Syllabus

TE | Comp | Sem - V

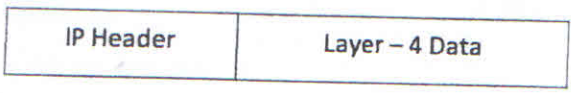
Data Communicam & Network

Q. 1 a) What is IPV4 protocol? Explain the Header format of IPV4. (2,4)

Solution:

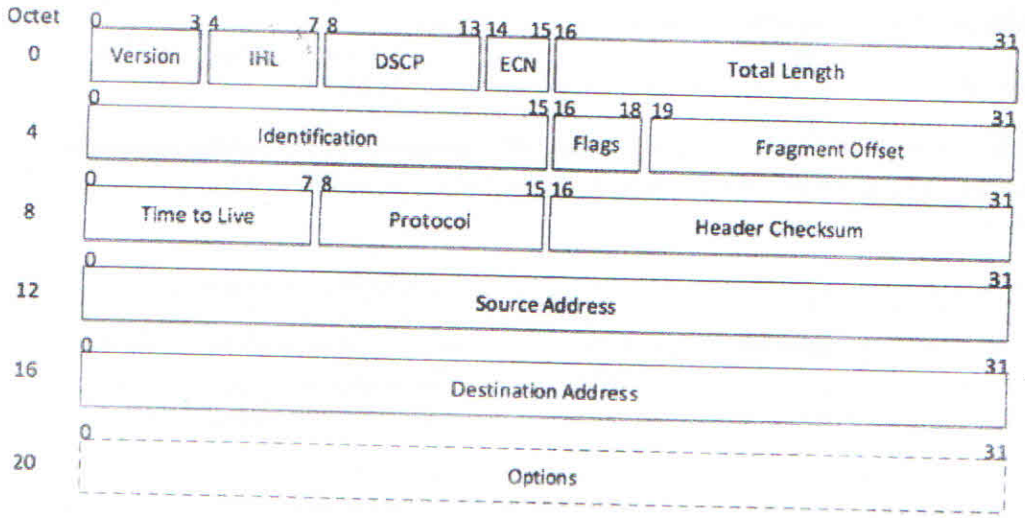
Internet Protocol version 4 (IPv4) is the fourth version in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. It provides the logical connection between network devices by providing identification for each device. There are many ways to configure IPv4 with all kinds of devices – including manual and automatic configurations – depending on the network type.

Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information.



(IP Encapsulation)

The encapsulated data is referred to as IP Payload. IP header contains all the necessary information to deliver the packet at the other end.



[Image: IP Header]

IP header includes many relevant information including Version Number, which, in this context, is 4. Other details are as follows:

- **Version:** Version no. of Internet Protocol used (e.g. IPv4).
- **IHL:** Internet Header Length; Length of entire IP header.
- **DSCP:** Differentiated Services Code Point; this is Type of Service.
- **ECN:** Explicit Congestion Notification; It carries information about the congestion seen in the route.
- **Total Length:** Length of entire IP Packet (including IP header and IP Payload).

- **Identification:** If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.
- **Flags:** As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.
- **Fragment Offset:** This offset tells the exact position of the fragment in the original IP Packet.
- **Time to Live:** To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
- **Protocol:** Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- **Header Checksum:** This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- **Source Address:** 32-bit address of the Sender (or source) of the packet.
- **Destination Address:** 32-bit address of the Receiver (or destination) of the packet.
- **Options:** This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

Q. 1 b) Explain need of layer design for communication and networking. (1 introduction and each point 1, 1x5)

Solution:

The basic reason for using a layered networking approach is that a layered model takes a task, such as data communications, and breaks it into a series of tasks, activities, or components, each of which is defined and developed independently.

The Reasons for a Layered Model:

Change: When changes are made to one layer, the impact on the other layers is minimized. If the model consists of a single, all-encompassing layer, any change affects the entire model.

Design: A layered model defines each layer separately. As long as the interconnections between layers remain constant, protocol designers can specialize in one area (layer) without worrying about how any new implementations affect other layers.

Learning: The layered approach reduces a very complex set of topics, activities, and actions into several smaller, interrelated groupings. This makes learning and understanding the actions of each layer and the model generally much easier.

Troubleshooting: The protocols, actions, and data contained in each layer of the model relate only to the purpose of

that layer. This enables troubleshooting efforts to be pinpointed on the layer that carries out the suspected cause of the problem.

Standards: Probably the most important reason for using a layered model is that it establishes a prescribed guideline for interoperability between the various vendors developing products that perform different data communications tasks. Remember, though, that layered models, including the OSI model, provide only a guideline and framework, not a rigid standard that manufacturers can use when creating their products.

Q. 1 b) Compare OSI reference model with TCP/IP. (Each valid point 1 mark)

Solution:

OSI(Open System Interconnection)	**TCP/IP(Transmission Control Protocol / Internet Protocol)**
1. OSI provides layer functioning and also defines functions of all the layers.	1. TCP/IP model is more based on protocols and protocols are not flexible with other layers.
2. In OSI model the transport layer guarantees the delivery of packets	2. In TCP/IP model the transport layer does not guarantees delivery of packets.
3. Follows horizontal approach	3. Follows vertical approach.
4. OSI model has a separate presentation layer	4. TCP/IP does not have a separate presentation layer
5. OSI is a general model.	5. TCP/IP model cannot be used in any other application.
6. Network layer of OSI model provide both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.

7. OSI model has a problem of fitting the protocols in the model	7. TCP/IP model does not fit any protocol
8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them.	9. In TCP/IP it is not clearly separated its services, interfaces and protocols.
10. It has 7 layers	10. It has 4 layers

Q.2 a) Discuss various propagation modes in fiber optics cable? Explain the limitations of fiber optics cable. (each 2 mode for 2 marks and limitations 2 marks)

Solution:

Propagation Modes

Fiber-optic cable has two propagation modes: multimode and single mode. They perform differently with respect to both attenuation and time dispersion. The single-mode fiber-optic cable provides much better performance with lower attenuation

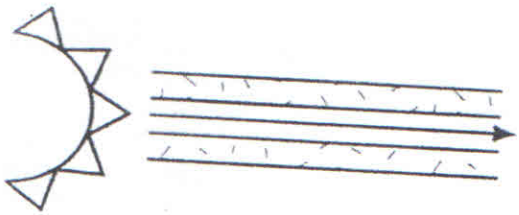
Single Mode cable is a single stand (most applications use 2 fibers) of glass fiber with a diameter of 8.3 to 10 microns that has one mode of transmission. Single Mode Fiber with a relatively narrow diameter, through which only one mode will propagate typically 1310 or 1550nm. Carries higher bandwidth than multimode fiber, but requires a light source with a narrow spectral width. Synonyms mono-mode optical fiber, single-mode fiber, single-mode optical waveguide, uni-mode fiber.

Single Modem fiber is used in many applications where data is sent at multi-frequency (WDM Wave-Division-Multiplexing) so only one cable is needed - (single-mode on one single fiber)

Single-mode fiber gives you a higher transmission rate and up to 50 times more distance than multimode, but it also costs more. Single-mode fiber has a much smaller core than multimode. The small core and single light-wave virtually eliminate any distortion that could result from overlapping light pulses, providing the least signal attenuation and the highest transmission speeds of any fiber cable type.

Single-mode optical fiber is an optical fiber in which only the lowest order bound mode can propagate at the wavelength of interest typically 1300 to 1320nm.

"Single mode fiber"
single path through the fiber

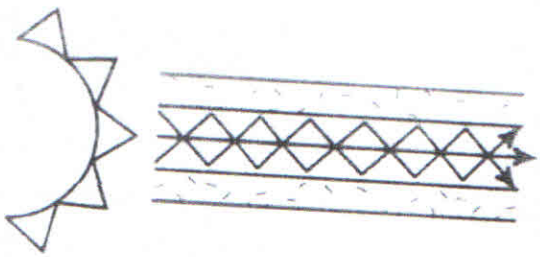


jump to single mode fiber page

Multi-Mode cable has a little bit bigger diameter, with a common diameters in the 50-to-100 micron range for the light carry component (in the US the most common size is 62.5um). Most applications in which Multi-mode fiber is used, 2 fibers are used (WDM is not normally used on multi-mode fiber). POF is a newer plastic-based cable which promises performance similar to glass cable on very short runs, but at a lower cost.

Multimode fiber gives you high bandwidth at high speeds (10 to 100MBS - Gigabit to 275m to 2km) over medium distances. Light waves are dispersed into numerous paths, or modes, as they travel through the cable's core typically 850 or 1300nm. Typical multimode fiber core diameters are 50, 62.5, and 100 micrometers. However, in long cable runs (greater than 3000 feet [914.4 meters), multiple paths of light can cause signal distortion at the receiving end, resulting in an unclear and incomplete data transmission so designers now call for single mode fiber in new applications using Gigabit and beyond.

"Multimode fiber"
multiple paths through the fiber



Disadvantages/ Limitations of Optical Fiber Cable Networks:

- Optical Fiber cables have limited bend radius (about 30 mm). So, if they are bent more, it might lead to some signal loss. But recently, bend resistant fibers have been introduced which have higher tolerance to bending.
- Unlike Copper UTP cables which have standard Rj-45 Jacks and connectors (mostly), optical fiber cables have many types of connectors and this lack of standardization adds confusion.
- By bending the normal optical fiber cables, some leakage of signal could be induced and that can be used for hacking the information in them. So, even though doing that might be difficult, they are not totally tamper proof

- Single mode cables and their associated optics (active components) are very expensive. Even though multi-mode cables/ optics are less expensive, they are not even close to the costs of copper UTP cables/ ports. Moreover, multi-mode cables have restrictions in distance for supporting higher bandwidth (like 1 Gbps and 10 Gbps).
- There are outdoor fiber cables but they need to be shielded well. This shielding makes them less agile/ flexible to run in all the places and it increases the cost of cables as well.

Q. 2 b) a) If bandwidth of channel is 8 kbps. How long does it take to send a frame 200000 bits out of any device? (3)

Solution: Here bandwidth = 8 kbps.

Frame = 200000 bits

Therefore, 200000 bits / 8 kbps = 25 s.

Q. 2 b) b) What is signal to noise ratio? How to calculate bit rate in noise less channel? (1.2)

In analog and digital communications, signal-to-noise ratio, often written S/N or SNR, is a measure of signal strength relative to background noise. The ratio is usually measured in decibels (dB) using a signal-to-noise ratio formula. If the incoming signal strength in microvolts is V_s, and the noise level, also in microvolts, is V_n, then the signal-to-noise ratio, S/N, in decibels is given by the formula: $S/N = 20 \log_{10}(V_s/V_n)$

Two theoretical formulas were developed to calculate the data rate : one by Nyquist for a noiseless channel, another by Shannon for a noisy channel.

1. **Noiseless Channel : Nyquist Bit Rate –**
   For a noiseless channel, the Nyquist bit rate formula defines the theoretical maximum bit rate

   BitRate = 2 * Bandwidth * log2(L)

   In the above equation, bandwidth is the bandwidth of the channel, L is the number of signal levels used to represent data, and BitRate is the bit rate in bits per second. Bandwidth is a fixed quantity, so it cannot be changed. Hence, the data rate is directly proportional to the number of signal levels.

Q. 3 a) Explain PPP protocol along with its frame format. (2.4)

Solution: **PPP:**

1. PPP stands for Point-To-Point Protocol.
2. It is Data Link Protocol.
3. This protocol is widely used to connect home computers to the server of an Internet Service Provider.
4. PPP is used to control and manage the data transfer.
5. PPP provides Error Detection.
6. It defines how two devices can authenticate each other.
7. It defines link control protocol (LCP) for:

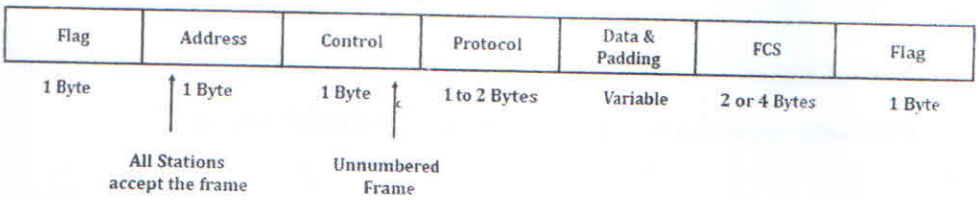
   a. Establishing the link between two devices.

   b. Maintaining this established link.

c. Configuring this link.

d. Terminating this link after the transfer.

PPP Frame Format:



The frame format of PPP resembles HDLC frame. Its various fields are:

I) Flag field:

a. PPP Frame always begin & end with the standard HDLC Flag.

b. Flag byte is 01111110. (1 byte).

II) Address field:

a. This field is of 1 byte and is always 11111111.

b. This address is the broadcast address.

c. All 1's in the address field indicates that all stations are to accept the frame.

III) Control field:

a. This field is also of 1 byte.

b. This field uses the format of the U-frame (unnumbered) in HDLC.

c. The value is always 00000011 to show that the frame does not contain any sequence numbers.

d. There is no flow control or error control.

IV) Protocol field:

a. This field specifies the kind of packet in the data field i.e. what is being carried in data field. b. The data field can contain the user data or other information.

V) Data field:

a. Its length is variable.

b. If the length is not negotiated using LCP during line set up, a default length of 1500 bytes is used.

c. It carries user data or other information.

VI) FCS field:

a. FCS stands for Frame Check Sequence.

b. It is either of 2 bytes or 4 bytes.

c. It contains the checksum.

Q. 3 b) Explain how the value of 'n' is decided in n bit sliding window protocol. Explain advantage of selective repeat over go back n protocol. (2,4)

Solution: **Comparison Chart**

BASIS FOR COMPARISON	GO-BACK-N	SELECTIVE REPEAT
Basic	Retransmits all the frames that sent after the frame which suspects to be damaged or lost.	Retransmits only those frames that are suspected to lost or damaged.
Bandwidth Utilization	If error rate is high, it wastes a lot of bandwidth.	Comparatively less bandwidth is wasted in retransmitting.
Complexity	Less complicated.	More complex as it require to apply extra logic and sorting and storage, at sender and receiver.
Window size	N-1	<= (N+1)/2
Sorting	Sorting is neither required at sender side nor at receiver side.	Receiver must be able to sort as it has to maintain the sequence of the frames.
Storing	Receiver do not store the frames received after the damaged frame until the damaged frame is retransmitted.	Receiver stores the frames received after the damaged frame in the buffer until the damaged frame is replaced.
Searching	No searching of frame is required neither on sender side nor on receiver	The sender must be able to search and select only the requested frame.

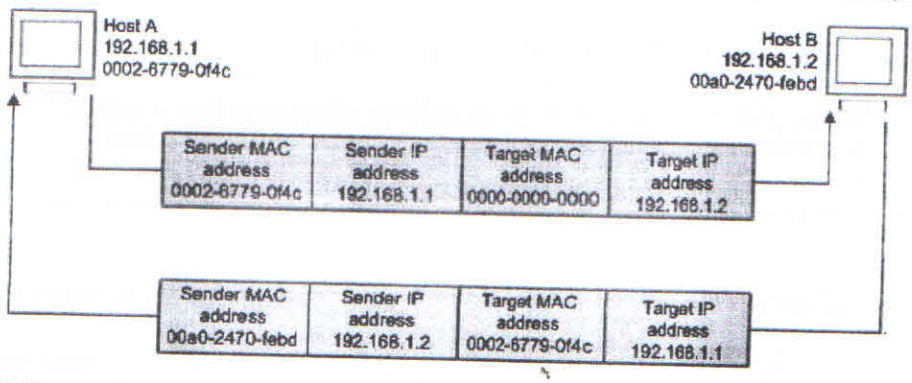
BASIS FOR COMPARISON	GO-BACK-N	SELECTIVE REPEAT
ACK Numbers	NAK number refer to the next expected frame number.	NAK number refer to the frame lost.
Use	It more often used.	It is less in practice because of its complexity.

Q. 4 a) Discuss the protocol in details for the following.

a) Conversion of logical address to physical address (3)

1. Address Resolution Protocol (ARP) –

Address Resolution Protocol is a communication protocol used for discovering physical address associated with given network address. Typically, ARP is a network layer to data link layer mapping process, which is used to discover MAC address for given Internet Protocol Address.
In order to send the data to destination, having IP address is necessary but not sufficient; we also need the physical address of the destination machine. ARP is used to get the physical address (MAC address) of destination machine.



Before sending the IP packet, the MAC address of destination must be known. If not so, then sender broadcasts the ARP-discovery packet requesting the MAC address of intended destination. Since ARP-discovery is broadcast, every host inside that network will get this message but the packet will be discarded by everyone except that intended receiver host whose IP is associated. Now, this receiver will send a unicast packet with its MAC address (ARP-reply) to the sender of ARP-discovery packet. After the original sender receives the ARP-reply, it updates ARP-cache and start sending unicast message to the destination.

b) Conversion of physical address to logical address (3)

2. Reverse Address Resolution Protocol (RARP) –

Reverse ARP is a networking protocol used by a client machine in a local area network to request its Internet Protocol address (IPv4) from the gateway-router's ARP table. The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address. When a new machine is setup or any machine which don't have memory to store IP address, needs an IP address for its own use. So the machine sends a RARP broadcast packet which contains its own MAC address in both sender and receiver hardware address field.

A special host configured inside the local area network, called as RARP-server is responsible to reply for these kind of broadcast packets. Now the RARP server attempt to find out the entry in IP to MAC address mapping table. If any entry matches in table, RARP server send the response packet to the requesting device along with IP address.

- LAN technologies like Ethernet, Ethernet II, Token Ring and Fiber Distributed Data Interface (FDDI) support the Address Resolution Protocol.
- RARP is not being used in today's networks. Because we have much great featured protocols like BOOTP (Bootstrap Protocol) and DHCP(Dynamic Host Configuration Protocol).

Q. 4 b) Explain in details with example, concepts of subnetting and supernetting. (3,3)

Solution:

What is Subnetting?

The process of dividing the single network into the multiple subnets is called as subnetting.

Suppose there an organization which has class A or class B block of the addresses assigned. An organization can divide these addresses into multiple contiguous groups. This individual group of addresses is called as a subnet.

You can read the detail of **different IP address classes and its range**. It will help you to understand this topic very well.

Advantages of Subnetting over Supernetting:

There are many advantages of using subnetting.

- It is difficult to maintain and administrate a big network with lots of systems connected. Dividing all these systems in multiple networks make easy to maintain and administrate for the network administrator.
- Restructuring of the networks become simple.
- As of dividing the network into multiple subnets, every subnet works independently. This improves the overall security of the network.

- In a case of any system failure, we don't need to troubleshoot complete network, rather subnet.

Disadvantages of Subnetting:

- If you are sending a data packet to any of the systems in the subnet, a packet has to be delivered to the particular network, then to subnet and then system. Evey node (network, subnet, system) performs filtering operation on the data packet. The operation for subnet filtering gives extra overhead.
- It complicates the communication process.
- To identify each subnet in a network, we need to assign an id for each subnet. Some extra bits are borrowed from IP address for the subnet id. So we loose some IP addresses.

What is Supernetting?

The process of aggregating two or more networks for which it generates single IP address is called as supernetting.

It is considered as the reverse process of subnetting.

Why is suppernetting required?

Let's take an example.

Class C block provides 256 host addresses.

Class B block provides 65536 host IP addresses.

If any of the organization wants 500 IP addresses,

class B block will not be sufficient.

Having 65536 addresses in class C block

is a waste of IP addresses.

To tackle with this, an organization can apply for

two contiguous class C block of IP addresses and combine both of them.

The combined network is called as supernet and the process of aggregation is called as supernetting.

Limitation of supernetting over subnetting:

- All the network in supernet must be using same IP address class.
- As it is an aggregating process, it does not make sense to apply on the single network.

Q. 4 b) Explain the limitations of IPV4 and how it is overcome by IPV6 protocol. (each valid point 1 mark)

Solution:

Why IPv6?	IPv4	IPv6
IPv6 has more addresses	4.3 billion addresses	340 trillion trillion trillion addresses
IPv6 networks are easier and cheaper to manage	Networks must be configured manually or with DHCP. IPv4 has had many overlays to handle Internet growth, which demand increasing maintenance efforts.	IPv6 networks provide autoconfiguration capabilities. They are simpler, flatter and more manageable for large installations.
IPv6 restores end-to-end transparency	Widespread use of NAT devices means that a single NAT address can mask thousands of non-routable addresses, making end-to-end integrity unachievable.	Direct addressing is possible due to vast address space – the need for network address translation devices is effectively eliminated.
IPv6 has improved security features	Security is dependent on applications – IPv4 was not designed with security in mind.	IPSEC is built into the IPv6 protocol, usable with a suitable key infrastructure.
IPv6 has improved mobility capabilities	Relatively constrained network topologies restrict mobility and interoperability capabilities in the IPv4 Internet.	IPv6 provides interoperability and mobility capabilities which are already widely embedded in network devices.
IPv6 encourages innovation	IPv4 was designed as a transport and communications medium, and increasingly any work on IPv4 is to find ways around the constraints.	Given the numbers of addresses, scalability and flexibility of IPv6, its potential for triggering innovation and assisting collaboration is unbounded.

Q. 5 a) What do you mean by classless address and why it is required? (1.2)

Solution: **Network Address and Mask**
Network address – It identifies a network on internet. Using this, we can find range of addresses in the network and total possible number of hosts in the network.

Mask – It is a 32-bit binary number that gives the network address in the address block when AND operation is bitwise applied on the mask and any IP address of the block.

The default mask in different classes are :

Class A – 255.0.0.0

Class B – 255.255.0.0

Class C – 255.255.255.0

Example : Given IP address 132.6.17.85 and default class B mask, find the beginning address (network address).

Solution : The default mask is 255.255.0.0, which means that the only the first 2 bytes are preserved and the other 2 bytes are set to 0. Therefore, the network address is 132.6.0.0.

Subnetting: Dividing a large block of addresses into several contiguous sub-blocks and assigning these sub-blocks to different smaller networks is called subnetting. It is a practice that is widely used when classless addressing is done.

Classless Addressing
To reduce the wastage of IP addresses in a block, we use sub-netting. What we do is that we use host id bits as net id bits of a classful IP address. We give the IP address and define the number of bits for mask along with it (usually followed by a '/' symbol), like, 192.168.1.1/28. Here, subnet mask is found by putting the given number of bits out of 32 as 1, like, in the given address, we need to put 28 out of 32 bits as 1 and the rest as 0, and so, the subnet mask would be 255.255.255.240.

Some values calculated in subnetting :
1. Number of subnets : Given bits for mask – No. of bits in default mask

2. Subnet address : AND result of subnet mask and the given IP address

3. Broadcast address : By putting the host bits as 1 and retaining the network bits as in the IP address

4. Number of hosts per subnet : $2^{(32 - \text{Given bits for mask})} - 2$
5. First Host ID : Subnet address + 1 (adding one to the binary representation of the subnet address)

6. Last Host ID : Subnet address + Number of Hosts

Example : Given IP Address – 172.16.0.0/25, find the number of subnets and the number of hosts per subnet. Also, for the first subnet block, find the subnet address, first host ID, last host ID and broadcast address.

Solution : This is a class B address. So, no. of subnets = $2^{(25-16)} = 2^9 = 512$.
No. of hosts per subnet = $2^{(32-25)} - 2 = 2^7 - 2 = 128 - 2 = 126$
For the first subnet block, we have subnet address = 0.0, first host id = 0.1, last host id = 0.126 and broadcast address = 0.127

Q. 5 a) Find range of address in the following blocks.(each range carries 1 mark)

1. 200.17.21.128/27

First IP 200.17.21.129

Last IP 200.17.21.158
Broadcast 200.17.21.159

2.17.34.16.0/23
First IP 17.34.16.1
Last IP 17.34.17.254
Broadcast 17.34.17.255

3. 123.56.77.32/29

First IP 123.56.77.33
Last IP 123.56.77.33
Broadcast 123.56.77.39

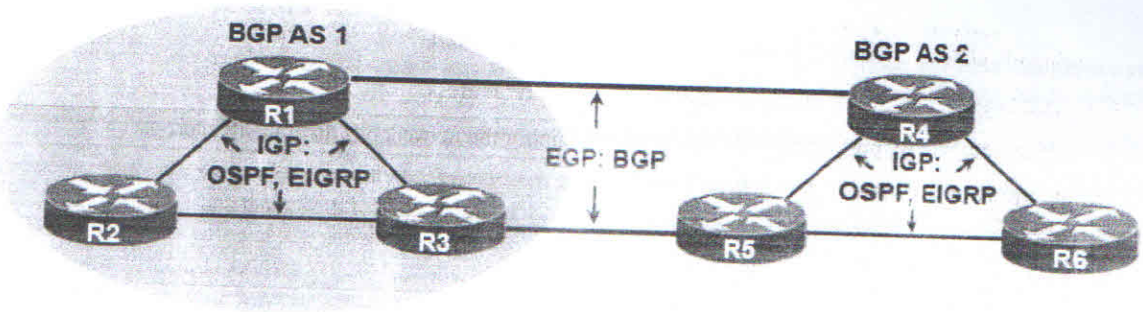
Q. 5 b) Which protocol is suitable for inter domain routing? Explain BGP with suitable diagram. (1.5)

Solution: Inter-domain (between domains) is any routing protocols that you have setup between two different networks. These are usually called Autonomous Systems (AS). The main inter-domain protocol is BGP. Most of the time when talking about inter-domain is routing on the internet.

Basic understanding about BGP

We really want to show you why we need BGP first but it is very difficult to explain without understanding a bit about BGP. So we will learn some basic knowledge about BGP first.

First we need to understand about the different between Interior Gateway Protocol and Exterior Gateway Protocol. The difference between them is shown below:



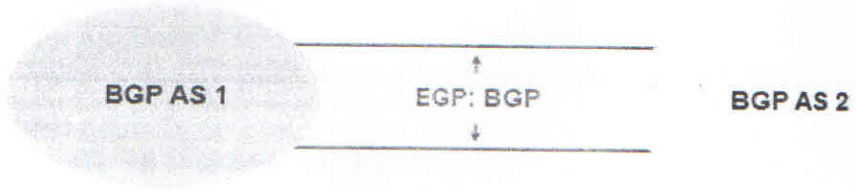
– **Interior Gateway Protocol (IGP)**: A routing protocol operating within an Autonomous System (AS) like OSPF, EIGRP... Usually routers running IGP are under the same administration (of a company, corporation, individual)
– **Exterior Gateway Protocol (EGP)**: A routing protocol operating between different AS. BGP is the only EGP used nowadays

In the topology above R1, R2 and R3 should run an IGP to communicate with each other because they are in the same AS. But to connect with other routers in another AS (like a different ISP), R1 and R3 must use an EGP.

With BGP, the term *autonomous system* (AS) refers to a network that operates separately from other networks and usually operates within a single administrative domain. Each AS is represented by an AS number. It is similar to EIGRP AS in this aspect. BGP is used mainly by the Internet Service Provider (ISP) all over the world. Each ISP usually has one BGP AS number (some very big ISP may have a few AS numbers). BGP AS numbers can be between 1 to 65,535.

In the topology above R1 and R3 are operating in BGP AS 1. If an AS connects to the public Internet using an EGP, then it must be assigned a unique AS number which is managed by the Internet Assigned Numbers Authority (IANA). IANA manages the AS numbers from **1** to **64,512** for public use (similar to public IP addresses) while **64,512** to **65,535** numbers are reserved for private use (similar to private IP addresses).

If we don't want to show the routers inside each AS we can simply ignore them:



In fact, the Internet that we are going "online" everyday is a collection of interconnected autonomous systems and BGP is running to provide routing between them.

Other BGP terms that you should learn are listed below:
+ **BGP speaker**: a router running BGP
+ **BGP peer** or **BGP neighbor**: Any two routers that have formed a TCP connection to exchange BGP routing information (as BGP runs over TCP on port 179, not UDP)
+ **Prefix**: Maybe you learned the word "subnet". In BGP world, it is usually called "prefix" because BGP usually does not advertise small subnets. It advertises blocks of large subnets so "prefix" is often used instead
+ **Internal BGP** (iBGP): refers to the BGP neighbor relationship within the same AS. The iBGP neighbor does not have to be directly connected
+ **External BGP** (eBGP): refers to the BGP neighbor relationship between two peers belongs to different AS. It is recommended that eBGP should be directly connected. Never run an IGP between eBGP peers.

In the below topology suppose all routers are running BGP then R1 is considered internal BGP to R2 and R3 (as they are running same AS 1) but is external BGP to R4. R5 is internal to R4 and R6 but external to R3.