INSTITUTE OF ENGINEERING
CENTRAL CAMPUS,PULCHOWK

COMPUTER NETWORK

ASSIGNMNENT #3

Computer Network Assignmnent #3

Submitted BY:
AMRIT PRASAD PHUYAL
Roll: PULL074BEX004

Submitted To:
SHARAD KUMAR GHIMIRE
Department of Electronics and
Computer Engineering

December 12, 2020

Table of Contents

List of Tables

List of Figures

1 Question -1

List out typical features of the following networking devices:

Answer:

- **Repeater:**

  Repeater or single booster amplify or regenerate the received signal and transmit it further.

  - Operates at Physical Layer of OSI model.
  - Have only 2 ports , one incoming and one outgoing.
  - Cannot connect dissimilar network.
  - Simple to install and extend and cheaper too.

- **Hub:**

  Hub is a networking device used to connect devices to the network.

  - Operates at Physical Layer of OSI model.
  - A virtual LAN can't be created using a hub
  - It doesn't have IP address.
  - It broadcast the received packets to all ports.
  - Unable to create VLAN.

- **Bridge:**

  Bridge is a networking device that connects multiple LANs to acts as a single unit.

  - Operates at the data link layer of the OSI model
  - More expensive than repeaters
  - Connects two or more LANs that has a same protocol
  - Bridges operate with MAC addresses.

- **Switch:**

  Switch is a active networking device used to connect devices to the network.

  - Operates at the data link layer of the OSI model
  - Have ability to forward data to specific destination device.
  - Able to create VLAN.

- **Router:**

  Router is a networking device capable to connect and communicate between and among different Networks.

  - Operates on the network layer of OSI model.
  - Each port can be configured as per requirement.
  - Intelligent device with filtering and routing the packets to its destination network.

- **Gateway:**

  Gateway is a networking device capable to connect and communicate between and among different Networks operating with different transmission protocols.

  - Generally Operates on the network layer of OSI model but capable to operate on any layer.
  - Operates as a protocol converter, providing compatibility between the different protocols used in the two different networks.

2 Question -2

Why is a logical address necessary for network communication, though there is unique physical address? Explain.

Answer:

Logical address is the IP address and physical address is the MAC address. Manufactures assign the MAC address serially and that can device can be locate din any part of globe . So, if physical addressing is used either a large database is required for storing current location and routes to particular devices. Or the data packet Have travel the world before it reaches the destination.

If logical addressing is used the packet intended for a student of PCampus using Samsung device can receive the without travelling the whole world as the source can forward to NEPAL Telecommunication. then to NTC then to Pulchowk area and then to ICTC and finally to the student device.

3 Question -3

What is private and public IP address? How can a network having private addresses be connected with the global Internet? Explain.

Answer:

Private IP address is used with a local network and public IP address is used outside the network and generally assigned by ISP. Private IP addresses belong to the blocks 100.0.0.0/24, 172.16.0.0/20 and 192.168.0.0/16. All IP besides Private range are Public IP beleonging to Different Classes.

Devices with Private IPs cant connect to internet directly. It is only possible with NAT(Network Address Translation) enabled Router . When Router receives the data from its private IPs it then translate it to Public IP which is assigned by ISP and then forward the Packet to the destination. Similarly the internet and devices on other network dosesn't know the device private IP so it forward to ISP then to Home Router and then to NAT again translate the Public IP to Private and send packet to the requested Host.

4 Question -4

What is subnetting? Why is it important in networking? Explain with suitable examples.

Answer:

Subnetting is the technique to prevent formation of complex large network and instead divide that network and create fast, efficient and secure network and routes. There are two subnetting techniques (VLSM) variable Length Subnet Mask and (FLSM) fixed length. In FLSM all subnet has equal host and uses same subnet mask wasting lot of IP whereas VLSM Subnet has variable host and uses different subnet mask with reduced ip wastage.

Some importance of subnetting are:

- Divides the broadcast domain improving the network performance
- The data intended for host within the same subnet will not leave the subnet thus reducing the congestion and improving security.
- It also helps to organize the complex network into subnets based on departments and location.

In the example below IOE was given 202.70.90.0/24 ranges of IPs.Without subnetting the whole IOE network become complex and unsecure as Student and Department are under same subnet (/24) but after the VLSM subnetting is done as Student has need of 120 host and

Department has need of 50 host only so they are divided into two subnets using subnet mask (/25) and (/26) respectively. There is still unused IP range from 202.70.90.192 - 202.70.90.255 which wil be beneficial for further expansion of departments and future use.

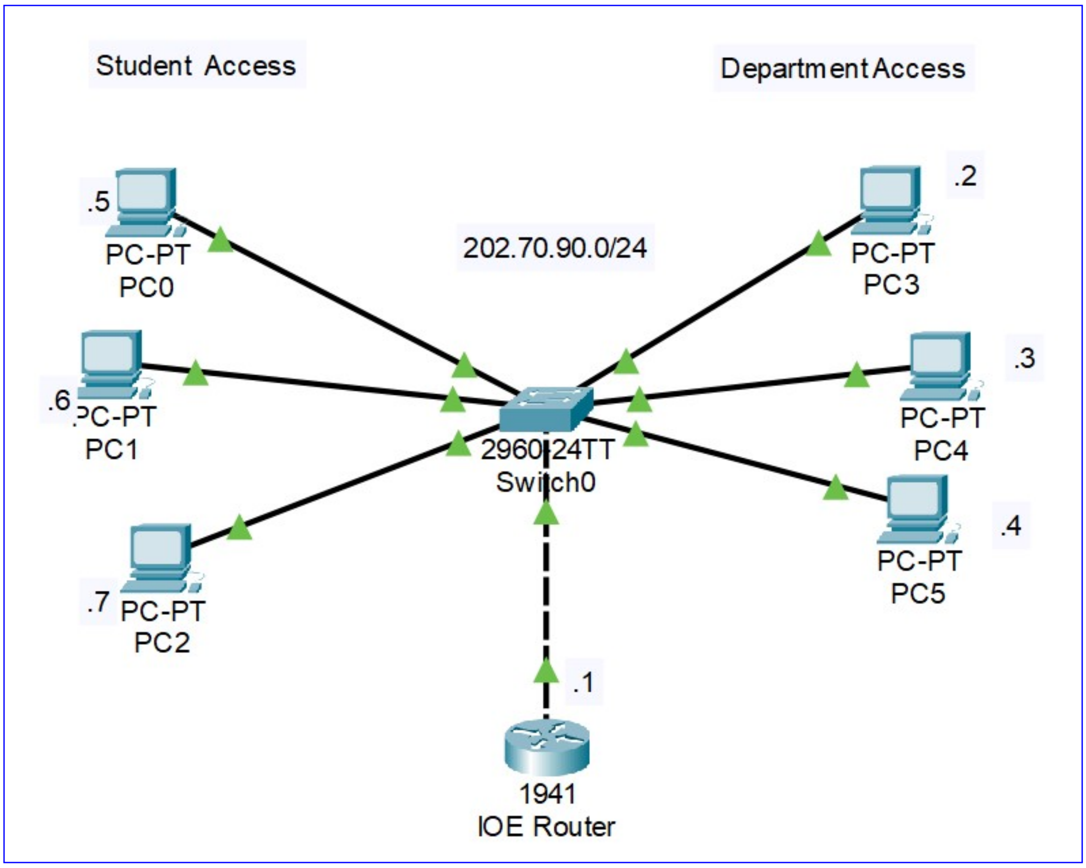
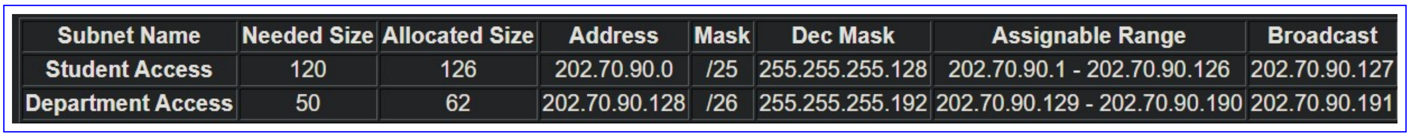


Figure 1: IOE network before subnetting



Subnet Name	Needed Size	Allocated Size	Address	Mask	Dec Mask	Assignable Range	Broadcast
Student Access	120	126	202.70.90.0	/25	255.255.255.128	202.70.90.1 - 202.70.90.126	202.70.90.127
Department Access	50	62	202.70.90.128	/26	255.255.255.192	202.70.90.129 - 202.70.90.190	202.70.90.191

Figure 2: Details of IOE Subnets

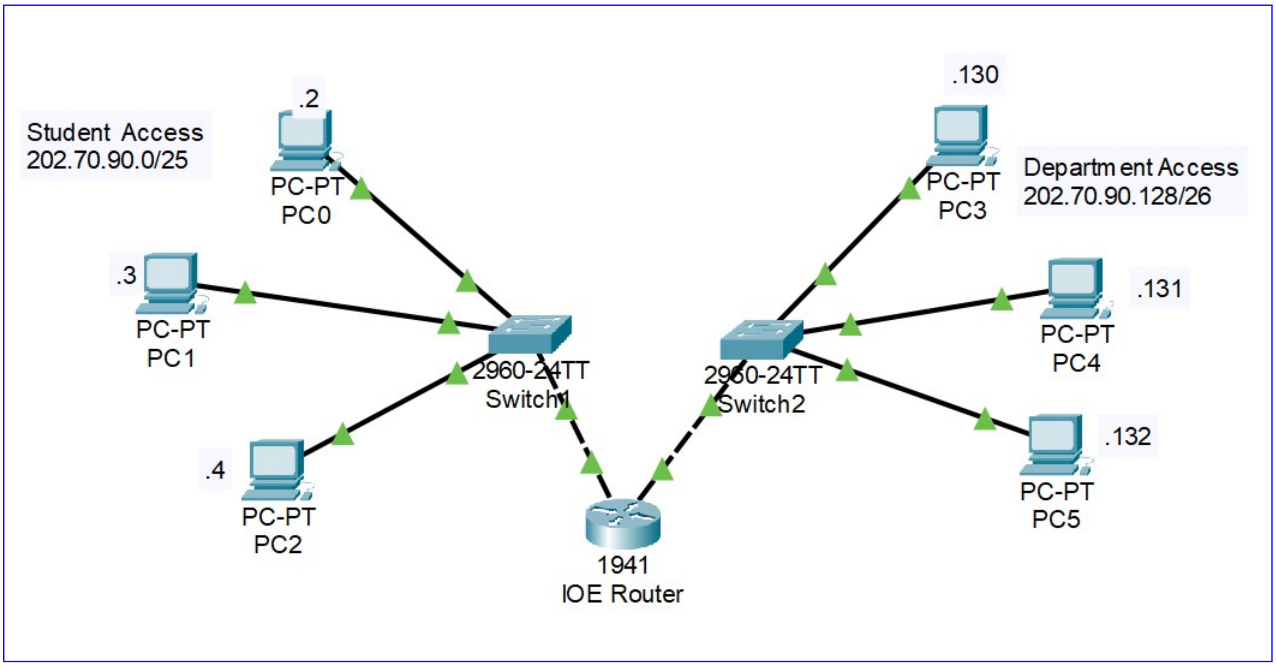


Figure 3: IOE network after subnetting

5 Question -5

Suppose you have given the IP address of 102.5.4.0/23 for your company. There are five different departments having 200, 100, 40, 20 and 12 hosts. Two additional point-to-point links are there for interconnection between routers. Divide the given IP address for above requirements. List out the network address, broadcast address, usable IP address range and subnet mask of each subnet.

Answer:

As we know subnet can be created in Block size of 2^n number of host with (2^n -2) usable host. So we have to choose the subnet equal to or greater than Block size after adding network and broadcast address.

Starting with Department A we need 200 usable host so block size greater or qual to (200+2) is 256 with usable host 254. Here **102.5.4.0 /24** will be network ID , **255.255.255.0** will be subnet mask, **102.5.4.1 - 102.5.4.254** will be available usable host range and **102.5.4.255** will be broadcast ID.

Similarly for all other Department and 2 Interlink the required range is calculated and listed int he table below. There is unused Ip range from **102.5.5.248 - 102.5.255.255**.

Subnet Name	Needed Size	Allocated Size	Network Address	Mask	Dec Mask	Assignable Range	Broadcast
Department A	200	254	102.5.4.0	/24	255.255.255.0	102.5.4.1 - 102.5.4.254	102.5.4.255
Department B	100	126	102.5.5.0	/25	255.255.255.128	102.5.5.1 - 102.5.5.126	102.5.5.127
Department C	40	62	102.5.5.128	/26	255.255.255.192	102.5.5.129 - 102.5.5.190	102.5.5.191
Department D	20	30	102.5.5.192	/27	255.255.255.224	102.5.5.193 - 102.5.5.222	102.5.5.223
Department E	12	14	102.5.5.224	/28	255.255.255.240	102.5.5.225 - 102.5.5.238	102.5.5.239
Interlink 0	2	2	102.5.5.240	/30	255.255.255.252	102.5.5.241 - 102.5.5.242	102.5.5.243
Interlink 1	2	2	102.5.5.244	/30	255.255.255.252	102.5.5.245 - 102.5.5.246	102.5.5.247

Table 1: Network address, broadcast address, usable IP address range and subnet mask

6 Question -6

What is the count to infinity problem in distance vector routing? How can it be addressed? Explain with example.

Answer:

Distance Vector Routing is one of the dynamic routing algorithm in which Router maintain its routing table and informs its neighbors about the distance to other node in the network. This routing technique has Count to infinity problem.

When an interface is down or when two routers send updates at the same time, other routers unknowingly given information that they know how to reach a disconnected node. This false information will propagate to all routers and leading to infinity Loop problem of count to infinity. the following example will further clear the concepts.

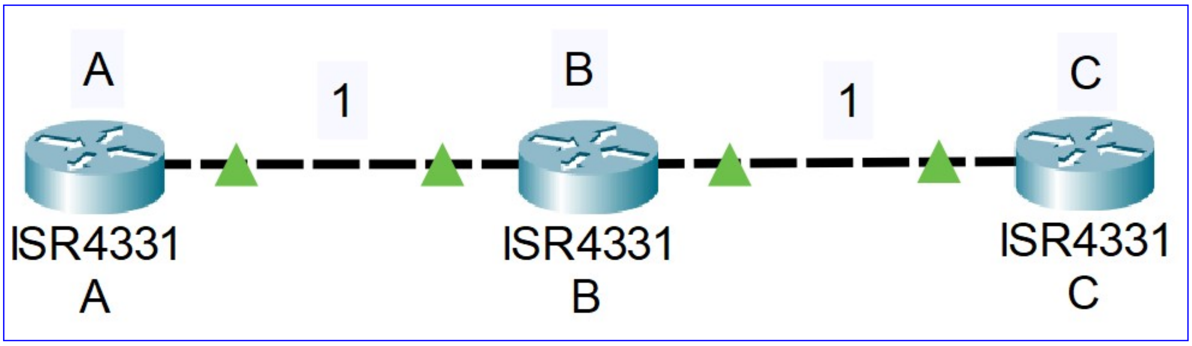


Figure 4: Router A, B and C before breakage

In the above configuration Router B will know that it can reach to C at cost 1 , and A will know it can reach to C via B at the cost of 1.

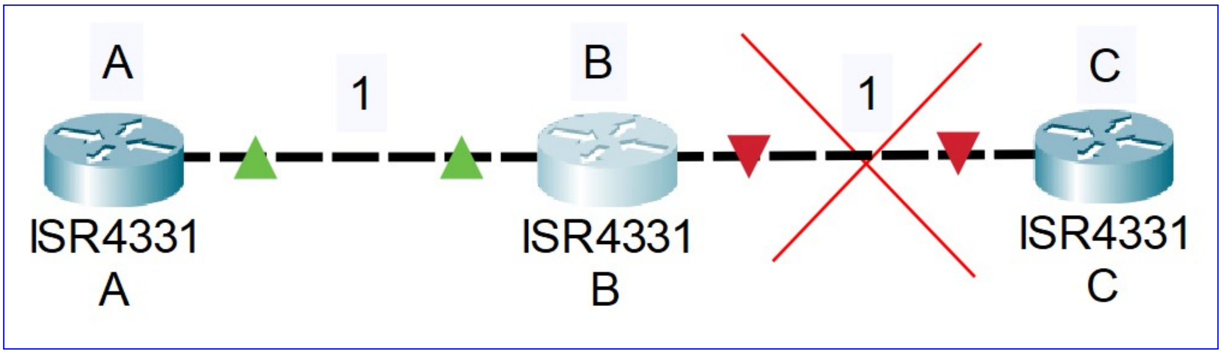


Figure 5: Router A, B and C after breakage

What if the link between B and C disconnected , and B knows that it can no longer reach C and updates its Routing table . There is possibility that Router B receives update from Router A informing that it can reach C at cost of 2 , before B can broadcast its updated Routing table to its neighbors. In that case B will update its Routing table that it can reach C at cost of 3 via A. Similarly router A will update its routing table that it can reach C via B at cost of 4. This process for large no. of times or cost reaches very large number (infinity).

There are several technique to prevent Count to infinity Problem. Two of them are explained below.

- **Route Poisoning:**

  In Route poisoning whenever router detects bad route or router failure then that particular router inform its neighbors that cost to that router is higher than threshold and that router informs its other neighbors and remove that faulty route or router from its table.

  For example when Router C is down it advertise the cost to C vis B is 16 which is above the threshold 15 , so Router A will remove information about router C from its routing Table.

- **Split horizon:**

  Split horizons states that if a neighboring router sends a route to a router , the receiving router will not propagate this route back to the advertising router on the same interface.

  In our example Router B won't inform updated router to Router A and prevent the further confusion and chance to count to infinity problem.

7 Question -7

What is unicast, multicast and broadcast? How does multicast differ from multiple unicast? Why do routers not forward broadcast packets? Explain.

Answer:

Unicast is common form of data transfer in which single sender send packets to a particular recipients. In simple terms it is one to one transmission.

Multicast data transfer involves one sender and multiple recipients. In simple terms it is one to many transmission.

Broadcast data transfer involves one sender and all other host as receiver . it is one to all transmission.

In multicast transmission there is multicast group identified by multicast address. here router duplicate the data packets direct to the destination host. However in multiple unicast sender direct the individual data packets to individual receiver all by itself increasing network traffic and wasting resources.

Forwarding broadcast packets will be waste of resources and increase traffic congestion in the whole network as a single host is capable to populate the whole WAN(Internet) with garbage data.

8 Question -8

Differentiate:

- **Distance vector vs. link state routing**

KEYS	Distance vector	Link state routing
Defination	Each router computes distance between itself and its immediate neighbors.	Each router shares knowledge of its neighbors with every other router in the network.
Algorithm	Bellman ford	Dijsktra
Best Route	Least number of hops	Least cost
Updates frequency	Periodic updates	Triggered updates
Converge Time	Slower	Faster
Problems	Count to infinity	Problems –

Table 2: Distance vector VS Link state routing

- **IGP vs. EGP**

KEYS	IGP	EGP
Full form	Interior Gateway Protocol (IGP)	Exterior Gateway Protocol (EGP)
Working area	Within an Autonomous System.	Between different Autonomous Systems
Colmplexity	Simple	Complex
Available Protocols	RIP, OSPF, ISIS, EIGRP	RIP, OSPF, ISIS, EIGRP

Table 3: IGP VS EGP

- ## SNAT vs. DNAT

KEYS	SNAT	DNAT
Fullform	Source Network Address Translation	Destination Network Address Translation.
Address Change	Changes the source address of packets	Changes the destination address of packets
Order of opreration	After the routing decision is made.	Before the routing decision is made.
Working	Convert the private IP address assigned by the router to the public IP address.	Forward the data coming in a public ip address to a private network.

Table 4: SNAT VS DNAT

- ## ARP vs. RARP

KEYS	ARP	RARP
Fullform	Address Resolution Protocol.	Address Resolution Protocol.
Address fetched	Receiver's MAC address	IP address is fetched.
Mapping	ARP maps 32-bit logical (IP) address to 48-bit physical address.	RARP maps 48-bit physical address to 32-bit logical (IP) address.
Use	Still in use	Replaced by DHCP
Table upadate	Uses ARP reply	RARP reply for configuration of IP addresses .

Table 5: ARP VS RARP

9 Question -9

Discuss briefly on:

Answer:

- ### RIP:

  Routing Information Protocol uses distance vector algorithm to maintain the routing tables.The cost metric is the number of hops to reach the destination. The number of hops available in a network would be the cost. The hop count is the number of networks required to reach the destination.In RIP, infinity is defined as 16, this will prevent count to infinity problem. The maximum number of hops that RIP can contain is 15 hops, i.e., it should not have more than 15 hops as 16 is infinity.Some advantages of RIP are easy to configure, less comlexity and less CPU utilization.

- ### OSPF:

  Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP) used to find the shortest path between source and destination.It uses Dijkstra's shortest path algorithm. After shortest path is found it is broadcasted to all routers.

- ### BGP:

  Border Gateway Protocol (BGP) is one of the types of Protocol of Exterior gateway protocol (EGP) where the routers exchange network reachability information with their nearest neighbors.The neighbors then decide the shortest route to particular destination and update its table and then broadcast to its neighbors.To avoid the count to infinity and looping problems the router sends routing information to another router with its own AS number included so that whenever it can check for routing loops by verifying if its AS number is present or not.

- **ICMP:**

  Internet Control Message Protocol(ICMP) is used to transmit error messages.For example, if a packet of data is too large for a router, the router will drop the packet and send an ICMP message back to the original source for the data. Ping and Trace route are commonly used ICMP protocols.