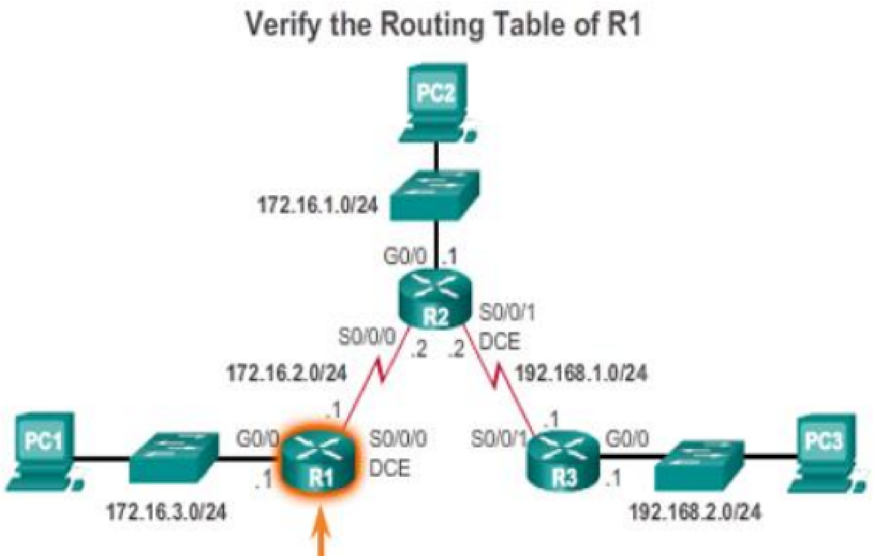
Tutorial 1: IP Static Routing Troubleshoot Static and Default Routes

1. With reference to R1's partial output of "show ip route" command, differentiate the two static routes



```
R1# show ip route

S 192.168.2.0/24 [1/0] via 172.16.2.2
S 192.168.1.0 /24 is directly connected, serial s0/0/0
```

http://cisco.num.edu.mn/CCNA_R&S2/course/module6/6.2.1.3/6.2.1.3.html

S 192.168.2.0/24 [1/0] via 172.16.2.2

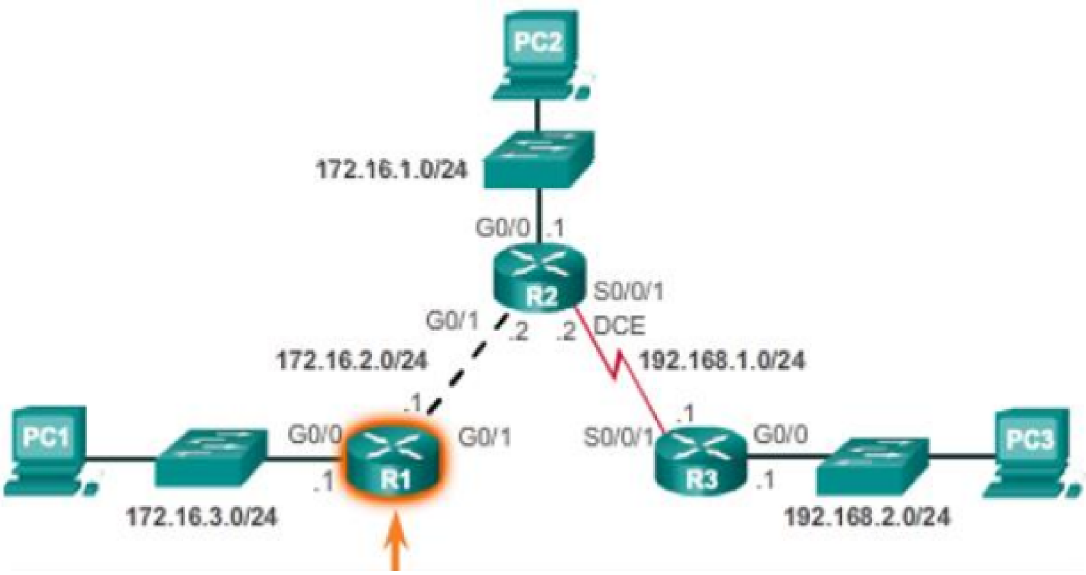
- This is a **next-hop static route** in which only the next-hop address is specified.
- For this static route, it references only a next-hop IPv4 address and does not reference an exit interface. Thus, it must have the next-hop IPv4 address resolved using another router in the routing table with an exit interface.
- Therefore, it needs to take two routing table lookup processes to forward any packet to the 192.168.2.0/24 network.
- When the router performs multiple lookups in the routing table before forwarding a packet, it is performing a process known as a recursive lookup.
- Recursive lookups consume router resources, they should be avoided when possible.

http://cisco.num.edu.mn/CCNA_R&S2/course/module6/6.2.1.4/6.2.1.4.html

S 192.168.1.0 /24 is directly connected, serial s0/0/0

- This is a **directly connected static route** in which only the exit interface is specified.
- This method can avoid the recursive lookup problem as it allows the routing table to resolve the exit interface in a single search (single-lookup) instead of two searches.
- Although the routing table entry indicates "directly connected", the administrative distance of the static route is still 1. Only a directly connected interface can have an administrative distance of 0.

2. Identify and illustrate one of the types of static route shown in R1's running-configuration.



R1# show ip route **(to show routing table)**
S 192.168.2.0/24 [1/0] via 172.16.2.2, GigabitEthernet 0/1

http://cisco.num.edu.mn/CCNA_R&S2/course/module6/6.2.1.5/6.2.1.5.html

Types of static route

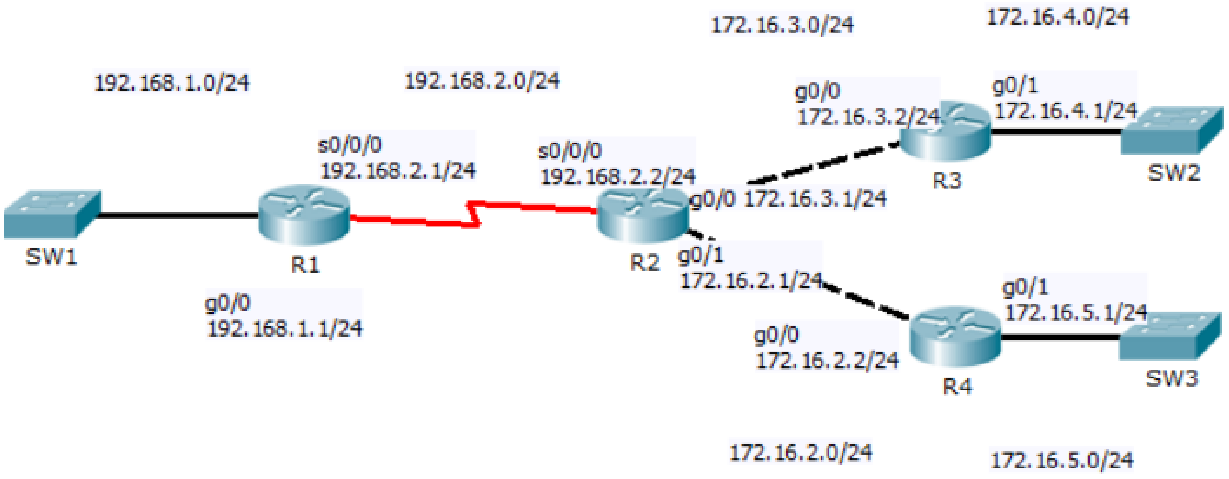
IPv4 fully specified static route

Illustration

- In the fully specified static route, both the exit interface and the next-hop IP address are specified.
- This form of static route is used when the output interface is a multi-access interface (ie Ethernet) and it is necessary to explicitly identify the next hop. The next hop must be directly connected to the specified exit interface.
- The next hop must be directly connected to the specified exit interface.
- To eliminate the recursive lookup, a directly connected static route can be implementing using the following command :
  - R1(config)# ip route 192.168.2.0 255.255.255.0 g0/1.
- However, this may cause unexpected or inconsistent results. With Ethernet networks, there may be many different devices sharing the same multi-access network, including hosts and even multiple routers.
- By only designating the Ethernet exit interface in the static route, the router will not have sufficient information to determine which device is the next-hop device.
- R1 knows that the packet needs to be encapsulated in an Ethernet frame and sent out the G0/1 interface.
- However, R1 does not know the next-hop IPv4 address and therefore it cannot determine the destination MAC address for the Ethernet frame.

- It is recommended that when the exit interface is an Ethernet network, a fully specified static route is used which includes both the exit interface and the next-hop address
  - R1# ip route 192.168.2.0 255.255.255.0 g0/1 172.16.2.2

3. Based on the network topology below, answer the following questions:



a. In router R1, write a command to configure a **default static route** using the **exit interface**.
R1(config)# ip route 0.0.0.0 0.0.0.0 s0/0/0

b. In router R1, write a command to configure a **summary static route** for network 172.16.2.0/24 – 172.16.5.0/24 using the **next hop IP address**.
https://study-ccna.com/static-summary-route/

Static route that can be be summarized	
172.16.2.0	**10101100.00010000.00000**010.00000000
172.16.3.0	**10101100.00010000.00000**011.00000000
172.16.4.0	**10101100.00010000.00000**100.00000000
172.16.5.0	**10101100.00010000.00000**101.00000000

Summarized Route	
172.16.0.0	**10101100.00010000.00000**000.00000000
255.255.248.0	**11111111.11111111.11111**000.00000000

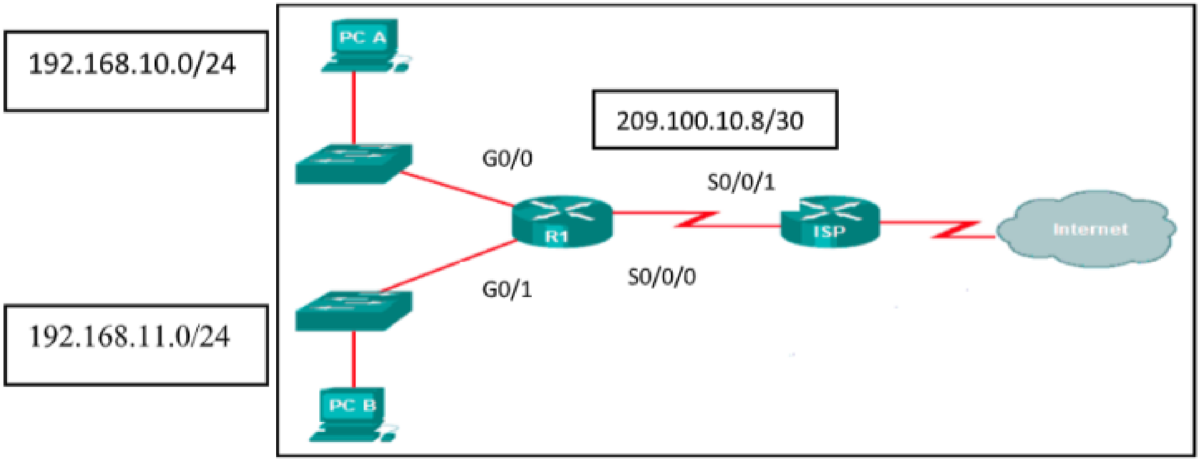
R1(config)# ip route 172.16.0.0 255.255.248.0 192.168.2.2

c. In router R2, write a command to configure a **standard static route** for network 192.168.1.0/24 using the **exit interface**.
R2(config)# ip route 192.168.1.0 255.255.255.0 s0/0/0

d. In router R2, write two commands to configure **fully specified static routes** for network 172.16.4.0/24 and 172.16.5.0/24.

```
R2(config)# ip route 172.16.4.0 255.255.255.0 g0/0 172.16.3.2
R2(config)# ip route 172.16.5.0 255.255.255.0 g0/1 172.16.2.2
```

4. Suggest the most appropriate routing methods to be implemented for a small network topology shown below to forward packets from R1 to ISP and vice versa. Justify your answers.



Most appropriate routing methods

Static route

Reason of using static routing

- Static routing does not advertise over the network, thus more secure compared to dynamic static routing
- Static route is suitable for a small network topology as it uses less bandwidth than dynamic routing protocols since the routers do not exchange routes.

R1 (border router) can be configured as the default static route.

- Configuration : ip route 0.0.0.0 0.0.0.0 s0/0/0
- Default static route is appropriate when a border router (R1) connects to an ISP network - ***capture other Networks and point to ISP router***
- A default static route is a static route that matches all packets. Rather than storing all routes to networks in the routing table, a router can store a single default route to represent any network that is not in the routing table

Refer C1 P1 pg 22

ISP can be configured as a summary static route to minimize the number of static routes in the routing table and lessen the administrative overhead that may impact the memory usage of the routers. The reason as follow:

- The destination networks are contiguous and can be summarized into a single network address.
- The multiple static routes all use the same exit interface or next-hop IP address.

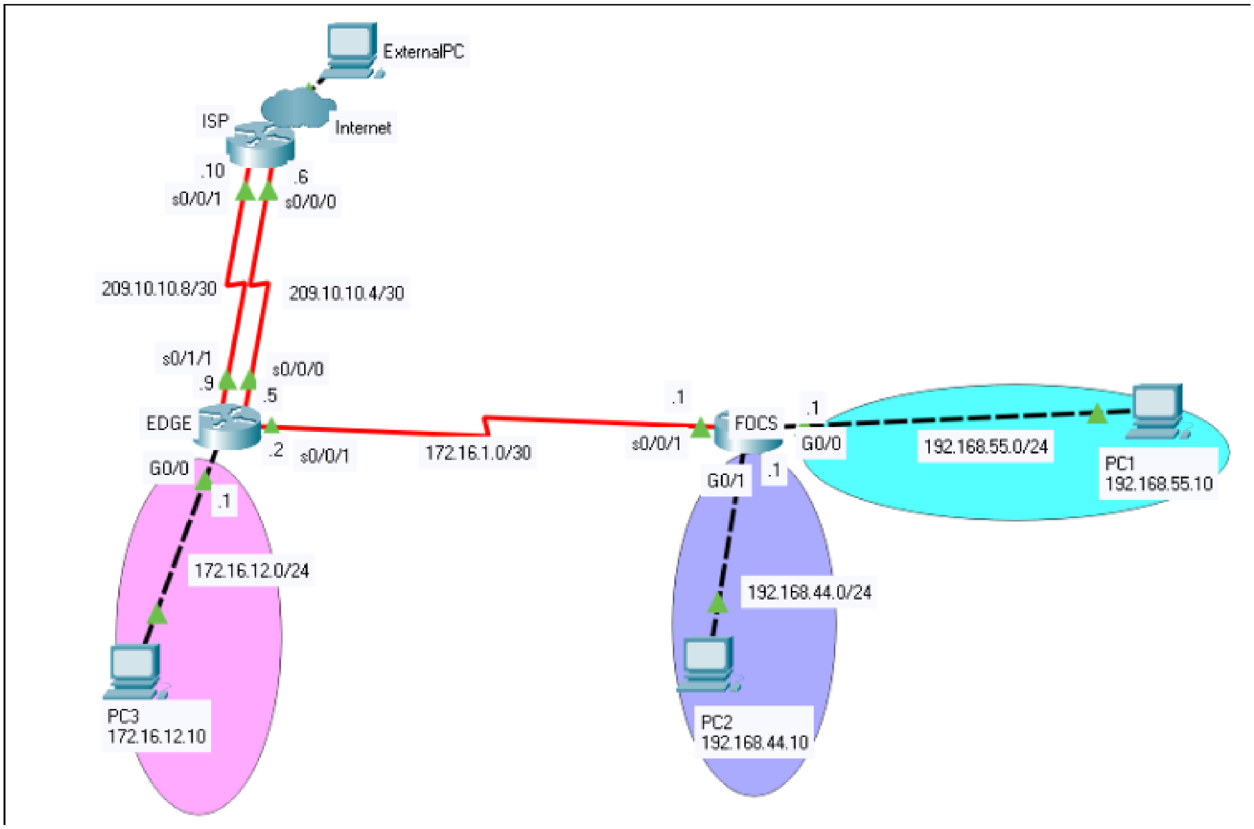
https://www.ciscopress.com/articles/article.asp?p=2180209&seqNum=4

Static route that can be be summarized	
192.168.10.0	**11000000.10101000.0000101**0.00000000
192.168.11.0	**11000000.10101000.0000101**1.00000000

Summarized Route	
192.168.10.0	**11000000.10101000.0000101**0.00000000
255.255.254.0	**11111111.11111111.1111111**0.00000000

- Configuration : ip route 192.168.10.0 255.255.254.0 s0/0/1

5. Figure 1-1 shows a network topology with the Internet Protocol version 4 (IPv4) configurations done on all router interfaces and Personal Computers (PCs).



Based on Figure 1-1, determine the appropriate static routes configurations with justifications in the respective routers (EDGE and FOCS). ISP is already pre-configured with static routing. Use Table 1-1 to document your answer.

i. Standard static routes using next hop IP address. PC1 and PC2 are able to communicate with PC3.

ii. Default static route as a primary route using next hop IP address. PC3 is able to ping ExternalPC. Make your assumptions.

iii. Default static route as a secondary route or backup route using next hop IP address. PC3 is able to ping ExternalPC. Make your assumptions.

Table 1-1: Documentation Table

Item	Router Name	Static route configurations	Justification
(i)	EDGE	`EDGE(config)# ip route 192.168.55.0 255.255.255.0 172.16.1.1`	Standard static routes are configured to communicate to remote networks as the routing table initially will only consist of

	FOCS	`EDGE(config)#ip route 192.168.44.0 255.255.255.0 172.16.1.1`
		`FOCS(config)# 172.16.12.0 255.255.255.0 172.16.1.2`
			directly connected network C.
			Routers are unable to forward packets to remote networks without static route configuration *(no routing entry).*
			2-way configuration on EDGE and FOCS router so that EDGE learns the 192.168.55.0 and 192.168.44.0 network while FOCS learns the 172.16.12.0 network.

(ii)	EDGE	`EDGE(config)# ip route 0.0.0.0 0.0.0.0 209.10.10.10`
		`OR`
		`EDGE(config)# ip route 0.0.0.0 0.0.0.0 209.10.10.6`
			The default static route is configured on the EDGE router (edge router) to match all packets to be sent to the ISP.
			Notes: You can assume to use 209.10.10.10 or 209.10.10.6 as the next-hop address

(iii)	EDGE	`EDGE(config)# ip route 0.0.0.0 0.0.0.0 209.10.10.10 88`
		`OR`
		`EDGE(config)# ip route 0.0.0.0 0.0.0.0 209.10.10.6 88`
			The floating default route is configured to provide a backup path to the primary route.
			The floating IP default route will only be used when the primary route is not available/fails.
			The default administrative distance is 1. Thus, the floating IP default route is configured with a higher administrative distance (AD) [2 - 255].

Notes from tutor

Criteria considered for summarized route - contiguous network address *192.168.44.0* and *192.168.55.0* is not suitable for summarized route because between it still has 45, 46, 47, 48 …55

6. As a network associate, you have been consulted to provide solutions to a network topology with the Internet Protocol version 6 (IPv6) addressing and configurations in all router interfaces and Personal Computers (PCs) as shown in Figure 1-1.

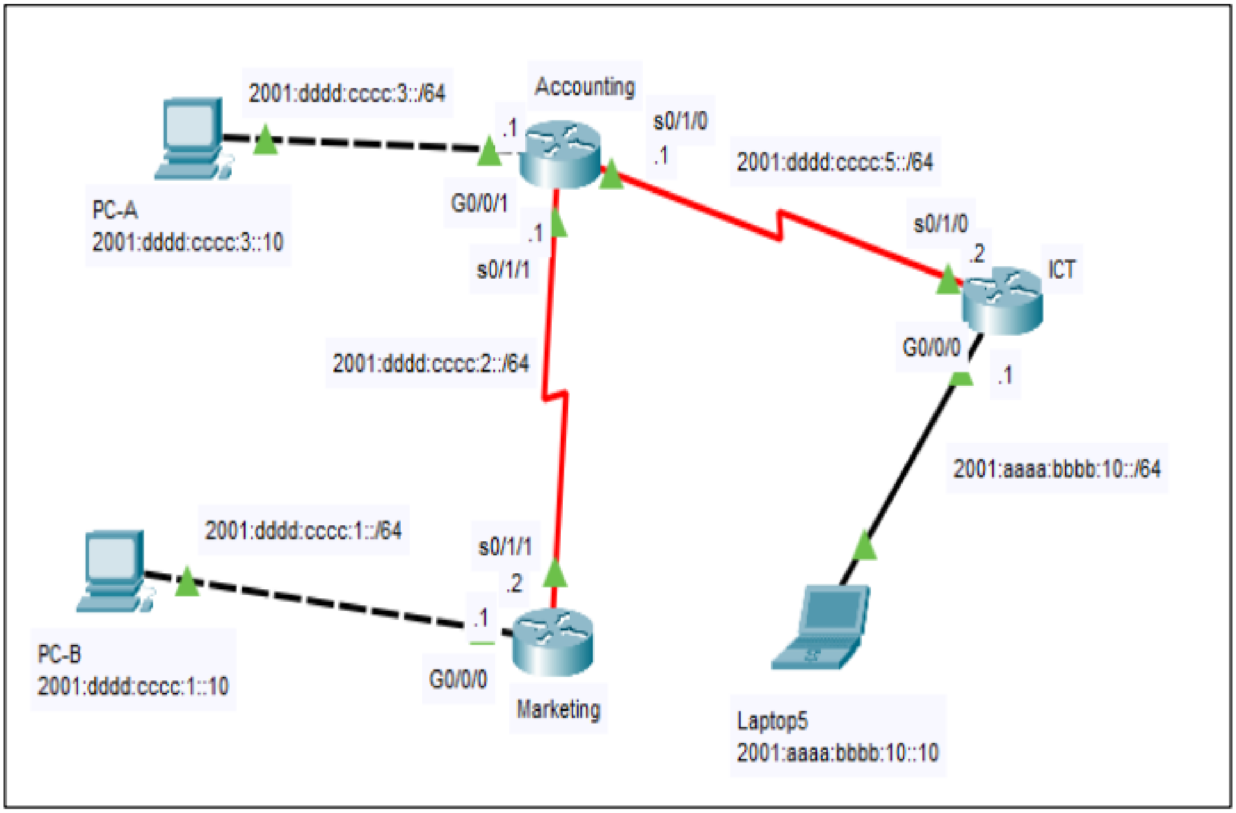


Figure 1-1: A network topology (202201)

Analyze and propose IPv6 standard static routes using **next hop IP address** configurations in all routers shown in Figure 1-1. Use Table 1-1 to document your answer. This is to provide communications between PC-A, PC-B and Laptop5. (13 marks)

Static route - configure using remote network (can use `sh ip route` to show all the routing entries)

Table 1-1: Documentation Table

Router name	**Static route configuration**

Marketing	`Marketing(config)# ipv6 unicast-routing`
	`Marketing(config)# ipv6 route 2001:dddd:cccc:3::/64 2001:dddd:cccc:2::1`
	`Marketing(config)# ipv6 route 2001:dddd:cccc:5::/64 2001:dddd:cccc:2::1`
	`Marketing(config)# ipv6 route 2001:aaaa:bbbb:10::/64`

	`2001:dddd:cccc:2::1`

Accounting	`Accounting(config)# ipv6 unicast-routing`
	`Accounting(config)# ipv6 route 2001:dddd:cccc:1::/64 2001:dddd:cccc:2::2`
	`Accounting(config)# ipv6 route 2001:aaaa:bbbb:10::/64 2001:dddd:cccc:5::2`

ICT	`ICT(config)# ipv6 unicast-routing`
	`ICT(config)# ipv6 route 2001:dddd:cccc:3::/64 2001:dddd:cccc:5::1`
	`ICT(config)# ipv6 route 2001:dddd:cccc:2::/64 2001:dddd:cccc:5::1`
	`ICT(config)# ipv6 route 2001:dddd:cccc:1::/64 2001:dddd:cccc:5::1`

Notes !!!

It is very important that you specify `ipv6 unicast-routing` to enable the IPv6 on that network device.

Tutorial 2: Single Area OSPFv2 Concepts

1. With reference to Figure 2-1 and Figure 2-2, all the routers have been configured with Open Shortest Path First (OSPF) configurations and the routers have reached the convergence state.

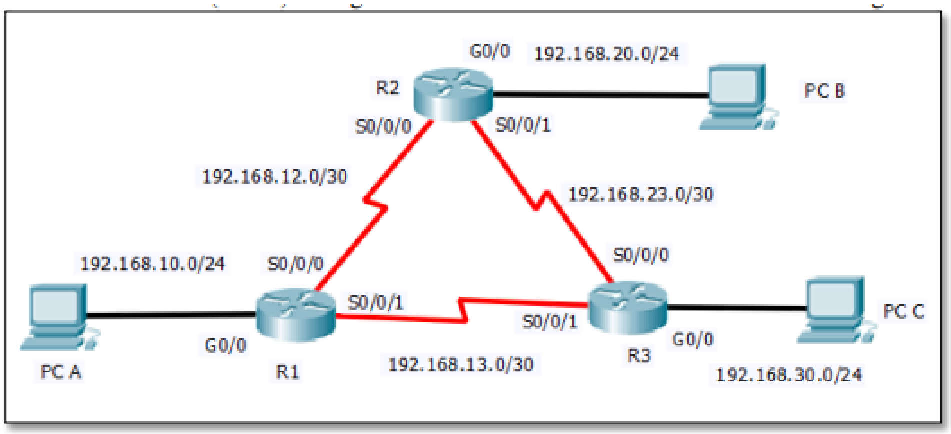
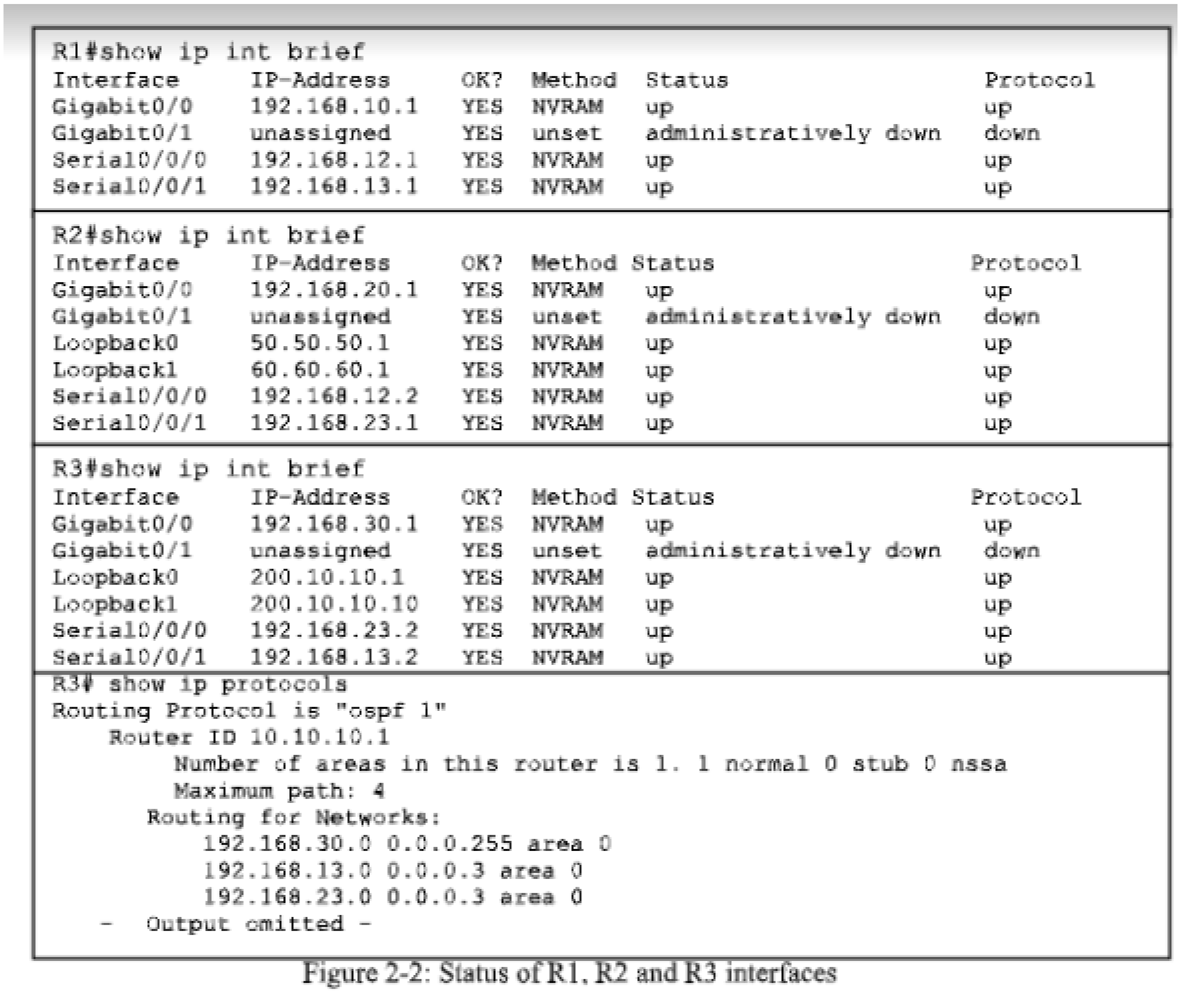


Figure 2-1: A network topology



```
R1#show ip int brief
Interface       IP-Address      OK?  Method  Status                   Protocol
Gigabit0/0      192.168.10.1    YES  NVRAM   up                       up
Gigabit0/1      unassigned      YES  unset   administratively down    down
Serial0/0/0     192.168.12.1    YES  NVRAM   up                       up
Serial0/0/1     192.168.13.1    YES  NVRAM   up                       up
```

```
R2#show ip int brief
Interface       IP-Address      OK?  Method Status                  Protocol
Gigabit0/0      192.168.20.1    YES  NVRAM   up                       up
Gigabit0/1      unassigned      YES  unset   administratively down    down
Loopback0       50.50.50.1      YES  NVRAM   up                       up
Loopback1       60.60.60.1      YES  NVRAM   up                       up
Serial0/0/0     192.168.12.2    YES  NVRAM   up                       up
Serial0/0/1     192.168.23.1    YES  NVRAM   up                       up
```

```
R3#show ip int brief
Interface       IP-Address      OK?  Method Status                  Protocol
Gigabit0/0      192.168.30.1    YES  NVRAM   up                       up
Gigabit0/1      unassigned      YES  unset   administratively down    down
Loopback0       200.10.10.1     YES  NVRAM   up                       up
Loopback1       200.10.10.10    YES  NVRAM   up                       up
Serial0/0/0     192.168.23.2    YES  NVRAM   up                       up
Serial0/0/1     192.168.13.2    YES  NVRAM   up                       up
```

```
R3# show ip protocols
Routing Protocol is "ospf 1"
    Router ID 10.10.10.1
         Number of areas in this router is 1. 1 normal 0 stub 0 nssa
         Maximum path: 4
       Routing for Networks:
           192.168.30.0 0.0.0.255 area 0
           192.168.13.0 0.0.0.3 area 0
           192.168.23.0 0.0.0.3 area 0
   -   Output omitted -
```

Figure 2-2: Status of R1, R2 and R3 interfaces

(i) Describes the precedence of how the router derives router ID.

Router derives its router ID based on one of the three criterias in the following preferential order:

1. The router ID is explicitly configured using the OSPF ***router-id rid*** router configuration mode command.
2. If no router IDs are configured, the router ID is determined by the highest loopback IPv4 address.
3. If no loopback interfaces are configured, the router ID is determined by the highest active IPv4 address from any configured physical interfaces.

(ii) Identify the router ID for R1, R2 and R3. Justify your answer.

Router ID for R1 : 192.168.13.1 (Serial0/0/1)

- R1 is not explicitly configured using ***router-id rid*** and it does not configure any loopback interfaces. Hence, the highest active IPv4 address of physical interfaces in R1 which is 192.168.13.1 of Serial0/0/1 has been chosen as router ID.

Router ID for R2 : 60.60.60.1 (Loopback 1)

- R1 is not explicitly configured using ***router-id rid*** but it has been configured with 2 loopback interfaces. Hence, the highest loopback interface which is 60.60.60.1 of Loopback 1 has been chosen as router ID.

Router ID for R3 : 10.10.10.1 [router-id 10.10.10.1]

- R1 is explicitly configured using the OSPF router-id 10.10.10.1. Hence, it will be the router ID for R3.

(iii) Refer to the network topology shown in Figure 2-1, will a Designated Router (DR) and a Backup Designated Router (BDR) be elected? Justify your answer.

No, DR and BDR is not necessary in a Point-to-Point network whereby each router has a single adjacency with the router sitting on the other end of the link. Only multi access network / Ethernet network shared such as Ethernet requires DR and BDR election.

2. Refer to the OSPF configuration shown in Figure 3-1 and the network topology shown in Figure 3-2, answer the following questions:

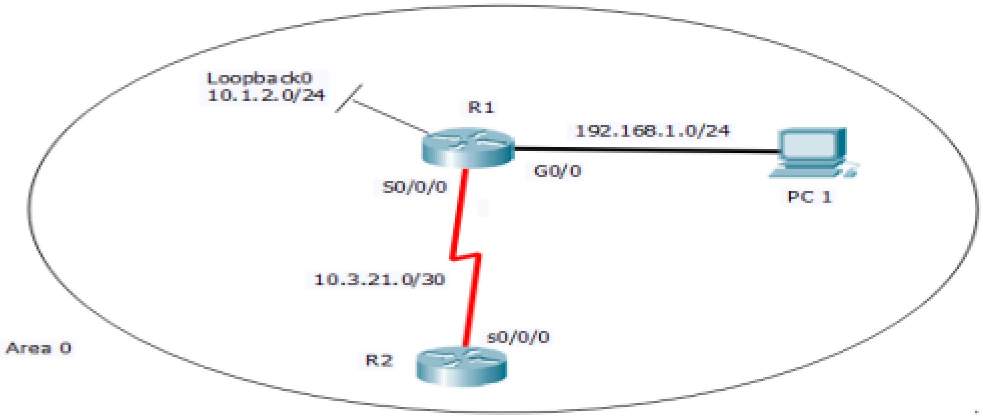
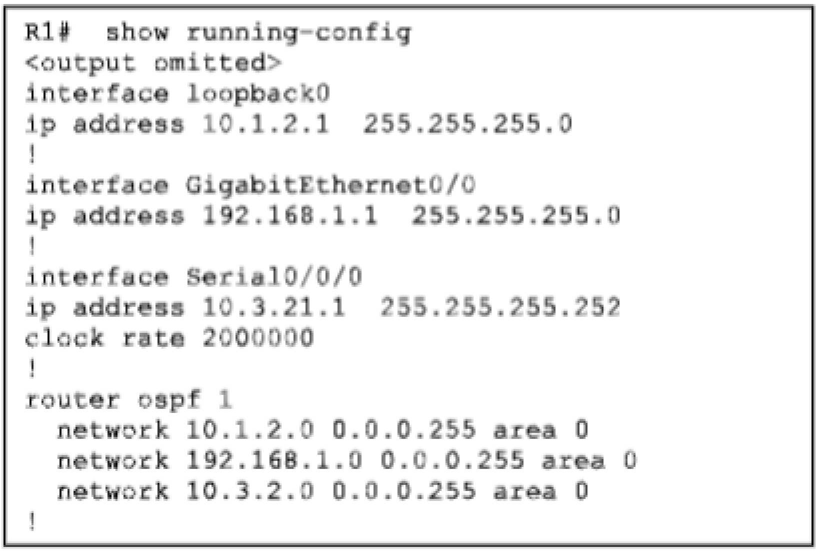


Figure 3-2: A network topology



```
R1#  show running-config
<output omitted>
interface loopback0
ip address 10.1.2.1  255.255.255.0
!
interface GigabitEthernet0/0
ip address 192.168.1.1  255.255.255.0
!
interface Serial0/0/0
ip address 10.3.21.1  255.255.255.252
clock rate 2000000
!
router ospf 1
  network 10.1.2.0 0.0.0.255 area 0
  network 192.168.1.0 0.0.0.255 area 0
  network 10.3.2.0 0.0.0.255 area 0
!
```

Figure 3-1: OSPF configuration

A. Determine the router ID for R1 in Figure 3-1. Justify your answer
   The router ID for R1 will be 10.1.2.1 on loopback 0 interface.

   Justification
   R1 is not explicitly configured using ***router-id rid*** but it has been configured with a loopback interface. Hence, the IPv4 address of loopback 0 (10.1.2.1) will be the router ID for R1.

B. Refer to both Figure 3-1 and Figure 3-2, identify and rectify any OSPF configuration error(s).

OSPF configuration error	Solution
The network statement for `network 10.3.2.0 0.0.0.255 area 0` is wrong. Wrong network address and wildcard mask.	Change the network statement to `network 10.3.21.0 0.0.0.3 area 0` Notes: Subnet mask for /30 - 255.255.255.252 Wildcard mask for /30 - 0.0.0.3 (inverse of the subnet mask)

C. Refer to the network topology shown in Figure 4-1, provide TWO (2) reasons why it is recommended to set interface G0/0 on R1 to passive interface.

- To ensure a sufficient use of bandwidth by suppressing unnecessary update traffic especially when the G0/0 interface is a LAN interface with no other OSPF routers connected.
- To increase security control by preventing unknown rogue routing devices from receiving OSPF updates.

3. Multiaccess networks can create two challenges for OSPF regarding the flooding of LSAs. What are these challenges?

Creation of multiple adjacencies
Ethernet networks could potentially interconnect many OSPF routers over a common link. Creating adjacencies with every router would lead to an excessive number of LSAs exchanged between routers on the same network.

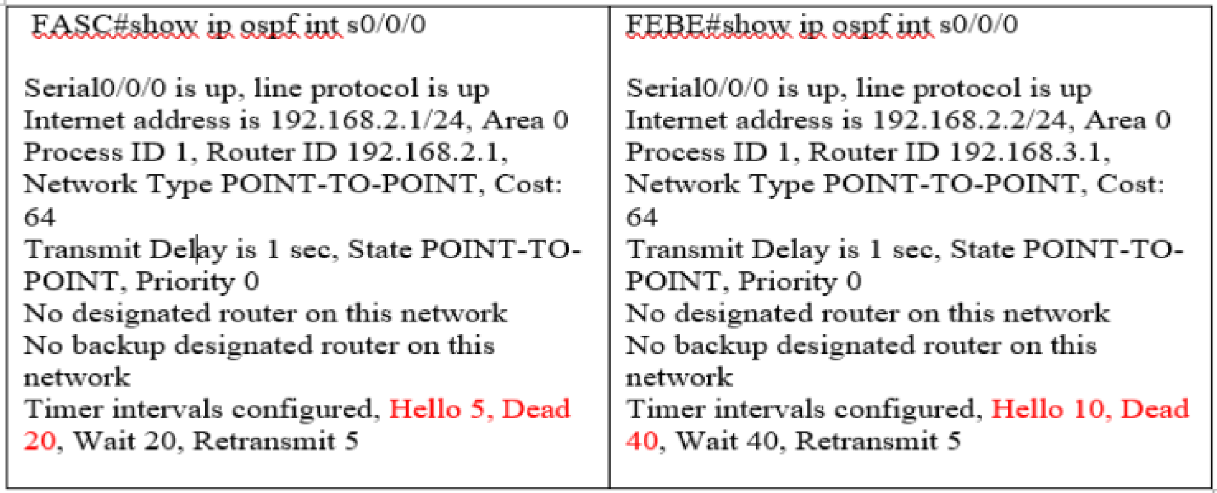
Extensive flooding of LSAs
Link-state routers flood their LSAs any time OSPF is initialized, or when there is a change in the topology. This flooding can become excessive.

4. In a multiarea environment, it is normal that the link-state update overhead is high and the SPF calculation runs frequently across all the routers running Open Shortest Path First (OSPF). Justify your answer.

- I'm not agree with the statement above. The following are my justifications.
- The hierarchical-topology design options with multiarea OSPF enable smaller routing tables as there are fewer routing table entries. This is because network addresses can be summarized between areas.

- Multiarea OSPF reduces link-state update overhead as it minimizes processing and memory requirements.
- Multiarea OSPF reduces frequency of SPF calculations as it localizes the impact of a topology change within an area. For instance, it minimizes routing update impact because LSA flooding stops at the area boundary (area border router).

5. A network associate is troubleshooting the OSPF configuration in two routers named FASC and FEBE. The routers are unable to establish an adjacency between them. Figure 4-1 shows the output of the show ip ospf interface s0/0/0 command for routers FASC and FEBE. Analyze the output shown in Figure 4-1, identify the error(s) and proposed the solutions



FASC#show ip ospf int s0/0/0	FEBE#show ip ospf int s0/0/0
Serial0/0/0 is up, line protocol is up Internet address is 192.168.2.1/24, Area 0 Process ID 1, Router ID 192.168.2.1, Network Type POINT-TO-POINT, Cost: 64 Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0 No designated router on this network No backup designated router on this network Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5	Serial0/0/0 is up, line protocol is up Internet address is 192.168.2.2/24, Area 0 Process ID 1, Router ID 192.168.3.1, Network Type POINT-TO-POINT, Cost: 64 Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0 No designated router on this network No backup designated router on this network Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Figure 4-1 Output of **show ip ospf interface s0/0/0**

OSPF configuration error	**Solution**

Hello interval and Dead interval mismatch between the FASC and FEBE which cause the neighbor adjacency cannot occur.	Modify the OSPFv2 interval to make it compatible.
	Configure hello and dead interval of s0/0/0 in FEBE to 5 and 20
	`FEBE(config) # int s0/0/0`
	`FEBE(config-if) # ip ospf hello-interval 5`
	`FEBE(config-if) # ip ospf dead-interval 20`
	OR
	Configure hello and dead interval of s0/0/0 in FASC to 10 and 40
	`FASC(config) # int s0/0/0`
	`FASC(config-if) # ip ospf hello-interval 10`
	`FASC(config-if) # ip ospf dead-interval 40`

6. With reference to the Figure 5-1, answer the following questions.

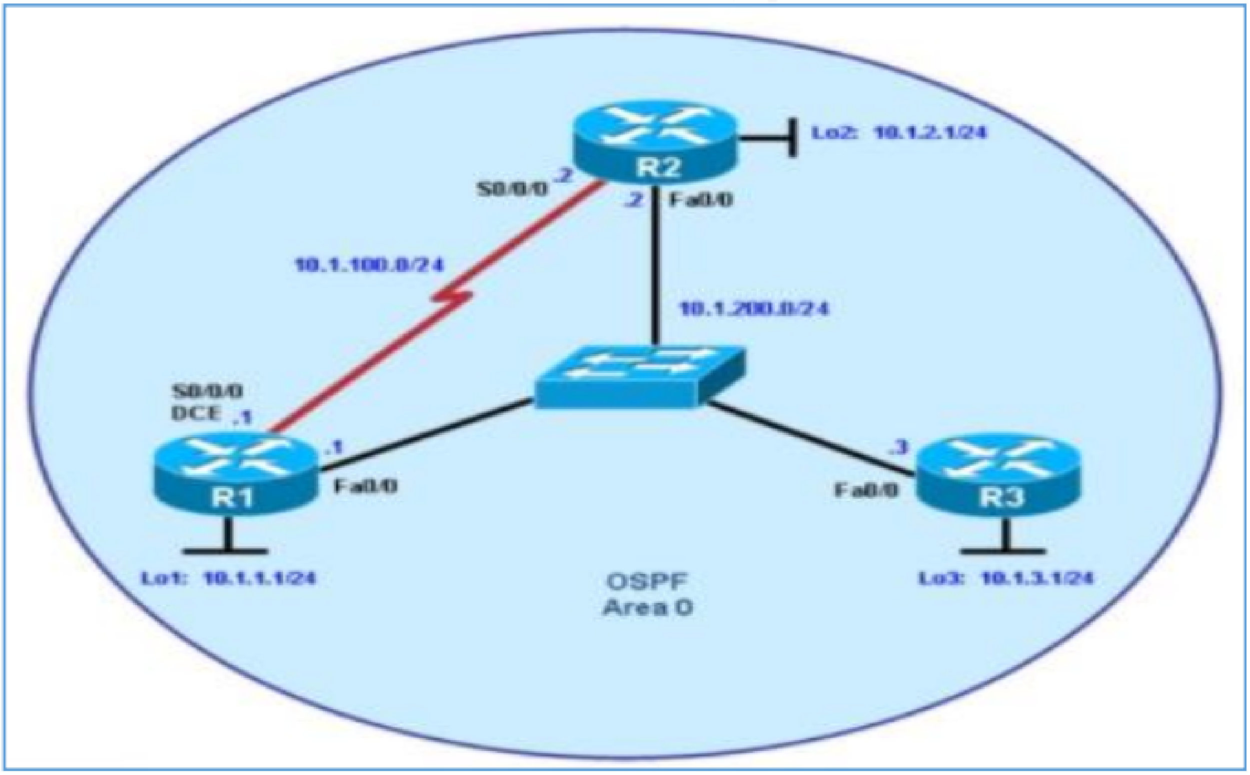


Figure 5-1: An OSPF network

i. What is the default interface priority for R1, R2 and R3?
The default interface priority for R1, R2 and R3 is 1

ii. What is the router ID for R1, R2 and R3?
Router ID for R1 : 10.1.1.1
Router ID for R2 : 10.1.2.1
Router ID for R3 : 10.1.3.1

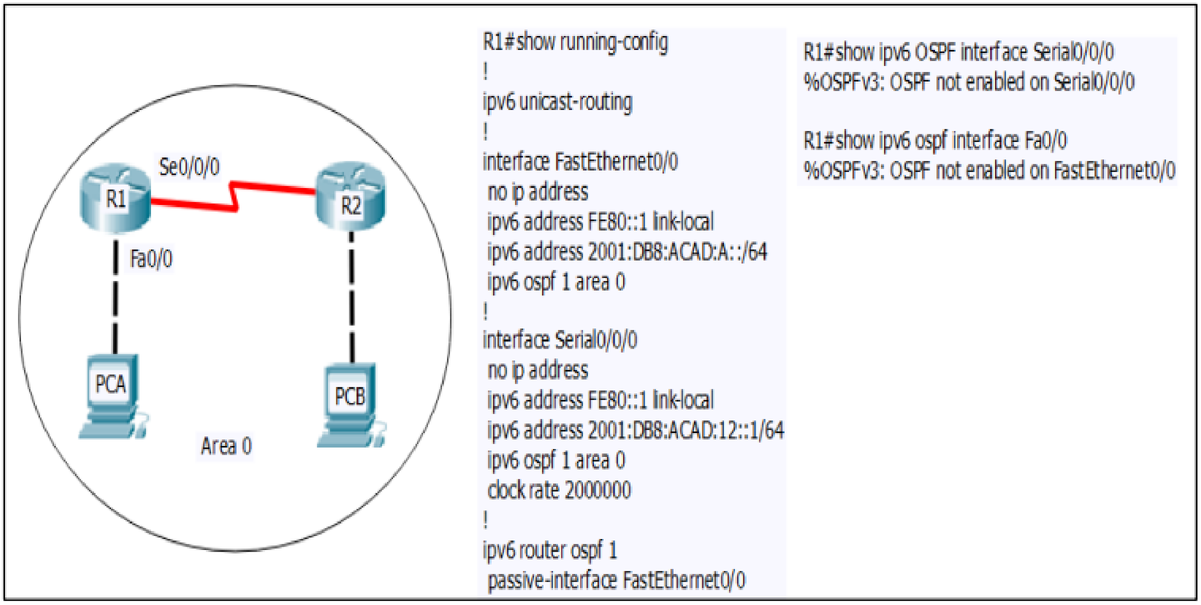
iii. Which routers are DR, BDR and DRothers?
DR : R3
BDR : R2
DROTHER : R1

iv. Modify the interface priorities to make R1 a DR and R3 a BDR.
Cisco commands

```
R1(config) # int f0/0
R1(config-if) # ip ospf priority 255
R1(config-if) # end
R1 # clear ip ospf process
```

```
R3(config) # int f0/0
R3(config-if) # ip ospf priority 200
R3(config-if) # end
R3 # clear ip ospf process
```

7. A network associate is troubleshooting the OSPF configurations of router R1. As shown in Figure 6-1, the router R1 could not have the OSPF enabled. With the assumption that the configurations in R2 are correct and there is no hardware problem, evaluate the possible cause of this problem.



```
R1#show running-config
!
ipv6 unicast-routing
!
interface FastEthernet0/0
 no ip address
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:A::/64
 ipv6 ospf 1 area 0
!
interface Serial0/0/0
 no ip address
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:12::1/64
 ipv6 ospf 1 area 0
 clock rate 2000000
!
ipv6 router ospf 1
 passive-interface FastEthernet0/0
```

```
R1#show ipv6 OSPF interface Serial0/0/0
%OSPFv3: OSPF not enabled on Serial0/0/0

R1#show ipv6 ospf interface Fa0/0
%OSPFv3: OSPF not enabled on FastEthernet0/0
```

Figure 6-1 An OSPF network

(8 marks)

OSPFv3 > OSPF Implementation | Cisco Press.

Probable cause

The OSPF process for IPv6 does not require an IPv4 address to be configured on the router, but it does require a 32-bit value for the router ID which uses IPv4 address notation. In figure 6-1, we can see that the R1 does not have router ID because

- It does not explicitly configured a router ID using ***router-id RID***
- It does not have any loopback interface with IPv4 address
- It does not have any active IPv4 address

Hence, the process fails to start which causes the router R1 to not have the OSPF enabled.

8. Based on Figure 1-1, determine the OSPF using network command configurations in EDGE and FOCS routers to allow PC1, PC2, PC3 and any PCs on the Internet to communicate with each other. Use OSPF process-id 54 and area-id 0. Configuration of default static routes completed in the respective router (EDGE router). Use Table 1-2 to document your answer.

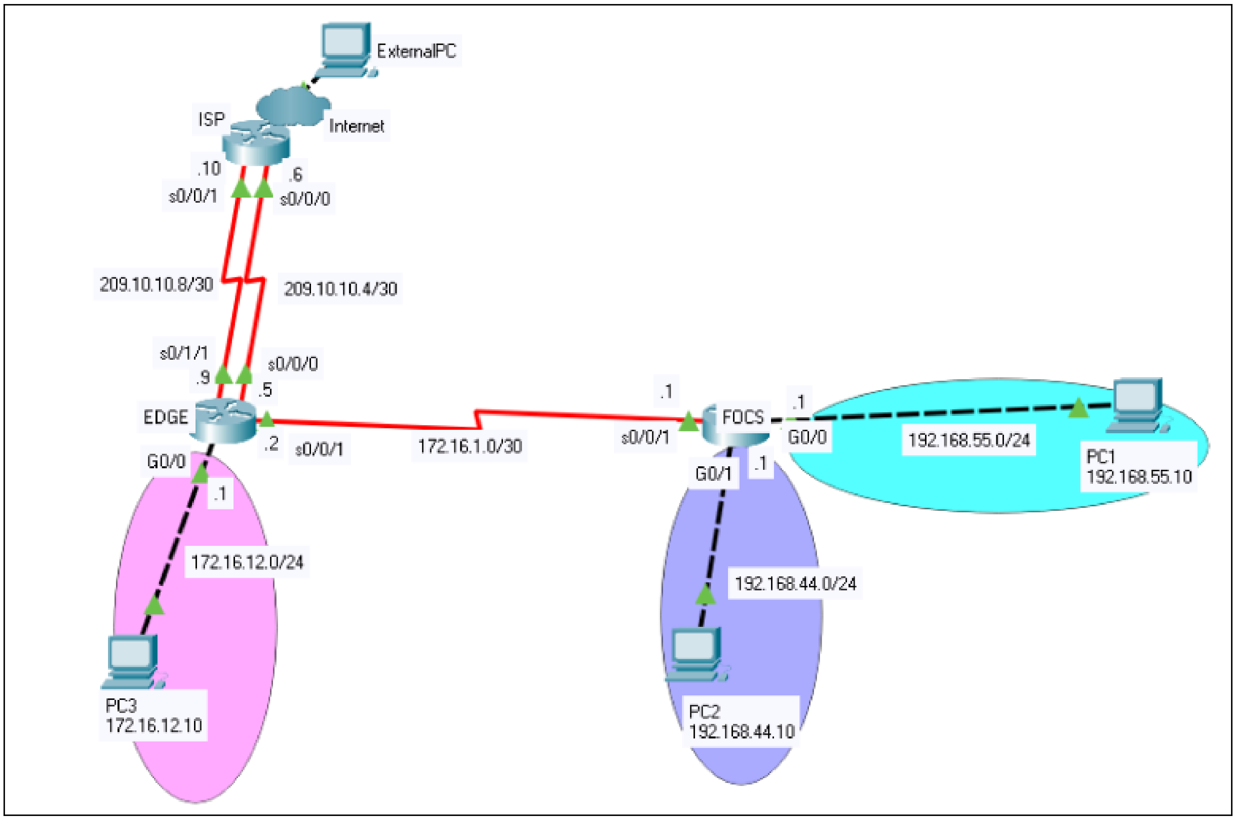


Figure 1-1: A network topology

Table 1-2 : Documentation Table

Router	OSPF Configurations
EDGE	EDGE(config) # router ospf 54 EDGE(config-router) # network 172.16.12.0 0.0.0.255 area 0 EDGE(config-router) # network 172.16.1.0 0.0.0.3 area 0 EDGE(config-router) # default-information originate EDGE(config-router) # passive interface g0/0
FOCS	FOCS(config) # router ospf 54 FOCS(config-router) # network 192.168.55.0 0.0.0.255 area 0 FOCS(config-router) # network 192.168.44.0 0.0.0.255 area 0 FOCS(config-router) # network 172.16.1.0 0.0.0.3 area 0 FOCS(config-router) # passive interface g0/0 FOCS(config-router) # passive interface g0/1

9. **202201 past year question**
   a. (i) Examine the network topology in Figure 1-2 and determine Open Shortest Path First (OSPF) configurations using network commands in AQUARIUS and CAPRICORN routers to allow PC11, Laptop33 and External_Laptop to communicate with each other. Use OSPF process-id 655 and area-id 0. **Assume the default route had been configured in the edge router (CAPRICORN).** Use Table 1-2 to document your answer.

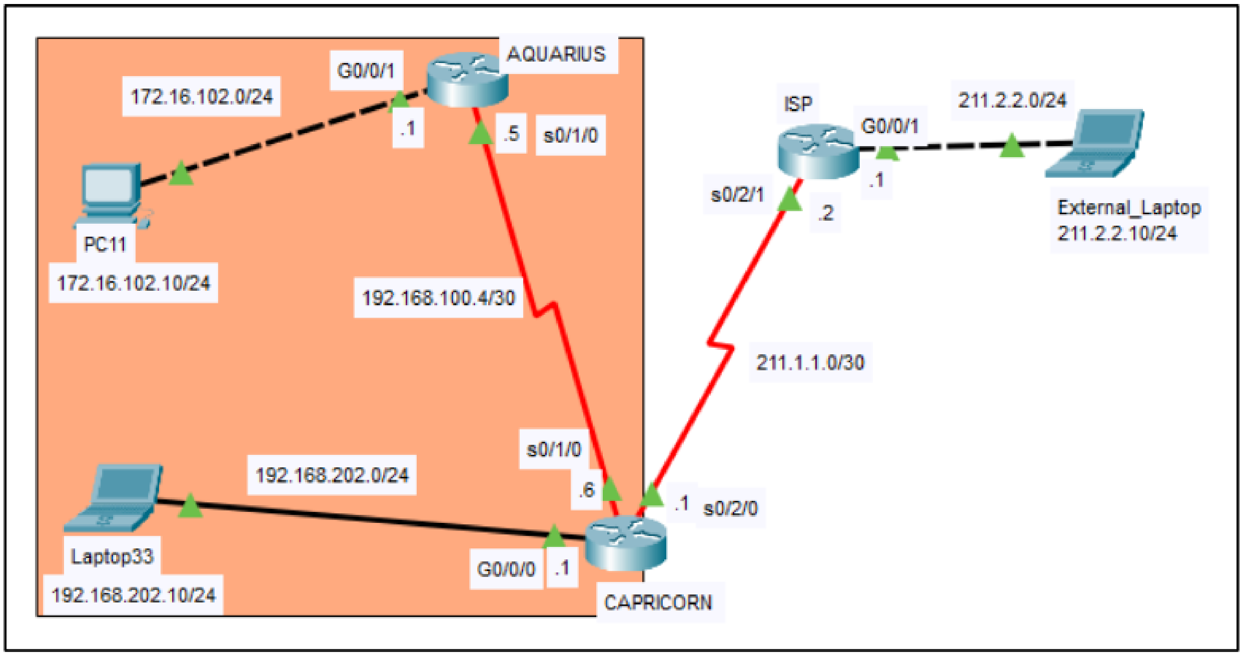


Figure 1-2: A network topology

Router	OSPF Configurations

AQUARIUS	`AQUARIUS(config) # router ospf 655`
	`AQUARIUS(config-router) # network 172.16.102.0 0.0.0.255 area 0`
	`AQUARIUS(config-router) # network 192.168.100.4 0.0.0.3 area 0`
	`AQUARIUS(config-router) # passive interface g0/0/1`

CAPRICORN	`CAPRICORN(config) # router ospf 655`
	`CAPRICORN(config-router) # network 192.168.100.4 0.0.0.3 area 0`
	`CAPRICORN(config-router) # network 192.168.202.0 0.0.0.255 area 0`
	`CAPRICORN(config-router) # default-information originate`
	`CAPRICORN(config-router) # passive interface g0/0/0`

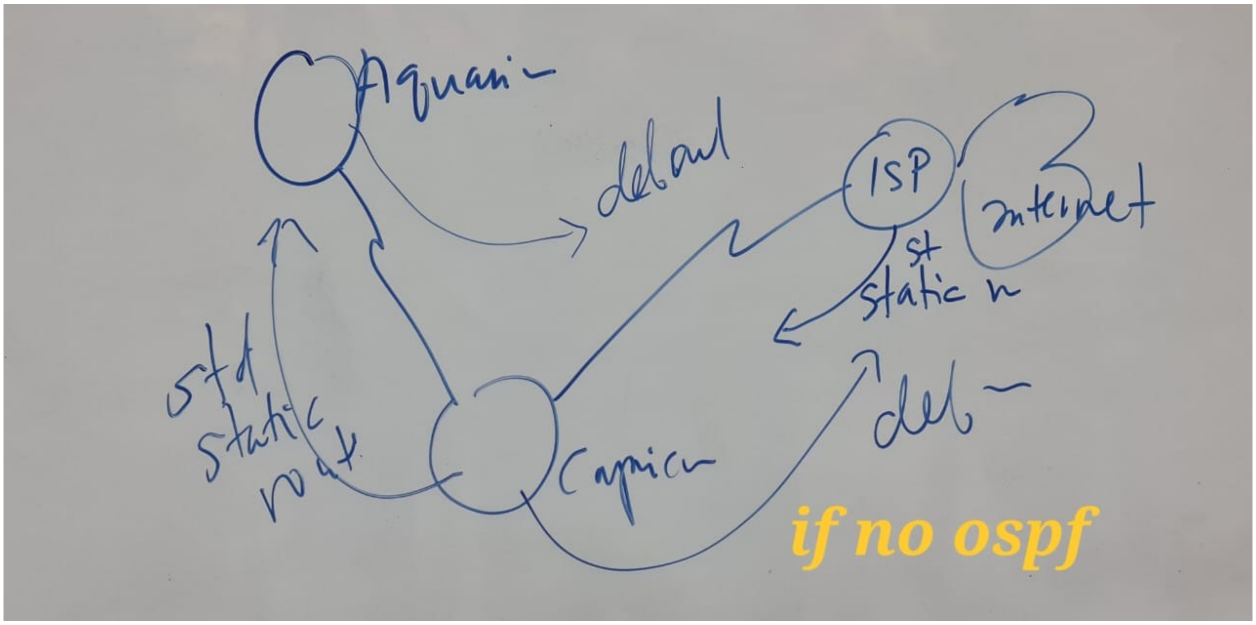
(ii) Configure a **default static route** and **standard static routes** using exit interfaces in the respective routers to enable PC11, Laptop33 and External_Laptop communications. Use Table 1-3 to document your answer.

	Router name	**Configuration**
Default static route	**CAPRICORN**	CAPRICORN(config) # ip route 0.0.0.0 0.0.0.0 s0/2/0
Standard static route	**ISP**	ISP(config) # ip route 172.16.102.0 255.255.255.0 s0/2/1 ISP(config) # ip route 192.168.202.0 255.255.255.0 s0/2/1

Extra Notes for this question 9 (ii)

Since OSPF has been configured within the internal network (the orange background), we only need to configure a standard static route on the ISP router to enable it to route back to the internal networks (PC11 and Laptop33), so called 2 way communication.

If without OSPF configuration within the figure 1.2 network topology,



Required configuration:

- Aquarium - default static route (to outside network)
- Capricorn - default static route and standard static route
- ISP - standard static route

Tutorial 3: Network Security Concepts

1. Explain the difference between a white and black hacker.

White Hat Hacker	Black Hat Hacker
An ethical hacker uses their programming abilities to discover security flaws within a system and report it to the developers to fix before the vulnerabilities can be exploited by an attacker.	An unethical hacker who compromises computer networks with malicious intent or self-serving reasons such as financial gain or revenge.

2. What are the uses of Malware?
    ○ Many early infectious programs, including the first Internet Worm, were written as experiments or pranks
    ○ Today, malware is used primarily to steal sensitive personal, financial, or business information for the benefit of others
    ○ Malware is sometimes used broadly against government or corporate websites to gather guarded information, or to disrupt their operation in general
    ○ All of these

3. What is the importance of firewalls in network security?

    - The firewalls permit or deny network transmissions by enforcing an access control policy.
    - They prevent the exposure of sensitive hosts, resources, and applications to untrusted users.
    - They sanitize protocol flow, which prevents the exploitation of protocol flaws.
    - They block malicious data from servers and clients.
    - They reduce security management complexity by off-loading most of the network access control to a few firewalls in the network.

4. Why do we need IPS?
    - An Intrusion Prevention System (IPS) monitors incoming and outgoing traffic looking for malware, network attack signatures. If it recognizes a threat, it can immediately stop it.
    - To illustrate, IPS technologies detect patterns in network traffic using signatures, which is a set of rules that is used to detect malicious activity. IPS technologies can detect atomic signature patterns (single-packet) or composite signature patterns (multi-packet).

5. What are the four elements of secure communication?
    - **Data Integrity**
      Guarantees that the message was not altered. Any changes to data in transit will be detected. Integrity is ensured by implementing either of the Secure Hash Algorithms (SHA-2 or SHA-3). The MD5 message digest algorithm is still widely in use but it is inherently insecure and creates vulnerabilities in a network. The use of MD5 should be avoided.

    - **Origin Authentication**
      Guarantees that the message is not a forgery and does actually come from whom it states. Many modern networks ensure authentication with protocols, such as hash message authentication code (HMAC).

    - **Data Confidentiality**
      Guarantees that only authorized users can read the message. If the message is intercepted, it cannot be deciphered within a reasonable amount of time. Data confidentiality is implemented using symmetric and asymmetric encryption algorithms.

    - **Data Non-Repudiation**
      Guarantees that the sender cannot repudiate, or refute, the validity of a message sent. Nonrepudiation relies on the fact that only the sender has the unique characteristics or signature for how that message is treated

6. Explain the difference between asymmetric and symmetric encryption.

Symmetric encryption	**Asymmetric encryption**
Known as shared-secret key algorithms	Known as public key algorithms
A sender and receiver must share a secret key	A sender and receiver uses pairs of keys which are public key and private key
Fast encryption as it is based on simple mathematical operations	Slower encryption as it is based on complex computational algorithms
E.g Data Encryption Standard (DES), Advanced Encryption Standard (AES)	E.g Rivest–Shamir–Adleman (RSA)

7. a. Compare and contrast TWO (2) social engineering attacks.

Phishing	**Spear phishing**
A threat actor sends a fraudulent email that is disguised as a legitimate, trusted source to trick the recipient into installing malware on their device or sharing personal or financial information.	A threat actor creates a targeted phishing attack tailored for a specific individual or organization.

b. Which of these two social engineering attacks is more commonly encountered among businesses? Include your reasons to support your answer.

Spear phishing

Spear phishing messages usually impersonate people or businesses known to the target, such as business partners, senior managers or even online services the cyber criminal knows the target to use.

Impersonation

This often occurs in the real world when the attacker uses spoof emails to pose as employees or trusted vendors and clients to gain the trust from the victim and ask them to send fraudulent payments or share sensitive information which affects the business badly.

Tutorial 4

1. Refer workbook
2. Refer workbook

3. Figure 2-1 shows a network topology where the Access Control List (ACLs) are to be applied to the router's interface to secure the network.

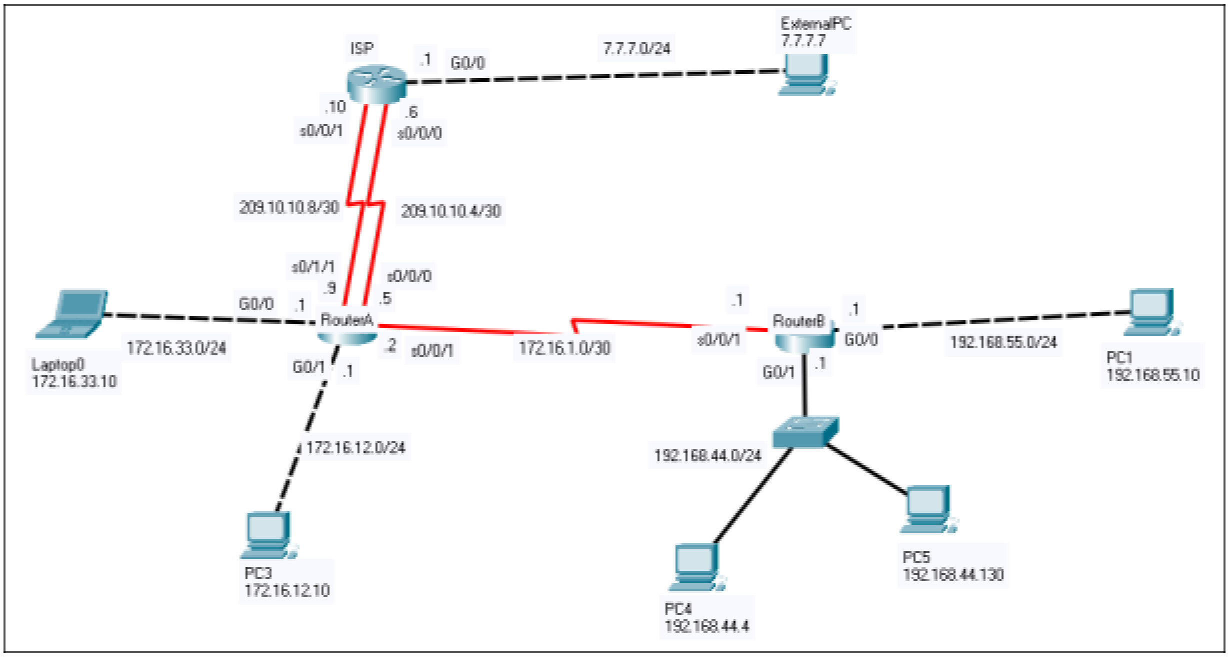


Figure 2-1: A network topology

Analyze Figure 2-1 and answer the following questions.

(i) Write an access list numbered 30 to allow PC3 to telnet into RouterA. Deny all other telnet traffic to RouterA which must be explicitly written in your Access Control List (ACL). Use suitable keyword(s) in the ACL. Indicate the router, interface and direction to apply the ACL. (5m)

Router - RouterA
Interface - line vty 0 4
Direction - In
Access-list - 30

```
RouterA# conf t
RouterA(config)# access-list 30 permit host 172.16.12.10
RouterA(config)# access-list 30 deny any

RouterA# line vty 0 4
RouterA(config-line)# access-class 30 in
```

(ii) Write an **extended access list** named HALF_NET to block Laptop0 from receiving information from the second half of usable addresses from the 192.168.44.0/24 network. Permit all other traffic. Use suitable keyword(s) in your ACL. Indicate the router, interface and direction to apply the ACL. (7m)

Source	-	Second half of usable addresses [upper half] from the 192.168.44.0/24
Destination	-	Laptop0
Interface	-	G0/1
Access-list	-	HALF_NET

```
RouterB# conf t
RouterB(config)# ip access-list extended HALF_NET
RouterB(config-ext-nacl)# deny ip 192.168.44.128 0.0.0.127 host 172.16.33.10
RouterB(config-ext-nacl)# permit ip any any

RouterB(config)# int g0/1
RouterB(config)# ip access-group HALF_NET in
```

C5 pg31 - NAT

ip nat pool NAT-POOL1 **209.165.200.226 209.165.200.240** netmask **255.255.255.224**

netmask - which address bits belong to the network and which bits belong to the host for that range of addresses.

209.165.200.226 to 209.165.200.240
226 - 11100010
227 - 11100011
228 - 11100100
229 - 11100101
230 - 11100110
" "
240 - 11110000

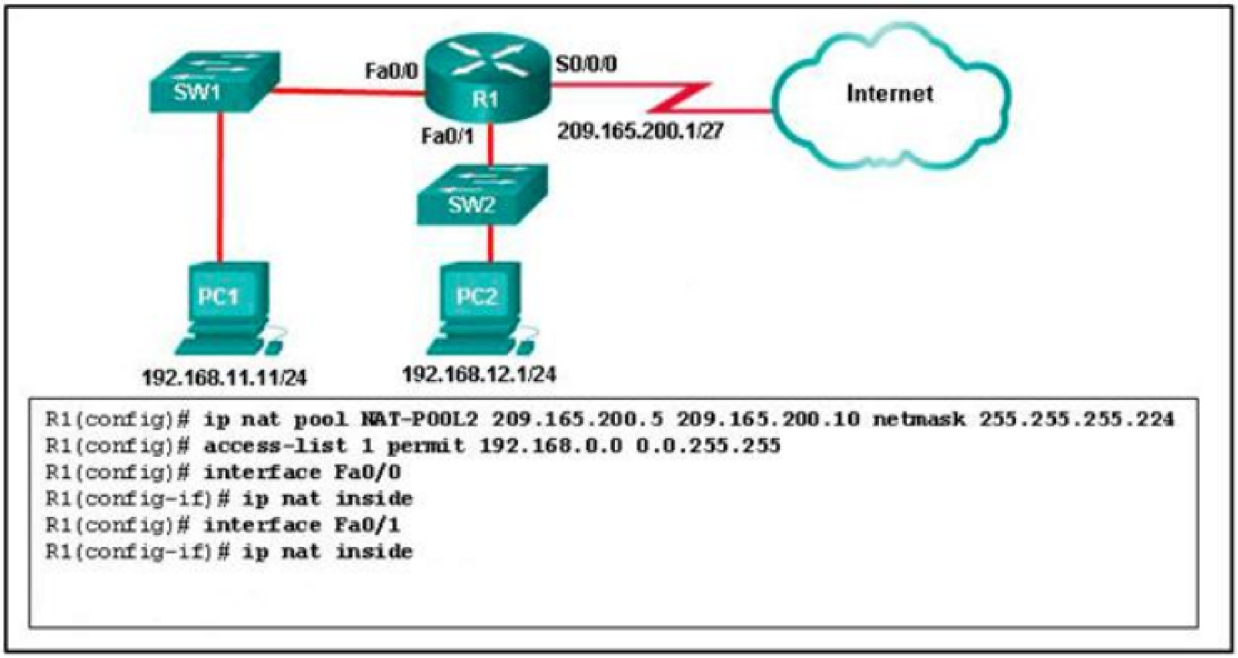
summarization

```
11010001.10100101.11001000.11100000    209.165.200.224
11111111.11111111.11111111.11100000    255.255.255.224 /27
```

incorrect.

Tutorial 5: NAT

1. Based on Figure 1-4, analyze the configurations of router R1.
   i. Illustrate the problems and suggest the solutions in order for PC1 and PC2 to communicate with other PCs on the Internet



```
R1(config)# ip nat pool NAT-POOL2 209.165.200.5 209.165.200.10 netmask 255.255.255.224
R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R1(config)# interface Fa0/0
R1(config-if)# ip nat inside
R1(config)# interface Fa0/1
R1(config-if)# ip nat inside
```

Figure 1-4: NAT

Dynamic NAT	
Problems	**Solutions**
The ACL didn't bind to the NAT-POOL2	Bind the ACL to the NAT-POOL2 using the *ip nat inside source list* command Step 3 `R1(config)# ip nat inside source list 1 pool NAT-POOL2 [overload]`

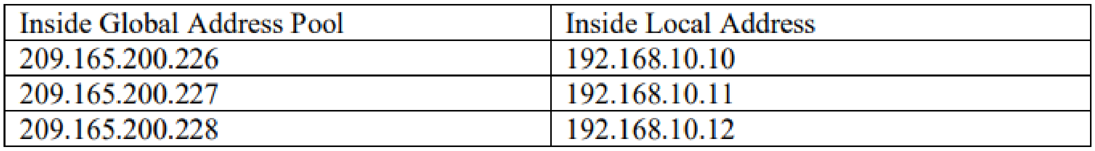
No outside interface specified	Specify the outside interface
	`R1(config-if)# interface s0/0/0`
	`R1(config-if)# ip nat outside`

Steps for Dynamic NAT

Define the pool
Configure ACL
Bind the ACL to the pool

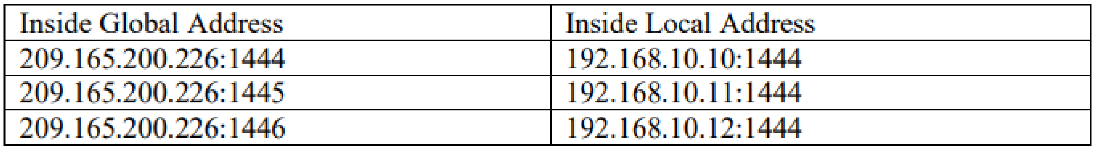
Apply (specify the inside and outside interface)

2. Identify the types of Network Address Translation (NAT) shown in Table 3-2a and 3-2b. Compare and contrast differences between these two NATs



Inside Global Address Pool	Inside Local Address
209.165.200.226	192.168.10.10
209.165.200.227	192.168.10.11
209.165.200.228	192.168.10.12

Table: 3-2a Network Address Translation



Inside Global Address	Inside Local Address
209.165.200.226:1444	192.168.10.10:1444
209.165.200.226:1445	192.168.10.11:1444
209.165.200.226:1446	192.168.10.12:1444

Table: 3-2b Network Address Translation

Table 3-2a: Dynamic NAT	**Table 3-2b: PAT (NAT Overload)**
Uses a pool of public addresses and assigns them on a first come, first-served basis	Maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses
Uses only IPv4 addresses in the translation process.	Uses IPv4 addresses and TCP or UDP source port numbers in the translation process.
A unique Inside Global address is required for each inside host accessing the outside network.	A single unique Inside Global address can be shared by many inside hosts accessing the outside network

3. An internal corporate server can be accessed by internal PCs, but not by external Internet users that should have access. What could be the issue?

   Issue

   Static NAT has not been configured or configured wrongly. Which is, the internal corporate server only has the private IPv4 address which only allows it to communicate locally. This is because private IPv4 addresses cannot be routed over the internet.

   Solution

   Static NAT should be configured to translate the private IPv4 address to public IPv4 address which initializes the communication from inside to outside (Internet).

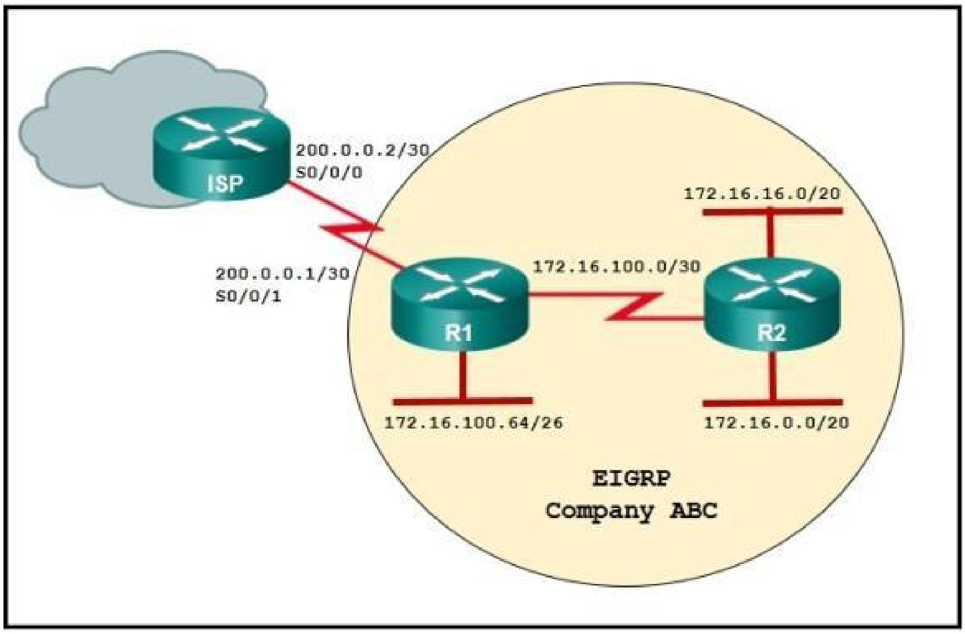
   Sample Configuration

   ```
   ip nat inside source static <private address> <public address>
   ```

   Specify inside interface

   Specify outside interface

4. Refer to the exhibit. NAT with **overload** (PAT) is configured on router R1 and uses the NAT pool of addresses 209.165.201.9 through 209.165.201.10. What type of route would the ISP need in order for communication to occur between hosts in Company ABC and the Internet?



- ip route 209.165.201.8 255.255.255.252 s0/0/0

5. What benefit does NAT64 provide?

   It allows sites to connect IPv6 hosts to an IPv4 network by translating the IPv6 addresses to IPv4 addresses. NAT64 is a temporary IPv6 transition strategy that allows sites to use IPv6 addresses and still be able to connect to IPv4 networks. This is accomplished by translating the IPv6 addresses into IPv4 addresses before sending the packets onto the IPv4 network.

6. Analyze Figure 3-1 and Figure 3-2. Identify and rectify the errors for static NAT and dynamic NAT with PAT to be implemented successfully in the network topology. Use Table 3-1 to document your answers. (15 marks)

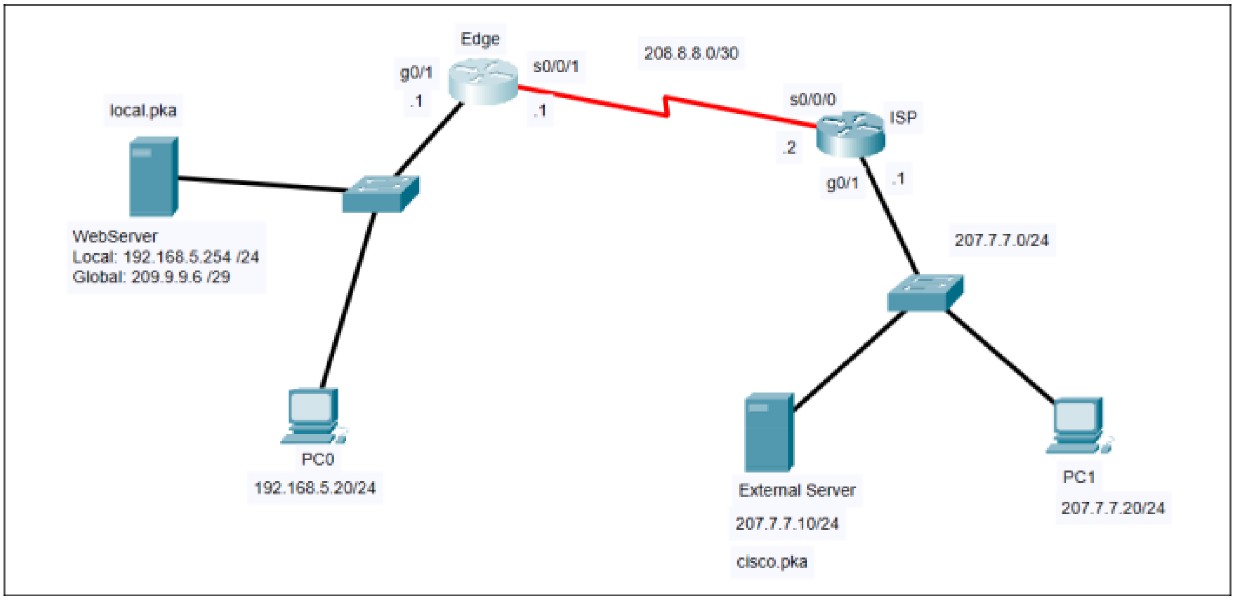
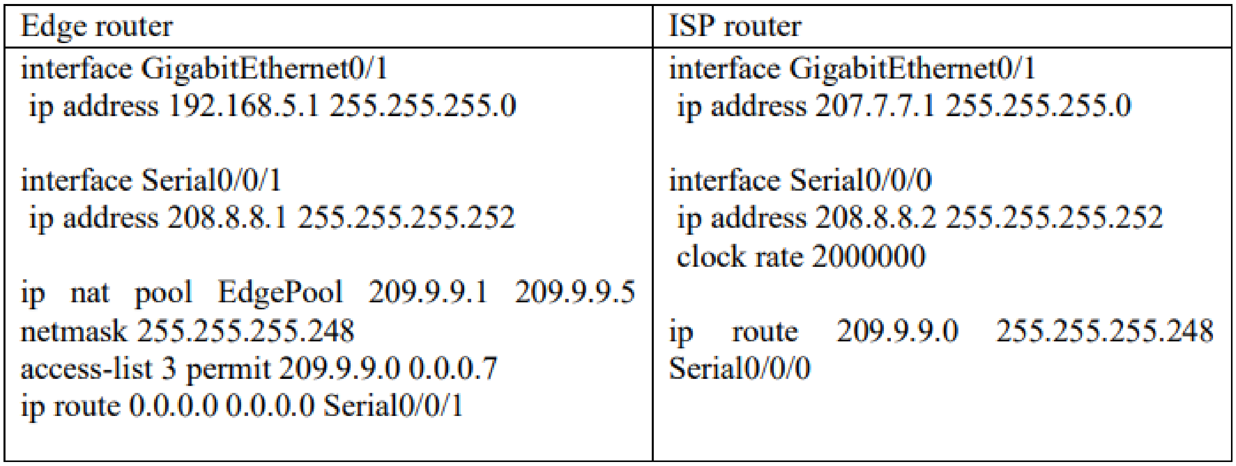


Figure 3-1: Network Topology



Edge router	ISP router
interface GigabitEthernet0/1 ip address 192.168.5.1 255.255.255.0 interface Serial0/0/1 ip address 208.8.8.1 255.255.255.252 ip nat pool EdgePool 209.9.9.1 209.9.9.5 netmask 255.255.255.248 access-list 3 permit 209.9.9.0 0.0.0.7 ip route 0.0.0.0 0.0.0.0 Serial0/0/1	interface GigabitEthernet0/1 ip address 207.7.7.1 255.255.255.0 interface Serial0/0/0 ip address 208.8.8.2 255.255.255.252 clock rate 2000000 ip route 209.9.9.0 255.255.255.248 Serial0/0/0

Figure 3-2: Partial output of "show run"

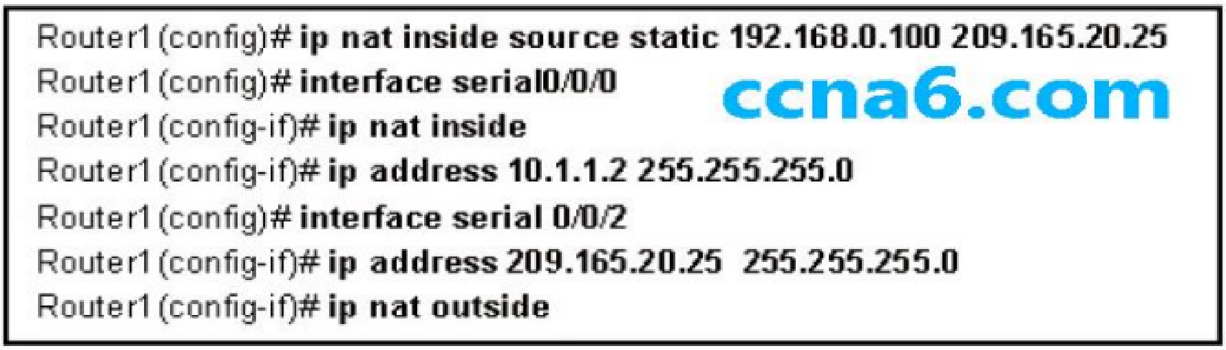
Item	Problems	Solutions
i.	Missing mapping between the inside local address and the inside global addresses	`ip nat inside source static 192.168.5.254 209.9.96`
ii.	The ACL didn't bind to the EdgePool	`ip nat inside source list 3 pool EdgePool`
iii.	access-list incorrect	`access-list 3 permit 192.168.5.0`

		`0.0.0.255`

ii.	Missing ip nat inside in interface G0/1 on Edge router	`Edgerouter(config)# interface g0/1`
		`Edgerouter(config-if)# ip nat inside`

iii.	Missing ip nat outside in interface S0/0/1 on Edge router	`Edgerouter(config)# interface s0/0/1`
		`Edgerouter(config-if)# ip nat outside`

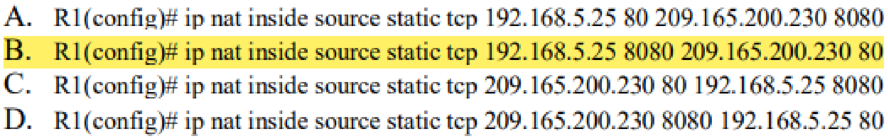
7. Refer to the following exhibit. Which address or addresses represent the **inside global address**?



```
Router1(config)# ip nat inside source static 192.168.0.100 209.165.20.25
Router1(config)# interface serial0/0/0
Router1(config-if)# ip nat inside
Router1(config-if)# ip address 10.1.1.2 255.255.255.0
Router1(config)# interface serial 0/0/2
Router1(config-if)# ip address 209.165.20.25  255.255.255.0
Router1(config-if)# ip nat outside
```

Inside local address: 192.168.0.100
Inside global address: 209.165.20.25

8. A network administrator is configuring a static NAT on the border router for a web server located in the DMZ network. The web server is configured to listen on **TCP port 8080**. The web server is paired with the **internal IP address of 192.168.5.25** and the **external IP address of 209.165.200.230**. For easy access by hosts on the Internet, external users do not need to specify the port when visiting the web server. Which command will configure the static NAT?



A. R1(config)# ip nat inside source static tcp 192.168.5.25 80 209.165.200.230 8080
B. R1(config)# ip nat inside source static tcp 192.168.5.25 8080 209.165.200.230 80
C. R1(config)# ip nat inside source static tcp 209.165.200.230 80 192.168.5.25 8080
D. R1(config)# ip nat inside source static tcp 209.165.200.230 8080 192.168.5.25 80

9. Refer to Figure 3-1. Write the configurations for **Port Address Translation (PAT)** using the single IP address assigned to the external interface in the BE-NAT router. Access-list number is 18. All the PCs should be able to ping ExternalPC.

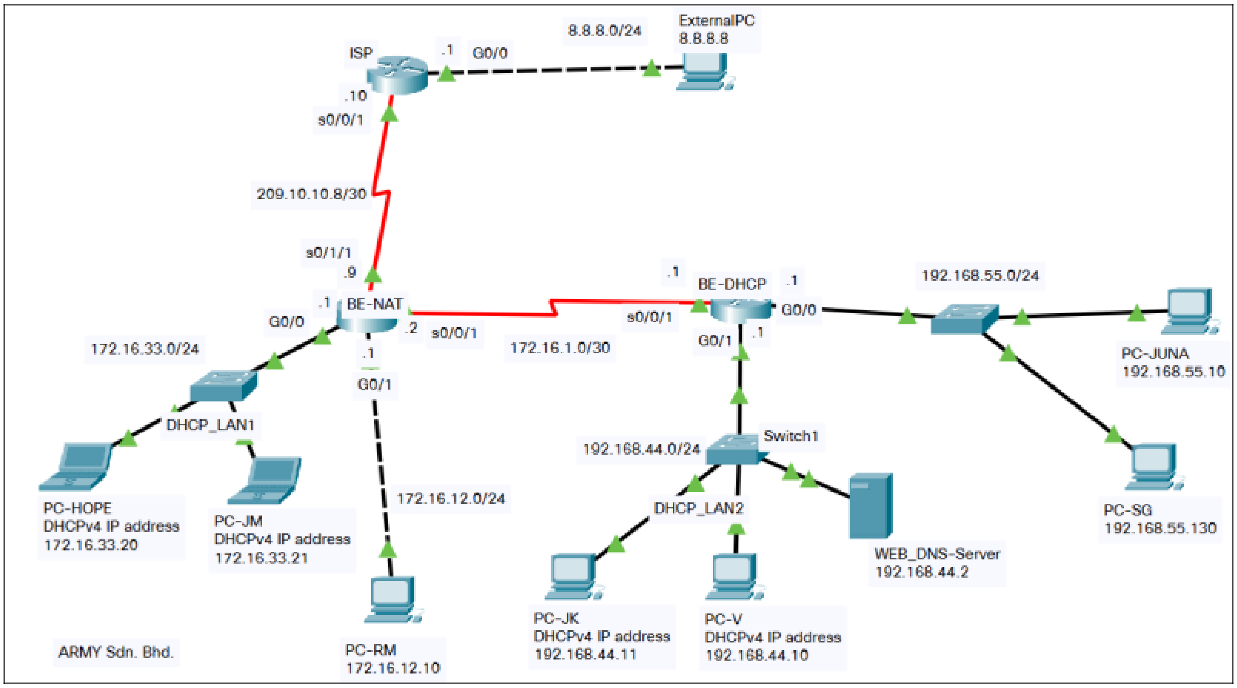


Figure 3-1: A network topology

```
ip nat inside source list 18 interface s0/1/1 overload
access-list 18 permit 192.168.44.0 0.0.0.255
access-list 18 permit 192.168.55.0 0.0.0.255
access-list 18 permit 172.16.12.0 0.0.0.255
access-list 18 permit 172.16.33.0 0.0.0.255
interface s0/0/1
ip nat inside
interface g0/0
ip nat inside
interface g0/1
ip nat inside
interface s0/1/1
ip nat outside
```

10. A network topology with IPv4 addressing, OSPF configurations and static routing were configured in the respective routers in Figure 3-1 network topology. All PCs are able to communicate with each other. Refer to Figure 3-1, answer the following questions. (202201 pass year)

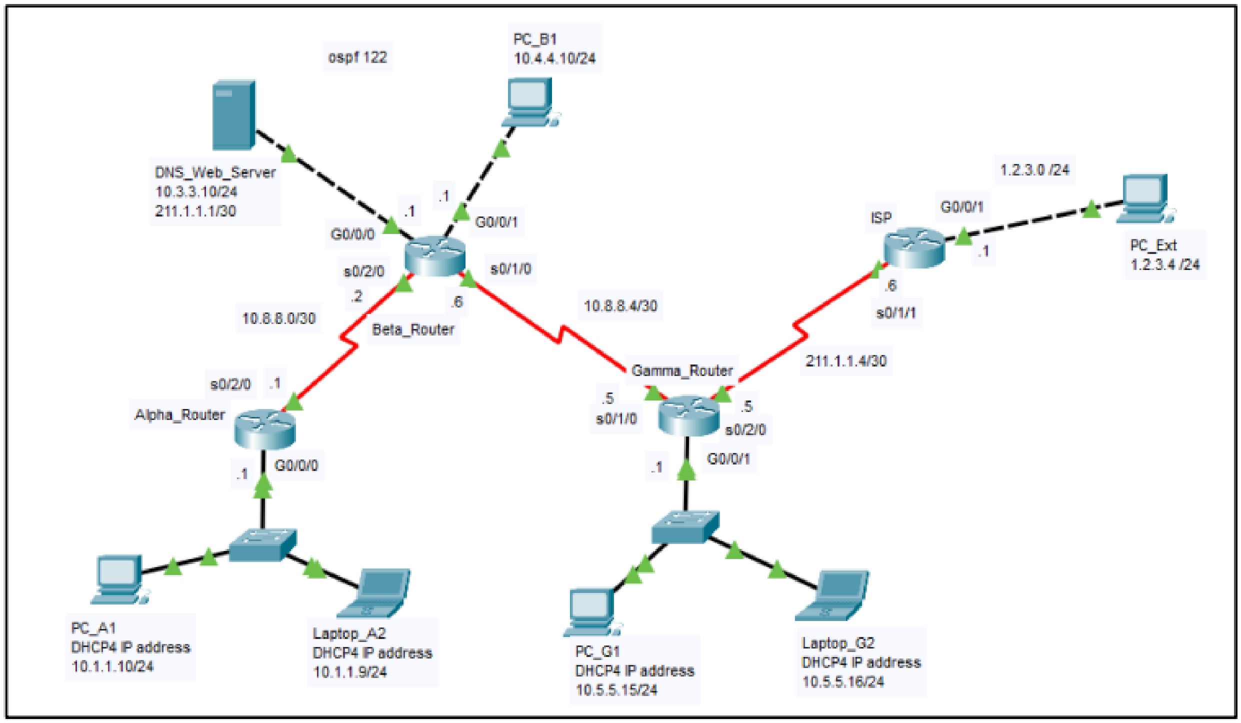


Figure 3-1: A network topology

a. i. Analyze Figure 3-1 and write a Static NAT configuration in order for DNS_Web_Server to be directly reachable from the Internet. Specify the router to implement **Static NAT**.

Edge router: Gamma_Router

```
ip nat inside source static 10.3.3.10 211.1.1.1
int s0/1/0
ip nat inside
int s0/2/0
ip nat outside
```

ii. Examine Figure 3-1 and write the configurations for Port Address Translation (PAT) using the single IP address assigned to the **external interface** in Gamma_Router. Access-list number is 72. All the PCs should be able to ping the PC_Ext.

```
ip nat inside source list 72 interface s0/2/0 overload
access-list 72 permit 10.1.1.0 0.0.0.255
access-list 72 permit 10.3.3.0 0.0.0.255
access-list 72 permit 10.4.4.0 0.0.0.255
access-list 72 permit 10.5.5.0 0.0.0.255
interface g0/0/1
ip nat inside
```

Short notes:

ip nat inside has been configured at s0/1/0 while ip nat outside has been configured at s0/2/0
Never use summarize route if the question didn't mention

Tutorial 6: DHCP

1. R1 acts as Cisco IOS DHCPv4 server assigns and manages IPv4 addresses from specified address pools within the router to DHCPv4 clients. You are required to exclude the first 5 IP addresses from both of the LANs. Write down the commands for R1.

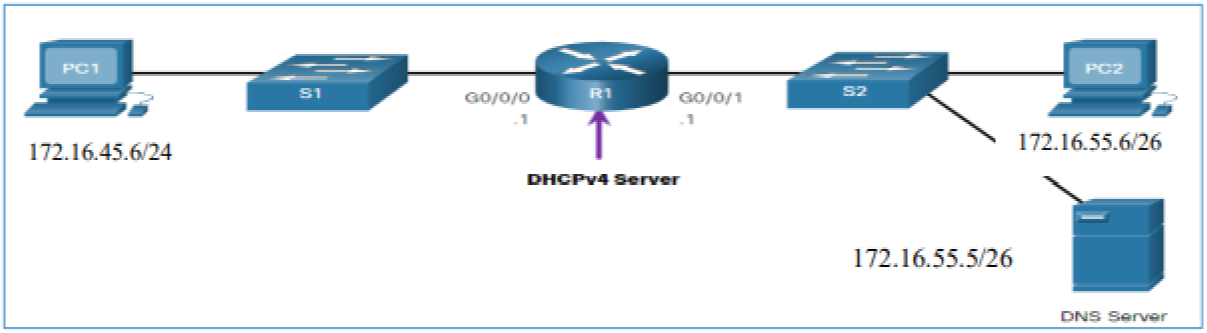


Figure 1-1: A network topology

```
ip dhcp excluded-address 172.16.45.1 172.16.45.5
ip dhcp pool LAN-POOL-45
network 172.16.45.0 255.255.255.0
default-router 172.16.45.1
dns-server 172.16.55.5

ip dhcp excluded-address 172.16.55.1 172.16.55.5
ip dhcp pool LAN-POOL-55
network 172.16.55.0 255.255.255.192
default-router 172.16.55.1
dns-server 172.16.55.5
```

Short Notes

A DHCP address is assigned to a DHCP client based on first-come-first-serve basis. From the topology, we can see that the address assigned to PC1 is 172.16.45.6 which is the first available address. Hence, we can conclude that 172.16.45.1 - 172.16.45.5 are being reserved/excluded.

2. A network administrator has set up a network topology as shown in Figure2-1 and configures DHCP, Syslog and NTP services as shown in Figure 2-2.

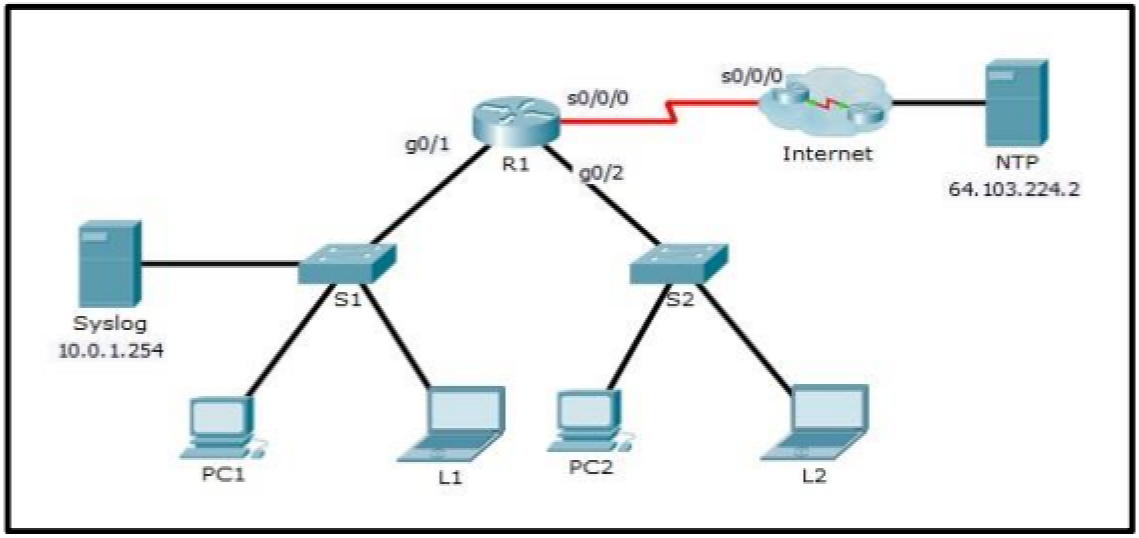
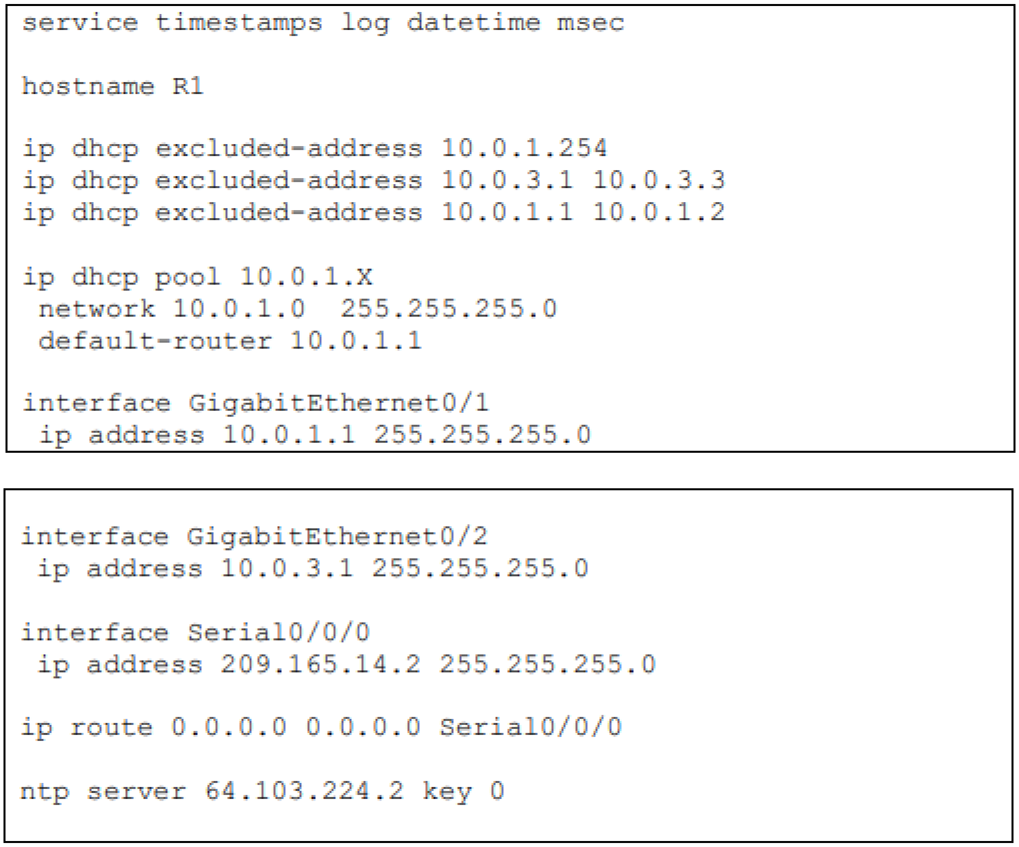


Figure 2-1: A network topology

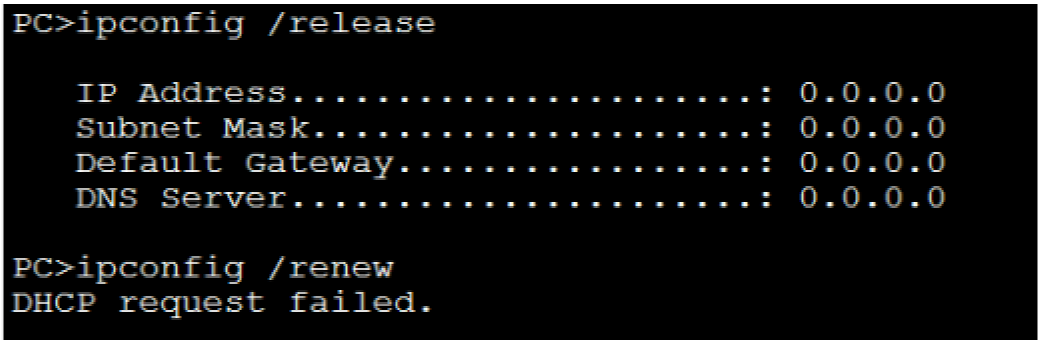


```
service timestamps log datetime msec

hostname R1

ip dhcp excluded-address 10.0.1.254
ip dhcp excluded-address 10.0.3.1 10.0.3.3
ip dhcp excluded-address 10.0.1.1 10.0.1.2

ip dhcp pool 10.0.1.X
 network 10.0.1.0  255.255.255.0
 default-router 10.0.1.1

interface GigabitEthernet0/1
 ip address 10.0.1.1 255.255.255.0
```

```

interface GigabitEthernet0/2
 ip address 10.0.3.1 255.255.255.0

interface Serial0/0/0
 ip address 209.165.14.2 255.255.255.0

ip route 0.0.0.0 0.0.0.0 Serial0/0/0

ntp server 64.103.224.2 key 0
```

Figure 2-2: Partial output of "show running-config"

(i) **DHCP is not functioning for PC2 and L2** when the network administrator tries to release and renew IP addresses as shown in Figure 2-3. Based on Figure 2-1 and Figure 2-2, identify and rectify the problem.



```
PC>ipconfig /release

   IP Address......................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: 0.0.0.0
   DNS Server......................: 0.0.0.0

PC>ipconfig /renew
DHCP request failed.
```

Figure2-3: Sample output of “ipconfig /release” and “ipconfig /renew”

Problem	**Solution**

The DHCPv4 pool for 10.0.3.0 is not defined.	`ip dhcp pool 10.0.3.X`
	`network 10.0.3.0 255.255.255.0`
	`default-router 10.0.3.1`

3. PC1 is attempting to acquire an IPv4 address from a DHCPv4 server using a broadcast message. In this scenario, R1 is not configured as a DHCPv4 server and does not forward the broadcast.

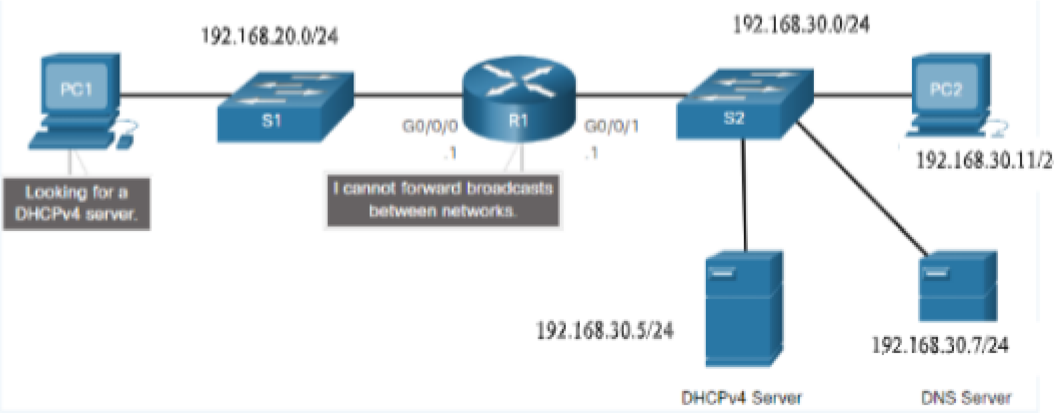


Figure 3-1: A network topology

(i) Can PC1 obtain a DHCP IPv4 address from the DHCPv4 Server? Justify your answer.
No, because the DHCPv4 Server is located on a different subnet/network with PC1 and by default the router does not forward the broadcast message between networks. Hence, PC1 cannot receive an IP address from DHCPv4 Server.

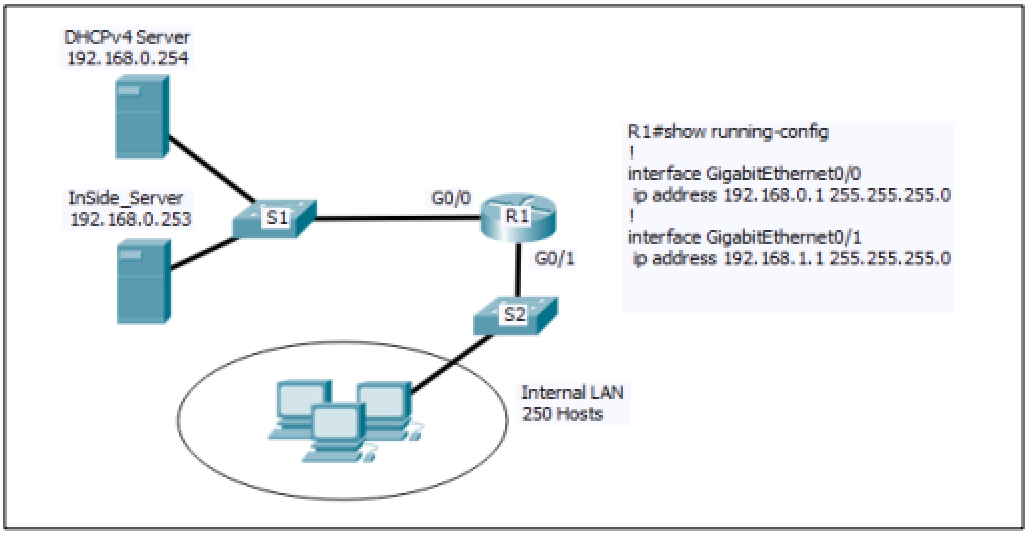
(ii) How to allow PC1 to obtain a DHCP IPv4 address from the DHCPv4 Server. Propose a solution and write the commands
Configure R1 as a DHCPv4 relay agent with the ip helper-address which enables R1 to relay DHCPv4 broadcasts to the DHCPv4 server.

R1

```
int g0/0/0
ip address 192.168.20.1 255.255.255.0
ip helper-address 192.168.30.5
```

Notes: When R1 has been configured as a DHCPv4 relay agent, it accepts broadcast requests for the DHCPv4 service and then forwards those requests as a unicast to the IPv4 address 192.168.30.5

4. Given the following network physical topology and partial configurations shown in Figure 4-1, all the hosts attached to the Internal LAN are not able to acquire TCP/IP configuration information from the DHCPv4 Server. As a network associate, you are required to troubleshoot and correct the configuration errors. Document the problem discovered, explanations and a detailed solution.



```
R1#show running-config
!
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
```

Figure 4-1 A network with a DHCPv4 server

Problem	**Solution**

DHCPv4 Server is located on a different network with the host attached to the internal network and the DHCPv4 Relay is not configured on R1.	Configure ip helper-address on G0/1 of the R1 as a DHCPv4 relay agent to accept broadcast requests for the DHCPv4 services and forward those request as a unicast to the IPv4 address 192.168.0.254
	Cisco commands
	`int g0/1`
	`ip helper-address 192.168.0.254`

5. CEO of ARMY Sdn. Bhd. has employed you to ensure all the PCs in the company are able to communicate with each other. Assume all the IPv4 addressing, static routing and OSPF configurations are configured in the respective routers. With reference to a network topology shown in Figure 5-1, answer the following questions

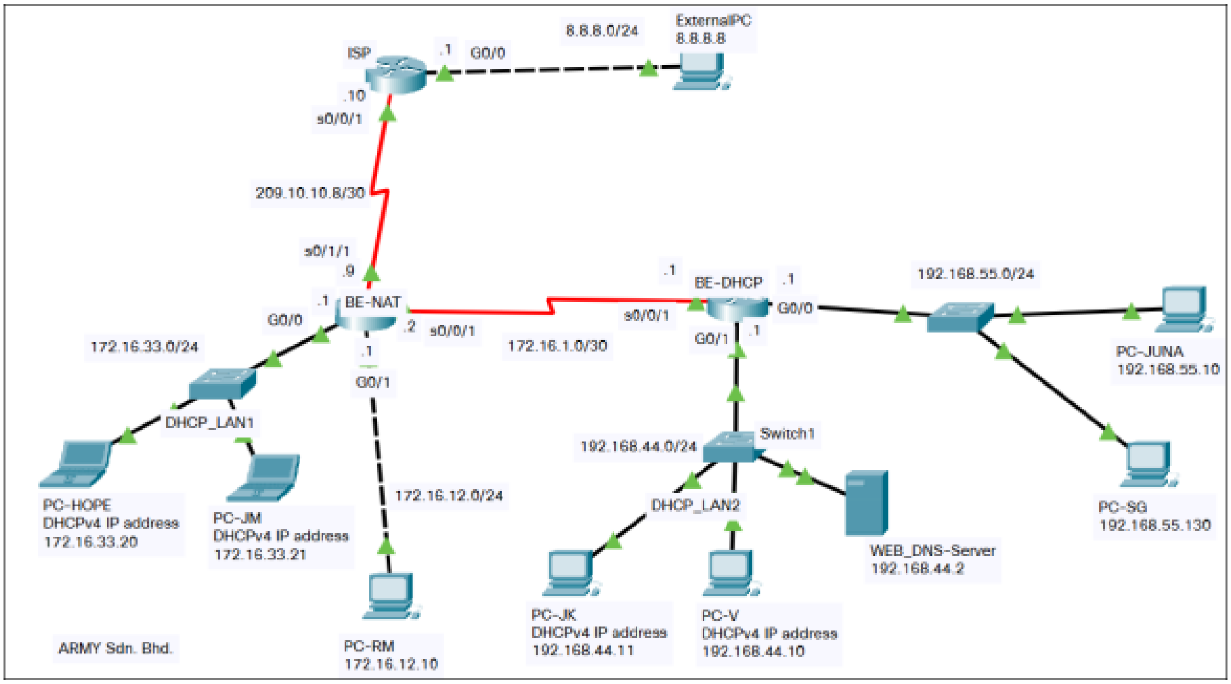


Figure 5-1: A network topology

a. DHCP (Dynamic Host Configuration Protocol) configurations are to be configured in the BE-DHCP router. PC-V, PC-JK, PC-HOPE and PC-JM should obtain the IP addresses and other DHCP configurations automatically from the BE-DHCP router as shown in Figure 5-1. Use Table 5-1 to document the DHCP configurations with justifications. (16 marks)

Router Name	**Configurations**
BE_DHCP	ip dhcp excluded-address 172.16.33.1 172.16.33.19 ip dhcp pool LAN-POOL-33 network 172.16.33.0 255.255.255.0 default-router 172.16.33.1 dns-server 192.168.44.2 **Justification** The LAN-POOL-33 is specifically for the 192.168.33.0 network. DHCP excluded IP addresses from 1 to 19 because IpV4 addresses for PC-JM starts from 172.16.44.20, the first available address assigned by DHCPv4 server. The default gateway is 192.168.33.1 to route to remote sites. DNS server has been configured with ip address 192.168.44.2 **Configurations** ip dhcp excluded-address 192.168.44.1 192.168.44.9 ip dhcp pool LAN-POOL-44 network 192.168.44.0 255.255.255.0 default-router 192.168.44.1

	`dns-server 192.168.44.2` **Justification** The LAN-POOL-44 is specifically for the 192.168.44.0 network. DHCP excluded IP addresses from 1 to 9 because IpV4 addresses for PC-JK starts from 172.16.44.10, the first available address assigned by DHCPv4 server. The default gateway is 192.168.44.1 to route to remote sites. DNS server has been configured with ip address 192.168.44.2

Router Name
BE-NAT
	Configurations
	`int g0/0`
	`ip helper-address 172.16.44.1`
	Justification
	Since DHCPv4 Server is located on a different network with the host within network 172.17.33.0. Hence, configure ip helper-address on G0/0 of the BE-NAT as a DHCPv4 relay agent to accept broadcast requests for the DHCPv4 services and forward those request as a unicast to the IPv4 address 172.16.44.1

Notes
The helper address can be any active IPv4 address from the DHCPv4 server (BE-DHCP router)

6. A network topology with IPv4 addressing, OSPF configurations and static routing were configured in the respective routers in Figure 3-1 network topology. All PCs are able to communicate with each other. Refer to Figure 3-1, answer the following questions. (202201 Pass Year)

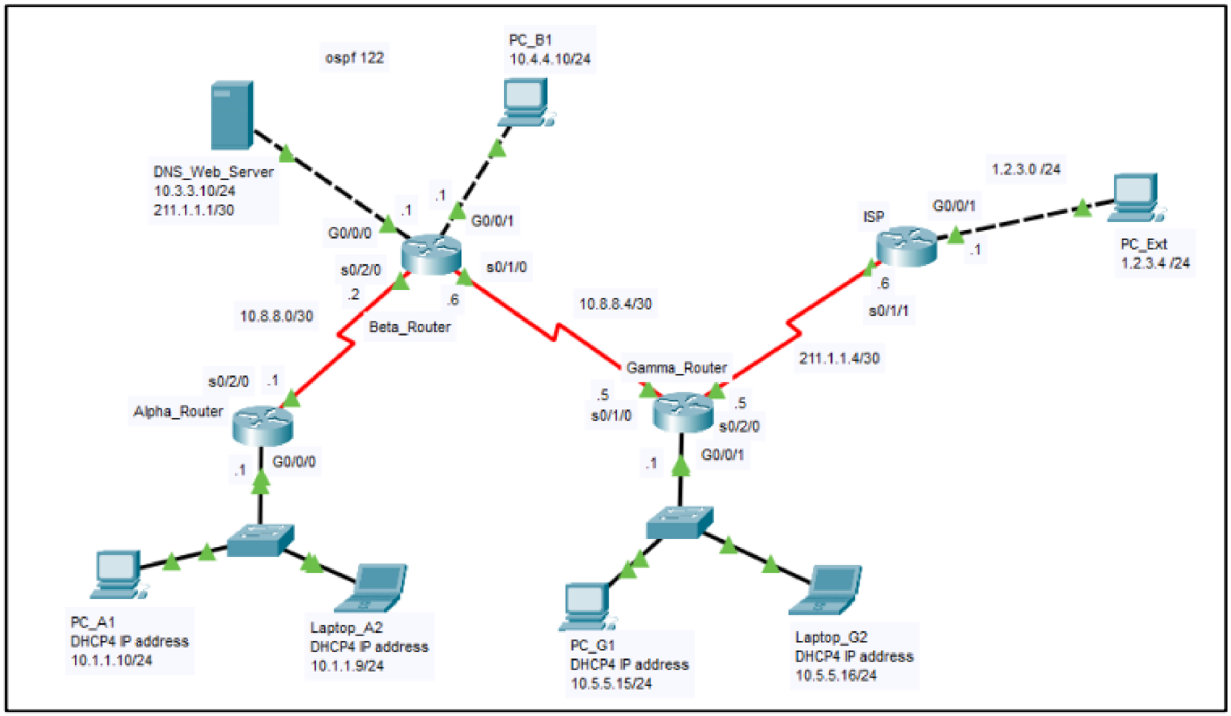


Figure 3-1: A network topology

b. Alpha_Router is the DHCP (Dynamic Host Configuration Protocol) server. PC_A1, Laptop_A2, PC_G1 and Laptop_G2 should obtain the IP addresses and other DHCP configurations automatically from Alpha_Router as shown in Figure 3-1. DHCP pool names are ALPHA_DHCP and GAMMA_DHCP respectively. Use Table 3-1 to document the DHCP configurations with justifications. (14 marks)

Router Name	Configurations
Alpha_Router	ip dhcp excluded 10.1.1.1 10.1.1.8 ip dhcp pool ALPHA_DHCP network 10.1.1.0 255.255.255.0 default-router 10.1.1.1 dns-server 10.3.3.10 **Justification** DHCP excluded IP addresses from 1 to 8 because IpV4 addresses for Laptop_A2 starts from 10.1.1.8. The default gateway is 10.1.1.1 to route to remote sites. ip dhcp excluded 10.5.5.1 10.5.5.14 ip dhcp pool GAMMA_DHCP network 10.5.5.0 255.255.255.0 default-router 10.5.5.1

	`dns-server 10.3.3.10` **Justification** DHCP excluded IP addresses from 1 to 14 because IpV4 addresses for pc_g1 starts from 10.1.1.15. The default gateway is 10.5.5.1 to route to remote sites.

Gamma_Router	`int g0/0/1`
	`ip helper-address 10.1.1.1`
	Justification
	Since DHCPv4 Server is located on a different network with the host within network 10.5.5.0. Hence, configure ip helper-address on G0/0/1 of the Gamma_Router as a DHCPv4 relay agent to accept broadcast requests for the DHCPv4 services and forward those request as a unicast to the IPv4 address 10.1.1.1

7. With reference to a network topology shown in Figure 4-1 and output of “show run” configurations in Figure 4-2, answer the following.

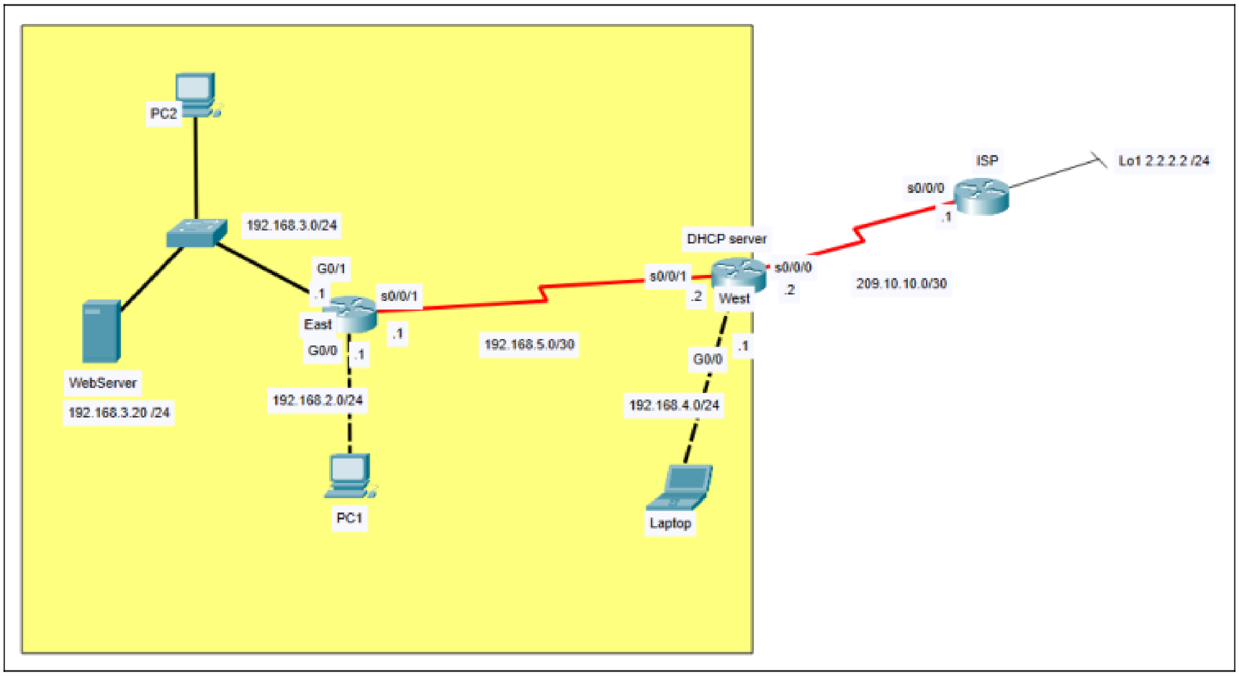
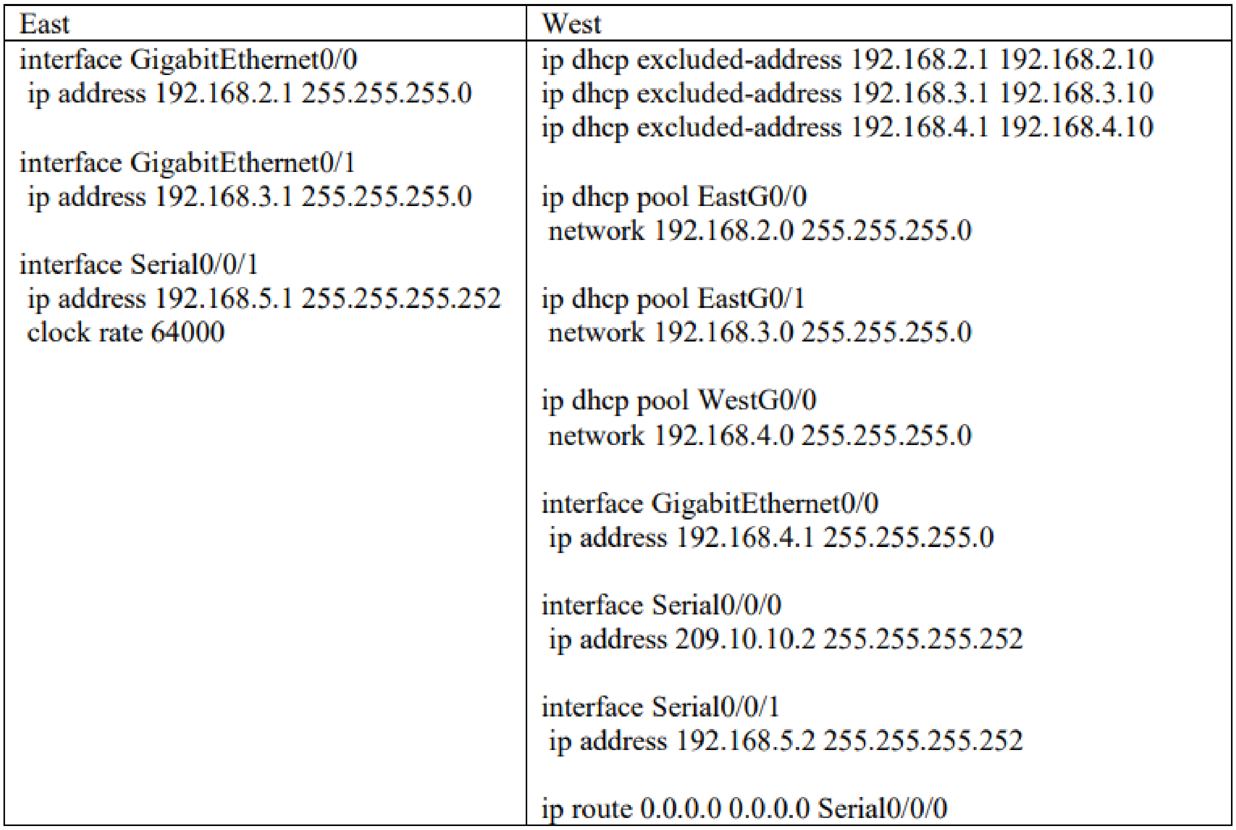


Figure 4-1: A network topology



East	West
interface GigabitEthernet0/0 ip address 192.168.2.1 255.255.255.0 interface GigabitEthernet0/1 ip address 192.168.3.1 255.255.255.0 interface Serial0/0/1 ip address 192.168.5.1 255.255.255.252 clock rate 64000	ip dhcp excluded-address 192.168.2.1 192.168.2.10 ip dhcp excluded-address 192.168.3.1 192.168.3.10 ip dhcp excluded-address 192.168.4.1 192.168.4.10 ip dhcp pool EastG0/0 network 192.168.2.0 255.255.255.0 ip dhcp pool EastG0/1 network 192.168.3.0 255.255.255.0 ip dhcp pool WestG0/0 network 192.168.4.0 255.255.255.0 interface GigabitEthernet0/0 ip address 192.168.4.1 255.255.255.0 interface Serial0/0/0 ip address 209.10.10.2 255.255.255.252 interface Serial0/0/1 ip address 192.168.5.2 255.255.255.252 ip route 0.0.0.0 0.0.0.0 Serial0/0/0

Figure 4-2: Output of "show run" command

a. DHCP (Dynamic Host Control Protocol) server configurations were configured in the West router. PC1, PC2 and Laptop were unable to obtain the IP addresses and other DHCP configurations successfully. Evaluate the DHCP configurations in Figures 4-1 and 4-2. Use Table 4-1 to document the identified errors, provide the solutions/correct configurations for the respective errors and lastly justified your answers. (9 marks)

Item	Problems	Solutions	Justification

1	Missing default-gateway in West router	**West Router**
		
		EastG0/0 pool
		`default-router 192.168.2.1`
		
		EastG0/1 pool
		`default-router 192.168.3.1`
		
		WestG0/0 pool
		`default-router 192.168.4.1`
			Default gateway with the `default-router <ip address>` command has to be configured to route to remote sites.

2	Missing relay agent in East router	**East Router** `int g0/0`	Since DHCPv4 Server is located on a different network with the host

		ip helper-address 192.168.5.2 Notes: The helper address can be any active IPv4 address from the DHCPv4 server	within the network 192.168.2.0 and 192.168.4.0. Hence, configure ip helper-address on G0/0 of the Gamma_Router as a DHCPv4 relay agent to accept broadcast requests for the DHCPv4 services and forward those requests as a unicast to the IPv4 address 192.168.5.2

Tutorial 7: Wan Concepts

1. Modern Wide Area Network (WAN) technologies are continually emerging. An organization has options to choose a modern Wide Area Network (WAN) to connect their Local Area Networks (LANs) to the remote LANs. Propose and illustrate the most appropriate **modern WAN solution** for the following scenario.

   (i) A company with branches at different locations using **Ethernet technology**. (5 marks)

   Ethernet WAN

   - **Reduced expenses and administration** - Ethernet WAN provides a switched, high-bandwidth Layer 2 network capable of managing data, voice, and video all on the same infrastructure. This increases bandwidth and eliminates expensive conversions to other WAN technologies. The technology enables businesses to inexpensively connect numerous sites in a metropolitan area, to each other, and to the internet.
   - **Easy integration with existing networks** - Ethernet WAN connects easily to existing Ethernet LANs, reducing installation costs and time.
   - **Enhanced business productivity** - Ethernet WAN enables businesses to take advantage of productivity-enhancing IP applications that are difficult to implement on TDM or Frame Relay networks, such as hosted IP communications, VoIP, and streaming and broadcast video.

   (ii) **Local subscriber using coaxial cable** to have Internet connection. (5 marks)

   Cable Technology

   Cable technology is a high-speed always-on connection technology that uses a coaxial cable from the cable company to provide IP services to users. Like DSL, cable technology is a popular choice for home users and for enterprise IT departments to support remote workers.

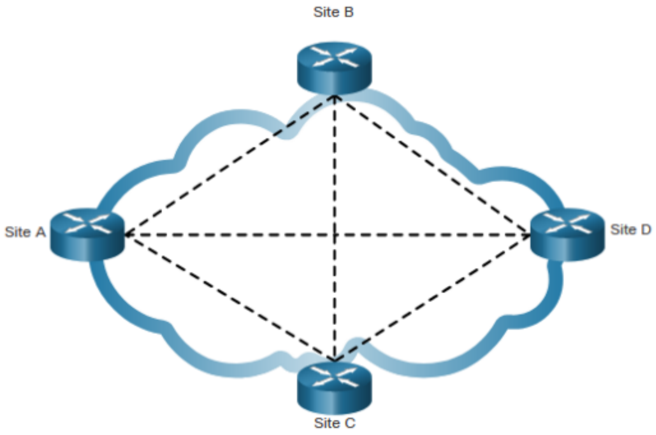
2. Compare a private WAN to a public WAN.

Private WAN	Public WAN
• A connection that is dedicated to a single customer • Guaranteed service level • Consistent bandwidth • Security	• A connection that is typically provided by an ISP or telecommunications service provider using the internet. • The service levels and bandwidth may vary, and the shared connections do not guarantee security.

3. Identify the type of WAN network design that is the most fault-tolerant and draw the topology diagram.

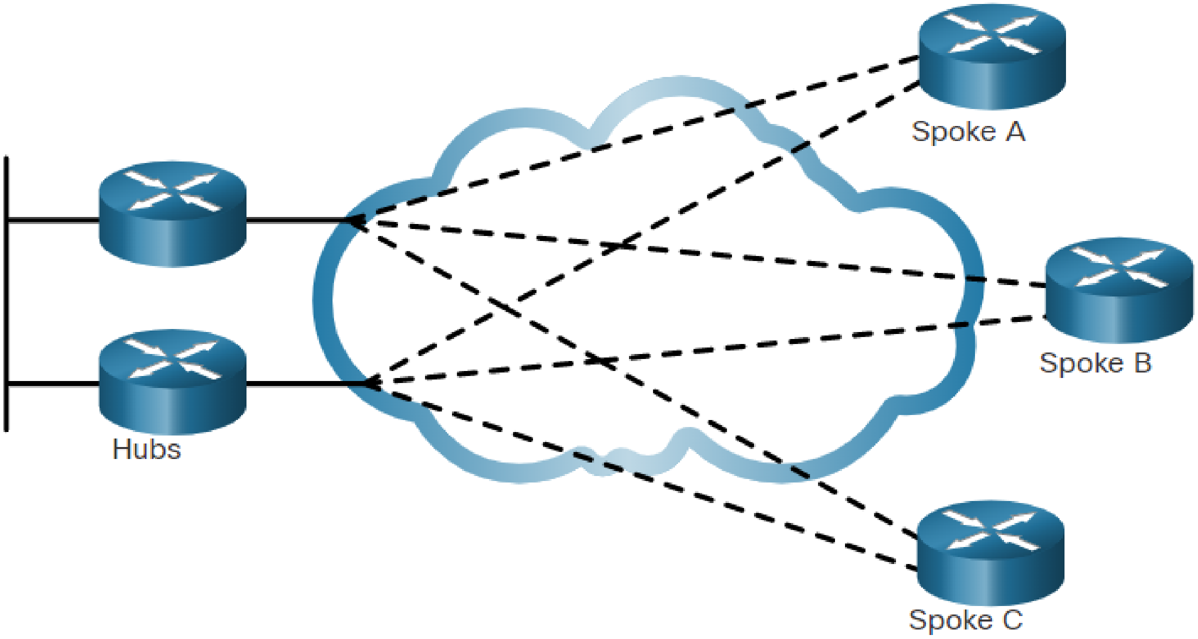
   Fully Meshed Topology

   - It uses multiple virtual circuits to connect all sites.



4. One of the Wide Area Network (WAN) topologies is Dual-homed topology. With the aid of a diagram, illustrate the Dual-homed topology. What is the advantage and disadvantage of Dual-homed Topology?

   - A dual-homed topology provides redundancy. As shown in the figure, two hub routers are dual-homed and redundantly attached to three spoke routers across a WAN cloud.



   - The advantage of dual-homed topologies is that they offer enhanced network redundancy, load balancing, distributed computing and processing, and the ability to implement backup service provider connections.

- The disadvantage is that they are more expensive to implement than single-homed topologies. This is because they require additional networking hardware, such as additional routers and switches. Dual-homed topologies are also more difficult to implement because they require additional, and more complex, configurations.

5. WAN operates at layer 1, layer 2 and layer 3 of the OSI model. Do you agree with the statement? Justify your answer.
   - This is an incorrect statement because most WAN standards focus on the physical layer (OSI Layer 1) and the data link layer (OSI Layer 2).
   - **Layer 1 Protocols**
     - Layer 1 protocols describe the electrical, mechanical, and operational components needed to transmit bits over a WAN. For example, service providers commonly use high-bandwidth optical fiber media to span long distances (i.e., long haul) using the following Layer 1 optical fiber protocol standards:
       - Synchronous Digital Hierarchy (SDH)
       - Synchronous Optical Networking (SONET)
       - Dense Wavelength Division Multiplexing (DWDM)
       - SDH and SONET essentially provide the same services and their transmission capacity can be increased by using DWDM technology.
   - **Layer 2 Protocols**
     - Layer 2 protocols define how data will be encapsulated into a frame.
     - Several Layer 2 protocols have evolved over the years including the following:
       - Broadband (i.e., DSL and Cable)
       - Wireless
       - Ethernet WAN (Metro Ethernet)
       - Multiprotocol Label Switching (MPLS)
       - Point-to-Point Protocol (PPP) (less used)
       - High-Level Data Link Control (HDLC) (less used)
       - Frame Relay (legacy)
       - Asynchronous Transfer Mode (ATM) (legacy)

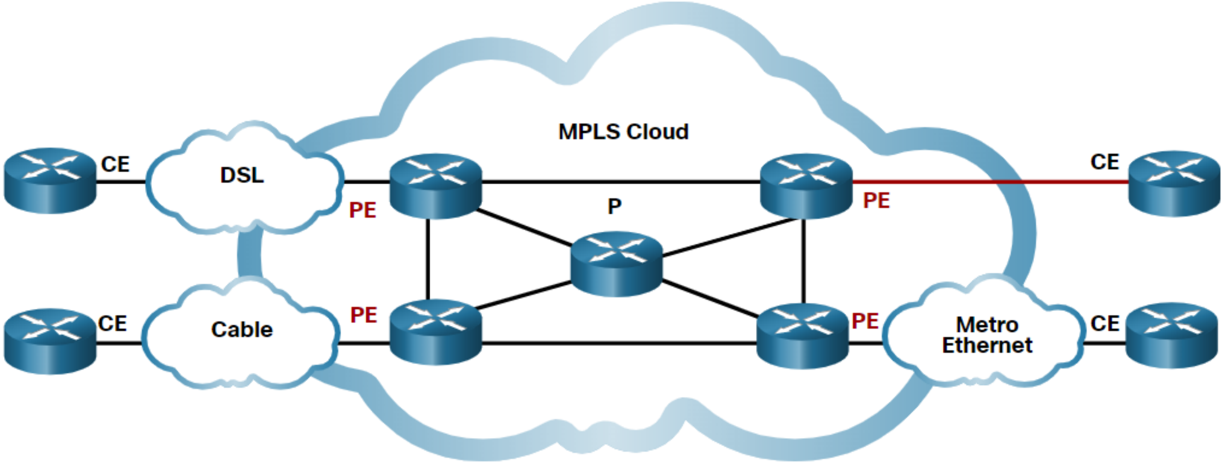
6. Identify the communication method that is used in all WAN connections. What is the advantage of using this communication method?
   - **Serial communication**. Almost all network communications occur using a serial communication delivery. Serial communication transmits bits sequentially over a single channel. In contrast, **parallel communications** simultaneously transmit several bits using multiple wires.
   - A parallel connection theoretically transfers data eight times faster than a serial connection; it is prone to synchronization problems. As the cable length

increases, the synchronization timing between multiple channels becomes more sensitive to distance. For this reason, parallel communication is limited to very short distances only (e.g., copper media is limited to less than 8 meters (i.e., 26 feet).

7. What type of network communication is used by Ethernet WAN (Metro Ethernet), Multiprotocol Label Switching (MPLS), as well as legacy Frame Relay and legacy Asynchronous Transfer Mode (ATM)? Describe this network communication.
   Packet-Switched Communication
   - Packet-switching segments traffic data into packets that are routed over a shared network. Packet-switched networks do not require a circuit to be established, and they allow many pairs of nodes to communicate over the same channel.
   - Packet switching is much less expensive and more flexible than circuit switching. Although susceptible to delays (latency) and variability of delay (jitter), modern technology allows satisfactory transport of voice and video communications on these networks.

8. Explain Multiprotocol Label Switching (MPLS).

Multiprotocol Label Switching (MPLS) is a high-performance service provider WAN routing technology to interconnect clients without regard to access method or payload. MPLS supports a variety of client access methods (e.g., Ethernet, DSL, Cable, Frame Relay). MPLS can encapsulate all types of protocols including IPv4 and IPv6 traffic.



An MPLS router can be a customer edge (CE) router, a provider edge (PE) router, or an internal provider (P) router. Notice that MPLS supports a variety of client access connections.
MPLS routers are label switched routers (LSRs). This means that they attach labels to packets that are then used by other MPLS routers to forward traffic. When traffic is leaving the CE, the MPLS PE router adds a short fixed-length label in between the frame header and packet header. MPLS P routers use the label to determine the next hop of the packet. The label is removed by the egress PE router when the packet leaves the MPLS network.

MPLS also provides services for QoS support, traffic engineering, redundancy, and VPNs.

9. Internet-based broadband connectivity is an alternative to using dedicated WAN options. Internet-based connectivity can be divided into wired and wireless options. Explain the wired and wireless options and give relevant examples.

Wired options

Wired options use permanent cabling (e.g., copper or fiber) to provide consistent bandwidth, and reduce error rates and latency. Examples of wired broadband connectivity are Digital Subscriber Line (DSL), cable connections, and optical fiber networks.

Wireless options

Wireless options are less expensive to implement compared to other WAN connectivity options because they use radio waves instead of wired media to transmit data. However, wireless signals can be negatively affected by factors such as distance from radio towers, interference from other sources, weather, and number of users accessing the shared space. Examples of wireless broadband include cellular 3G/4G/5G or satellite internet services. Wireless carrier options vary depending on location.

10. Internet-based broadband solutions have advantages and disadvantages. Illustrate the factors to be considered when multiple broadband solutions are available.

- **Cable**: Bandwidth is shared by many users; upstream data rates are often slow during high-usage hours in areas with over-subscription.
- **DSL**: Limited bandwidth that is distance sensitive (in relation to the ISP's central office); the upstream rate is proportionally quite small compared to the downstream rate.
- **Cellular/mobile**: Coverage is often an issue, even within a SOHO where bandwidth is relatively limited.
- **Wi-Fi mesh**: Most municipalities do not have a mesh network deployed; if it is available and the SOHO is in range, it is a viable option.
- **Satellite Internet**: This option is expensive, has limited capacity per subscriber. Typically used when no other option is available

Tutorial 8: VPN and IPSec Concepts

1. Differentiate two types of Enterprise managed VPN.

Site-to-site VPNs	**Remote Access VPNs**
A site to site VPN is terminated on VPN gateways. VPN traffic is only encrypted between the gateways. Internal host does not have knowledge that a VPN is being used.	A remote access VPN is dynamically created to establish a secure connection between the VPN client and VPN terminating device, usually a VPN gateway
Supports IPsec technology	Supports SSL and IPsec technology

2. What are the benefits of using a VPN?

Cost savings
VPN reduces cost of connectivity while simultaneously increasing the connection bandwidth.

Security
Encryption and authentication protect data from unauthorized access

Scalability
Allow organization to use the internet, making it easy to add new user without adding significant infrastructure

Compatibility
VPN can be implemented across a wide variety of WAN link options including broadband technologies.

3. What is the difference between IPsec and SSL VPNs?

Feature	**IPsec**	**SSL**
Applications supported	**Extensive** – All IP-based applications	**Limited** – Only web-based applications and file sharing
Authentication strength	**Strong** – Two-way authentication with shared keys or digital certificates	**Moderate** – one-way or two-way authentication
Encryption strength	**Strong** – Key lengths 56 – 256 bits	**Moderate to strong** - Key lengths 40 – 256 bits

Connection complexity	**Medium** – Requires VPN client installed on a host	**Low** – Requires web browser on a host

4. What is the term used to describe the encapsulation of GRE over IPsec tunnel?
   Passenger protocol
   This is the original packet that is to be encapsulated by GRE. It could be an IPv4 or IPv6 packet, a routing update, and more.

   Carrier protocol
   GRE is the carrier protocol that encapsulates the original passenger packet.

   Transport protocol
   This is the protocol that will actually be used to forward the packet. This could be IPv4 or IPv6.

5. Which security scheme is provided by IPsec?
   Confidentiality - IPsec uses encryption algorithms to prevent cybercriminals from reading the packet contents.

   Integrity - IPsec uses hashing algorithms to ensure that packets have not been altered between source and destination.

   Origin authentication - IPsec uses the Internet Key Exchange (IKE) protocol to authenticate source and destination. Methods of authentication include using pre-shared keys (passwords), digital certificates, or RSA certificates.

   Diffie-Hellman - Secure key exchange typically using various groups of the DH algorithm.

6. What are the two modes of IPSec?
   Transport mode - the outer header determines the IPsec policy that protects the inner IP packet.

   Tunnel mode - the inner IP packet determines the IPsec policy that protects its contents.

7. “Due to Covid-19 pandemic, many people are working from home during the lockdown including many sectors that were not previously home working. Companies’ management staff and their employees are keeping operations under social distancing restrictions. These mobile workers are using Virtual Private Networks (VPNs) to connect to the companies.” Evaluate the usage of VPNs by mobile workers based on the above statements. (9 marks)

- Remote-access VPNs let remote and mobile users securely connect to the enterprise.
- Remote-access VPNs are typically enabled dynamically by the user when required and can be created using either IPsec or SSL.
- Clientless VPN connection - The connection is secured using a web browser SSL connection.
- Client-based VPN connection - VPN client software such as Cisco Any Connect Secure Mobility Client must be installed on the remote user's end device.

8. Differentiate Clientless Virtual Private Networks (VPN) connection with Client-based VPN connection. - remote access VPNs

   Clientless VPN connection

   The connection is secured using a web browser SSL connection.

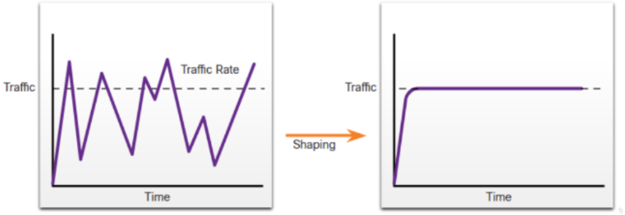
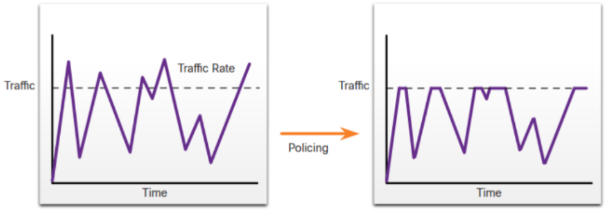
   Client-based VPN connection

   VPN client software such as Cisco Any Connect Secure Mobility Client must be installed on the remote user's end device.

Tutorial 9: Quality of Service Concepts

1. (i) “Without Quality of Service (QoS), network devices will forward all packets during congestion”. Do you agree with this statement? Appraise this statement.
   No, without any QoS mechanisms in place, packets are processed in the order in which they are received. When congestion occurs, network devices such as routers and switches will drop the packets instead of forward them.

   (ii) Two mechanisms provided by Cisco IOS QoS software to prevent congestion are Traffic shaping and traffic policing. Differentiate these mechanisms.

Traffic shaping	Traffic policing
Traffic shaping retains excess packets in a queue and then schedules the excess for later transmission over increments of time. Traffic shaping results in a smoothed packet output rate. Shaping is an outbound concept; packets going out an interface get queued and can be shaped. In contrast, policing is applied to inbound traffic on an interface. 	Policing is applied to inbound traffic on an interface. Policing is commonly implemented by service providers to enforce a contracted customer information rate (CIR). However, the service provider may also allow bursting over the CIR if the service provider’s the network is not currently experiencing congestion. 

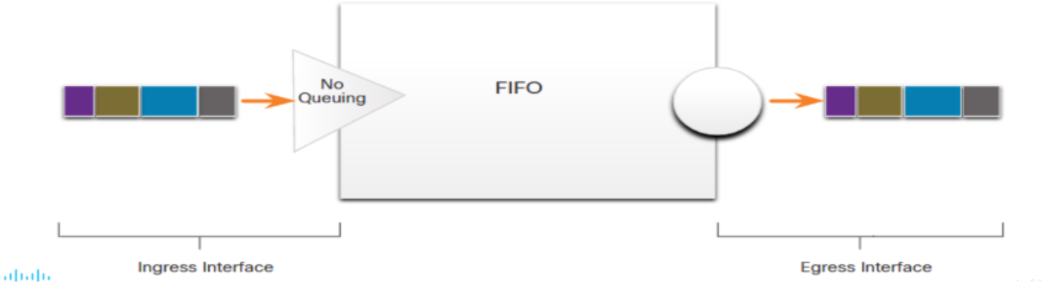
2. "First-In, First-Out (FIFO) algorithm is suitable to be used for a very congested network." Comment on the above statement.
   This statement is wrong because FIFO is equivalent to no QoS implementation. To illustrate, FIFO queues buffers and forwards packets in the order of their arrival. It has no concept of priority or classes of traffic and consequently, makes no decision about packet priority. There is only one queue, and all packets are treated equally. Hence, it is not suitable to be used in a very congested network.

3. Illustrate the queuing algorithm that has only a single queue and treats all packets equally. Use a diagram to aid your explanation

First In First Out (FIFO) queuing buffers and forwards packets in the order of their arrival.

FIFO has no concept of priority or classes of traffic and consequently, makes no decision about packet priority.

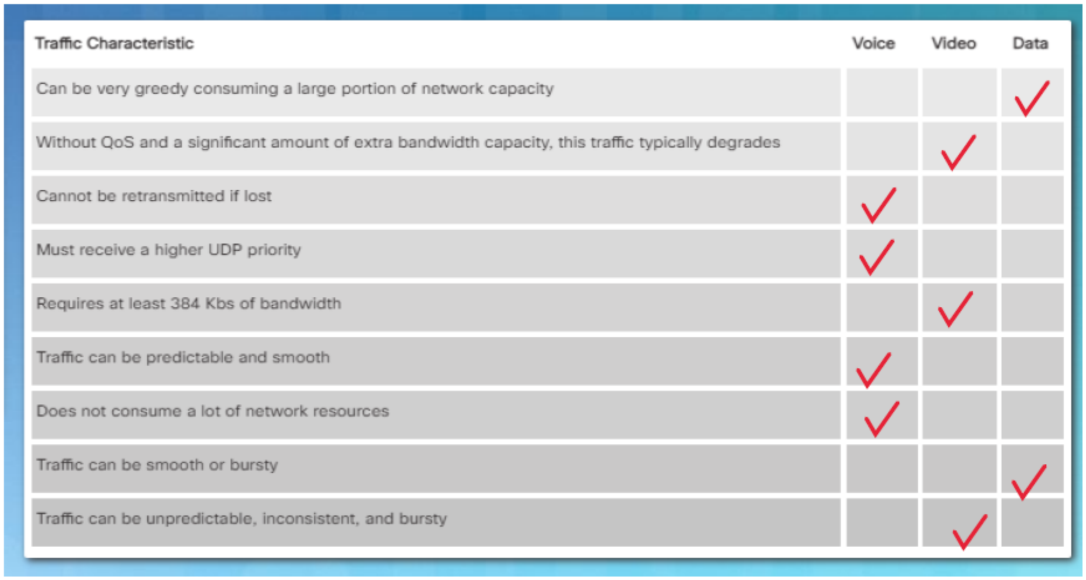
- There is only one queue, and all packets are treated equally.
- Packets are sent out an interface in the order in which they arrive.



4. A network engineer is selecting a QoS method to control congestion on a VPN tunnel link between the headquarters site and a branch office. Which queuing method (algorithms) cannot be used to classify and control VPN traffic? Give your explanation.

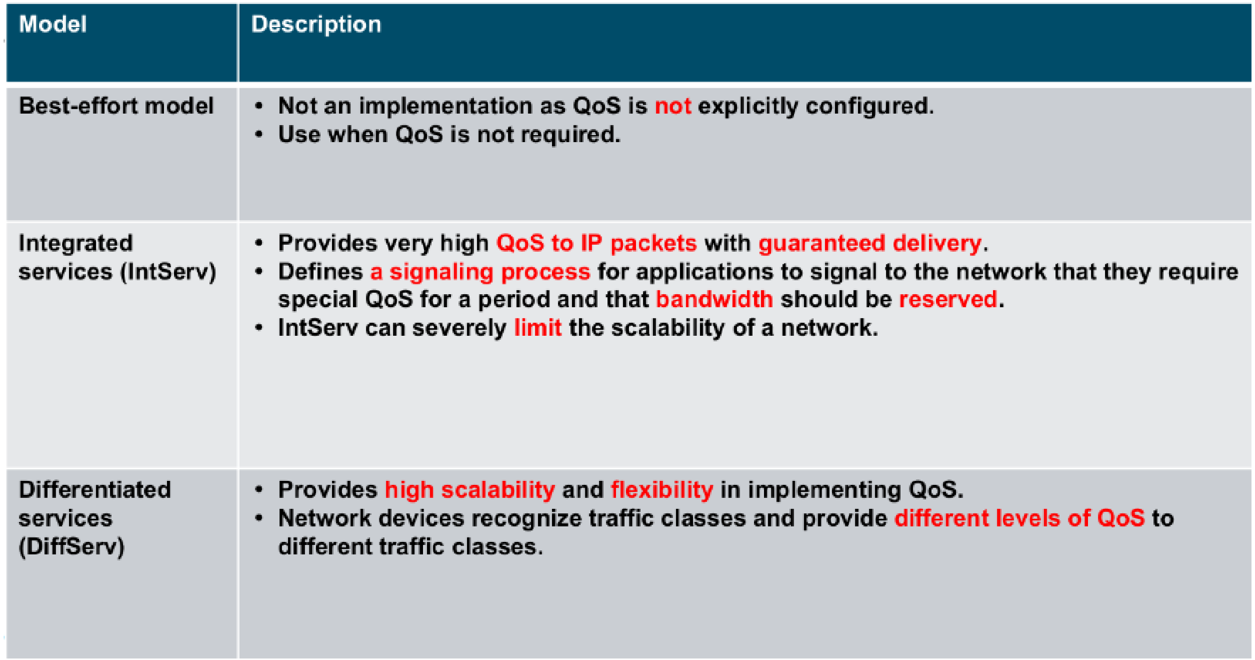
Weighted fair queuing (WFQ) does not support **tunneling and encryption** because these features modify the packet **content information** required by WFQ for classification.

5. Differentiate voice, video, and data traffic. by electing the traffic that has the characteristics listed below:



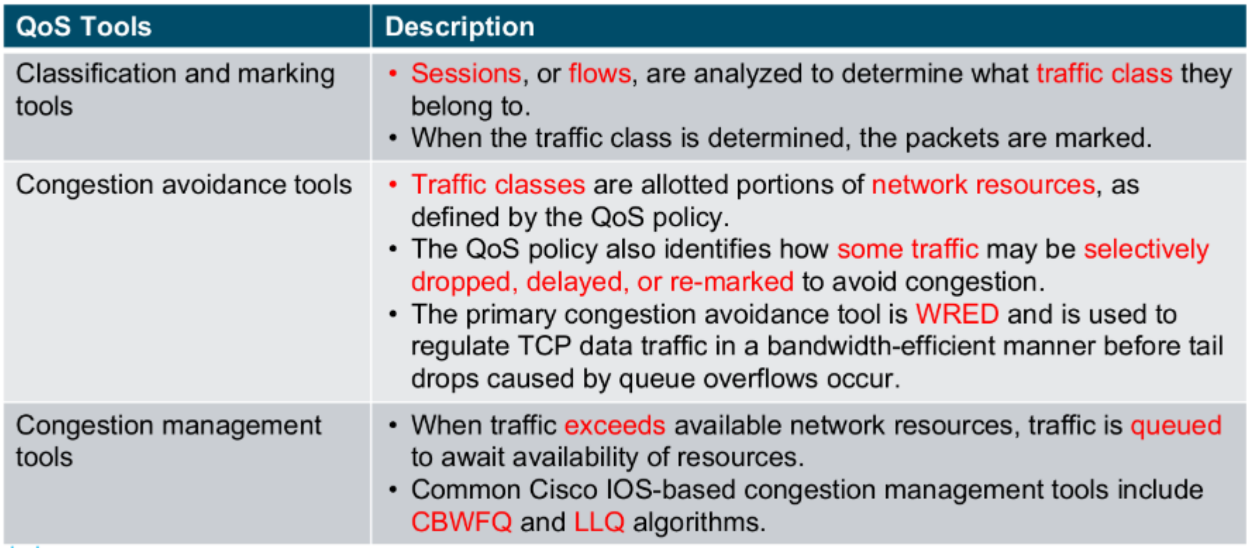
Traffic Characteristic	Voice	Video	Data
Can be very greedy consuming a large portion of network capacity			✓
Without QoS and a significant amount of extra bandwidth capacity, this traffic typically degrades		✓	
Cannot be retransmitted if lost	✓		
Must receive a higher UDP priority	✓		
Requires at least 384 Kbs of bandwidth		✓	
Traffic can be predictable and smooth	✓		
Does not consume a lot of network resources	✓		
Traffic can be smooth or bursty			✓
Traffic can be unpredictable, inconsistent, and bursty		✓	

6. Describe the 3 models for implementing QoS and list the benefits and drawbacks of each method.



Model	Description
Best-effort model	• Not an implementation as QoS is not explicitly configured. • Use when QoS is not required.
Integrated services (IntServ)	• Provides very high QoS to IP packets with guaranteed delivery. • Defines a signaling process for applications to signal to the network that they require special QoS for a period and that bandwidth should be reserved. • IntServ can severely limit the scalability of a network.
Differentiated services (DiffServ)	• Provides high scalability and flexibility in implementing QoS. • Network devices recognize traffic classes and provide different levels of QoS to different traffic classes.

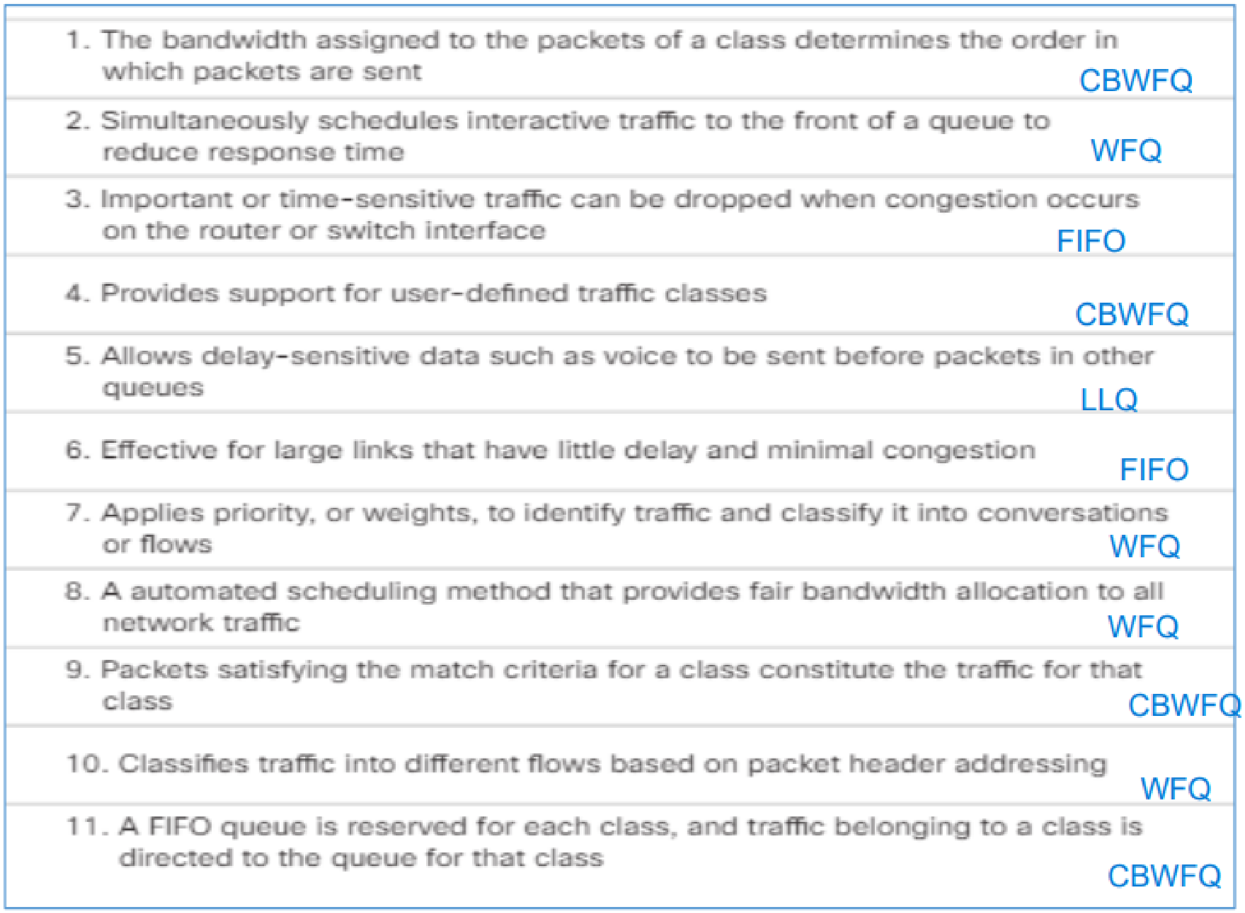
7. List the 3 tools for implementing QoS and write the description



QoS Tools	Description
Classification and marking tools	• Sessions, or flows, are analyzed to determine what traffic class they belong to. • When the traffic class is determined, the packets are marked.
Congestion avoidance tools	• Traffic classes are allotted portions of network resources, as defined by the QoS policy. • The QoS policy also identifies how some traffic may be selectively dropped, delayed, or re-marked to avoid congestion. • The primary congestion avoidance tool is WRED and is used to regulate TCP data traffic in a bandwidth-efficient manner before tail drops caused by queue overflows occur.
Congestion management tools	• When traffic exceeds available network resources, traffic is queued to await availability of resources. • Common Cisco IOS-based congestion management tools include CBWFQ and LLQ algorithms.

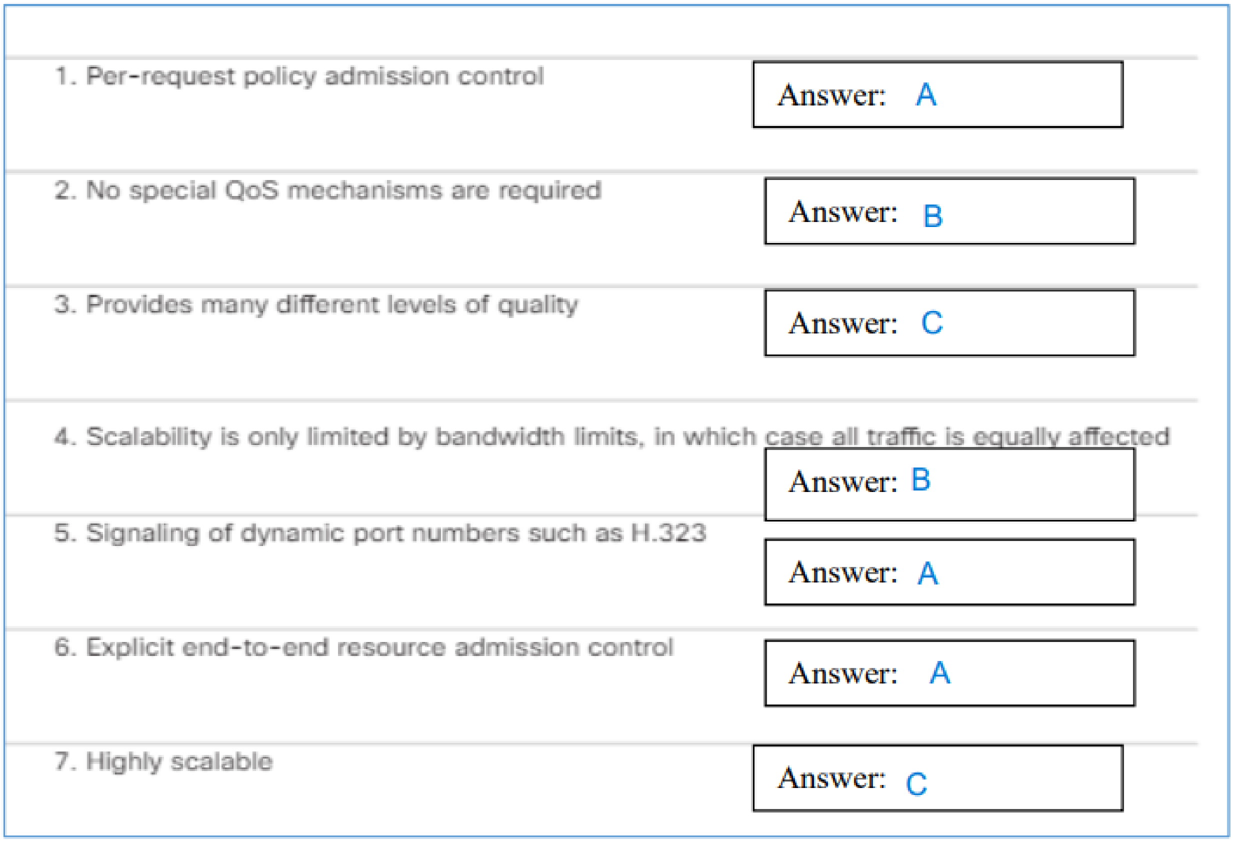
8. Match the below to the following queueing algorithms

CBWFQ	WFQ	FIFO	LLQ



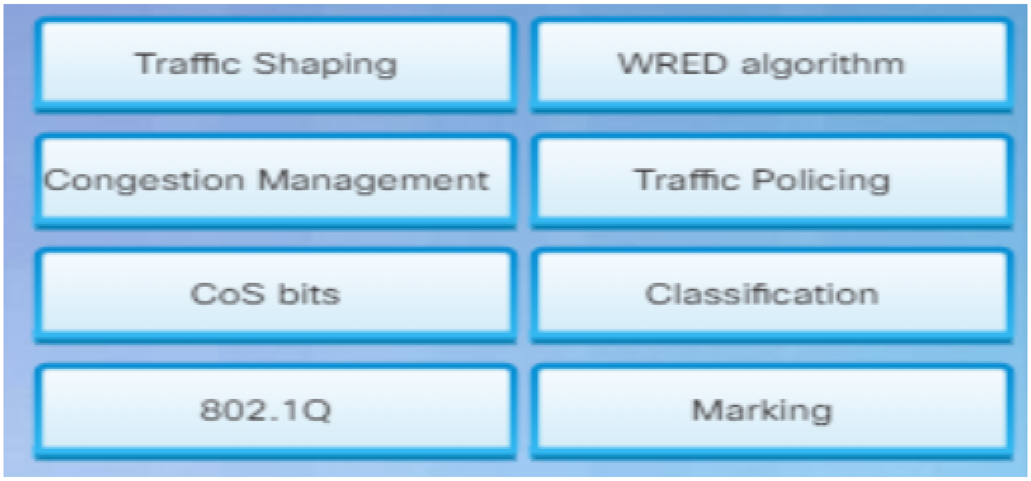
1. The bandwidth assigned to the packets of a class determines the order in which packets are sent CBWFQ
2. Simultaneously schedules interactive traffic to the front of a queue to reduce response time WFQ
3. Important or time-sensitive traffic can be dropped when congestion occurs on the router or switch interface FIFO
4. Provides support for user-defined traffic classes CBWFQ
5. Allows delay-sensitive data such as voice to be sent before packets in other queues LLQ
6. Effective for large links that have little delay and minimal congestion FIFO
7. Applies priority, or weights, to identify traffic and classify it into conversations or flows WFQ
8. A automated scheduling method that provides fair bandwidth allocation to all network traffic WFQ
9. Packets satisfying the match criteria for a class constitute the traffic for that class CBWFQ
10. Classifies traffic into different flows based on packet header addressing WFQ
11. A FIFO queue is reserved for each class, and traffic belonging to a class is directed to the queue for that class CBWFQ

9. Choose the correct model for each benefit.
   A. Integrated Services
   B. Best Effort
   C. Differentiated Services

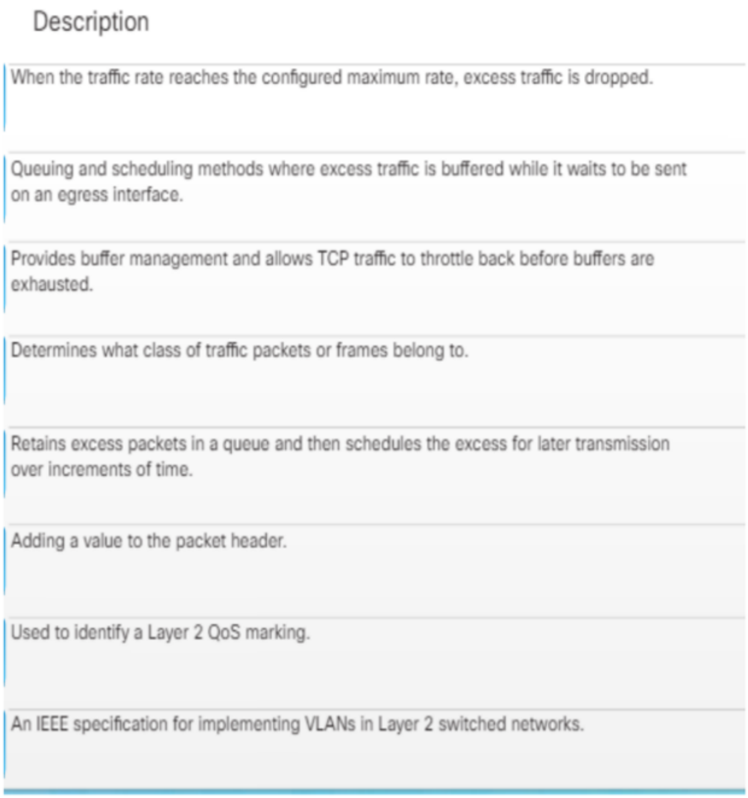


1. Per-request policy admission control	Answer: A
2. No special QoS mechanisms are required	Answer: B
3. Provides many different levels of quality	Answer: C
4. Scalability is only limited by bandwidth limits, in which case all traffic is equally affected	Answer: B
5. Signaling of dynamic port numbers such as H.323	Answer: A
6. Explicit end-to-end resource admission control	Answer: A
7. Highly scalable	Answer: C

10. Match each term to its description.



Traffic Shaping	WRED algorithm
Congestion Management	Traffic Policing
CoS bits	Classification
802.1Q	Marking



Description	
When the traffic rate reaches the configured maximum rate, excess traffic is dropped.	Answer: Traffic policing
Queuing and scheduling methods where excess traffic is buffered while it waits to be sent on an egress interface.	Answer: Congestion Management
Provides buffer management and allows TCP traffic to throttle back before buffers are exhausted.	Answer: WRED algorithm
Determines what class of traffic packets or frames belong to.	Answer: Classification
Retains excess packets in a queue and then schedules the excess for later transmission over increments of time.	Answer: Traffic shaping
Adding a value to the packet header.	Answer: CoS bits
Used to identify a Layer 2 QoS marking.	Answer: Marking
An IEEE specification for implementing VLANs in Layer 2 switched networks.	Answer: 802.1Q