CST 303 COMPUTER NETWORKS

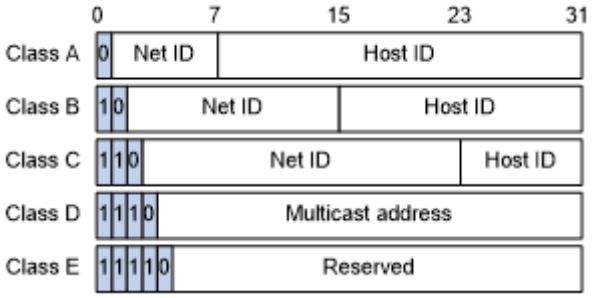
QUESTION BANK

MODULE 4

1. Compare classful and classless addressing, giving examples for both.

Classful:

The first addressing system to be implemented as part of the Internet Protocol was Classful Addressing. **Class A, Class B, Class C, Class D, and Class E** are the five varieties of Classful addresses. In IPv4, this classification is known as Classful addressing or IP address classes.



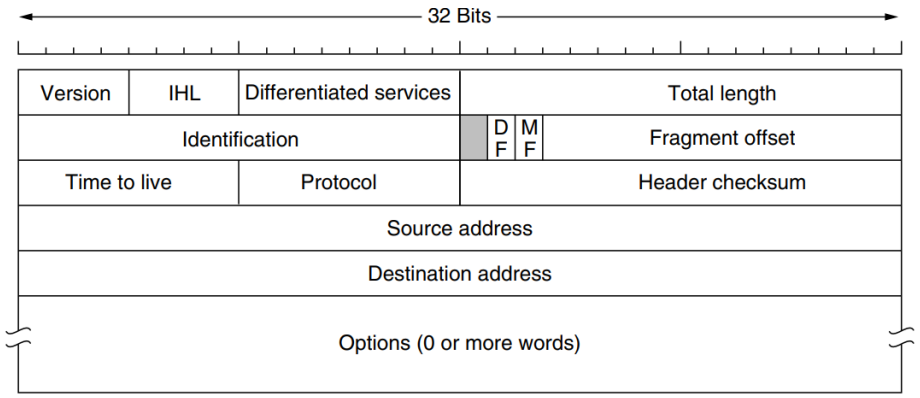
Classless:

Classless Inter-Domain Routing (CIDR) is another name for classless addressing. This addressing type aids in the more efficient allocation of IP addresses. This technique assigns a block of IP addresses based on specified conditions when the user demands a specific amount of IP addresses. This block is known as a "CIDR block", and it contains the necessary number of IP addresses.

When allocating a block, classless addressing is concerned with the following three rules.

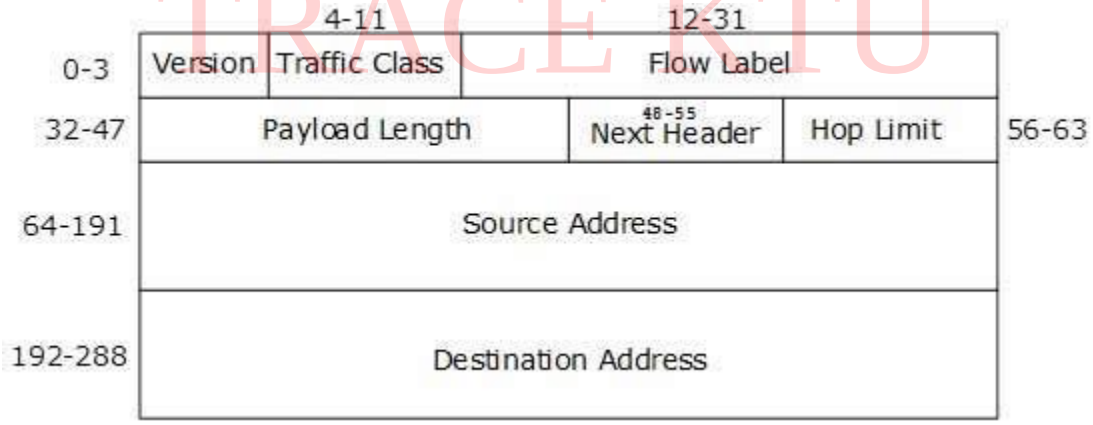
- **Rule 1** − The CIDR block's IP addresses must all be contiguous.
- **Rule 2** − The block size must be a power of two to be attractive. Furthermore, the block's size is equal to the number of IP addresses in the block.
- **Rule 3** − The block's first IP address must be divisible by the block size.

2. Describe the format of IPv4 datagram with the help of a diagram, highlighting the significance of each field.



VERSION: Version of the IP protocol (4 bits), which is 4 for IPv4
IHL: IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.
Differentiated Service (Type of service): Low Delay, High Throughput, Reliability (8 bits)
Total Length: Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.
Identification: Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)
Flags: 3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)
Fragment Offset: Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.
Time to live: Datagram's lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.
Protocol: Name of the protocol to which the data is to be passed (8 bits)
Header Checksum: 16 bits header checksum for checking errors in the datagram header
Source IP address: 32 bits IP address of the sender
Destination IP address: 32 bits IP address of the receiver
Option: Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.

3. Draw the IPv6 fixed header format.



<explain the fields>

4. Define Subnetting. What are the advantages of Subnetting? Explain with an example

Subnetting is the practice of dividing a network into two or more smaller networks. It increases routing efficiency, enhances the security of the network and reduces the size of the broadcast domain.

Advantages:

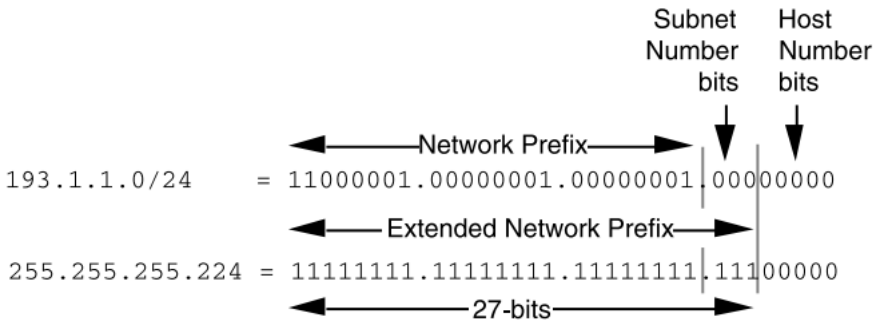
1. It provides security to one network from another network. eg) In an Organisation, code of the Developer department must not be accessed by another department.

2. It may be possible that a particular subnet might need higher network priority than others. For example, a Sales department need to host webcasts or video conferences.
3. In the case of Small networks, maintenance is easy.

Example:

An organization is assigned the network number 193.1.1.0/24 and it needs to define six subnets. The largest subnet is required to support 25 hosts.

Defining the Subnet Mask / Extended Prefix Length - The first step in defining the subnet mask is to determine the number of bits required to define the six subnets. Here we need 3 extra bits to create 6 subnets. In this example, the organization is subnetting a /24 so it will need three more bits, or a /27, as the extended network prefix. A 27-bit extended network prefix can be expressed in dotted-decimal notation as 255.255.255.224.



A 27-bit extended network prefix leaves 5 bits to define host addresses on each subnet.

Subnet Numbers/Addresses:

The eight subnet numbers for this example are listed in the following code sample. The underlined portion of each address identifies the extended network prefix, while the bold digits identify the 3 bits repre senting the subnet number field:

Base Net: 11000001.00000001.00000001 .00000000 = 193.1.1.0/24

Subnet #0: 11000001.00000001.00000001.000 00000 = 193.1.1.0/27

Subnet #1: 11000001.00000001.00000001.001 00000 = 193.1.1.32/27

Subnet #2: 11000001.00000001.00000001.010 00000 = 193.1.1.64/27

Subnet #3: 11000001.00000001.00000001.011 00000 = 193.1.1.96/27

Subnet #4: 11000001.00000001.00000001.100 00000 = 193.1.1.128/27

Subnet #5: 11000001.00000001.00000001.101 00000 = 193.1.1.160/27

Subnet #6: 11000001.00000001.00000001.110 00000 = 193.1.1.192/27

Subnet #7: 11000001.00000001.00000001.111 00000 = 193.1.1.224/27

4. Divide the network 220.125.5.192/26 into 8 sub networks. How many hosts can be connected in each network? Show their IP range, network address and broadcast address.

New subnet mask will be: For 8 network 3 bits are required to add to /26 mask, so new mask will be 26+3=29. Host bits = 32-29 = 3

Number of hosts in each subnet = 8 (2^3)

Sub network	Network range	Network Address	Broadcast Address
1	220.125.5.192/29-220.125.5.199/29	220.125.5.192/29	220.125.5.199/29
2	220.125.5.200/29-220.125.5.207/29	220.125.5.200/29	220.125.5.207/29
3	220.125.5.208/29-220.125.5.215/29	220.125.5.208/29	220.125.5.215/29
4	220.125.5.216/29-220.125.5.223/29	220.125.5.216/29	220.125.5.223/29
5	220.125.5.224/29-220.125.5.231/29	220.125.5.224/29	220.125.5.231/29
6	220.125.5.232/29-220.125.5.239/29	220.125.5.232/29	220.125.5.239/29
7	220.125.5.240/29-220.125.5.247/29	220.125.5.240/29	220.125.5.247/29
8	220.125.5.248/29-220.125.5.255/29	220.125.5.248/29	220.125.5.255/29

5. Differentiate between BOOTP and DHCP.

S.NO	BOOTP	DHCP
1.	BOOTP stands for Bootstrap Protocol.	While DHCP stands for Dynamic host configuration protocol.
2.	BOOTP does not provide temporary IP addressing.	While DHCP provides temporary IP addressing for only limited amount of time.
3.	BOOTP does not support DHCP clients.	While it support BOOTP clients.
4.	In BOOTP, manual-configuration takes place.	While in DHCP, auto-configuration takes place.
5.	BOOTP does not support mobile machines.	Whereas DHCP supports mobile machines.
6.	BOOTP can have errors due to manual-configuration.	Whereas in DHCP errors do not occur mostly due to auto-configuration.

6. Explain how routing is done using BGP

Border Gateway Protocol (BGP) is used to Exchange routing information for the internet and is the protocol used between ISP which are different ASes.
The protocol can connect together any internetwork of autonomous system using an arbitrary topology. The only requirement is that each AS have at least one router that is able to run

BGP and that is router connect to at least one other AS's BGP router. BGP's main function is to exchange network reach-ability information with other BGP systems. Border Gateway Protocol constructs an autonomous systems' graph based on the information exchanged between BGP routers.

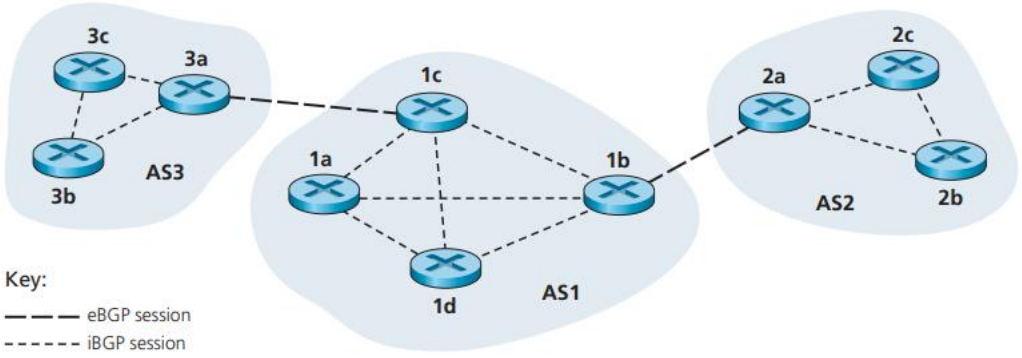
As an inter-AS routing protocol, BGP provides each AS a means to

- Obtain subnet reachability information from neighboring ASs.
- Propagate the reachability information to all routers internal to the AS.
- Determine "good" routes to subnets based on the reachability information and on AS policy.

In BGP, pairs of routers exchange routing information over semipermanent TCP connections using port 179. For each TCP connection, the two routers at the end of the connection are called BGP peers, and the TCP connection along with all the BGP messages sent over the connection is called a BGP session. Furthermore, a BGP session that spans two ASs is called an external BGP (eBGP) session, and a BGP session between routers in the same AS is called an internal BGP (iBGP) session.

BGP Attributes

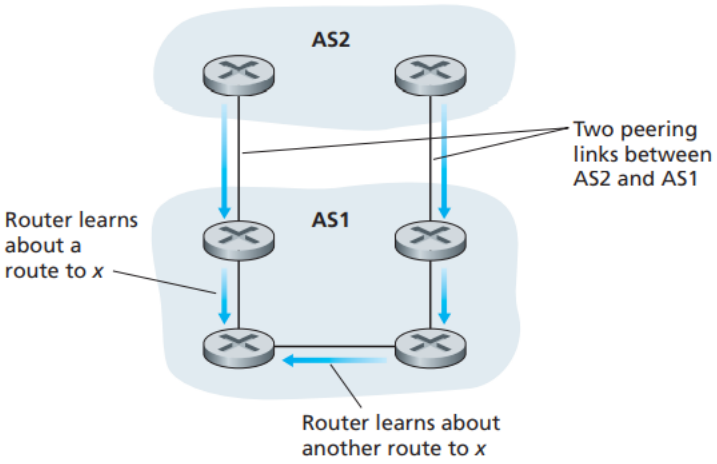
AS-PATH. This attribute contains the ASs through which the advertisement for the prefix has passed. When a prefix is passed into an AS, the AS adds its ASN to the AS-PATH attribute. For example, consider Figure below and suppose that prefix 138.16.64/24 is first advertised from AS2 to AS1; if AS1 then advertises the prefix to AS3, AS-PATH would be AS2 AS1. Routers use the AS-PATH attribute to detect and prevent looping advertisements; specifically, if a router sees that its AS is contained in the path list, it will reject the advertisement.



NEXT-HOP.

Use 1: Providing the critical link between the inter-AS and intra-AS routing protocols, the NEXT-HOP attribute has a subtle but important use. The NEXT-HOP is the router interface that begins the AS-PATH.

Use 2: In this figure below, AS1 and AS2 are connected by two peering links. A router in AS1 could learn about two different routes to the same prefix x. These two routes could have the same AS-PATH to x, but could have different NEXT-HOP values corresponding to the different peering links. Using the NEXT-HOP values and the intra-AS routing algorithm, the router can determine the cost of the path to each peering link, and then apply hot-potato routing



7. What is the use of ARP? Explain ARP operation.

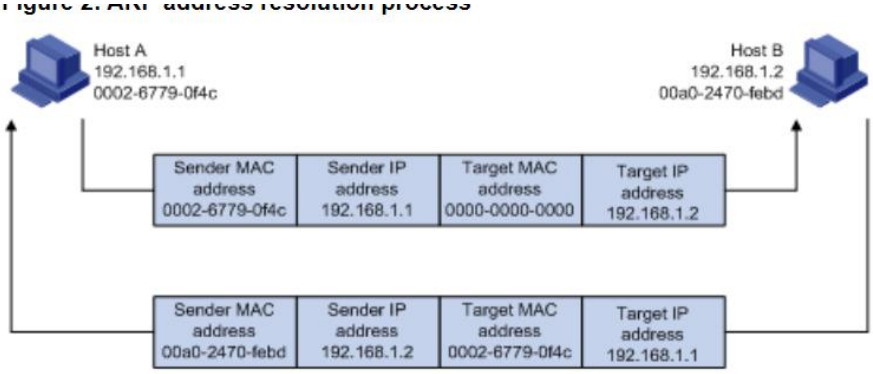
The acronym ARP stands for **Address Resolution Protocol** which is one of the most important protocols of the Network layer in the OSI model. ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address.

Operation of ARP

If Host A and Host B wishes to communicate, then Host A sends a packet to Host B, as shown in figure below:

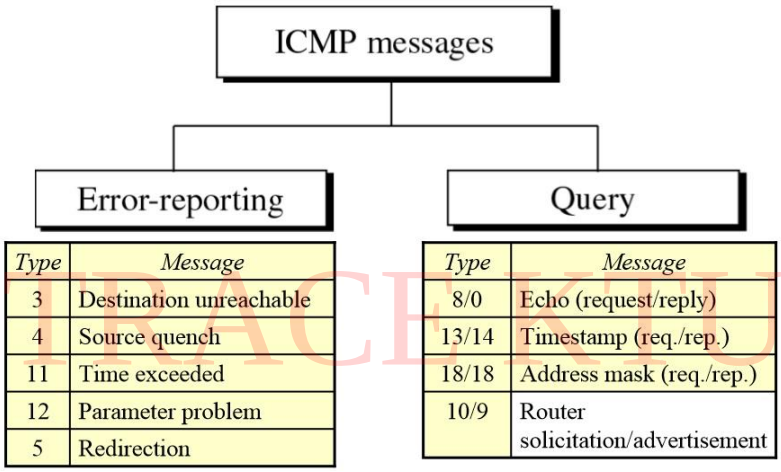
1. Host A looks in its ARP table to see whether there is an ARP entry for Host B. If yes, Host A uses the MAC address in the entry to encapsulate the IP packet into a data link layer frame and sends the frame to Host B.
2. If Host A finds no entry for Host B, Host A buffers the packet and broadcasts an ARP request using the following information.
    a. Source IP address and source MAC address: Host A's own IP address and the MAC address.
    b. Target IP address: Host B's IP address.
    c. Target MAC address: An all-zero MAC address.

    Because the ARP request is broadcast, all hosts on this subnet can receive the request, but only the requested host (Host B) will process the request.
3. Host B compares its own IP address with the target IP address in the ARP request. If they are the same, Host B:
    a. Adds the sender IP address and sender MAC address to its ARP table
    b. Encapsulates its MAC address into an ARP reply
    c. Unicasts the ARP reply to Host A.
4. After receiving the ARP reply, Host A:
    a. Adds the MAC address of Host B to its ARP table
    b. Encapsulates the MAC address in the IP packet and sends it to Host B.



ARP Cache: The ARP Cache is a collection of ARP entries (mostly dynamic) that are created when a hostname is resolved to an IP address and then an IP address is resolved to a MAC address (so the computer can effectively communicate with the IP address)

8. List and explain the different types of error reporting messages used by ICMP.



Type	*Message*
3	Destination unreachable
4	Source quench
11	Time exceeded
12	Parameter problem
5	Redirection

Type	*Message*
8/0	Echo (request/reply)
13/14	Timestamp (req./rep.)
18/18	Address mask (req./rep.)
10/9	Router solicitation/advertisement

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo and echo reply	Check if a machine is alive
Timestamp request/reply	Same as Echo, but with timestamp
Router advertisement/solicitation	Find a nearby router

<Refer Page 465 of Computer networks by Tanenbaum>

9. How does BGP avoid count to infinity problem?

Basic solution: Extend distance-vector (array of distances) with more information

BGP is a distance-vector protocol used to communicate between different ASes. Instead of maintaining just the cost to each destination, each BGP router keeps track of the exact path

used. Similarly, instead of periodically giving each neighbour its estimated cost to each destination, each BGP router tells its neighbours the path it is using. Every BGP router contains a module that examines routes to a given destination and scores them returning a number for destination to each route. Any route violating a policy constraint automatically gets a score of infinity. The router adapts a route with shortest distance. The scoring function is not a part of the BGP protocol and can be any function that the system managers want. BGP easily solves the count to infinity problem that plagues other distance-vector algorithms as whole path is known.

10. Explain RARP

RARP is abbreviation of **Reverse Address Resolution Protocol** which is a protocol based on computer networking which is employed by a client computer to request its IP address from a gateway server's Address Resolution Protocol table or cache. The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address.
This protocol is used to communicate data between two points in a server. The client doesn't necessarily need prior knowledge the server identities capable of serving its request. Medium Access Control (MAC) addresses requires individual configuration on the servers done by an administrator. RARP limits to the serving of IP addresses only.
When a replacement machine is set up, the machine may or might not have an attached disk that may permanently store the IP Address so the RARP client program requests IP Address from the RARP server on the router. The RARP server will return the IP address to the machine under the belief that an entry has been setup within the router table.

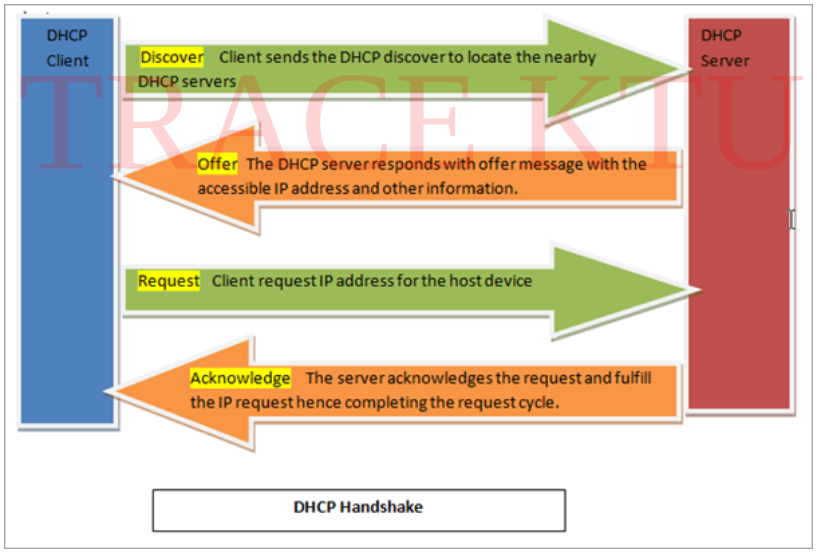
Working of RARP :

- The RARP is on the Network Access Layer and is employed to send data between two points in a very network.
- Each network participant has two unique addresses:- IP address (a logical address) and MAC address (the physical address).
- The IP address gets assigned by software and after that the MAC address is constructed into the hardware.
- The RARP server that responds to RARP requests, can even be any normal computer within the network. However, it must hold the data of all the MAC addresses with their assigned IP addresses. If a RARP request is received by the network, only these RARP servers can reply to it. The info packet needs to be sent on very cheap layers of the network. This implies that the packet is transferred to all the participants at the identical time.
- The client broadcasts a RARP request with an Ethernet broadcast address and with its own physical address. The server responds by informing the client its IP address.

RARP	ARP
RARP stands for Reverse Address Resolution Protocol	ARP stands for Address Resolution Protocol
In RARP, we find our own IP address	In ARP, we find the IP address of a remote machine
The MAC address is known and the IP address is requested	The IP address is known, and the MAC address is being requested
It uses the value 3 for requests and 4 for responses	It uses the value 1 for requests and 2 for responses

11. Explain DHCP Handshake.

The Dynamic Host Configuration Protocol (DHCP) has been devised to provide static and dynamic IP address allocation that can be manual or automatic.



12. Explain how IGMP supports internet multicasting?

Multicasting is when a group of devices all receive the same messages or packets. Multicasting works by sharing an IP address between multiple devices. Any network traffic directed at that IP address will reach all devices that share the IP address, instead of just one device. This is much like when a group of employees all receive company emails directed at a certain email alias.

Computers and other devices connected to a network use IGMP when they want to join a multicast group. A router that supports IGMP listens to IGMP transmissions from devices in order to figure out which devices belong to which multicast groups.

IGMP uses IP addresses that are set aside for multicasting. Multicast IP addresses are in the range between 224.0.0.0 and 239.255.255.255. (In contrast, anycast networks can use any regular IP address.) Each multicast group shares one of these IP addresses. When a router receives a series of packets directed at the shared IP address, it will duplicate those packets, sending copies to all members of the multicast group.

IGMP multicast groups can change at any time. A device can send an IGMP "join group" or "leave group" message at any point.

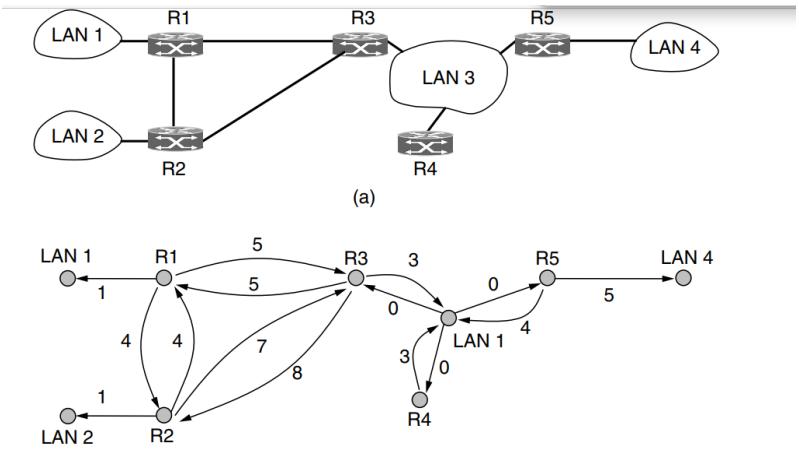
IGMP works directly on top of the Internet Protocol (IP). Each IGMP packet has both an IGMP header and an IP header. Just like ICMP, IGMP does not use a transport layer protocol such as TCP or UDP.

13. What is OSPF Routing?

OSPF -Open shortest path first – An interior gateway protocol

Internet is made up of a large number of independent networks or ASes (Autonomous Systems) that are operated by different organizations, usually a company, university, or ISP. Inside of its own network, an organization can use its own algorithm for internal routing, or intradomain routing, as it is more commonly known.

OSPF operates by abstracting the collection of actual networks, routers, and links into a directed graph in which each arc is assigned a weight (distance, delay, etc.). A point-to-point connection between two routers is represented by a pair of arcs, one in each direction. Their weights may be different. A broadcast network is represented by a node for the network itself, plus a node for each router. The arcs from that network node to the routers have weight 0. They are important nonetheless, as without them there is no path through the network. Other networks, which have only hosts, have only an arc reaching them and not one returning. This structure gives routes to hosts, but not through them.



What OSPF fundamentally does is represent the actual network as a graph like this and then use the link state method to have every router compute the shortest path from itself to all other nodes. Multiple paths may be found that are equally short. In this case, OSPF remembers the set of shortest paths and during packet forwarding, traffic is split across them. This helps to balance load. It is called ECMP (Equal Cost MultiPath).

OSPF Areas