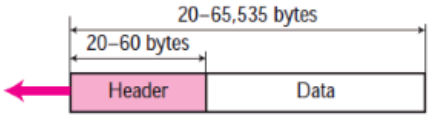
MODULE 4

1.What is Internet protocol(IP)? Explain IP Addressing and its type./explain the IP frame format and IP address classes in detail.

A:

Internet protocol (IP)

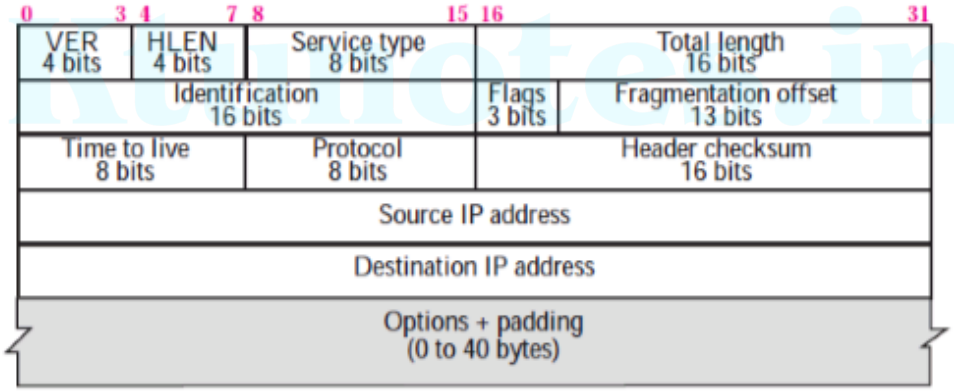
- Internet protocol is a host to host delivery protocol designed for the internet and it is a connectionless datagram protocol with no guarantee of reliability
- It does not provide any error control or flow control.
- It can only detect error, if error is detected the packet is discarded.
- **IP Datagram**



a. IP datagram

  - Packets in the IP layer/ protocol are called datagram.
  - In datagram, header filed is 20-69 bytes long and data is 20-65,535 bytes.

- **Header format of IP Datagram**



b. Header format

  - IP Header contain routing information associated with datagram delivery.
  - **Version (VER):** This 4-bit field defines the version of the IP protocol.
  - **Header length (HLEN):** This 4-bit field defines the total length of the datagram header in 4-byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes).
  - **Service type:** This is a 8-bit field which defines the class of service.
  - **Total length:** This is a 16-bit field that defines the total length (header plus data) of the IP datagram in bytes.
  - **Identification:** This field is used in fragmentation. Identification number helps to identify different fragment of same datagram.
  - **Flags:** This field is used in fragmentation.
  - **Fragmentation offset:** Show the relative position of the fragment with respect to the whole datagram.

- **Time to live:** This 8-bit long field is used to limit the packet life time in Internet. It holds a timestamp, which is decremented by each visited router.
- **Protocol:** This 8-bit field defines the higher-level protocol that uses the services of the IP layer.
- **Checksum:** The error detection method used by most TCP/IP protocols is called the checksum. The checksum protects against the corruption that may occur during the transmission of a packet.
- **Source address:** This 32-bit field defines the IP address of the source.
- **Destination address:** This 32-bit field defines the IP address of the destination.
- **Options:** Options are not required for every datagram they are for testing and debugging.

IP Addresses

- The identifier that is used in the Network Layer (OSI Model) or Internet Layer (TCP/IP Model) is called internet protocol address or IP address.
- It is a 32-bit binary address, implemented uniquely and universally defines a host or router on the internet.
- Every host and router on internet has an unique universally identified IP address.
- This 32 bit long address are used in source address and destination address field of IP packets.
- **Classes and Classfull Addressing:**
  - The IP addresses are divided into five categories or five classes.
  - The allocation of IP address in the different classes is called Classfull Addressing.
  - 5 classes of IP addresses are:
    1. **Class A:** In a Class A type of network, the first 8 bits (also called the first octet) identify the network.
    - The leftmost bit must be zero to define class A , the remaining 7 bit define different networks.
    - The number of networks that have class A IP adress is very limited - 2^7 = 128 networks, among which two of the addresses are reserved for special purposes.
    - In class A, 24 bits are used to define host id
    - 2^24 = 16,777,216 hosts can be connected to class A network, two of them are reserved for special purposes.
    - Address range : 0.0.0.0 to 127.255.255
    2. **Class B:** In a Class B type of network, the first 16 bits (the two octet) define the network id.
    - Two leftmost bit are '10' to define class B, next 14 bit define different networks.
    - There are 2^14 = 16,384 class B networks.
    - In class B 16 bits are used to define hosts.
    - 2^16 = 65,536 hosts.
    - Address range: 128.0.0.0 to 191.255.255.255
    3. **Class C:** In Class C 3 octets define net id and one octet define host id
    - The 3 leftmost bit is set to 110 to define class C and remaining 21 bit to define networks.
    - 2^21 = 2,097,152 networks

- 8 bits are used to define host id.
- 2^8 = 256 hosts, two address is used for special function.
- Class C address are designed for small organization that have smaller number of computer attached to network.
- Adress range: 192.0.0.0 to 223.255.255.255

4. **Class D:** The Class D address is defined for multicasting.

- Here there is no network id or host id.
- The whole address is used for multicasting.
- The first for bits is set to 1110 , which define class D, remaining bits define different multicast address.
- Address range: 224.0.0.0 to 239.255.255.255

5. **Class E:** Class E is reserved by internet for special use

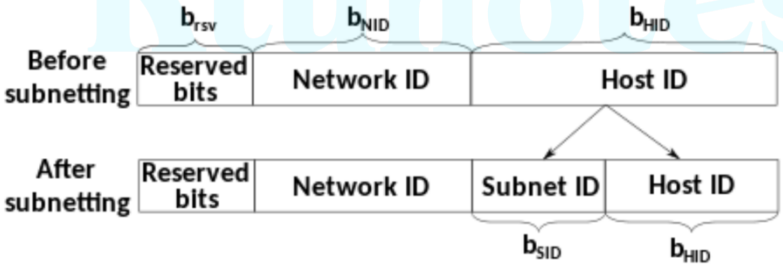
- There is no net id or host is in class E.
- First four bit is set to 1111 to define class E.
- Address range : 240.0.0.0 to 255.255.255.255

2.What is subnetting and subnet mask?

A:

Sub netting

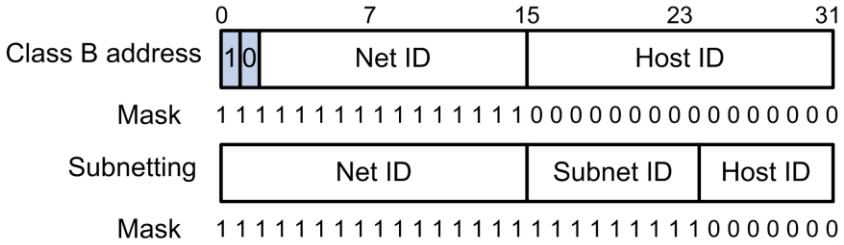
- Subnetting divides a network down into smaller networks called subnets by using some bits of the host ID to create a subnet ID.
- A subnetwork or subnet is a logical subdivision of an IP network.



- Subnetting increases the number of addresses that cannot be assigned to hosts. Therefore, using subnets means accommodating fewer hosts.
- For example, a Class B network without subnetting can accommodate 1022 more hosts than the same network subnetted into 512 subnets.
- Subnets allow network traffic to pass through a minimum number of routers so that data packets only need to traverse a shorter distance to reach the target destination within a large network.

Subnet masking

- Subnet Masking identifies the boundary between the host ID and the combination of net ID and subnet ID.
- Each subnet mask comprises 32 bits that correspond to the bits in an IP address.
- It gives the network address in the address block when AND operation is bitwise applied on the mask and any IP address of the block.



- In a subnet mask, the consecutive ones represent the net ID and subnet ID, and consecutive zeros represent the host ID.
- The default mask in different classes are :
    - Class A
        - Dotted decimal: 255.0.0.0
        - Binary : 11111111 00000000 00000000 00000000
    - Class B
        - Dotted decimal: 255.255.0.0
        - Binary: 11111111 11111111 00000000 00000000
    - Class C
        - Dotted decimal: 255.255.255.0
        - Binary: 11111111 11111111 11111111 00000000

- **Some values calculated in subnetting :**
    a. Number of subnets : Given bits for mask – No. of bits in default mask.
    b. Subnet address : AND result of subnet mask and the given IP address.
    c. Broadcast address : By putting the host bits as 1 and retaining the network bits as in the IP address.
    d. Number of hosts per subnet : 2(32 – Given bits for mask) – 2.
    e. First Host ID : Subnet address + 1 (adding one to the binary representation of the subnet address)
    f. Last Host ID : Subnet address + Number of Hosts

- **Advantages of subnetting are as follows:**
    a. Reduce network congestion.
    b. Control network growth.
    c. Ease administration.
    d. Boost network security.

3. What are the internet control protocols? list them.

A:

Internet control protocols

- The Internetwork Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination.
- Data transferred in the Internet is divided into smaller pieces, called packets.
- IP information is attached to each packet, and this information helps routers to send packets to the right place.

- Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed.
- Following are the internet control protocols:
    - **Address resolution protocol (ARP):** ARP is used to find the physical address of node when it's internet address is known.
    - **Reverse address resolution protocol (RARP):** RARP is used when internet address of host is unknown and physical address is known.
    - **Internet control message protocol (ICMP):** ICMP is a mechanism used by hosts and routers to sending error messages and operations information.
    - **Internet group message protocol (IGMP):** IGMP is used by hosts and routers that supports multicasting. It lets all the systems on a physical network know which host currently belong to which multicast group.
    - **Boot starp protocol (BOOTP):** BOOTP enables a configuration server to automatically assign an IP address to network systems in IP networks.

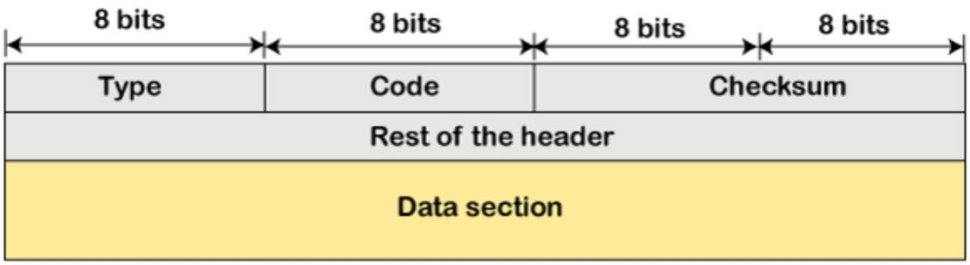
4. Explain internet control message protocol (ICMP) and internet group message protocol (IGMP).

A:

Internet control message protocol (ICMP)

- IP does not have an inbuilt mechanism for sending error and control messages.
- It depends on Internet Control Message Protocol(ICMP) to provide an error control.
- It is used for reporting errors and management queries.
- ICMP is a mechanism used by hosts and routers to sending error messages and operations information.
- Always report the error message to the orginal source.

- **ICMP message format**



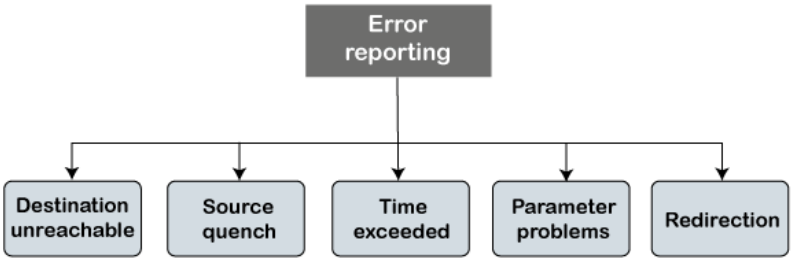
    - **Type:** It is an 8-bit field. It defines the ICMP message type.
      The values range from 0 to 127 are defined for ICMPv6, and the values from 128 to 255 are the informational messages.
    - **Code**: It is an 8-bit field that defines the subtype of the ICMP message.
    - **Checksum**: It is a 16-bit field to detect whether the error exists in the message or not.

- **ICMP messages**
    - ICMP messages are usually divided into two categories:

ICMP messages

Category	Type	Message
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply

- **Error-reporting messages:** The error-reporting message means that the router encounters a problem when it processes an IP packet then it reports a message.
  The error-reporting messages are broadly classified into the following categories:



1. Destination unreachable: The destination unreachable error occurs when the packet does not reach the destination. Suppose the sender sends the message, but the message does not reach the destination, then the intermediate router reports to the sender that the destination is unreachable.
2. Source quench: Source quench message is a request to decrease the traffic rate for messages sending to the host(destination).
   ICMP will take the source IP from the discarded packet and informs the source by sending a source quench message. Then source will reduce the speed of transmission so that router will be free from congestion.
3. Time exceeded: When the sender sends the packet, then it moves in a routing loop.
   The time exceeded is based on the time-to-live value. When the packet traverses through the router, then each router decreases the value of TTL by one.
   Whenever a router decreases a datagram with a time-to-live value to zero, then the router discards a datagram and sends the time exceeded message to the original source.
4. Parameter problem: Whenever packets come to the router then the calculated header checksum should be equal to the received header checksum then the only the packet is accepted by the router.
   If there is a mismatch, packet will be dropped by the router. ICMP will take the source IP from the discarded packet and informs to the source by sending a parameter problem message.

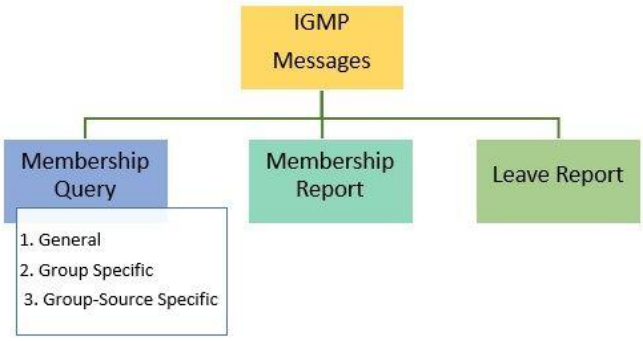
5. Redirection: When the packet is sent, then the routing table is gradually augmented and updated. The tool used to achieve this is the redirection message.

- **Query Message :**The query messages are those messages that help the host to get the specific information of another host.
  The ICMP query messages are of two types:
  1. Echo-request and echo-reply message : A router or a host can send an echo-request message. It is used to ping a message to another host that "Are you alive".
     If the other host is alive, then it sends the echo-reply message.
     An echo-reply message is sent by the router or the host that receives an echo-request message.
  2. Timestamp-request and timestamp-reply message: The timestamp-request and timestamp-reply messages are also a type of query messages.
     Suppose the computer A wants to know the time on computer B, so it sends the timestamp-request message to computer B.
     The computer B responds with a timestamp-reply message.

Internet group message protocol (IGMP)

- It is a protocol that allows several devices to share one IP address so they can all receive the same data.
- IGMP is not a multicasting routing protocol; it is a protocol that manages group membership. In any network, there are one or more multicast routers that distribute multicast packets to hosts or other routers.
- The IGMP protocol gives the multicast routers information about the membership status of hosts (routers) connected to the network.
- Like ICMP, IGMP is considered part of the IP layer.
- Also like ICMP, IGMP messages are transmitted in IP datagrams.
- Unlike other protocols, IGMP has a fixed-size message, with no optional data.
- **Advantages of IGMP protocol**
  - IGMP communication protocol efficiently transmits the multicast data to the receivers and so, no junk packets are transmitted to the host which shows optimized performance.
  - Bandwidth is consumed totally as all the shared links are connected.
  - Hosts can leave a multicast group and join another.

- **IGMP messages**



a. Membership Query: The query messages are sent by the query router of the network to enquire about the active members of a group. The query messages are further classified as:
   - General Query Message: With this query message the router enquires host about all the groups the host is involved in.
   - Group-Specific Query Message: With this query message the router enquires the host or router if there are interested in a specific multicast group.
   - Group-Source Specific Query Message: With this query message the query router enquires the hosts or router if it is still interested in the specific multicast group coming from a specific source.

b. Membership Report: The receiving members of the multicast group send the membership report either in response to the membership query message or if they are registering the group for the first time.

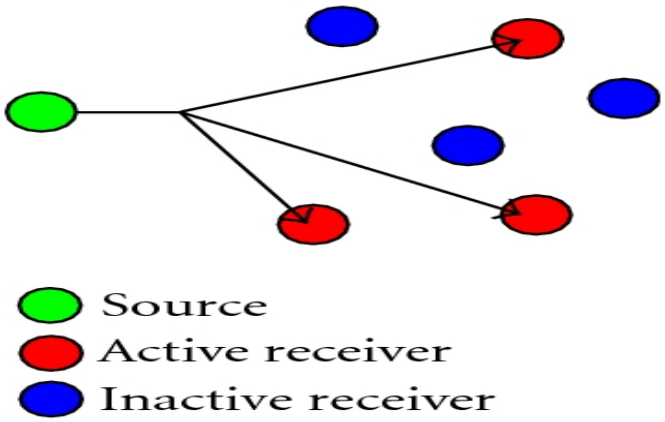
c. Leave Group: The receiving members of the multicast group sent this message to the multicast router if they are not interested in a specific multicast group anymore.

5.What is Internet multicasting? What are the applications of multicasting?

A:

Internet Multicasting

- In multicast communication, there is one source and a group of destinations. The relationship is one-to-many. In this type of communication, the source address is a unicast address, but the destination address is a group address, which defines one or more destinations. The group address identifies the members of the group,
- A multicast packet starts from the source S1 and goes to all destinations that belong to group G1.
- In multicasting, when a router receives a packet, it may forward it through several of its interfaces.



- **Application of multicasting:**
  a. **Access to Distributed Databases:** Most of the large databases today are distributed. That is, the information is stored in more than on location, usually at the time of production.

The user who needs to access the database does not know the location of the information.
A user's request is multicast to all the database locations, and the location that has the information responds.

b. **Information Dissemination:** Businesses often need to send information to their customers. If the nature of the information is the same for each customer, it can be multicast.
In this way a business can send one message that can reach many customers. For example, a software update can be sent to all purchasers of a particular software package.
c. **Dissemination of News:** In a similar manner news can be easily disseminated through multicasting. One single message can be sent to those interested in a particular topic.
d. **Teleconferencing:** Teleconferencing involves multicasting. The individuals attending a teleconference, all need to receive the same information at the same time. Temporary or permanent groups can be formed for this purpose.
e. **Distance Learning:** One growing area in the use of multicasting is distance learning. Lessons taught by one single professor can be received by a specific group of students.

6.Explain the following protocols and it's working

1. **BOOTP**
2. **DHCP**
3. **OSPF**

A:

BOOTP (BOOTSTRAP PROTOCOL)

- The Bootstrap Protocol is a TCP/IP protocol
- It allows a configuration server to provide an IP address to network devices automatically in Internet Protocol networks.
- BOOTP uses a unique IP address algorithm to provide each system on the network with a completely different IP address in a fraction of a second.
- This shortens the connection time between the server and the client. It starts the proc
- ess of downloading and updating the source code even with very little information.
- BOOTP uses a combination of TFTP (Trivial File Transfer Protocol) and UDP (User Datagram Protocol) to request and receive requests from various network-connected participants and to handle their responses.
- In a BOOTP connection, the server and client just need an IP address and a gateway address to establish a successful connection.

- **Working of BOOTP**
  - When a BOOTP client is started, it has no IP address.
  - so it broadcasts a message containing its MAC address onto the network.
  - This message is called a “BOOTP request,”.
  - It is picked up by the BOOTP server, which replies to the client with the following information that the client needs:
    - The client’s IP address, subnet mask, and default gateway address

        - The IP address and host name of the BOOTP server
        - The IP address of the server that has the boot image, which the client needs to load its operating system
    - When the client receives this information from the BOOTP server, itconfigures and initializes its TCP/IP protocol stack, and then connects to the server on which the boot image is shared.
    - The client loads the boot image and uses this information to load and start its operating system.
- **Uses of BOOTP protocol**
    - Bootstrap (BOOTP) is primarily required to check the system on a network the first time you start your computer. Records the BIOS cycle of each computer on the network to allow the computer's motherboard and network manager to efficiently organize the data transfer on the computer as soon as it boots up.
    - BOOTP is mainly used in a diskless environment and requires no media as all data is stored in the network cloud for efficient use.
    - BOOTP is the transfer of a data between a client and a server to send and receive requests and corresponding responses by the networking server.
    - BOOTP supports the use of motherboards and network managers, so no external storage outside of the cloud network is required.

DHCP (Dynamic Host Configuration Protocol)

- Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to any device, or node, on a network so they can communicate using IP (Internet Protocol).
- DHCP assigns new IP addresses in each location when devices are moved from place to place, which means network administrators do not have to manually configure each device with a valid IP address or reconfigure the device with a new IP address if it moves to a new location on the network.
- DHCP manages the provision of all the nodes or devices added or dropped from the network.
- DHCP maintains the unique IP address of the host using a DHCP server.
- **Working of DHCP:**
    - When a device wants access to a network that's using DHCP, it sends a request for an IP address that is picked up by a DHCP server.
    - The server responds be delivering an IP address to the device, then monitors the use of the address and takes it back after a specified time or when the device shuts down.
    - The IP address is then returned to the pool of addresses managed by the DHCP server to be reassigned to another device as it seeks access to the network.
- **Components of DHCP:**
    - **DHCP server:** DHCP server is a networked device running the DCHP service that holds IP addresses and related configuration information.
      This is typically a server or a router but could be
      anything that acts as a host, such as an SD-WAN appliance.
    - **DHCP client:** DHCP client is the endpoint that receives configuration information from a DHCP server.

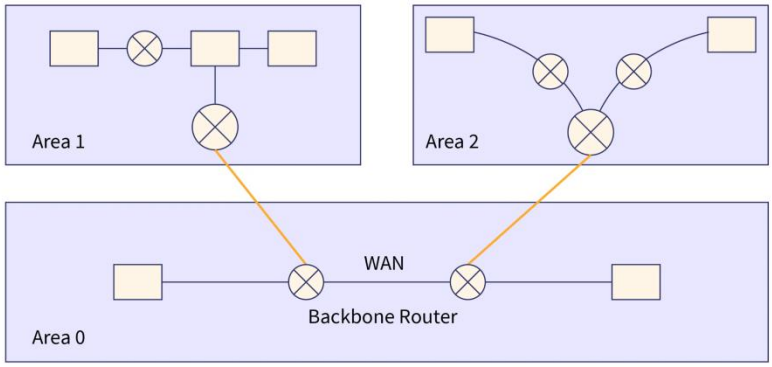
This can be any device like computer, laptop, IoT endpoint or anything else that requires connectivity to the network.
Most of the devices are configured to receive DHCP information by default.

- **IP address pool:**IP address pool is the range of addresses that are available to DHCP clients.
  IP addresses are typically handed out sequentially from lowest to the highest.
- **Subnet:**Subnet is the partitioned segments of the IP networks.
  Subnet is used to keep networks manageable.
- **Lease:**Lease is the length of time for which a DHCP client holds the IP address information.
  When a lease expires, the client has to renew it**.**

- **Advantages**:
  - Centralised management of IP addresses
  - Ease of adding new clients to a network
  - Reuse of IP addresses reducing the total number of IP addresses that are required
  - Simple reconfiguration of the IP address space on the DHCP server without needing to reconfigure each client
- **Disadvantage**:
  - IP conflict can occur

OSPF (Open Shortest Path First Protocol)

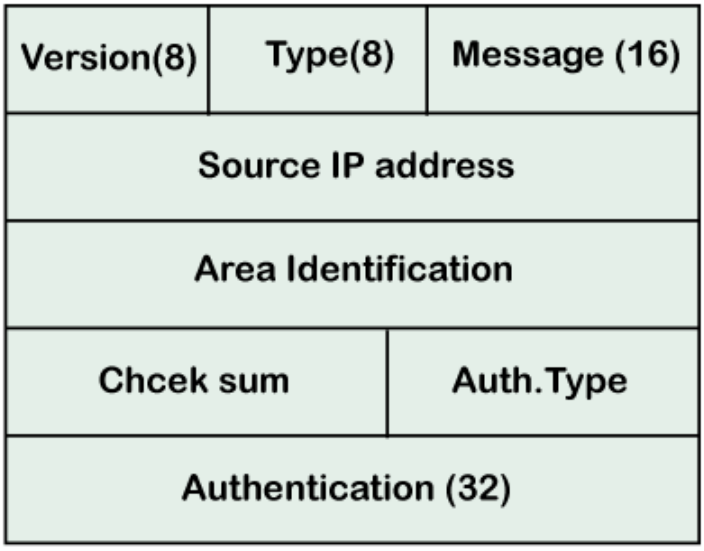
- Open Shortest Path First (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First.
- OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e, the protocol which aims at moving the packet within a large autonomous system or routing domain.
- OSPF uses multicast address 224.0.0.5 for normal communication.
- It is an intradomain protocol, which means that it is used within an area or a network.
- **OSPF Areas:**
  - OSPF divides the autonomous systems into areas where the area is a collection of networks, hosts, and routers.
  - Routers that exist inside the area flood the area with routing information
  - In Area, the special router also exists. The special routers are those that are present at the border of an area, and these special routers are known as Area Border Routers.
  - This router summarizes the information about an area and shares the information with other areas.
  - All the areas inside an autonomous system are connected to the backbone routers, and these backbone routers are part of a primary area.
  - The role of a primary area is to provide communication between different areas.



- **OSPF Working:**
  - Step 1: The first step is to become OSPF neighbors. The two connecting routers running OSPF on the same link **creates a neighbour relationship.**
  - Step 2: The second step is to exchange database information. After becoming the neighbors, the two routers **exchange the LSDB** information with each other.
  - Step 3: The third step is to **choose the best route.** Once the LSDB information has been exchanged with each other, the router chooses the best route to be added to a routing table based on the calculation of SPF.
- **Types of links in OSPF:**
  - In OSPF, the connection between two routers is known as link.
  - There are 4 types of link in OSPF.

1. **Point-to-point link:** The point-to-point link directly connects the two routers without any host or router in between.
2. **Transient link:** When several routers are attached in a network, they are known as a transient link.
   The transient link has two different implementations:
   Unrealistic topology: When all the routers are connected to each other, it is known as an unrealistic topology.
   Realistic topology: When some designated router exists in a network then it is known as a realistic topology. Here designated router is a router to which all the routers are connected. All the packets sent by the routers will be passed through the designated router.
3. **Stub link:** It is a network that is connected to the single router. Data enters to the network through the single router and leaves the network through the same router.
4. **Virtual link:**If the link between the two routers is broken, the administration creates the virtual path between the routers, and that path could be a long one also**.**

- **OSPF Message Format:**



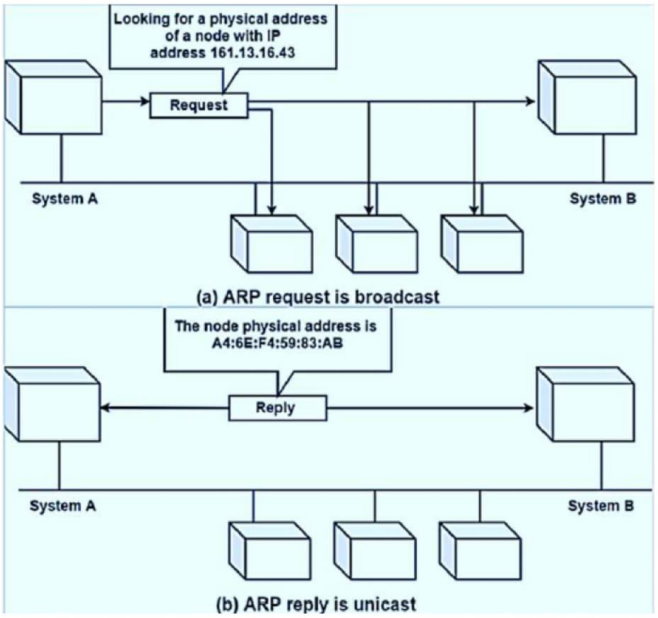
- **Version**: It is an 8-bit field that specifies the OSPF protocol version.
- **Type**: It is an 8-bit field. It specifies the type of the OSPF packet.
- **Message**: It is a 16-bit field that defines the total length of the message, including the header. Therefore, the total length is equal to the sum of the length of the message and header.
- **Source IP address:** It defines the address from which the packets are sent. It is a sending routing IP address.
- **Area identification:** It defines the area within which the routing takes place.
- **Checksum**: It is used for error correction and error detection.
- **Authentication type**: There are two types of authentication, i.e., 0 and 1. Here, 0 means for none that specifies no authentication is available and 1 means for pwd that specifies the password-based authentication.
- **Authentication**: It is a 32-bit field that contains the actual value of the authentication data.

7.Explain the functions of ARP and RARP.

A:

Address resolution protocol (ARP)

- Address Resolution Protocol (ARP) is a communication protocol used to find the MAC (Media Access Control) address of a device from its IP address.
- This protocol is used when a device wants to communicate with another device on a Local Area Network or Ethernet.
- ARP relates an IP address with the physical address. On a typical physical network such as LAN, each device on a link is identified by a physical address, usually printed on the network interface card (NIC).
- When one host wants to communicate with another host on the network, it needs to resolve the IP address of each host to the host's hardware address.
- **Working of ARP:**



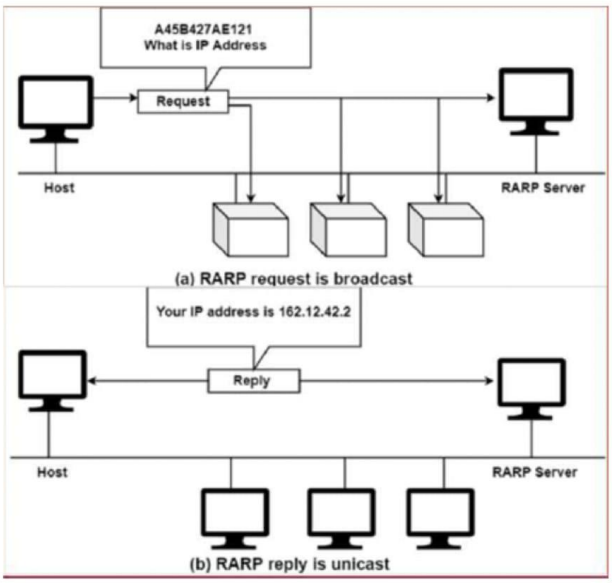
14

- When a host tries to interact with another host, an **ARP request is initiated**. If the IP address is for the local network, the source host checks its **ARP cache** to find out the hardware address of the destination computer.
- If the correspondence **hardware address is not found**, ARP **broadcasts** the request to all the local hosts.
- All hosts receive the broadcast and **check their own IP address**. If no match is discovered, the request is ignored.
- The destination host that finds the matching IP address sends an **ARP reply** to the source host along with its hardware address, thus **establishing the communication.**
- The **ARP cache is then updated** with the hardware address of the destination host.

Reverse Address Resolution Protocol (RARP)

- Reverse Address Resolution Protocol (RARP) is a network specific standard protocol.
- Some network hosts, such as a diskless workstation, do not know their own IP address when they are booted.
- Reverse Address Resolution Protocol (RARP) is a protocol a physical machine in a local area network (LAN) can use to request its IP address.
- It does this by sending the device's physical address to a specialised RARP server that is on the same LAN and is actively listening for RARP requests.
- **Working of RARP:**

WORKING OF RARP



18

1. The source device generates a RARP Request message.
2. The source broadcasts the RARP Request message on the local network.
3. The message is received by each device on the local network and processed. Devices that are not configured to act as RARP servers ignore the message.
4. Any device on the network that is a RARP server responds to the broadcast from the source device. It generates a RARP Reply
5. The RARP server sends the RARP Reply message unicast to the device looking to be configured.
6. The source device processes the reply from the RARP server. It then configures itself using the IP address in the Target Protocol Address supplied by the RARP server.

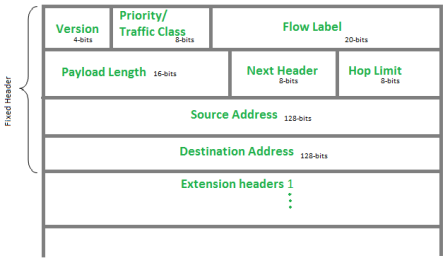
8. Explain IPv6 and ICMPv6 with its packet format.

A:

IPv6

- IPv6 is a set of specifications from the Internet Engineering Task Force (IETF) that's essentially an upgrade of IP version 4 (IPv4).
- The basics of IPv6 are similar to those of IPv4, devices can use IPv6 as source and destination addresses to pass packets over a network, and tools like ping work for network testing as they do in IPv4, with some slight variations.
- A main advantage of IPv6 is increased address space.
- The address space of IPv6 is 128- bit, while address space of IPv4 is of 32-bit length
- The size of the IPv6 address space makes it less vulnerable to malicious activities such as IP scanning.
- IPv6 packets can support a larger payload than IPv4 packets resulting in increased throughput and transport efficiency.
- IPv6 also support auto-configuration to help correct most of the shortcomings in version 4, and it has integrated security and mobility features.

- **IPv6 features**:
  - Supports source and destination addresses that are 128 bits (16 bytes) long.
  - Requires IPSec support.
  - Uses Flow Label field to identify packet flow for QoS handling by router.
  - Allows the host to send fragments packets but not routers.
  - Doesn't include a checksum in the header.
  - Uses a link-local scope all-nodes multicast address.
- **IPv6 packet format**

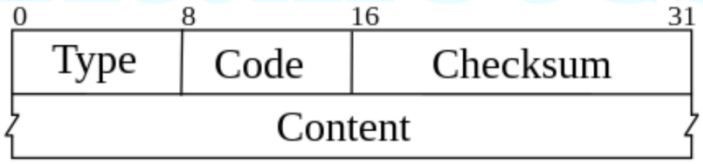


  - **Version (4-bits):** Indicates version of Internet Protocol which contains bit sequence 0110.
  - **Traffic Class (8-bits):** The Traffic Class field indicates class or priority of IPv6 packet. It helps routers to handle the traffic based on the priority of the packet. If congestion occurs on the router then packets with the least priority will be discarded.
  - **Flow Label (20-bits):** Flow Label field is used by a source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 routers.
    In order to distinguish the flow, an intermediate router can use the source address, a destination address, and flow label of the packets.
    Between a source and destination, multiple flows may exist because many processes might be running at the same time.
  - **Payload Length (16-bits):** It is a 16-bit (unsigned integer) field, indicates the total size of the payload which tells routers about the amount of information a particular packet contains in its payload.
    The payload Length field includes extension headers(if any) and an upper-layer packet.
  - **Next Header (8-bits):** Next Header indicates the type of extension header(if present) immediately following the IPv6 headers.
    In some cases it indicates the protocols contained within upper-layer packets, such as TCP, UDP.
  - **Hop Limit (8-bits):** It indicates the maximum number of intermediate nodes IPv6 packet is allowed to travel. Its value gets decremented by one, by each node that forwards the packet and the packet is discarded if the value decrements to 0.
    This is used to discard the packets that are stuck in an infinite loop because of some routing error.
  - **Source Address (128-bits):** Source Address is the 128-bit IPv6 address of the original source of the packet.

- **Destination Address (128-bits):** The destination Address field indicates the IPv6 address of the final destination. All the intermediate nodes can use this information in order to correctly route the packet.
- **Extension Headers:** In order to rectify the limitations of the IPv4 Option Field, Extension Headers are introduced in IP version 6. The extension header mechanism is a very important part of the IPv6 architecture. The next Header field of IPv6 fixed header points to the first Extension Header and this first extension header points to the second extension header and so on.

ICMPv6

- Internet Control Message Protocol (both ICMPv4 and ICMPv6) is a protocol which acts as a communication messenger protocol between the communicating devices in IP network.
- ICMP messages provide feedback, error reporting and network diagnostic functions in IP network which are necessary for the smooth operation of IPv6.
- ICMPv6 is a new version of the ICMP that forms an integral pan of the IPv6 architecture.
- ICMPv6 message are transported within an IPv6 packet that may include IPv6 extension within header.
- **Function of ICMPv6**
  - Error Reporting.
  - Network Diagnostics.
  - Neighbour Discovery.
  - Multicasting Membership Reporting
  - Router Solicitation and router Advertisements.
- **ICMPv6 packet format:**



  - **Type:** Defines the type of message.
  - **Code:** The code field value depends on the message type and provides an additional level of message granularity.
  - **Checksum:** The checksum field provides a minimal level of integrity verification for the ICMP message.
- **ICMPv6 message:**
  ICMPv6 messages are subdivided into two classes
  1: Error Messages: ICMPv6 error messages are used to report errors in the forwarding or delivery of IPv6 packets. The ICMPv6 "Type field" values for the error message are between O and 127.
  ICMPv6 error messages belong to four different categories:
  a. **Destination Unreachable:** Destination Unreachable ICMPv6 error message is generated by the source host or a router when an IPv6 datagram packet cannot be delivered for any reason other than congestion.
  b. **Packet Too Big**: Packet Ton Dig ICMPv6 error messages are generated by the router when a packet cannot be forwarded to the next hop link because the size of the IPv6 datagram is larger than the MTU (Maximum Transmission Unit) of the link. .

c. **Time Exceeded**: Hop Limit field in IPv6 datagram header is decremented by each router that forwards the packet.
When the Hop Limit field value in IPv6 header reaches zero, the router discards the IPv6 datagram packet and returns a "Time Exceeded" ICMPv6 error message to the source host.
d. **Parameter Problems:** When a problem or mistake with an IPv6 header make a router cannot process the packet, the router stops processing the IPv6 datagram packet discards the packet and returns a "Parameter Problem" ICMPv6 error message to the source host

- **2. information Messages:** ICMPv6 informational messages are used for network diagnostic functions and additional critical network functions like Neighbour Discovery.
ICMPv6 informational messages have values for the Type field (8 bit binary number) between 128 and 255.

a. **Diagnostic Messages:** ICMPv6 Echo request and Echo reply are the Diagnostic messages.
Every IPv6 host must return an ICMPv6 Echo reply when it receives an ICMPv6 Echo request.
b. **MLD (Multicast Listener Discovery) Messages:** ICMPv6 MLD Messages are used by an IPv6 enabled router to discover hosts who are interested in multicast packers, and the multicast addresses they are interested. MLD messages are used by MLD Protocol. MLD (Multicast Listener Discovery) Protocol is the IPv6 equivalent of IGMP (Internet Group Management) Protocol in IPv4.
c. **ND (Neighbour Discovery) Messages:** ICMPv6 ND Messages are used for the Neighbour Discovery Protocol (NDP). ND Messages includes Router Solicitation & Router Advertisement, Neighbour Solicitation and Neighbour Advertisement.

9.What is meant by exterior gateway routing protocol? Explain the working of BGP?

A:

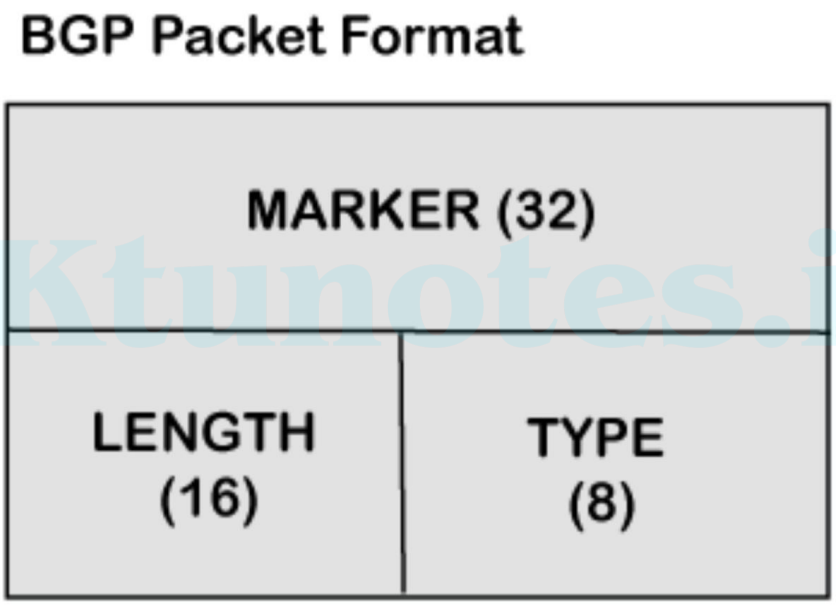
Exterior Gateway Routing Protocols.

- Protocols used to exchange routing information between autonomous systems are called exterior gateway routing protocols.
- Although interior routing protocols are usually designed to provide detailed routing information about all or most computers inside the autonomous systems, exterior protocols are designed to be more careful in the information they provide.
- Usually, exterior protocols provide information about only the preferred or best routes rather than all possible routes.
- Eg: Border gateway protocol

Border Gateway Protocol

- BGP is a complex, advanced distance Exterior Gateway Protocol (EGP).
- BGP exchange routing information between Autonomous Systems (ASS).

- BGP is especially used for exchanging routing information between all of the major Internet Service Providers (ISPs). as well between larger client sites and their respective ISPs. And, in some large enterprise networks, BGP is used to interconnect different geographical or administrative regions.
- Some of the primary attributes of BGP is the use of pieces of information about a known route, where it came from. and how to reach it, A BGP router will also generate an error message if it receives a route that is missing.
- **Characteristics of BGP:**
    - It is an advanced distance vector protocol.
    - It sends full routing updates at the start of the session, trigger updates are sent afterward.
    - BGP maintains connection by sending periodic keepalives
    - It creates and maintains connection by using TCP port 179.
    - It has its own routing table, although it is capable of both sharing and inquiring of the interior IP routing table.
- **BGP Message Format:**



1. **Marker**: It is a 32-bit field which is used for the authentication purpose.
2. **Length**: It is a 16-bit field that defines the total length of the message, including the header.
3. **Type**: It is an 8-bit field that defines the type of the packet.

- **BGP Message Types:**

  There are four different types of packets exist in BGP:

  a. **Open**: When the router wants to create a neighbourhood relation with another router, it sends the Open packet.

  b. **Update**: The update packet can be used in either of the two cases:
     - It can be used to withdraw the destination, which has been advertised previously.
     - It can also be used to announce the route to the new destination.

  c. **Keep Alive**: The keep alive packet is exchanged regularly to tell other routers whether they are alive or not.

For example, there are two routers, i.e., R1 and R2. The R1 sends the keep alive packet to R2 while R2 sends the keep alive packet to R1 so that R1 can get to know that R2 is alive, and R2 can get to know that R1 is alive.

d. **Notification**: The notification packet is sent when the router detects the error condition or close the connection.

10. 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.
- Number of subnets : 2^(Given bits for mask – No. of bits in default mask)
  - No of bits in mask = 25
  - No of bits in default mask = 16
  - **Number of subnets = 2^(25-16) = 2^9 = 512.**
- Number of hosts per subnet : 2^(32 – Given bits for mask) – 2
  = 2^(32-25) – 2 = 2^7 – 2 = 128 – 2 = 126
- Subnet address : AND result of subnet mask and the given IP address
  - **For the first subnet block, we have subnet address = 0.0**
- First Host ID : Subnet address + 1
  - **first host id = 0.1,**
- Last Host ID : Subnet address + Number of Hosts
  - No of hosts = 126
  - **last host id = 0.126**
- Broadcast address : By putting the host bits as 1 and retaining the network bits as in the IP address
  - **broadcast address = 0.127**