Final Exam

Name : Pritesh Gandhi

1) If you were to implement a switching network architecture for a financial firm where the speed, bandwidth and low latency switching are of utmost importance, what switching method would you use. Please provide a detailed explanation why you would choose this particular method and what importance it may hold in the overall design and implementation.

Answer

➔

Before deciding on which method to use, we will look into switching methods first. As we know, we have 2 **main** switching methods:

(a) Store-and-forward switching method
(b) Cut-through switching method

a) Store-and-forward switching method :
In this method, frame forwarding starts only after receiving the whole frame. The switch first receives the whole frame & checks for errors using FCS (Frame Check Sequence). The switch drops the packets with errors. This process takes very much time which in turn results in low speed & so high latency which is not desirable for the given scenario.

b) Cut-through switching method :
In this method, the switch starts frame forwarding immediately after receiving the destination MAC address. So the switch does not wait for the whole frame & starts immediate transmission, usually after receiving first 6 bytes where the destination MAC address resides in the frame, without checking the frame for the errors. Because of immediate frame forwarding, low latency & high speed is achieved but the bandwidth is consumed unnecessarily as the corrupt frames are forwarded by the switch. So efficient use of bandwidth is not achieved.

c) Fragment-free switching method :
This switching method is the variation of the cut-through method. The switch holds the first 64 bytes of the frames & checks for the collision. The switch discards the whole frame if it is damaged. Usually the first 64 bytes is where the errors occur. The frames which are less 64 bytes in size are called “Runts” which are discarded by the switch method. This helps in reducing the unnecessary traffic over the network which in turn **gives efficient use of bandwidth with speed & low latency**.

According to the above discussion, the **Fragment-free switching method is most desirable** method for the given scenario where speed, bandwidth & low latency switching are utmost importance.

3) A Tier 2 service provider is peering with two upstream Tier 1 service providers. This Tier 2 service provider is also peering with their customers. What protocol is being used between the Tier 2 and Tier 2 service providers and the Tier 2 service provider and its customers? Without going into detail with regard to specific IP Addressing, provide the diagram for this network topology using the appropriate terminology and make sure to specify the peering relationship in terms of the specified protocol.

Answer
➔

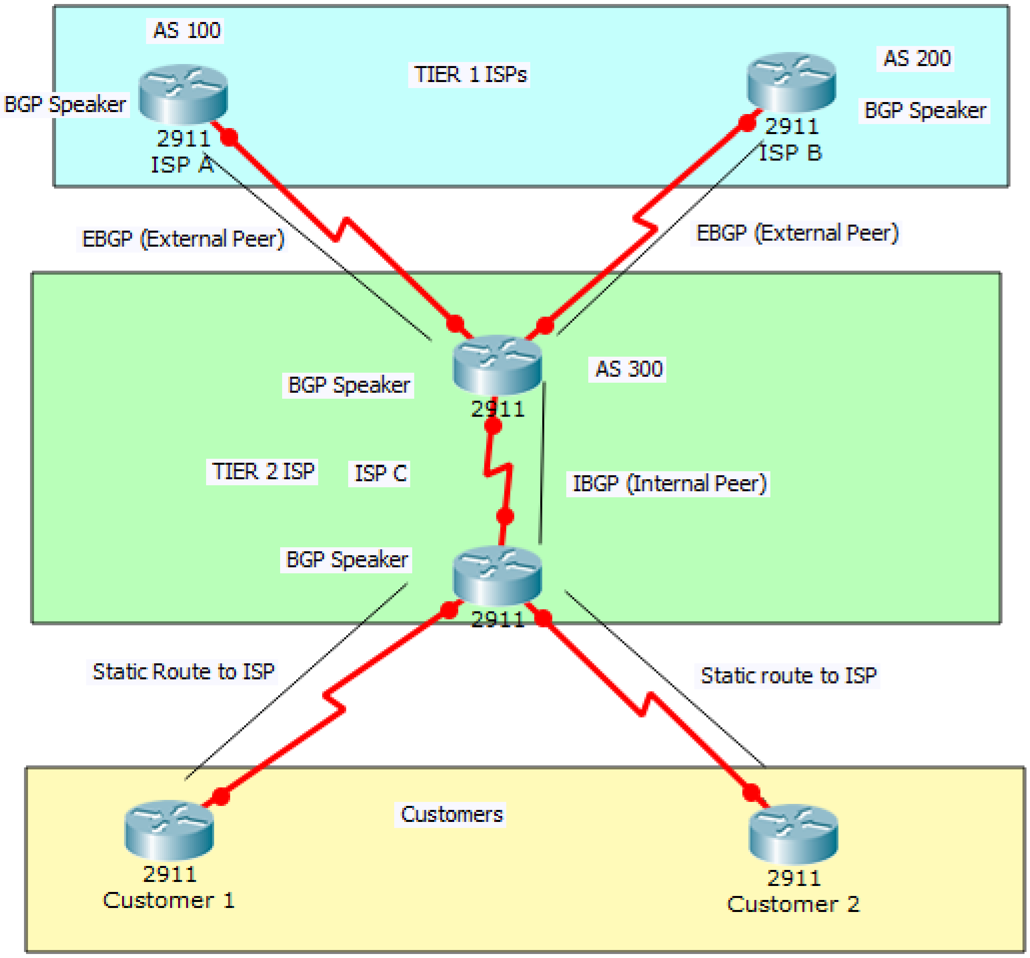
In this scenario, we have two cases:

(a) The Tier 2 and Tier 2 service providers connection
(b) The Tier 2 service provider and its customers (assuming the customers have only one ISP)

a) The Tier 2 and Tier 2 service providers connection :
In this case, we will use BGP (Border gateway protocol) as there are multiple Tier 1 ISPs (ISP A & ISP B) for Tier 2 ISP (ISP C). With BGP, we can use the connections to both the ISPs as primary & provide load balancing or we can get the most desirable shortest path to the destination.

b) The Tier 2 service provider and its customers :
In this case, as the customers have only one tier 2 ISP (ISP C) as ISP, we can directly use static routing to redirect the traffic to Tier 2 ISP (ISP C). So there is no need of use of any specific protocol for this case.

The topology would look like this:



4) You are provided a network address of 204.5.6.0/24. Utilize the most efficient ip addressing design for a network with the following criteria:

a. There are five locations.

b. Location1 is connected to Location2 via a WAN connection.

c. Location2 is connected to Location3 via a WAN connection.

d. Location1 is connected to Location4 via a WAN connection.

e. Location1 has two network segments on the same layer2 physical hardware.

f. Segment1a in Location1 has a maximum of 40 devices.

g. Segment1b in Location1 has a maximum of 50 devices.

h. Location2 has a maximum of 20 devices on its LAN.

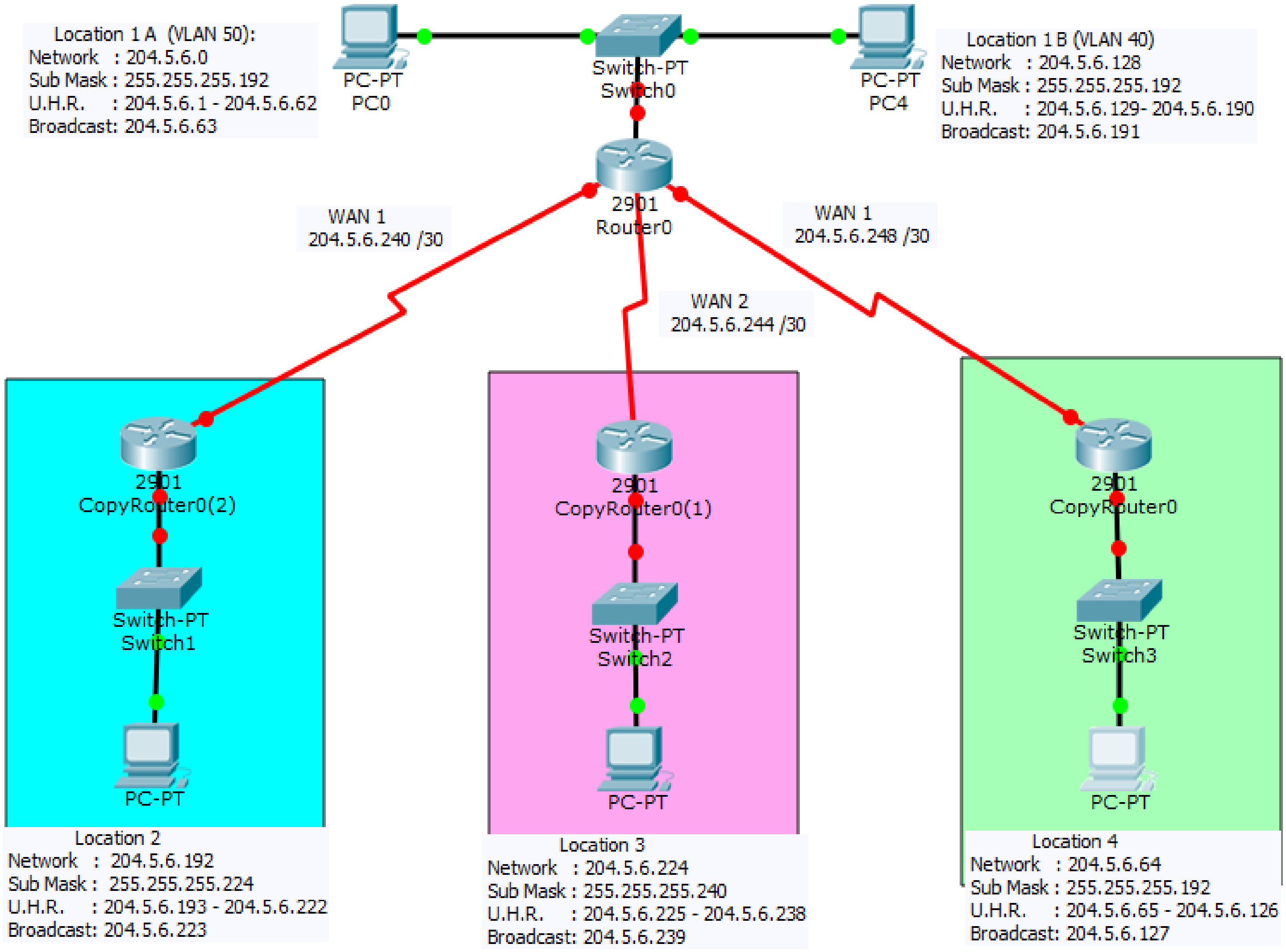
i. Location3 has a maximum of 10 devices on its LAN.

j. Location4 has a maximum of 50 devices on its LAN.

Answer

➔

Subnet Name	**No of Devices**	**Address**	**Mask**	**Usable Host Range (U.H.R.)**	**Broadcast**
Location 1 A	50	204.5.6.0	/26	204.5.6.1 - 204.5.6.62	204.5.6.63
Location 4	50	204.5.6.64	/26	204.5.6.65 - 204.5.6.126	204.5.6.127
Location 1 B	40	204.5.6.128	/26	204.5.6.129 - 204.5.6.190	204.5.6.191
Location 2	20	204.5.6.192	/27	204.5.6.193 - 204.5.6.222	204.5.6.223
Location 3	10	204.5.6.224	/28	204.5.6.225 - 204.5.6.238	204.5.6.239
WAN 1	2	204.5.6.240	/30	204.5.6.241 - 204.5.6.242	204.5.6.243
WAN 2	2	204.5.6.244	/30	204.5.6.245 - 204.5.6.246	204.5.6.247
WAN 3	2	204.5.6.248	/30	204.5.6.249 - 204.5.6.250	204.5.6.251



Location 1 A (VLAN 50):
Network : 204.5.6.0
Sub Mask : 255.255.255.192
U.H.R. : 204.5.6.1 - 204.5.6.62
Broadcast: 204.5.6.63

Location 1 B (VLAN 40)
Network : 204.5.6.128
Sub Mask : 255.255.255.192
U.H.R. : 204.5.6.129- 204.5.6.190
Broadcast: 204.5.6.191

WAN 1
204.5.6.240 /30

WAN 2
204.5.6.244 /30

WAN 1
204.5.6.248 /30

Location 2
Network : 204.5.6.192
Sub Mask : 255.255.255.224
U.H.R. : 204.5.6.193 - 204.5.6.222
Broadcast: 204.5.6.223

Location 3
Network : 204.5.6.224
Sub Mask : 255.255.255.240
U.H.R. : 204.5.6.225 - 204.5.6.238
Broadcast: 204.5.6.239

Location 4
Network : 204.5.6.64
Sub Mask : 255.255.255.192
U.H.R. : 204.5.6.65 - 204.5.6.126
Broadcast: 204.5.6.127

6) A hospital network is currently undergoing high latency through one particular segment of their network. When the radiology department of the hospital has a patient that requires an X-ray to be captured and sent directly to the server in the hospital's data center, it takes an extremely long time to complete the image transfer from the X-ray machine to the server causing high latency in that portion of the network. What technology could be used to mitigate this problem? Explain your reasoning why you chose this particular technology and what improvements would occur from its implementation.

Answer

➔

As the problem over here in this scenario is the network congestion causing high latency, we can use EtherChannel technology. The EtherChannel is a port aggregation or link aggregation technology. The purpose of EtherChannel is to group several physical link for providing fault tolerance, high bandwidth & low latency. It is used between switches, routers & servers.

So the **reasons for choosing this technology** are:

a) Even if EtherChannel includes multiple physical links, we have to assign only one IP address for the whole EtherChannel so it’s easier to do configuration.
b) It provides higher bandwidth (800 mbps for FastEthernet ports, 8 gbps for GigabitEthernet ports, 80 gbps for 10-GigabitEthernet ports depending on the ports used to create EtherChannel), low latency, fault tolerance to the network.
c) It is easier to implement & manage.
d) No other parts of the network needs to be configured except the devices within which it is to be implemented.

Improvements in the network:

a) Network where the high latency was encountered, now has low latency. So high latency problem is solved.
b) Along with low latency, the network becomes fault tolerant as the traffic of the failed link is distributed over the other links.
c) Traffic congestion has been taken care of.

7) In a medium-size business network there is a DHCP server in the data center. The network consists of large redundant and fault tolerant layer2 architecture. When a client boots, there DHCP request times out. What might be occurring within the network that is causing this problem? How would you resolve this problem?

Answer

➔ Here, we have 2 cases :

a) Command not present in access control list
b) Order of commands in the access control list

a) Command not present in access control list :

In this case, the configuration of router with the access control list seems to be the problem. Access control list provides the basic traffic filtering capabilities. So if the router is configured with access control list then router would drop the packets which does not satisfy the conditions given in the access control list so even if a device outside the network or a device without permission tries to access the other device then it will not allow it. When configuring if we put a command "deny ip any any" then it will not allow other IP address devices to access the network except which are permitted to access.

When the device boots up then it does not know to which network it belongs so it sends request for IP address to the DHCP server which dynamically allots the IP address to the devices. In the DHCP request packet, the destination address is 255.255.255.255 but the router does not allow the traffic with destination IP 255.255.255.255 as the permission is given to only specific IP address devices or specific network devices & deny any other packets from passing according to the command "**deny ip any any**". So it will filter out the packets with the 255.255.255.255 destination address which will in turn does not allow a client to receive the IP address when boots. So the DHCP request will fail.

To solve the problem, add the following command to the access control list :
permit udp any host 255.255.255.255 eq bootps

b) Order of commands in the access control list :

The other reason could be that the above statement may be present in the access control list but the **order of the commands** also matters in access control list. Lets consider two cases :

i) If the command order is like this :

```
deny ip any any
permit udp any host 255.255.255.255 eq bootps
```

In this case the deny command comes first so deny will be checked first which in turn make the router **drop the packet** then it will check for permit. This sequence of commands may make DHCP request fail.

ii) If the command order if like this :

```
permit udp any host 255.255.255.255 eq bootps
deny ip any any
```

In this case, the permit is processed first for the 255.255.255.255 destination packet which will **allow the packet.**

8) A company utilizes a central point of control to change its network configurations via open standards. They have 50 switches across their campus network all being managed from this central point of control. What technology is this referred as? What underlying protocol is used? What functionality can this standard provide?

➔

In this case, the most efficient protocol is VTP (VLAN Trunk protocol) or GVRP (Generic VLAN Registration Protocol) which can be used to configure the switches remotely. This protocol allows switched to dynamically propagate the changes. This protocol works on the basis of client-server relationship. The main switch (in this case central point switch) acts as the server & the other switches acts as clients. The links between these switches are converted to trunks. So whenever a change in the main switch(sever) is performed, they are immediately reflected on the other switches (clients). For this to be working, make sure that all the switches are configured to be in one “domain” only, otherwise the changes will not take place.
Example : If a VLAN 100 is created on the server switch then VLAN 100 will also be created on the other client switches. This protocol uses IEEE 802.1Q standard.