INSTITUTE OF ENGINEERING
PULCHOWK CAMPUS

COMPUTER NETWORKS

A

LAB REPORT

ON

Subnetting and Supernetting

Submitted by:
Aabhusan Aryal

076BCT001

Submitted to:
Department of Electronics and

Computer Engineering

30th June, 2023

Objectives

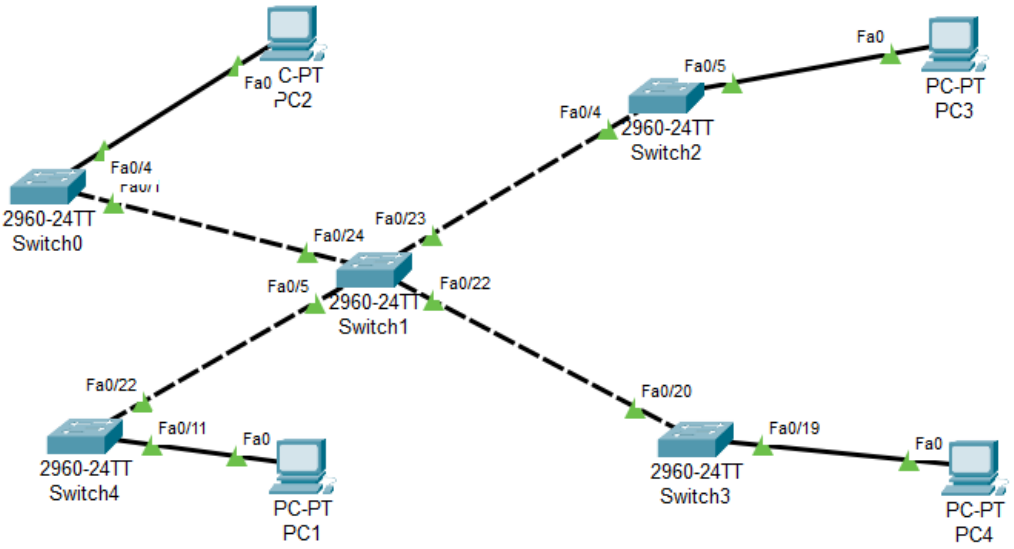
- To be familiar with subnetting with FLSM and VLSM
- To be familiar with supernetting and CIDR

Required Tools

- A computer with Packet Tracer installed

Activities

Activity A



Host	IP address	Subnet Mask	Subnet (Logical AND)
PC1	202.22.22.11	255.255.255.0	202.22.22.0
PC2	202.22.22.21	255.255.255.0	202.22.22.0
PC3	202.22.22.41	255.255.255.0	202.22.22.0
PC4	202.22.22.81	255.255.255.0	202.22.22.0

The IP addresses, subnet masks and the subnet each host belongs to is as mentioned in the table above.

Q2. Test the connectivity from each of the computers to all other computers using ping. Like from PC1 to other three computers, PC2 to other three computers and so on.

=> Since every PC belongs to the same subnet, we can ping any PC from any other PC.

Q3. Change the subnet mask of all computers to 255.255.255.192 and test the connectivity from each of the computers to all other computers using ping.
=>

Host	IP address	Subnet Mask	Subnet
PC1	202.22.22.11	255.255.255.192	202.22.22.0
PC2	202.22.22.21	255.255.255.192	202.22.22.0
PC3	202.22.22.41	255.255.255.192	202.22.22.0
PC4	202.22.22.81	255.255.255.192	202.22.22.64

Can ping PC2 and PC3 from PC1 but can't ping PC4. This is because PC1, PC2 and PC3 belong to the same subnet, while PC4 belongs to a different subnet.

Q4. Change the subnet mask of all computers to 255.255.255.224 and test the connectivity from each of the computers to all other computers using ping.
=>

Host	IP address	Subnet Mask	Subnet
PC1	202.22.22.11	255.255.255.224	202.22.22.0
PC2	202.22.22.21	255.255.255.224	202.22.22.0
PC3	202.22.22.41	255.255.255.224	202.22.22.32
PC4	202.22.22.81	255.255.255.224	202.22.22.64

PC1 and PC2 can ping each other but no other ping is successful.

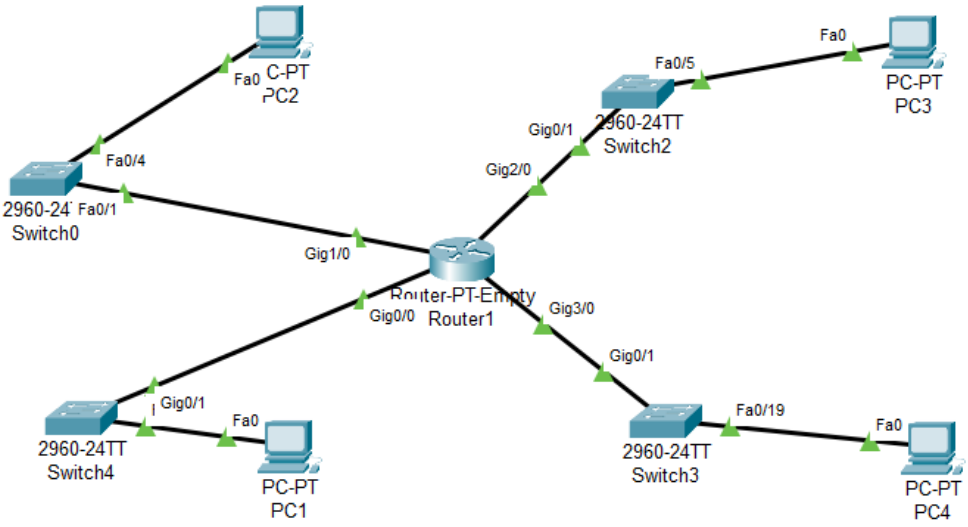
Q5. Change the subnet mask of all computers to 255.255.255.240 and test the connectivity from each of the computers to all other computers using ping.
=>

Host	IP address	Subnet Mask	Subnet
PC1	202.22.22.11	255.255.255.240	202.22.22.0
PC2	202.22.22.21	255.255.255.240	202.22.22.16
PC3	202.22.22.41	255.255.255.240	202.22.22.32

PC4	202.22.22.81	255.255.255.240	202.22.22.64

Since all PCs belong to different subnets, no ping is successful.

Q6 and Q7. Replace the switch with a router and test the connections.




```
C:\>ping 202.22.22.21

Pinging 202.22.22.21 with 32 bytes of data:

Request timed out.
Reply from 202.22.22.21: bytes=32 time<1ms TTL=127
Reply from 202.22.22.21: bytes=32 time<1ms TTL=127
Reply from 202.22.22.21: bytes=32 time<1ms TTL=127

Ping statistics for 202.22.22.21:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 202.22.22.41

Pinging 202.22.22.41 with 32 bytes of data:

Request timed out.
Reply from 202.22.22.41: bytes=32 time<1ms TTL=127
Reply from 202.22.22.41: bytes=32 time<1ms TTL=127
Reply from 202.22.22.41: bytes=32 time<1ms TTL=127

Ping statistics for 202.22.22.41:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

After replacing the switch with a router and configuring it, we observe that every PC can ping any other PC.

Activity B

Q1. Test the connectivity from each of the computers to another using ping.
=>

Host	IP address	Subnet Mask	Subnet
PC1	202.44.8.2	255.255.255.0	202.44.8.0
PC2	202.44.9.2	255.255.255.0	202.44.9.0
PC3	202.44.10.2	255.255.255.0	202.44.10.0
PC4	202.44.12.2	255.255.255.0	202.44.12.0

We observe that none of the pings are successful, and this is because every PC belongs to a different subnet (as in the table above).

Q2. Change the subnet mask of all computers to 255.255.254.0 and test the connectivity from each of the computers to another using ping.
=>

Host	IP address	Subnet Mask	Subnet
PC1	202.44.8.2	255.255.254.0	202.44.8.0
PC2	202.44.9.2	255.255.254.0	202.44.8.0
PC3	202.44.10.2	255.255.254.0	202.44.10.0
PC4	202.44.12.2	255.255.254.0	202.44.12.0

Since PC1 and PC2 belong to the same subnet, they can ping each other. No other ping is successful.

Q3. Change the subnet mask of all computers to 255.255.252.0 and test.
=>

Host	IP address	Subnet Mask	Subnet
PC1	202.44.8.2	255.255.252.0	202.44.8.0
PC2	202.44.9.2	255.255.252.0	202.44.8.0
PC3	202.44.10.2	255.255.252.0	202.44.8.0
PC4	202.44.12.2	255.255.252.0	202.44.12.0

Since PC1, PC2 and PC3 belong to the same subnet, they can ping each other. No other ping is successful.

Q4. Change the subnet mask of all computers to 255.255.248.0 and test the connectivity from each of the computers to another using ping.
=>

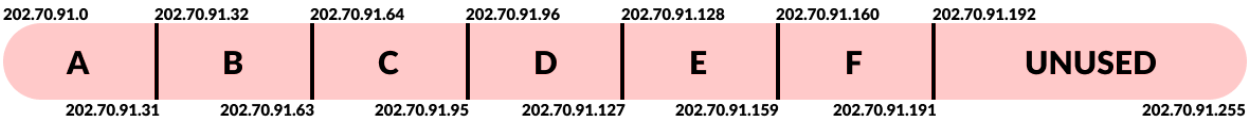
Host	IP address	Subnet Mask	Subnet
PC1	202.44.8.2	255.255.248.0	202.44.8.0
PC2	202.44.9.2	255.255.248.0	202.44.8.0
PC3	202.44.10.2	255.255.248.0	202.44.8.0
PC4	202.44.12.2	255.255.248.0	202.44.8.0

Since all PCs belong to the same subnet, every PC can ping every other PC.

Activity C

Since we need a total of 6 networks, we need at least 3 bits in the host part. Hence, the subnet mask should be 255.255.255.224 (/27). The Network Address, Broadcast Address and Subnet Mask for each network is listed in the table below.

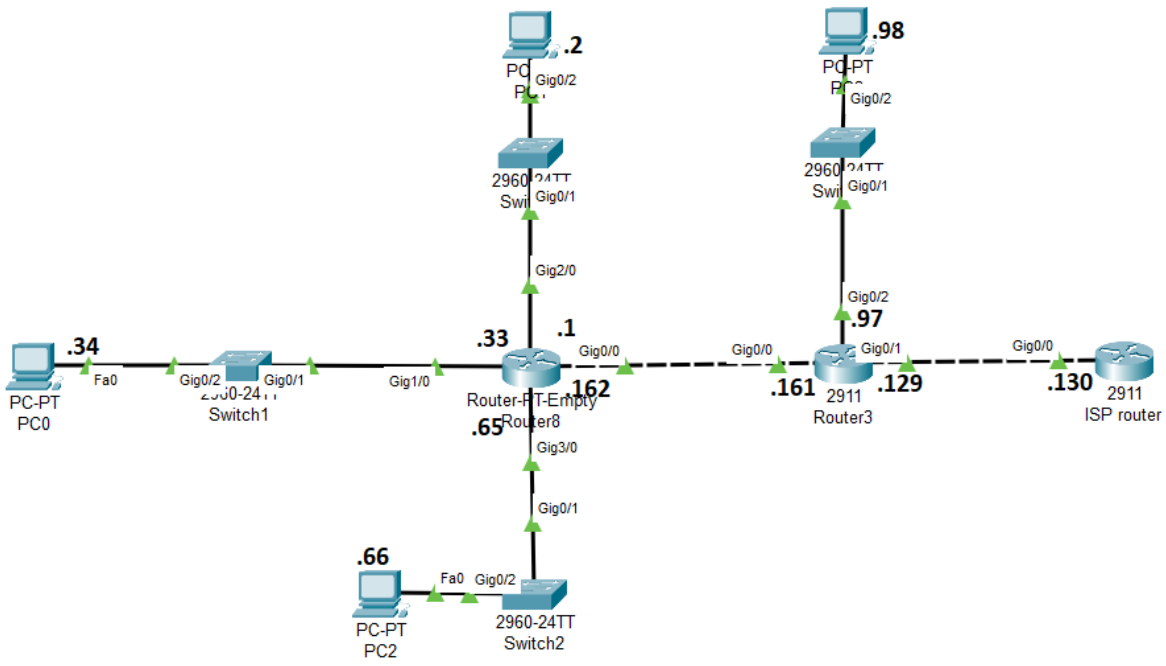
Network	Network Address	Broadcast	Subnet Mask
A	202.70.91.0	202.70.91.31	255.255.255.224
B	202.70.91.32	202.70.91.63	255.255.255.224
C	202.70.91.64	202.70.91.95	255.255.255.224
D	202.70.91.96	202.70.91.127	255.255.255.224
E	202.70.91.128	202.70.91.159	255.255.255.224
F	202.70.91.160	202.70.91.191	255.255.255.224



The IP range used for different networks is as shown in the figure above. We can see that IPs from 202.70.91.192 are unused. It is also worth noting that the networks F and E are only used for point-to-point connection of routers and hence need only 2 IPs. So a network supporting a total of 4 IPs (1 network address, 2 IPs for routers, 1 broadcast IP) should be sufficient. But since we're using FLSM, we have to create a /27 network for it also which means that 28 IPs are being wasted in each of those networks.

Finally, we should also consider the fact that not all department may need all of the available 30 IPs and hence there may be some IPs that are getting wasted.

The network topology with respective IP addresses for each interface is as shown below.



The routing was handled in the manner depicted below:

1. All traffic from Router0 was routed to 202.70.91.161 (Router1)

```
Router(config)#ip route 0.0.0.0 0.0.0.0 202.70.91.161
Router(config)#
```

2. Traffic from Router1 to subnet A, B and C were routed to 202.70.91.162 (Router0) and the default route was set to theISP's router.

```
Router(config)#ip route 202.70.91.0 255.255.255.128 202.70.91.162
Router(config)#ip route 0.0.0.0 0.0.0.0 202.70.91.130
```

3. Traffic from ISP's router to our complete network (202.70.91.0/24) was routed to 202.70.91.129 (Router1).

```
Router(config)#ip route 202.70.91.0 255.255.255.0 202.70.91.129
```

Q1. Test the connectivity from each of the networks to the rest of the given networks using ping.

=>

```
C:\>ping 202.70.91.66

Pinging 202.70.91.66 with 32 bytes of data:

Request timed out.
Reply from 202.70.91.66: bytes=32 time<1ms TTL=127
Reply from 202.70.91.66: bytes=32 time<1ms TTL=127
Reply from 202.70.91.66: bytes=32 time<1ms TTL=127

Ping statistics for 202.70.91.66:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 202.70.91.2

Pinging 202.70.91.2 with 32 bytes of data:

Request timed out.
Reply from 202.70.91.2: bytes=32 time<1ms TTL=127
Reply from 202.70.91.2: bytes=32 time<1ms TTL=127
Reply from 202.70.91.2: bytes=32 time<1ms TTL=127

Ping statistics for 202.70.91.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

All the pings were successful.

Q2. Observe the output of the traceroute from a computer of each of the networks to the rest of the given networks.

=>

```
C:\>tracert 202.70.91.66

Tracing route to 202.70.91.66 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      202.70.91.33
  2    0 ms      0 ms      0 ms      202.70.91.66

Trace complete.

C:\>tracert 202.70.91.98

Tracing route to 202.70.91.98 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      202.70.91.33
  2    0 ms      0 ms      0 ms      202.70.91.161
  3    0 ms      0 ms      0 ms      202.70.91.98

Trace complete.
```

We observed that routing was taking place as expected.

Q3.Observe the output by using traceroute to the destination address of 103.5.150.3.
=>

```
C:\>tracert 103.5.150.3

Tracing route to 103.5.150.3 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      202.70.91.33
  2    0 ms      0 ms      0 ms      202.70.91.161
  3    0 ms      0 ms      0 ms      202.70.91.130
  4    0 ms      *         0 ms      202.70.91.130
  5    *         0 ms      *         Request timed out.
  6    0 ms      *         0 ms      202.70.91.130
  7    *         1 ms      *         Request timed out.
  8    1 ms      *         1 ms      202.70.91.130
  9    *         0 ms      *         Request timed out.
  10    0 ms      *         0 ms      202.70.91.130
  11    *         0 ms      *         Request timed out.
  12    0 ms      *         0 ms      202.70.91.130
  13    *         0 ms      *         Request timed out.
  14    0 ms      *         0 ms      202.70.91.130
  15    *         0 ms      *         Request timed out.
  16    0 ms      *         0 ms      202.70.91.130
  17    *         0 ms      *         Request timed out.
  18    0 ms      *         0 ms      202.70.91.130
  19    *         0 ms      *         Request timed out.
  20    0 ms      *         0 ms      202.70.91.130
  21    *         0 ms      *         Request timed out.
  22    0 ms      *         0 ms      202.70.91.130
  23    *         0 ms      *         Request timed out.
  24    1 ms      *         0 ms      202.70.91.130
  25    *         0 ms      *         Request timed out.
  26    0 ms      *         0 ms      202.70.91.130
  27    *         0 ms      *         Request timed out.
  28    0 ms      *         0 ms      202.70.91.130
  29    *         1 ms      *         Request timed out.
  30    0 ms      *         0 ms      202.70.91.130

Trace complete.
```

Since 103.5.150.3 was not a part of our network (202.70.91.0/24), we see that the request was forwarded to the ISPs router. The request then times out and dies off after 30 hops because we haven’t added any entry to handle this IP or any default route in the ISPs router.

Activity D

The required network address, broadcast address, subnet mask etc. are listed out in the table below. The network topology and IP assignments to each interface is also shown in the image below.

Net	Hosts Required	Bits	Subnet Mask	Network Address	Broadcast	Total Hosts
A	100	7	255.255.255.128	202.51.78.0	202.51.78.127	128
B	40	6	255.255.255.192	202.51.78.128	202.51.78.191	64
C	50	6	255.255.255.192	202.51.78.192	202.51.78.255	64
D	60	6	255.255.255.192	202.51.79.0	202.51.79.63	64
E	12	4	255.255.255.240	202.51.79.64	202.51.79.79	16
F	20	5	255.255.255.224	202.51.79.80	202.51.79.111	32
G	2	2	255.255.255.252	202.51.79.112	202.51.79.115	4
H	2	2	255.255.255.252	202.51.79.116	202.51.79.119	4
I	2	2	255.255.255.252	202.51.79.120	202.51.79.123	4

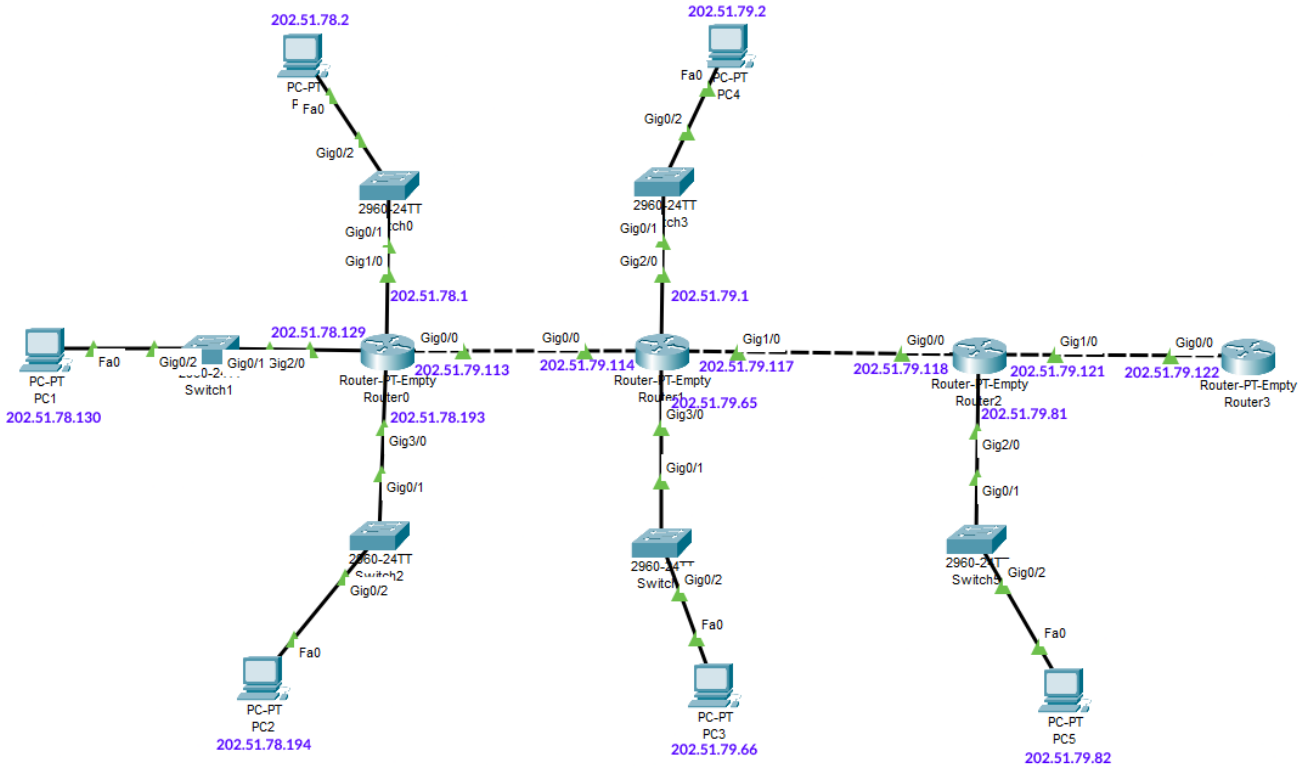
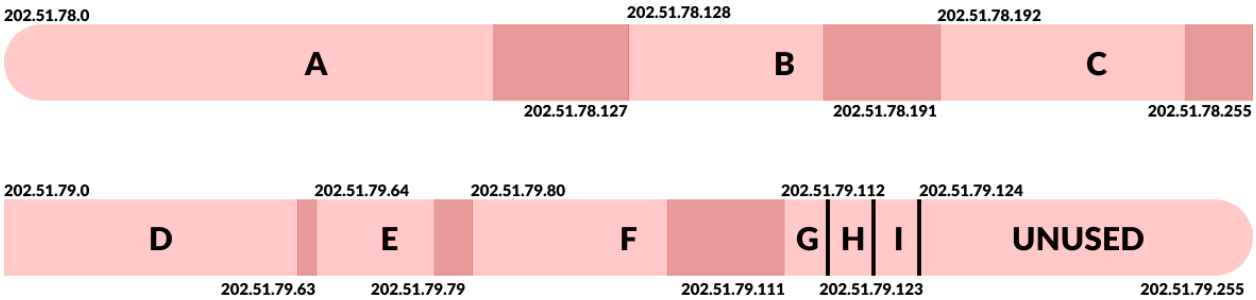


Fig: Network topology and IP assignments



In this case, we can see that different networks have different subnet masks and hence different numbers of usable hosts. In network A, a total of 100 hosts were required so a minimum of 7 bits are needed in this host part, which brings up the number of usable hosts to 128. So we're wasting 26 IP addresses since 2 IPs are reserved for network address and broadcast address. These wasted IPs are depicted in the figure above as a darker shade.

Similar calculations for each network is presented in the table below.

Net	Hosts Required (R)	Total Hosts (T)	Wasted IPs = T-R-2	Wasted IP range (inclusive)
A	100	128	26	202.51.78.101 - 202/51/78.126
B	40	64	22	202.51.78.69 - 202/51/78.190
C	50	64	12	202.51.78.243 - 202/51/78.254
D	60	64	2	202.51.79.61 - 202/51/79.62
E	12	16	2	202.51.79.77 - 202/51/79.68
F	20	32	10	202.51.79.101 - 202/51/79.110
G	2	4	0	-
H	2	4	0	-
I	2	4	0	-

Configurations for routers were made in the same was as in Activity C.

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname aabhusan1
aabhusan1(config)#ip route 202.51.78.0 255.255.255.0 202.51.79.113
aabhusan1(config)#ip route 0.0.0.0 0.0.0.0 202.51.79.118
aabhusan1(config)#
```

Fig: Configuration for Router1

```
ISP(config)#ip route 202.51.78.0 255.255.254.0 202.51.79.121
```

Fig: Configuration for ISP's route

Q1, Q2 and Q3.
=> The outputs were the same as that in Activity C.

Exercise

Q1. What is a subnet mask? Why is it used? Explain with examples.
=> A subnet mask is a number that looks like an IP address and it is used to divide an IP address into network portion and host portion in classless systems. In the classful system, the length of the network portion was predefined to be 8, 16 or 24 depending on the class it belongs to and the class could be determined by looking at the starting few bits.
In case of classless addressing scheme, the length of network potion is not predetermined and hence subnet masks carry this information.

For example, in Activity D we had a network with an address of 202.51.78.0 and the subnet mask of 255.255.255.128. Now, any given address can be checked to see if it belongs to the said network by logically ANDing it with the subnet mask. For eg, if the given address is 202.51.78.9, logically ANDing it with the subnet mask of 255.255.255.128 yields 202.51.78.0 which matches with the network address, and hence belongs to the network.

Q2. Explain subnetting and VLSM with their importance in networking with suitable examples.
=> VLSM stands for Variable Length Subnet Mask. In subnetting with VLSM, a network is divided into variable length subnets. An example of VLSM is the one we did in Activity D whereby we divided the given IP address space into subnets of different lengths for different departments. For eg - the Computer Engineering department may need more IPs as compared to the Mechanical Engineering department.

This is helpful because it helps us reduce the number of unused / wasted IPs which was a problem in the case of FLSM.

Q3. What is classless routing? Why is it used in the Internet system? Explain with suitable examples.
=> Before classless routing came into existence, we had a system of classful routing whereby the whole IPv4 space was divided into 5 classes (A-E). Class A had the least number of bits in the network part (8 bits) and the most number of bits in the host part (24 bits). This means that there could be over 6 million hosts in a single network for class A, but there could be only a total of 126 such networks in the whole world. This means that a few organizations could hold a lot of addresses while other organizations may not get sufficient addresses.

To solve this problem, the concept of classless routing was devised. In classless routing, there is no concept of class (hence the name). Rather, each organization is allocated an IP range based on their requirement. To recognize the network part and the host part, a subnet mask is used. In fact, classful addressing can be thought of as a special case of classless addressing. For ex - Class A addresses are addresses with subnet masks of 255.0.0.0.

Q4. Observe and note down the output of each of the above mentioned tasks and comment on the result by explaining the reason in detail.
=> As done in the activities above.

Conclusion

In this lab, we learnt the concepts of subnetting with both fixed and variable length subnet masks. We learnt how VLSM can be used to reduce the number of unused IPs which was a problem in the case of FLSM.