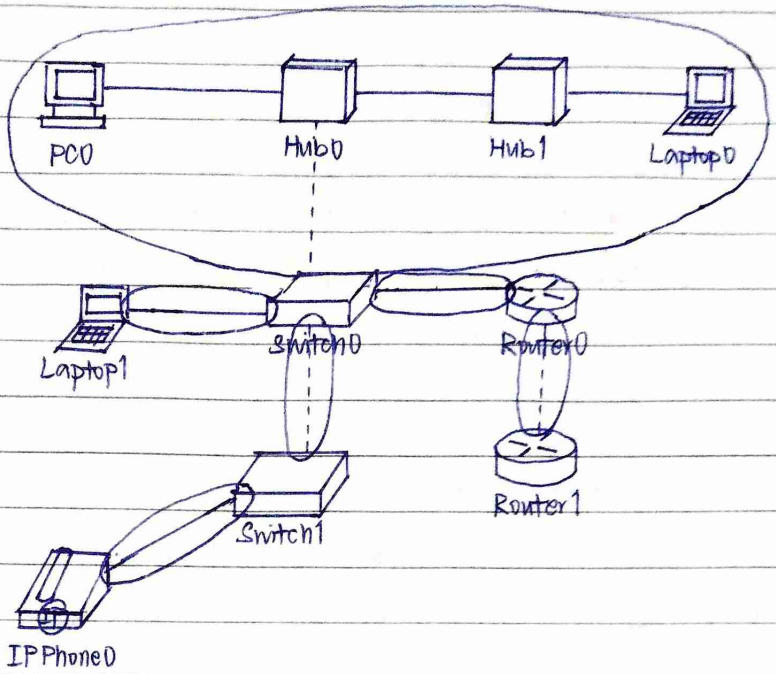
No: SRT Date:

9 May 2022

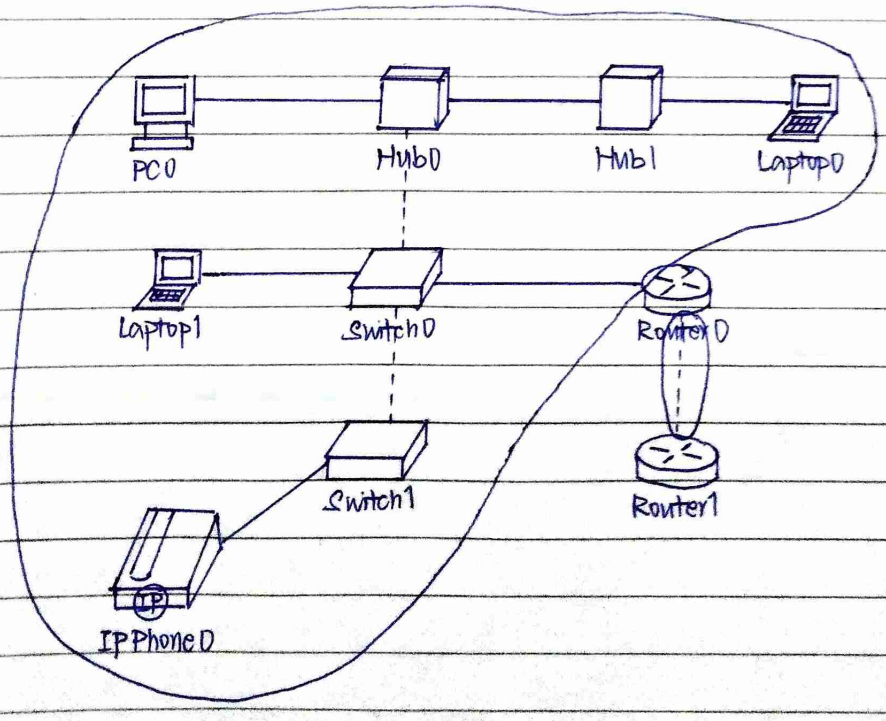
Question 1

a)(i)



6 collision domains

(ii)



2 broadcast domains

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

b) (i)

Source IP Address	Destination IP Address	Source MAC Address	Destination MAC Address
192.168.10.2	192.168.20.2	AA-AA-AA-AA-AA-AA	11-11-11-11-11-11

(ii) When Switch1 receives a frame from PC4, it will add the source MAC address (PC4) into the MAC address table.
Switch1 will examine the destination MAC address (PC3).
Since the destination MAC address is not exist in the MAC address table, all the interfaces are flooded out except the one it was received.

c) Store-and-forward switching method will perform error-checking. It will check the Frame Check Sequence (FCS) for CRC error. Besides, it will perform buffering. The ingress interface will buffer the frame while it checks FCS.

d) No. PC1 and Server are in different network. In Switch1, the vlans allowed on trunk do not include VLAN 20. Since VLAN 20 is not in the trunk, therefore Server cannot communicate with PC1 which in another network.

No: .....

Date: .....

Question 2

a) (i) Switch 3

(ii) Switch 1: F0/1

Switch 2: F0/1

Switch 4: F0/1

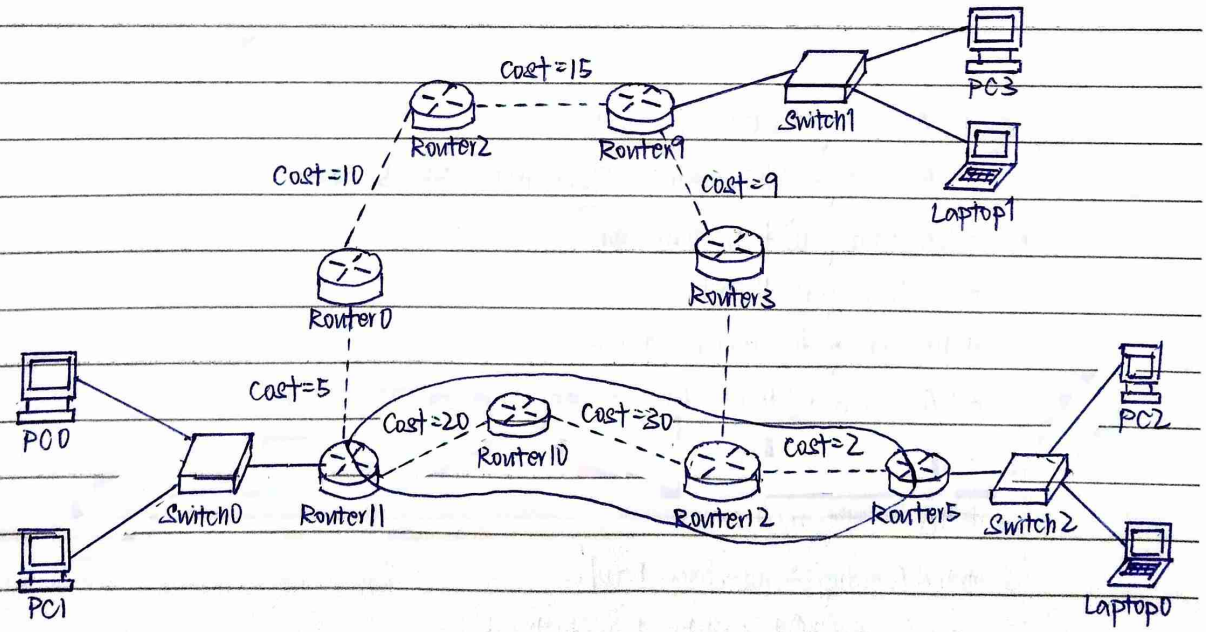
(iii) Switch 3: F0/1, F0/2

Switch 1: F0/2

Switch 2: F0/2

(iv) Switch 4: F0/2

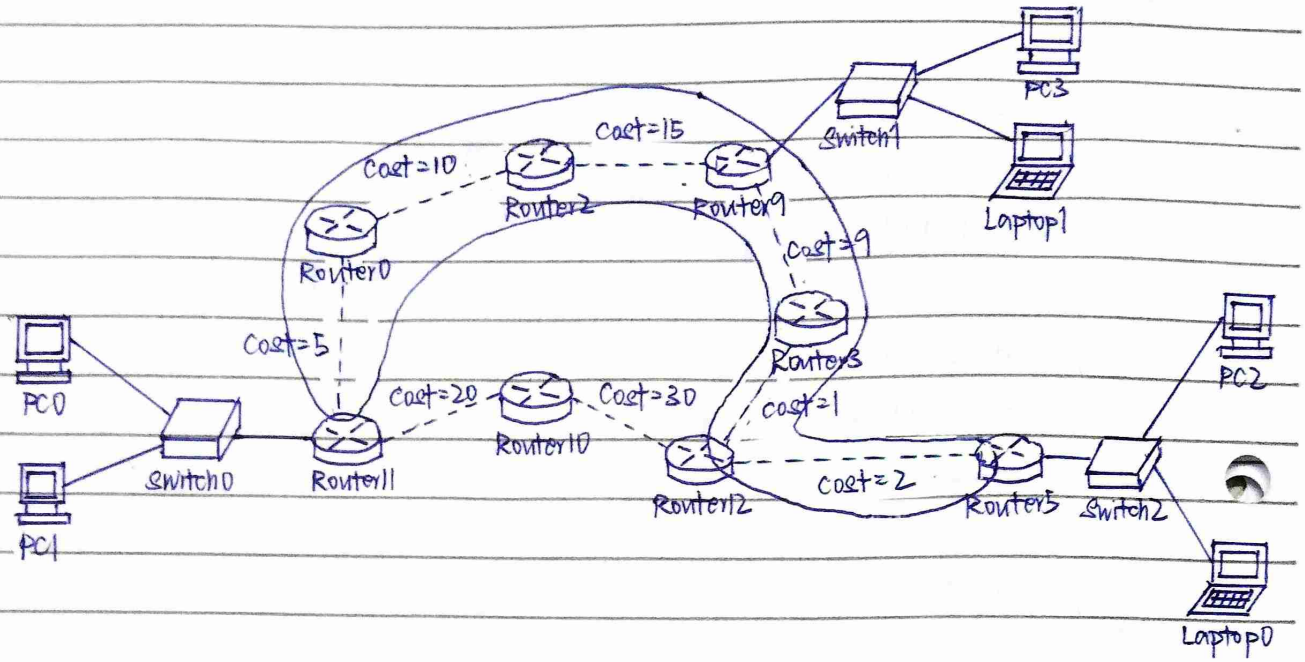
b) (i)



Path - 3 hop counts

No: Date:

(ii)



Path = 5+10+15+9+1+2

= 42

c) Switch A (config)# interface vlan 10
Switch A (config-if)# ip address 172.16.10.1 255.255.255.0
Switch A (config-if)# no shutdown
Switch A (config-if)# exit
Switch A (config)# interface vlan 20
Switch A (config-if)# ip address 172.16.20.1 255.255.255.0
Switch A (config-if)# no shutdown
Switch A (config-if)# exit
Switch A (config)# interface Fa0/1
Switch A (config-if)# switchport mode trunk
Switch A (config-if)# switchport trunk allowed vlan 10, 20
Switch A (config-if)# exit
Switch A (config)# interface Fa0/2
Switch A (config-if)# switchport mode trunk
Switch A (config-if)# switchport trunk allowed vlan 10,20
Switch A (config-if)# exit
Switch A (config)# end

No: Date:

Question 3

a) (i) Routing Information Protocol (RIP)

(ii) 2 directly connected routes

(iii) [120] represents the administrative distance. It used to determine which route to install in the routing table.
[1] represents the metric associated with the route.

(iv) "S*" is static candidate default. It is default gateway that connect to Internet Services Provider (ISP).

"S" stands for "Static" routes. Static routes are manually configured by the network administrator.

(v) Open Shortest Path First (OSPF) is an open standard protocol and is suitable for use within enterprise networks and Internet Service Provider (ISP) network.

Intermediate System to Intermediate System (IS-IS) operates by distributing link-state information through the network and calculating the best paths based on that information.

b) channel-group 1 mode in both switches S1 and S2 are passive. Although both of them are using LACP EtherChannel, the EtherChannel cannot form as both sides are waiting for other side to initiate the EtherChannel negotiation.

switchport trunk allowed vlan in switch S1 is vlan 1, vlan 2, vlan 3 and vlan 4, but for switch S2 only have vlan 1, vlan 2 and vlan 3. EtherChannel cannot be formed since both sides trunk allowed vlan are not the same.

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

c) Hot Standby Router Protocol (HSRP). It allows for transparent failover of a first-hop IPv4 device. HSRP is used in a group of routers for selecting an active device and a standby device. The standby device will take over when the active device fails.

Virtual Router Redundancy Protocol version 2 (VRRPv2). It is a non-proprietary election protocol that dynamically assigns responsibility for one or more virtual routers to the VRRP routers on an IPv4 address. One router is elected as the virtual router master, while other routers act as backups.

No: Date:

Question 4

a) AAA stands for Authentication, Authorization and Accounting. Authentication refers to who is permitted to access a network. Muthu only open the access to Ali instead of sharing to everyone or public. Authorization refers to what they can do while they are there. Ali can only view or read the top-secret solution for the final exam, he can't edit or make any changes on it. Accounting refers to audit what actions that performed while accessing the network. It collects and reports usage data to Muthu who is the owner of the document.

b)
```
Switch1 (config)# interface F0/1
Switch1 (config-if)# switchport mode access
Switch1 (config-if)# switchport access vlan 10
Switch1 (config-if)# switchport port-security
Switch1 (config-if)# switchport port-security mac-address sticky
Switch1 (config-if)# switchport port-security maximum 3
Switch1 (config-if)# switchport port-security violation restrict
```

c) MAC Table Attacks. It includes MAC address flooding attacks. 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.

To mitigate MAC address table overflow attacks, network administrators must implement port security. Port security will only allow a specified number of source MAC addresses to be learned on the port.