10.1.1.2

b. What is the IP address assigned to R2 g0/1?
   10.1.1.3

c. What is the virtual IP address for standby group 1 in R1?
   10.1.1.1

d. What is the virtual IP address for standby group 1 in R2?
   10.1.1.1

e. Is the virtual IP address for standby group 1 in R1 and R2 must be the same?
   Yes

f. What is the virtual IP address for standby group 2 in R1?
   10.1.1.5

g. What is the virtual IP address for standby group 2 in R2?
   10.1.1.5

h. Is the virtual IP address for standby group 2 in R1 and R2 must be the same?
   Yes

i. What is the default gateway IP address for PC1?
   Either 10.1.1.1 or 10.1.1.5

j. What is the default gateway IP address for PC2?
   Either 10.1.1.1 or 10.1.1.5

k. Explain “standby 1 priority 150”.
   - HSRP priority can be used to determine the active router
   - The router with the highest HSRP priority will become the active router
   - By default, the HSRP priority is 100
   - If the priorities are equal, the router with the numerically highest IPv4 address is elected as the active router
   - To configure a router to be the active router, use the standby priority interface command. The range of the HSRP priority is 0 to 255

l. Explain “standby 1 preempt”
   - Preemption is the ability of an HSRP router to trigger the re-election process. With the preemption enabled, a router that comes online with a higher HSRP priority will assume the role of the active router.
   - Preemption only allows a router to become the active router if it has a higher priority.

m. Why is the purpose setting 2 HSRP standby groups in R1 and R2
   - BY configuring multiple HSRP groups on a single interface, HSRP load balancing can be achieved.

Tutorial 7: Basic Routing Concepts and EIGRP

1. Discuss the purpose of routing and the functions of a router.

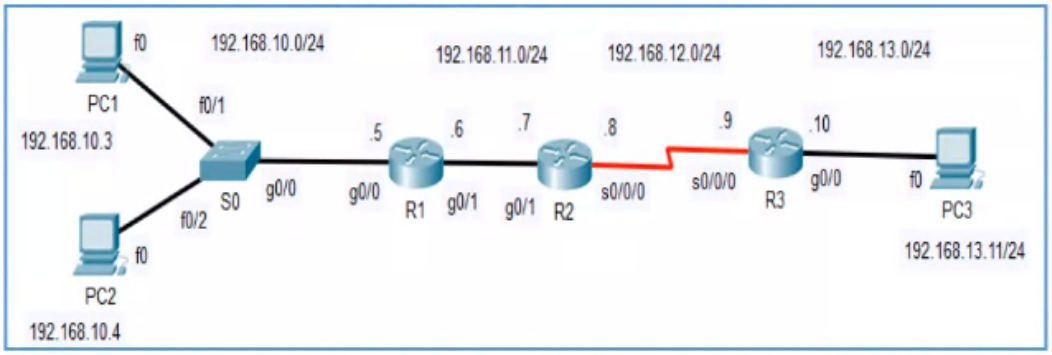
Purpose: A router is a specialized computers that connects multiple networks and responsible for the routing of traffic between networks.

Functions:

- Determine the best path to send packets
  Uses its routing table to determine path
- Forward packets toward their destination
  Forwards packet to interface indicated in routing table.
  Encapsulates the packet and forwards out toward destination.

2. What is the purpose of a routing protocol?
Answer: D
   A. It is used to build and maintain ARP tables.
   B. It provides a method for segmenting and reassembling data packets.
   C. It allows an administrator to devise an addressing scheme for the network.
   D. It allows a router to share information about known networks with other routers
   E. It provides a procedure for encoding and decoding data into bits for packet forwarding.

3. With reference to the following topology diagram, answer the questions:



   a. During the process of encapsulation, how does the PC1 determine if the packet is destined for a host on a remote network?
   Answer: by performing the AND operation on the destination IP address and its own subnet mask

   b. When PC1 sends a packet to PC2, the packet is forwarded out the host interface to switch and the switch forward it the destination device. The router does not need to get involved. True or False? True

c. When PC1 sends a packet to PC3, the packet is forwarded to the default gateway because the host device cannot communicate with devices outside of the local network. True or False? True

d. The default gateway is the device that routes traffic from the remote network to devices on local networks. True or False?
False. The default gateway is the device that routes traffic from the local network to devices on remote networks.

e. Fill in the information for R1. Assume that the network is already converged and the routing protocol used is RIP.

Network	Hops	Next-hop-IP	Exit Interface
192.168.10.0	0	Directly connected	g0/0
192.168.11.0	0	Directly connected	g0/1
192.168.12.0	1	192.168.11.7	g0/1
192.168.13.0	2	192.168.11.7	g0/1

f. Fill in the information for R2. Assume that the network is already converged and the routing protocol used is RIP.

Network	Hops	Next-hop-IP	Exit Interface
192.168.10.0	1	192.168.11.6	g0/1
192.168.11.0	0	Directly connected	g0/1
192.168.12.0	0	Directly connected	s0/0/0
192.168.13.0	1	192.168.12.9	s0/0/0

g. Fill in the information for R3. Assume that the network is already converged and the routing protocol used is RIP.

Network	Hops	Next-hop-IP	Exit Interface
192.168.10.0	2	192.168.12.8	s0/0/0
192.168.11.0	1	192.168.12.8	s0/0/0
192.168.12.0	0	Directly connected	s0/0/0
192.168.13.0	0	Directly connected	g0/0

4. "Best path is selected by a routing protocol based on the value or metric it uses to determine the distance to reach a network."
Explain the term "*metric*" in the given statement. Give **THREE (3)** examples of metric.

- A metric is the value used to measure the distance to a given network.
- Dynamic routing protocols use their own rules and metrics to build and update routing tables for example:
  - Routing Information Protocol (RIP) - **Hop count**
  - Open Shortest Path First (OSPF) - **Cost** based on cumulative bandwidth from source to destination
  - Enhanced Interior Gateway Routing Protocol (EIGRP) - **Bandwidth, delay, load, reliability**

5. When a router learns that multiple paths are available to a destination network from the same routing protocol, which factor is considered by a router to choose the best path to forward a packet?

R 192.168.30.0 [120/5] via 200.20.20.1, 00:00:07, s0/0/0
R 192.168.30.0 [120/3] via 200.20.20.1, 00:00:07, s0/0/0

Answer: The path with the lowest metric

6. When a router learns that multiple paths are available to a destination network from the different routing protocols, which factor is considered by a router to choose the best path to forward a packet?
R 192.168.30.0 [120/5] via 200.20.20.1, 00:00:07, s0/0/0
D 192.168.30.0 [90/2945137] via 200.20.20.1, 00:00:07, s0/0/1
D 192.168.30.0 [90/2782114] via 200.20.20.1, 00:00:07, s0/0/0

Answer: Choose the routing protocol with lower AD
then choose the best path which has lowest metric

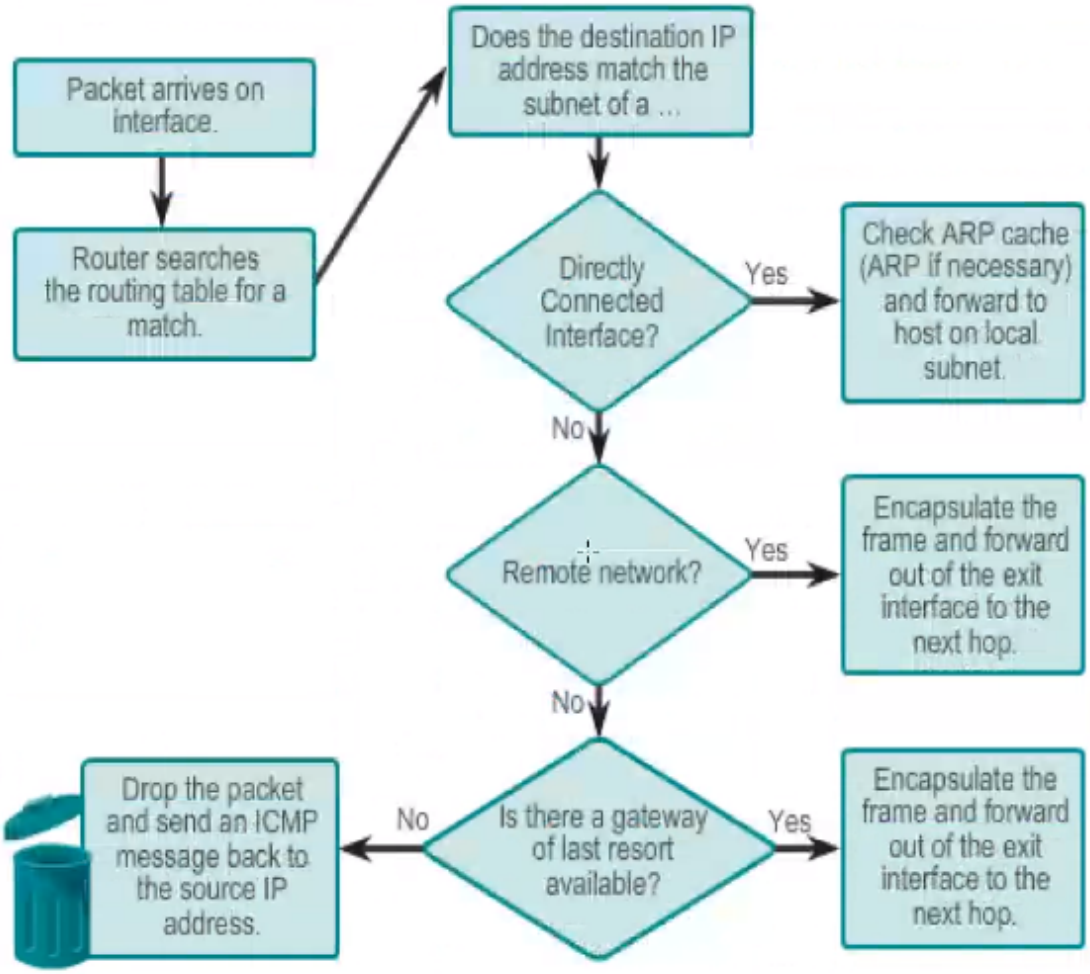
- With reference to Figure 1, when a packet with desination address 192.168.3.3/24 arrive at R1, what is the decision of the R1 ?
- When packet arrives on interface, router searches the routing table for a match.

- The destination IP address (192.168.3.3) matched the subnet of a remote network(192.168.3.0), it encapsulates the frame and forward out the exit interface(s0/0/0) to the next hop.

- With reference to Figure 1, when a packet with desination address 192.168.4.3/24 arrive at R1, what is the decision of the R1 ?
- When packet arrives on interface, router searches the routing table for a match.
- If the destination IP (192.168.4.3) does not match any directly connected interface or remote network, it checks the availability of a gateway of last resort (0.0.0.0/0). Gateway of last resort is **not** available in the routing table, it drops the packet and send an ICMP message back to the source IP address.

c. With reference to Figure 2, when a packet with desination address 192.168.4.3/24 arrive at R1, what is the decision of the R1 ?

- When packet arrives on interface, router searches the routing table for a match.
- If the destination IP (192.168.4.3) does not match any directly connected interface or remote network, it checks the availability of a gateway of last resort (0.0.0.0/0). Gateway of last resort is available in the routing table, it encapsulates the frame and forward out the exit interface(S0/0/0) to the next hop.


Packet arrives on interface.
Router searches the routing table for a match.
Does the destination IP address match the subnet of a ...
Directly Connected Interface?
Yes
Check ARP cache (ARP if necessary) and forward to host on local subnet.
No
Remote network?
Yes
Encapsulate the frame and forward out of the exit interface to the next hop.
No
Is there a gateway of last resort available?
No
Drop the packet and send an ICMP message back to the source IP address.
Yes
Encapsulate the frame and forward out of the exit interface to the next hop.

Answer:

Problems	Solutions
R2 is configured with wrong EIGRP	AS number must be the same = 100

AS number router eigrp 110	router eigrp 100
Missing a network statement in R2	Add the following network statement in R2. router eigrp 100 network 172.16.1.32 0.0.0.15
Missing default route in R1	ip route 0.0.0.0 0.0.0.0 Serial0/0/1
Missing redistribute static in R1	In router R1, add the statement redistribute static router eigrp 100 redistribute static

Tutorial 8

1. AAA stands for Authentication, Authorization, and Accounting, and provides the primary framework to set up access control on a network device. Explain Authentication, Authorization, and Accounting.
   - AAA is a way to control who is permitted to access a network (authenticate), what they can do while they are there (authorize), and to audit what actions they performed while accessing the network (accounting).

2. Local and server-based are two common methods of implementing AAA authentication. Differentiate Local AAA authentication and server-based AAA authentication.

Local AAA Authentication	**Server-Based AAA Authentication**
Method stores usernames and passwords locally in a network device (e.g., Cisco router).	With the server-based method, the router accesses a central AAA server.
Users authenticate against the local database.	The AAA server contains the usernames and password for all users.
Local AAA is ideal for small networks.	The router uses either the Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+) protocols to communicate with the AAA server.
	When there are multiple routers and switches, server-based AAA is more appropriate.

3. Briefly explain AAA authorization.
   - AAA authorization is automatic and does not require users to perform additional steps after authentication.
   - Authorization governs what users can and cannot do on the network after they are authenticated.
   - Authorization uses a set of attributes that describes the user's access to the network. These attributes are used by the AAA server to determine privileges and restrictions for that user.

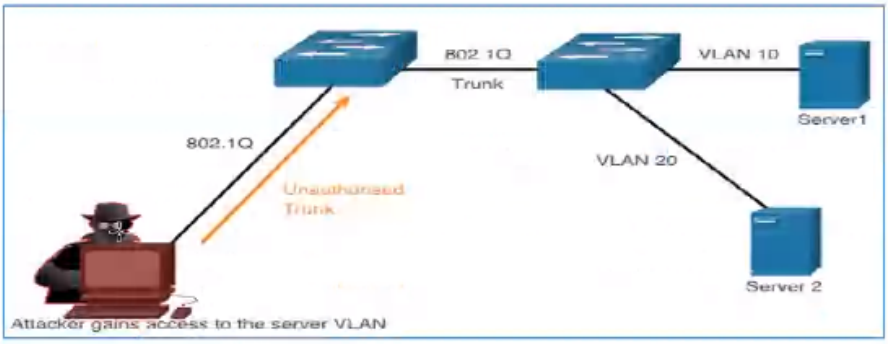
4. Briefly explain AAA accounting.
   - AAA accounting collects and reports usage data. This data can be used for such purposes as auditing or billing. The collected data might include the start and stop connection times, executed commands, number of packets, and number of bytes.
   - A primary use of accounting is to combine it with AAA authentication.
   - The AAA server keeps a detailed log of exactly what the authenticated user does on the device, as shown in the figure. This includes all EXEC and configuration commands issued by the user.
   - The log contains numerous data fields, including the username, the date and time, and the actual command that was entered by the user. This information is useful when troubleshooting devices. It also provides evidence for when individuals perform malicious acts.

5. Give example for the following of Switch Attack Categories.

Category	**Examples**
MAC Table Attacks	Includes MAC address flooding attacks.
VLAN Attacks	Includes VLAN hopping and VLAN double-tagging attacks. It also includes attacks between devices on a common VLAN.
DHCP Attacks	Includes DHCP starvation and DHCP spoofing attacks.
ARP Attacks	Includes ARP spoofing and ARP poisoning attacks.
Address Spoofing Attacks	Includes MAC address and IP address spoofing attacks.
STP Attacks	Includes Spanning Tree Protocol manipulation attacks.

6. Describe the MAC Address Table Flooding attack.
   - All MAC tables have a fixed size and consequently, a switch can run out of resources in which to store MAC addresses. MAC address flooding attacks take advantage of this limitation by bombarding the switch with fake source MAC addresses until the switch MAC address table is full.
   - When this occurs, the switch treats the frame as an unknown unicast and begins to flood all incoming traffic out all ports on the same VLAN without referencing the MAC table. This condition now allows a threat actor to capture all of the frames sent from one host to another on the local LAN or local VLAN.

7. With reference to the following diagram, explain VLAN Hopping Attacks.



   - A VLAN hopping attack enables traffic from one VLAN to be seen by another VLAN without the aid of a router. In a basic VLAN hopping attack, the threat actor configures a host to act like a switch to take advantage of the automatic trunking port feature enabled by default on most switch ports.
   - The threat actor configures the host to spoof 802.1Q signaling and Cisco-proprietary Dynamic Trunking Protocol (DTP) signaling to trunk with the connecting switch. If successful, the switch establishes a trunk link with the host, as shown in the figure. Now the threat actor can access all the VLANs on the switch. The threat actor can send and receive traffic on any VLAN, effectively hopping between VLANs.

8. Two types of DHCP attacks are DHCP starvation and DHCP spoofing. Explain DHCP starvation and DHCP spoofing attack.

- **DHCP Starvation Attack –** The goal of this attack is to create a DoS for connecting clients. DHCP starvation attacks require 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, including the following:
  - **Wrong default gateway** - The rogue server provides an invalid gateway or the IP address of its host to create a man-in-the-middle attack. This may go entirely undetected as the intruder intercepts the data flow through the network.
  - **Wrong DNS server** - The rogue server provides an incorrect DNS server address pointing the user to a nefarious website.
  - **Wrong IP address** - The rogue server provides an invalid IP address effectively creating a DoS attack on the DHCP client.

9. Fill in the blank. What are the mitigation methods for the following LAN attacks?

LAN attacks	**Mitigation methods**
MAC address flooding attacks	implement port security
VLAN hopping and VLAN double-tagging attacks	• Disable trunking on all access ports. • Disable auto trunking on trunk links so that trunks must be manually enabled. • Be sure that the native VLAN is only used for trunk links.
DHCP starvation and DHCP spoofing attacks	Both attacks are mitigated by implementing DHCP snooping.
ARP spoofing and ARP poisoning attacks	mitigated by implementing Dynamic ARP Inspection (DAI).
MAC address and IP address spoofing attacks.	mitigated by implementing IP Source Guard (IPSG).
Spanning Tree Protocol manipulation attacks	mitigated by implementing BPDU Guard on all access ports

Tutorial 9

1. The simplest and most effective method to prevent MAC address table overflow attacks is to enable port security. Explain port security.
   - Port security limits the number of valid MAC addresses allowed on a port. It allows an administrator to manually configure MAC addresses for a port or to permit the switch to dynamically learn a limited number of MAC addresses.
   - When a port configured with port security receives a frame, the source MAC address of the frame is compared to the list of secure source MAC addresses that were manually configured or dynamically learned on the port.
   - By limiting the number of permitted MAC addresses on a port to one, port security can be used to control unauthorized access to the network.

2. Explain the steps to mitigate a VLAN hopping attack.

   Use the following steps to mitigate VLAN hopping attacks:

Step 1:	Disable DTP (auto trunking) negotiations on non-trunking ports by using the switchport mode access interface configuration command.
Step 2:	Disable unused ports and put them in an unused VLAN.
Step 3:	Manually enable the trunk link on a trunking port by using the switchport mode trunk command.
Step 4:	Disable DTP (auto trunking) negotiations on trunking ports by using the switchport nonegotiate command.
Step 5:	Set the native VLAN to a VLAN other than VLAN 1 by using the switchport trunk native vlan vlan_number command.

3. The network attackers can manipulate the Spanning Tree Protocol (STP) to conduct an attack by spoofing the root bridge and changing the topology of a network. How to mitigate a STP attack?

   To mitigate STP attacks, use PortFast and Bridge Protocol Data Unit (BPDU) Guard:

   PortFast
   - PortFast immediately brings a port to the forwarding state from a blocking state, bypassing the listening and learning states.
   - Apply to all end-user access ports.

   BPDU Guard
   - BPDU guard immediately error disables a port that receives a BPDU.
   - Like PortFast, BPDU guard should only be configured on interfaces attached to end devices.

4. There are some port security configuration errors depicted in Figure 3-5. Interface g0/2 should be configured using sticky secure MAC addresses. In addition, the port is assigned to VLAN 20. The requirement is to set the maximum address to 5 and when violation occurred, the switch would drop unknown MAC address and a security notification is not presented by the switch. Document your answer using Table 3-2 in your answer sheet.

```
Switch(config-if)#int f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security max 6
Switch(config-if)#switchport port-security violation shutdown
```

Figure 3-5: Configuration for sticky secure MAC address

Error Configurations	Solutions

Table 3-2: Documentation Table

(10 marks)

Answer:

Error Configurations	Solutions
int f0/1 (1 mark)	Int g0/2 (1 mark)
Command missing (1 mark)	switchport access vlan 20 (1 mark)
switchport port-security max 6 (1 mark)	switchport port-security max 5 (1 mark)
Command missing (1 mark)	switchport port-security mac-address sticky (1 mark)
switchport port-security violation **shutdown** (1 mark)	switchport port-security violation **protect** (1 mark)

Tutorial 10

1. List the IEEE standard the following wireless network.

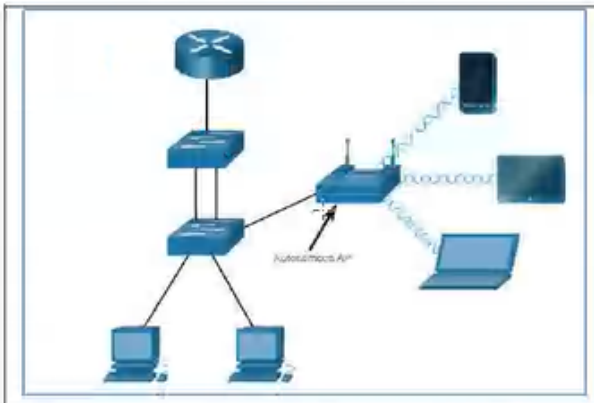
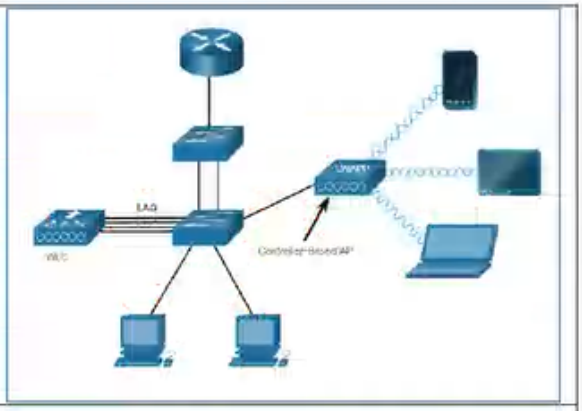
- **Wireless Personal-Area Network (WPAN)** – Low power and short-range (20-30ft or 6-9 meters). Based on IEEE 802.15 standard and 2.4 GHz frequency. Bluetooth and Zigbee are WPAN examples.
- **Wireless LAN (WLAN)** – Medium sized networks up to about 300 feet. Based on IEEE 802.11 standard and 2.4 or 5.0 GHz frequency.
- **WiMAX (Worldwide Interoperability for Microwave Access) – Alternative broadband wired internet connections. IEEE 802.16 WLAN standard for up 30 miles (50 km).**

2. Which 802.11 standards use both the 2.4GHz and 5 GHz radio frequencies?

IEEE Standard	Radio Frequency	Description
802.11n	2.4 and 5 GHz	Data rates 150 – 600 Mb/s Require multiple antennas with MIMO technology
802.11ax	2.4 and 5 GHz	High-Efficiency Wireless (HEW) Capable of using 1 GHz and 7 GHz frequencies

3. What is a function of a wireless router?

- **Access point** - This provides 802.11a/b/g/n/ac wireless access.
- **Switch** - This provides a four-port, full-duplex, 10/100/1000 Ethernet switch to interconnect wired devices.
- **Router** - This provides a default gateway for connecting to other network infrastructures, such as the internet.

	
These are standalone devices configured using a command line interface or a GUI, as shown in the figure.	These devices require no initial configuration and are often called lightweight APs (LAPs). LAPs use the Lightweight Access Point Protocol (LWAPP) to communicate with a WLAN controller (WLC), as shown in the next figure. Controller-based APs are useful in situations where many APs are required in the network. As more APs are added, each AP is automatically configured and managed by the WLC.
Autonomous APs are useful in situations where only a couple of APs are required in the organization.	Notice in the figure that the WLC has **four** ports connected to the switching infrastructure. These four ports are configured as a link aggregation group (LAG) to bundle them together. Much like how EtherChannel operates. LAG provides redundancy and load-balancing. All the ports on the switch that are connected to the WLC need to be trunking and configured with EtherChannel on. However, LAG does not operate exactly like EtherChannel. The WLC does not support Port Aggregation Protocol (PaGP) or Link Aggregation Control Protocol (LACP).

A home router is an example of an autonomous AP because the entire AP configuration resides on the device. If the wireless demands increase, more APs would be required.	The diagram illustrates the use of a lightweight access point and a wireless LAN controller. Several wireless devices are communicating with a controller-based AP using LWAPP. The AP has a wired connection to a central switch. Above the switch are two connections to another switch which is connected to a router. Two wired hosts are connected below the central switch. A WLC is connected to the central switch at the left via four physical links using LAG.
Each AP would operate independent of other APs and each AP would require manual configuration and management. This would become overwhelming if many APs were needed.	

5. WLANs use carrier sense multiple access with collision avoidance (CSMA/CA) as the method to determine how and when to send data on the network. Explain CSMA/CA.

A wireless client does the following:

- Listens to the channel to see if it is idle, which means that is senses no other traffic is currently on the channel. The channel is also called the carrier.
- Sends a ready to send (RTS) message to the AP to request dedicated access to the network.
- Receives a clear to send (CTS) message from the AP granting access to send.
- If the wireless client does not receive a CTS message, it waits a random amount of time before restarting the process.
- After it receives the CTS, it transmits the data.
- All transmissions are acknowledged. If a wireless client does not receive an acknowledgment, it assumes a collision occurred and restarts the process.

6. Explain Control and Provisioning of Wireless Access Points (CAPWAP).

- CAPWAP is an IEEE standard protocol that enables a WLC to manage multiple APs and WLANs. CAPWAP is also responsible for the encapsulation and forwarding of WLAN client traffic between an AP and a WLC.

- CAPWAP is based on LWAPP but adds additional security with Datagram Transport Layer Security (DTLS). CAPWAP establishes tunnels on User Datagram Protocol (UDP) ports. CAPWAP can operate either over IPv4 or IPv6, as shown in the figure, but uses IPv4 by default.

- IPv4 and IPv6 can use UDP ports 5246 and 5247. However, CAPWAP tunnels use different IP protocols in the frame header. IPv4 uses IP protocol 17 and IPv6 uses IP protocol 136.

7. What is Datagram Transport Layer Security (DTLS)?

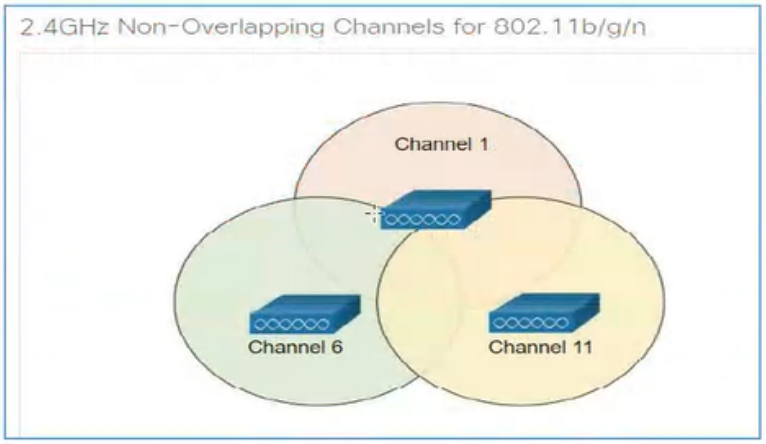
- DTLS is a protocol which provides security between the AP and the WLC. It allows them to communicate using encryption and prevents eavesdropping or tampering.
- DTLS is enabled by default to secure the CAPWAP control channel but is disabled by default for the data channel, as shown in the figure. All CAPWAP management and control traffic exchanged between an AP and WLC is encrypted and secured by default to provide control plane privacy and prevent Man-In-the-Middle (MITM) attacks.
- CAPWAP data encryption is optional and is enabled per AP. Data encryption requires a DTLS license to be installed on the WLC prior to being enabled on an AP. When enabled, all WLAN client traffic is encrypted at the AP before being forwarded to the WLC and vice versa.

8. The saturation of the wireless medium degrades the quality of the communication. Over the years, a number of techniques have been created to improve wireless communication and alleviate saturation. These techniques mitigate channel saturation by using the channels in a more efficient way.
List down the techniques used.
   - **Direct-Sequence Spread Spectrum (DSSS).**
   - **Frequency-Hopping Spread Spectrum (FHSS)**
   - **Orthogonal Frequency-Division Multiplexing (OFDM)**

- **Direct-Sequence Spread Spectrum (DSSS)** - A modulation technique designed to spread a signal over a larger frequency band. Used by 802.11b devices to avoid interference from other devices using the same 2.4 GHz frequency.
- **Frequency-Hopping Spread Spectrum (FHSS)** - Transmits radio signals by rapidly switching a carrier signal among many frequency channels. Sender and receiver must be synchronized to "know" which channel to jump to. Used by the original 802.11 standard.
- **Orthogonal Frequency-Division Multiplexing (OFDM)** - A subset of frequency division multiplexing in which a single channel uses multiple sub-channels on adjacent frequencies. OFDM is used by a number of communication systems including 802.11a/g/n/ac.

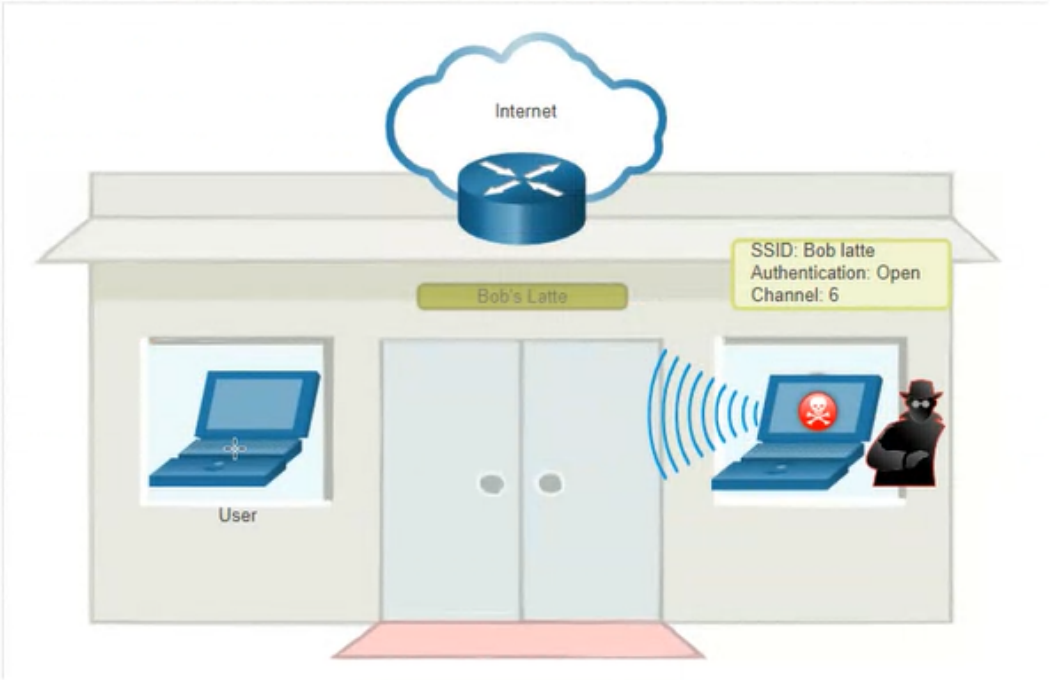
9. Interference occurs when one signal overlaps a channel reserved for another signal, causing possible distortion. How do you to solve this problem?

The best practice for 2.4GHz WLANs that require multiple APs is to use non-overlapping channels, although most modern APs will do this automatically. If there are three adjacent APs, use channels 1, 6, and 11, as shown in the figure.

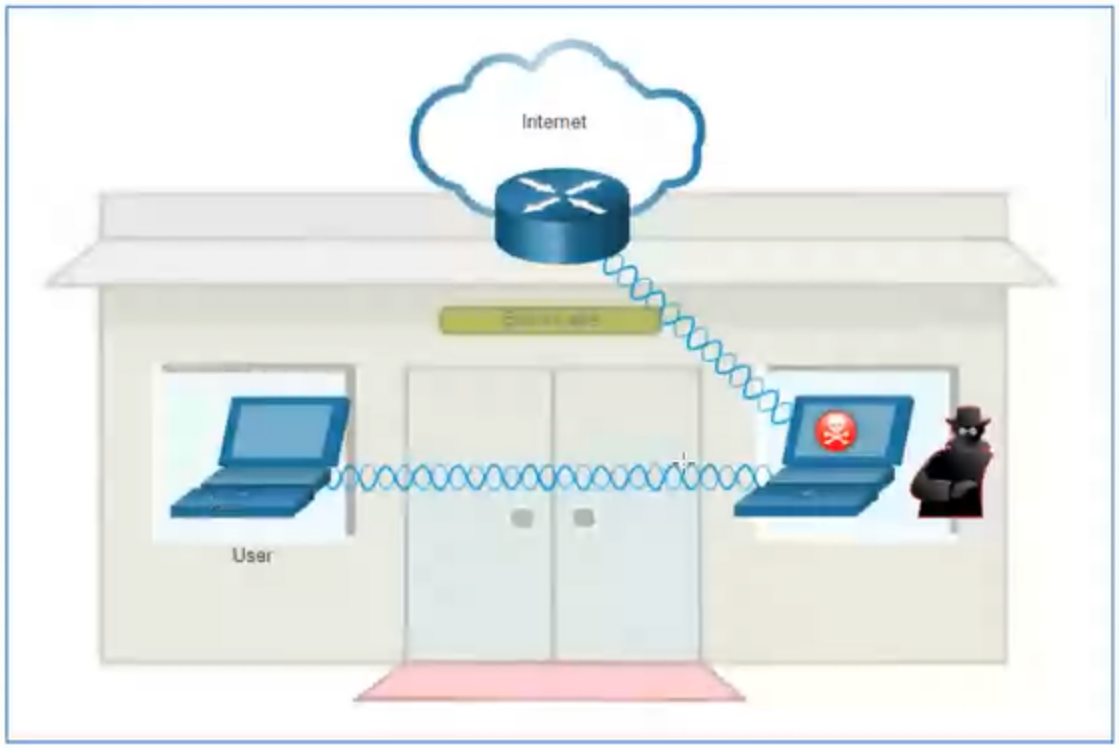


10. Explain man-in-the-middle (MITM) attack.

- 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. There are many ways in which to create a MITM attack.
- 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, as shown in the figure. Locations offering free Wi-Fi, such as airports, cafes, and restaurants, are particularly popular spots for this type of attack due to the **open authentication.**



- Wireless clients attempting to connect to a WLAN would see two APs with the same SSID offering wireless access. Those near the rogue AP find the stronger signal and most likely associate with it. User traffic is now sent to the rogue AP, which in turn captures the data and forwards it to the legitimate AP, as shown in the figure. Return traffic from the legitimate AP is sent to the rogue AP, captured, and then forwarded to the unsuspecting user. The attacker can steal the user's passwords, personal information, gain access to their device, and compromise the system.



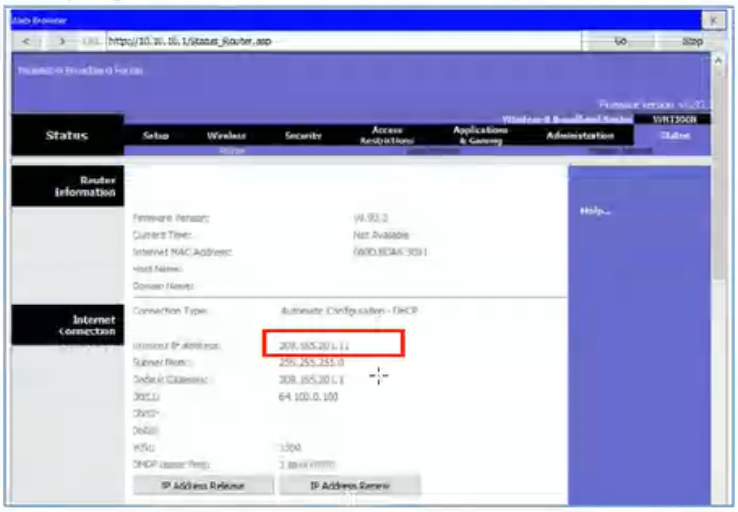
- Defeating an attack like an MITM attack depends on the sophistication pf the WLAN infrastructure and the **vigilance** in monitoring activity on the network. The process begins with identifying legitimate devices on the WLAN. To do this, users must be authenticated. After all of the legitimate devices are known, the network can be monitored for abnormal devices or traffic.

11. List down steps for the basic wireless setup

Basic wireless setup includes the following steps:

- View the WLAN defaults.
- Change the network mode.
- Configure the SSID.
- Configure the channel.
- Configure the security mode.
- Configure the passphrase.

12. Briefly explain Network Address Translation (NAT) based on the IP address given.



- The 209.165.201.11 IPv4 address is publicly routable on the internet.
- Any address with the 10 in the first octet is a private IPv4 address and cannot be routed on the internet.
- Therefore, the router will use a process called Network Address Translation (NAT) to convert private IPv4 addresses to internet-routable IPv4 addresses.
- With NAT, a private (local) source IPv4 address is translated to a public (global) address.
- The process is reversed for incoming packets. The router is able to translate many internal IPv4 addresses into public addresses, by using NAT.

13. Many wireless routers have an option for configuring Quality of Service (QoS). Why need to configure QoS?
    a. By configuring QoS, you can guarantee that certain traffic types, such as voice and video, are prioritized over traffic that is not as time-sensitive, such as email and web browsing.
    b. On some wireless routers, traffic can also be prioritized on specific ports.

14. What is port forwarding?

- Wireless routers typically block TCP and UDP ports to prevent unauthorized access in and out of a LAN.
- However, there are situations when specific ports must be opened so that certain programs and applications can communicate with devices on different networks.
- Port forwarding is a rule-based method of directing traffic between devices on separate networks.
- Port triggering allows the router to temporarily forward data through inbound ports to a specific device.
- You can use port triggering to forward data to a computer only when a designated port range is used to make an outbound request.