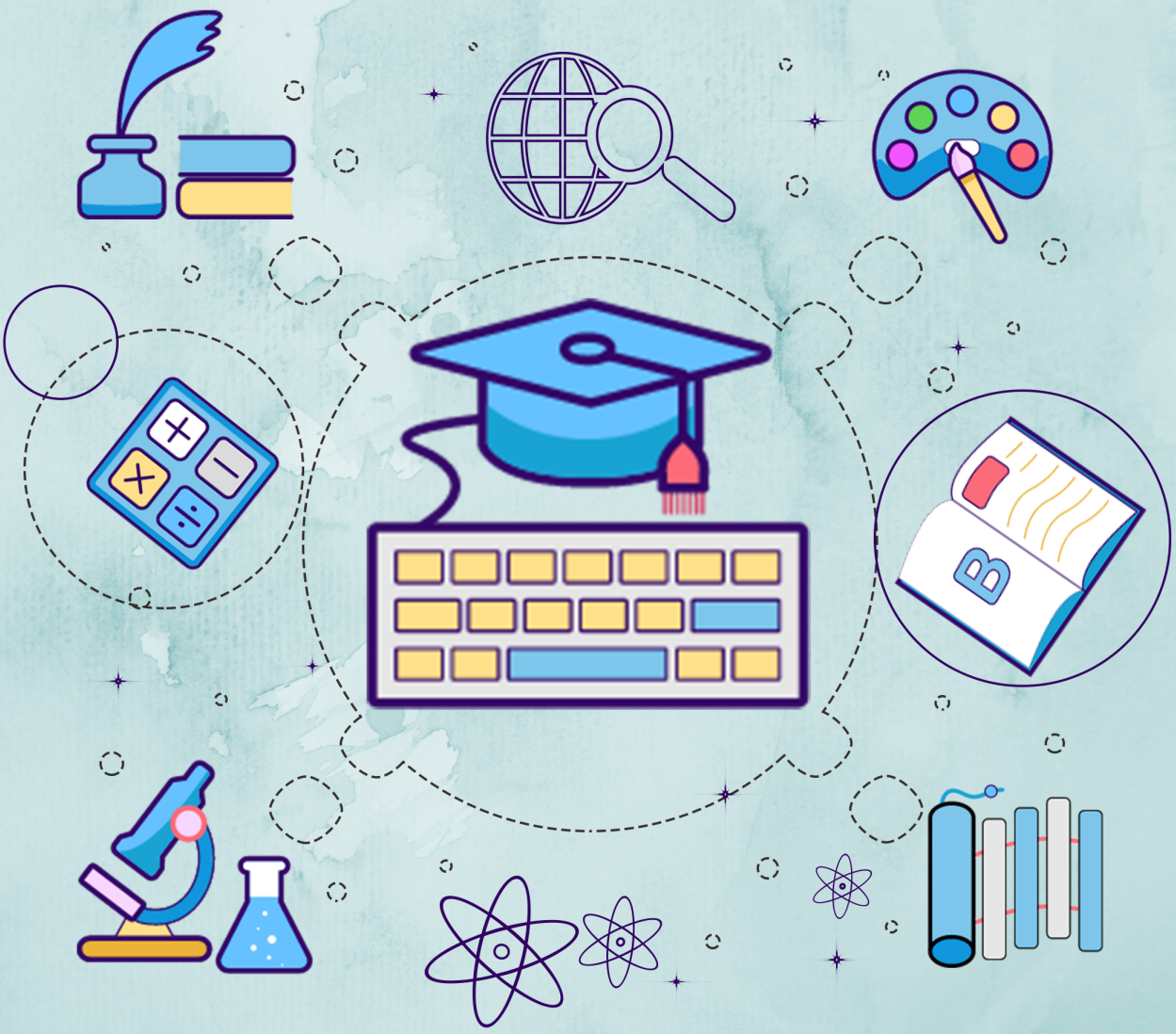
APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

KeralaNotes



SYLLABUS | STUDY MATERIALS | TEXTBOOK

PDF | SOLVED QUESTION PAPERS

www.keralanotes.com

KeralaNotes

KTU STUDY MATERIALS

COMPUTER NETWORKS

CST 303

Module 4

Related Link :

- KTU S5 STUDY MATERIALS
- KTU S5 NOTES
- KTU S5 SYLLABUS
- KTU S5 TEXTBOOK PDF
- KTU S5 PREVIOUS YEAR SOLVED QUESTION PAPER

CN

COMPUTER NETWORKS

Module 4

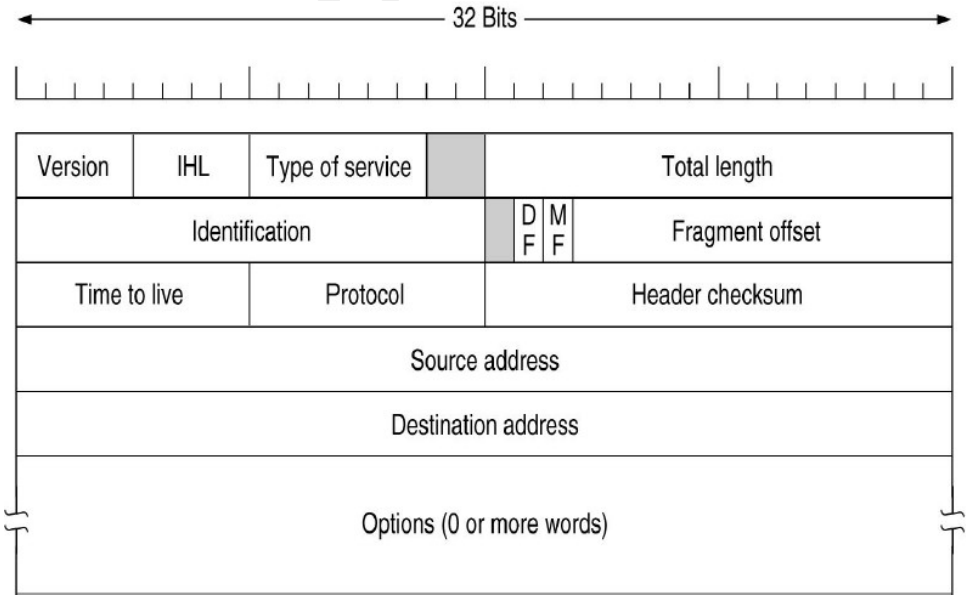
Module – 4 (Network Layer in the Internet)

IP protocol, IP addresses, Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), Bootstrap Protocol (BOOTP), Dynamic Host Configuration Protocol (DHCP). Open Shortest Path First(OSPF) Protocol, Border Gateway Protocol (BGP), Internet multicasting, IPv6, ICMPv6.

IP (Internet Protocol)

- Network layer protocol
- Datagram oriented protocol
- Packets in IP layer are called datagrams. A datagram has 2 parts – header & data

IP Header Structure :-



- ✓ **Version:**
  - Defines the version of IP
  - 4 bit long field
  - IPV4,IPV6
- ✓ **IHL (IP Header length):**
  - Defines length of datagram header
- ✓ **Total length**
  - Defines the total length of IP datagram
  - Length of header as well as data field
- ✓ **Type of service field:**
  - to distinguish between different classesof service
- ✓ **Identification field:**
  - Identifies each datagram from others
- ✓ **DF** stands for Do not Fragment
- ✓ **MF** stands for More Fragments.
- ✓ **Fragment offset**
  - Position of fragment w.r.t the whole datagram
  - Identifies the location of the fragment in a packet
- ✓ **Time to Live**
  - Age, lifetime
- ✓ **Protocol**
  - Defines the high level protocol
- ✓ **checksum**
  - to detect error
- ✓ **Source address**
  - Specifies address of sender
- ✓ **Destination address**
  - Specifies address of the receiving node
- ✓ **options**
  - Extra info, support various options , such as security

The Network Layer in the Internet

- At the network layer, the Internet can be viewed as a collection of sub networks or Autonomous Systems (AS) that are interconnected.
- The glue that holds the whole Internet together is the network layer protocol, IP (Internet Protocol).
- The job of the network layer is to provide a best-efforts way to transport datagram from source to destination

- The important principles used for the network layer design in the network are as follows :-

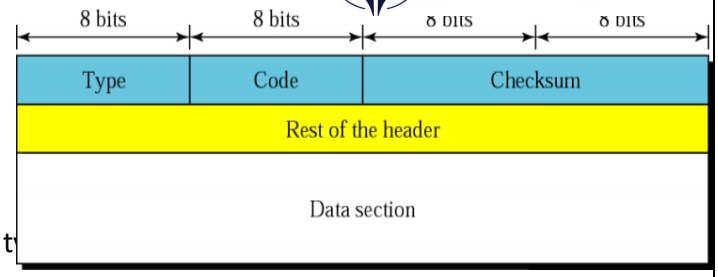
1. Make sure that the design works.
2. Keep the design simple.
3. Make clear choices.
4. Exploit modularity.
5. Expect heterogeneity.
6. Avoid static options and parameters.
7. Look for a good design; it need not be perfect.
8. Be strict when sending and tolerant when receiving.
9. scalability.
10. Consider performance and cost.

- At the network layer, the Internet can be viewed as a collection of sub networks or Autonomous Systems (AS) that are interconnected.
- There is no real structure, but several major backbones exist.
- These are constructed from high-bandwidth lines and fast routers.
- Attached to the backbones are regional (midlevel) networks
- The glue that holds the whole Internet together is the network layer protocol, IP (Internet Protocol).
- The job of the network layer is to provide a best-efforts way to transport datagram from source to destination

ICMP (Internet control message protocol)

- IP provides unreliable and connectionless datagram delivery.
- It was designed this way to make efficient use of network resources.
- The IP protocol is a best-effort delivery service that delivers a datagram from its original source to its final destination. However, it has **2 deficiencies**:
  - ✓ **lack of error control**
  - ✓ **lack of assistance mechanisms.**
- The IP protocol has no error-reporting or error-correcting mechanism. The IP protocol also lacks a mechanism for host and management queries. A host sometimes needs to determine if a router or another host is alive. And sometimes a network administrator needs information from another host or router.
- ICMP has been **designed to compensate** for the above **2 deficiencies**.
- It is a **companion t**o the **IP** protoco1.

❑ **ICMP Message Format =>**



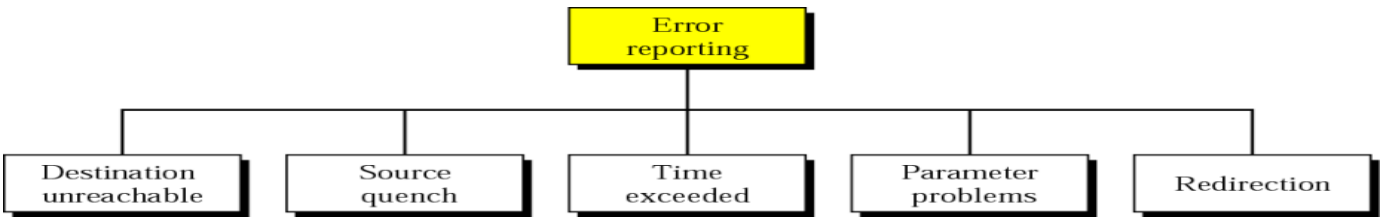
- type, defines the type of the message.
- code field specifies the reason for the particular message t
- checksum field – error calculation.
- The rest of the header is specific for each message type.
- The data section in error messages carries information for finding the original packet that had the error. In query messages, the data section carries extra information based on the type of the query

❑ **ICMP messages** are divided into **2** broad **categories:**

1) error-reporting messages
2) query messages.

1) Error-reporting messages

- One of the main responsibilities of ICMP is to report errors
- ICMP does not correct errors-it simply reports them.
- Error correction is left to the higher-level protocols.
- ICMP always reports error messages to the original source.



❑ **Destination Unreachable**

- When a router **cannot route a datagram** or a host **cannot deliver a datagram**, the datagram is discarded and the

  router or the host sends a destination-unreachable message back to the source host that initiated the datagram.

❑ **Source Quench**

- Host uses source-quench message to **report congestion** to the sender of the datagram.
- This message has two purposes. First, it informs the source that the datagram has been discarded. Second, it warns the source that there is congestion somewhere in the path and that the source should slow down (quench) the sending process.

❑ **Time Exceeded**

- time-exceeded message is generated when not all fragments that make up a message arrive at the destination host within a certain time limit.
- When the time-to-live value reaches 0, the router discards the datagram

❑ **Parameter Problem**

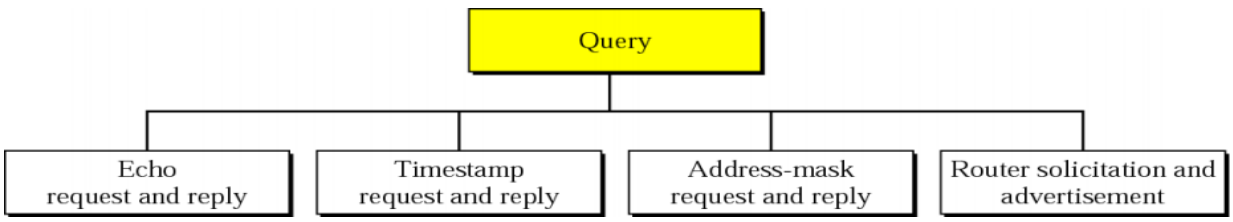
- If a router or the destination host discovers an ambiguous or missing value in any field of the datagram, it discards the datagram and sends a parameter-problem message back to the source.

❑ **Redirection**

- When a router/host send a packet to another network, then it should know ip address of next router. The router must have a routing table to find address of next router & table has to be updated constantly. For such updating ,ICMP sends a redirection message back to its host

2) Query Message

- ICMP can diagnose some network problems. This is accomplished through the query messages



Echo Request and Reply

- utilize this pair of messages to identify network problems. The combination of echo-request and echo-reply messages determines whether two systems (hosts or routers) can communicate with each other.

Address-Mask Request and Reply

- A host may know its IP address, but it may not know the corresponding mask. To obtain its mask, a host sends an address-mask-request message. If the host knows the address of the router, it sends the request directly to the router. If it does not know, it broadcasts the message. The router receiving the address-mask-request message responds with an address-mask-reply message, providing the necessary mask for the host

Timestamp Request and Reply

- Two machines (hosts or routers) can use the timestamp request and timestamp reply messages to determine the round-trip time needed for an IP datagram to travel between them

Router Solicitation and Advertisement

- A host that wants to send data to a host on another network needs to know the address of routers connected to its own network. Also, the host must know if the routers are alive and functioning. The router-solicitation and router-advertisement messages can help in this situation. A host can broadcast (or multicast) a router-solicitation message.
- The router or routers that receive the solicitation message broadcast their routing information using the router- advertisement message.
- Note that when a router sends out an advertisement, it announces not only its own presence but also the presence of all routers on the network of which it is aware.

Message type	Description
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Time stamp request	Same as echo request, but with time stamp
Time stamp reply	Same as echo reply, but with time stamp
Address-mask request and reply	To obtain the mask of IP address and reply provide the necessary mask for the host
Router solicitation	To know the address or routing information of router connected to its own network, by broadcasting router solicitation message
Router advertisement	Reply for router solicitation message broadcast routing information using this message.

ARP – Address Resolution Protocol

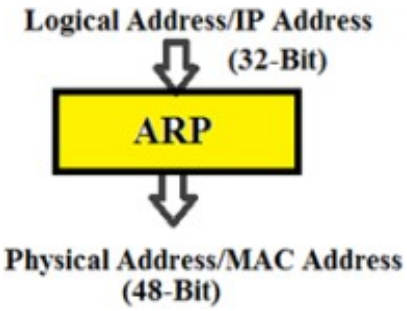
- ARP mapping logical address to

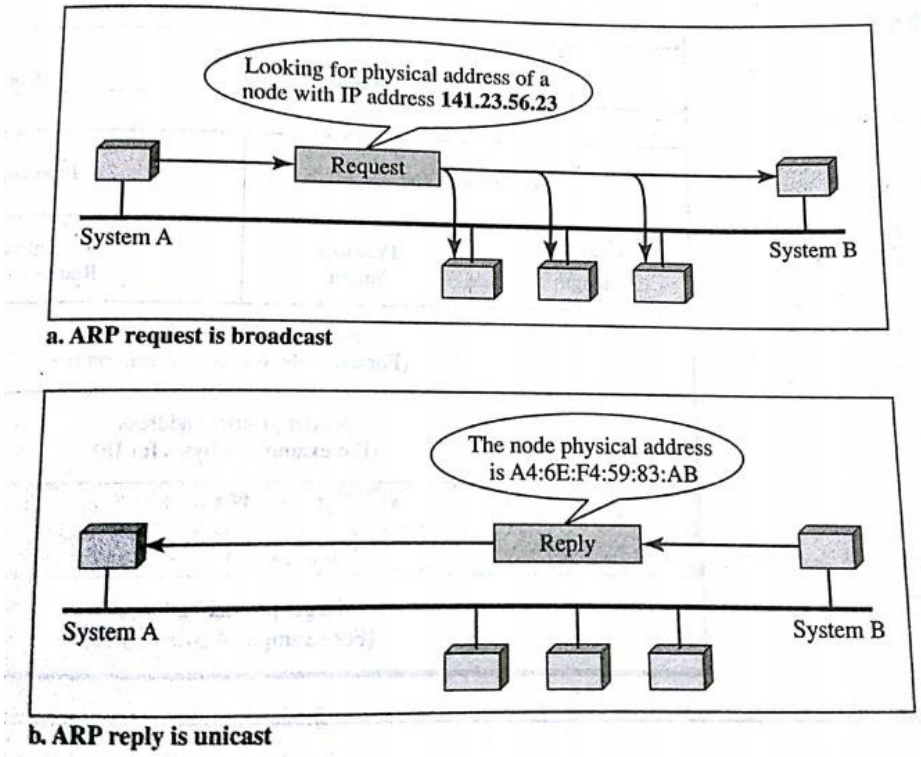
  physicaladdress. logical

  address :IP Address

  physical address : MAC address

ARP Operation:





Neethu Mathew , CSE Dept. EKCTC

- The **router or host**, who wants to find the MAC address of some other router, sends an ARP request packet.
- **ARP request packet** consist of IP and MAC address of sender and IP address of receiver/destination.
- The **request packet** is broadcasted over the network.
- Every host and router on the network receives and processes the ARP request packet.
- But only the intended receiver recognizes its IP address in the request packet and send back an ARP response packet.
- **ARP response packet** contains the IP Physical address of the **receiver**.
- ARP response packet is delivered only to **sender(unicast)**using A's physical address in the ARP request packet.

Neethu Mathew , CSE Dept. EKCTC

ARP Packet Format

Hardware Type (16-bit field)

- Defining the type of the network on which ARP run.

Protocol type

- Defining the Protocol using ARP.

Hardware length (8-bit field)

- Used to define the length of physicaladdress in bytes.

Protocol length

- Define the length of the IP address in bytes

Operation

- Define the type of packet
- The possible type of packets are
    1. ARP Request (field value-1)
    2. ARP Reply (field value-2)

Sender hardware address

- Defining the physical address of the sender.

Hardware Type (16 bits)		Protocol type (16 bits)
Hardware length	Protocol length	Operation request 1, Reply 2
Sender hardware address		
Sender protocol address		
Target hardware address		
Target protocol address		

Sender protocol address

- Defining the logical address of sender.

Target Hardware address

- Define the physical/MAC address of the target.
- For ARP request packet, the field contains all zeros Because the sender doesn't know the receivers physical address or MAC address.

Target protocol address:

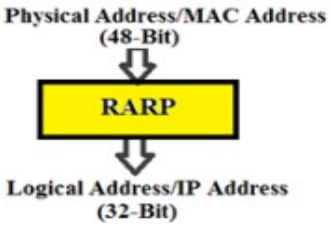
- Define the logical address of the target(IP Address)

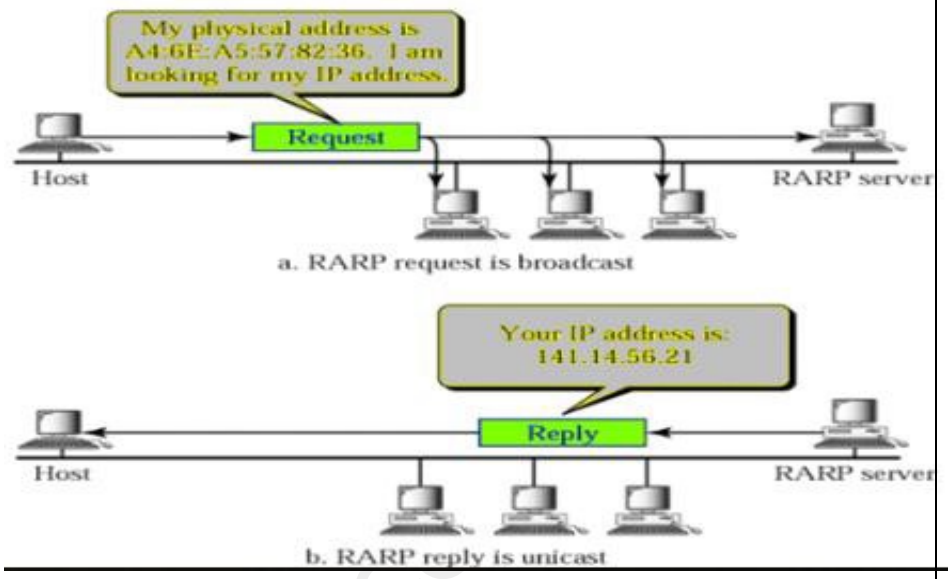
RARP – Reverse Address Resolution Protocol

- RARP mapping physical address to logical address.
- logical address :IP Address , physical address : MAC address
- There are occasions in which a host knows its physical address and unknowns its logical address
- RARP Packet format :

Hardware Type (16 bits)		Protocol type (16 bits)
Hardware length	Protocol length	Operation request 3 reply 4
Sender hardware address		
Sender protocol address		
Target hardware address		
Target protocol address		

RARP operation





Problem of RARP

- Broadcasting is done at the data link layer.
- The physical broadcast address doesn't pass the boundaries of network.
- This means that if an administrator has several networks or several subnets it need to assign a RARP server for each network or subnet.
  - ➢ This is the reason that RARP is almost outdated.
- Two protocols are commonly used for replacing RARP

1) BOOTP

2) DHCP

BOOTP - Bootstrap Protocol

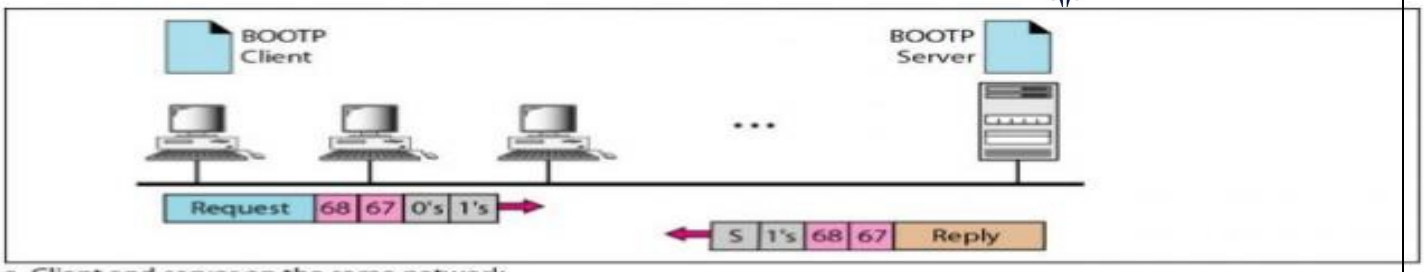
- Mapping **Physical address to logical address**
- BOOTP is a **client/server protocol** designed to provide physical address to logical address mapping.
- BOOTP is an **application layer protocol**, administrator may put the client and server on the same network or on different network.
- BOOTP message are **encapsulated in a UDP packet**, and the UDP packet itself encapsulated in an IP packet.

- The client may unknown about IP address, but it need to send IP datagram.
- The client simply uses all 0's as the source address and all 1's as the destination address.
- One of the advantage of BOOTP over RARP is that the client and server are application layer processes.

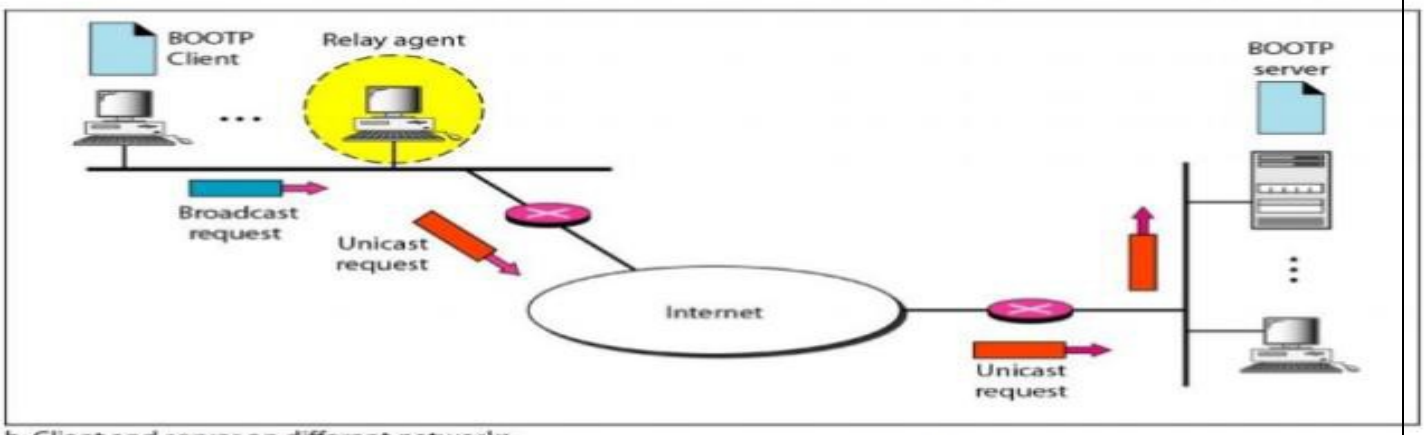
- As in other application-layer processes, a client can be in one network and the server in another, separated by several other networks. However, there is one problem that must be solved.

In client and server on different network:

- The BOOTP request is broadcast because the client does not know the IP address of the server.
- A broadcast IP datagram cannot pass through any router.
- To solve the problem, there is a need for an intermediary.
- One of the hosts can be used as a relay. The host in this case is called a relay agent.
- The relay agent knows the unicast address of a BOOTP server.
- When it receives this type of packet, it encapsulates the message in a unicast datagram and sends the request to the BOOTP server
- BOOTP server know the message comes from a relay agent because one of the field in the request message define the IP address of relay agent.
- The relay agent, after receiving reply, send it to BOOTP client.



a. Client and server on the same network



b. Client and server on different networks

Figure 3.34 BOOTP client and server on the same and different networks

- BOOTP is not a dynamic configuration protocol. When a client requests its IP address, the BOOTP server consults a table that matches the physical address of the client with its IP address. This implies that the binding between the physical address and the IP address of the client already exists. The binding is predetermined. However, what if a host moves from one physical network to another? What if a host wants a temporary IP address? BOOTP cannot handle these situations because the binding between the physical and IP addresses is static and fixed in a table until changed by the administrator. BOOTP is a static configuration protocol.

DHCP :- Dynamic Host Control Protocol

- A network management protocol used to assign ip address to any device
- DHCP has been devised to provide static and dynamic address allocation that can be manual or automatic.

Static Address Allocation

- In this capacity DHCP acts as BOOTP does. It is backward compatible with BOOTP, which means a host running the BOOTP client can request a static address from a DHCP server.
- A DHCP server has a database that statically binds physical addresses to IP addresses.

Dynamic Address Allocation

- DHCP has a second database with a pool of available IP addresses.
- This second database makes DHCP dynamic.
- When a DHCP client requests a temporary IP address, the DHCP server goes to the pool of available (unused) IP addresses and assigns an IP address for a negotiable period of time.

- When a DHCP client sends a request to a DHCP server, the server first checks its static database.
- If an entry with the requested physical address exists in the static database, the permanent IP address of the client is returned.
- On the other hand, if the entry does not exist in the static database, the server selects an IP address from the available pool, assigns the address to the client, and adds the entry to the dynamic database.
- The dynamic aspect of DHCP is needed when a host moves from network to network or is connected and disconnected from a network .
- DHCP provides temporary IP addresses for a limited time.
- The addresses assigned from the pool are temporary addresses.
- The DHCP server issues a lease for a specific time. When the lease expires, the client must either stop using the IP address or renew the lease.
- The server has the option to agree or disagree with the renewal.
- If the server disagrees, the client stops using the address

Manual and Automatic Configuration

- One major problem with the BOOTP protocol is that the table mapping the IP addresses to physical addresses needs to be manually configured.
- This means that every time there is a change in a physical or IP address, the administrator needs to manually enter the changes.
- DHCP, on the other hand, allows both manual and automatic configurations.
- Static addresses are created manually, dynamic addresses are created automatically.

IGMP :- Internet Group Management Protocol

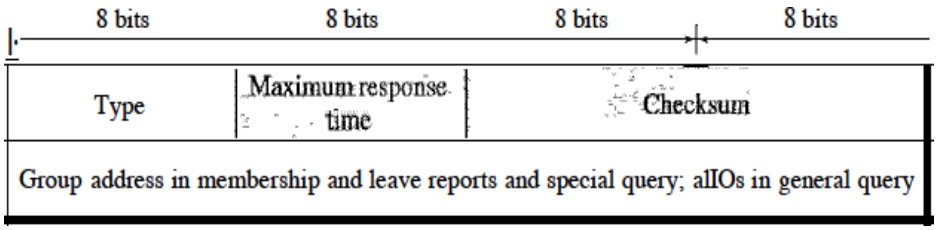
- one of the necessary, but not sufficient protocols that is involved in multicasting.
- IGMP is not a multicasting routing protocol; it is a protocol that manages group membership.
- In any network, there are one or more multicast routers that distribute multicast packets to hosts or other routers
- The IGMP protocol **gives** the **multicast routers information** about the membership status of hosts (routers) connected

  to the network
- IGMP is a group management protocol.
- It helps a multicast router create and update a list of loyal members related to each router interface
- IGMP is a companion to the IP protocol
- IGMP is defined in RFC 1112

❑ IGMP Messages

- IGMP has 2 versions :- IGMPv1 , IGMPv2

❑ IGMP Message Format



✓ **Type:** This 8-bit field defines the type of message

- IGMPv2 has 3 types of messages:
  - the query
  - the membership report
  - the leave report.
- There are 2 types of query messages: general and special
- The value of the type is shown in both hexadecimal and binary notation.

IGMP type field

Type	*Value*
General or special query	0x11 or 00010001
Membership report	0x16 or 00010110
Leave report	0x17 or 00010111

✓ **Maximum Response Time.**

- 8-bit field
- defines the amount of time in which a query must be answered.
- The value is in tenths of a second; for example, if the value is 100, it means 10 s.

✓ **Checksum.**

- 16-bit field
- Error
- The checksum is calculated over the 8-byte message.

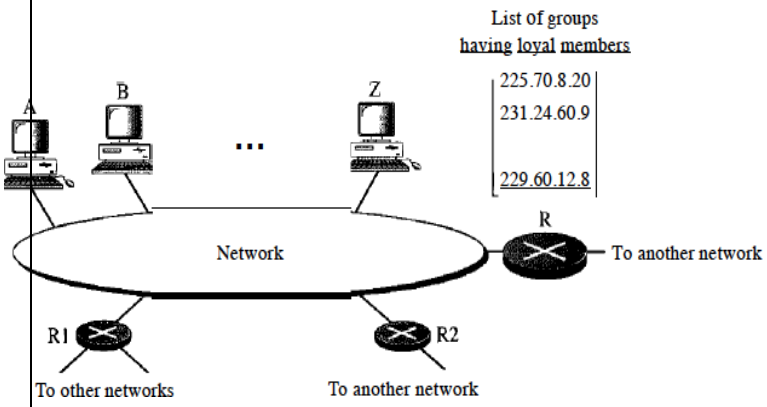
✓ **Group address.**

- The value of this field is 0 for a general query message.
- The value defines the groupid (multicast address of the group) in the special query, the membership report, and the leave report messages

IGMP Operation

- IGMP operates locally.
- In IGMP operation multicast router has a list of multicast addresses of the groups for which the router distributes packets.
- The packets are distributed to groups with at least one loyal member in that network.
- For each group, there is one router. Its duty is to distribute the multicast packets destined for that group.

IGMP operation



Here router R is the distributing router. There are two other multicast routers (R1 and R2) that, depending on the group list maintained by router R, could be the recipients of router R in this network. Routers RI and R2 may be distributors for some of these groups in other networks, but not on this network.

IGMP Operation

❑ **Joining a Group**

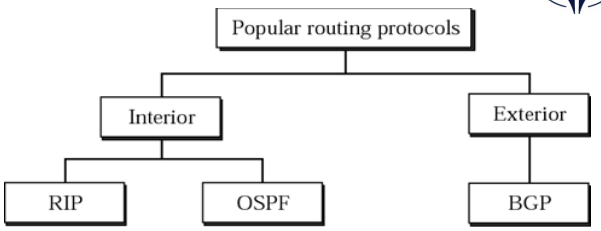
- A host or a router can join a group. A host maintains a list of processes that have membership in a group.
- When a process wants to join a new group, it sends its request to the host
- The host adds the name of the process and the name of the requested group to its list.
- If this is the first entry for this particular group, the host sends a membership report message.
- If this is not the first entry, there is no need to send the membership report since the host is already a member of the group; it already receives multicast packets for this group.
- The protocol requires that the membership report be sent twice, one after the other within a few moments. In this way, if the first one is lost or damaged, the second one replaces it

❑ Leaving a Group

- When a host sees that no process is interested in a specific group, it sends a leave report.
- Similarly, when a router sees that none of the networks connected to its interfaces is interested in a specific group, it sends a leave report about that group
- On receiving the leave report, the multicast router sends a special query message and inserts the groupid, or multicast address, related to the group.
- router allows a specified time for any host or router to respond.
- If, during this time, no interest (membership report) is received, the router assumes that there are no loyal members in the network and purges the group from its list.

❑ Monitoring Membership

- Consider the situation in which there is only one host interested in a group, but the host is shut down or removed from the system. The multicast router will never receive a leave report. How is this handled?
- The multicast router is responsible for monitoring all the hosts or routers in a LAN to see if they want to continue their membership in a group.
- The router periodically (by default, after every 125 s) sends a general query message.
- In this message, the group address field is set to 0.0.0.0. This means the query for membership continuation is for all groups in which a host is involved, not just one
- The general query message does not define a particular group.
- The router expects an answer for each group in its group list; even new groups may respond.
- The query message has a maximum response time of 10 s (the value of the field is actually 100, but this is in tenths of a second).
- query message must be sent by only one router (normally called the query router), also to prevent unnecessary traffic



Interior Routing Protocols

- Passes routing information between routers within Autonomous System(AS).
- Does not need to be implemented outside of the AS.

Exterior Routing Protocols

- Protocol used to pass routing information between routers in different ASs.

(Refer module 3 for RIP, OSPF)

BGP (Border Gateway Protocol)

- BGP is an inter domain routing protocol
- Introduced in 1989
- Based on routing method path vector routing
- has 4 versions.
- A unicast routing protocol
- Exterior Routing Protocols

BGP Header Format

All BGP message types use the basic packet header. Open, update, and notification messages have additional fields, but keep-alive messages use only the basic packet header. Figure 9.81 illustrates the fields used in the BGP header. Each BGP packet contains a header whose primary purpose is to identify the function of the packet in question.

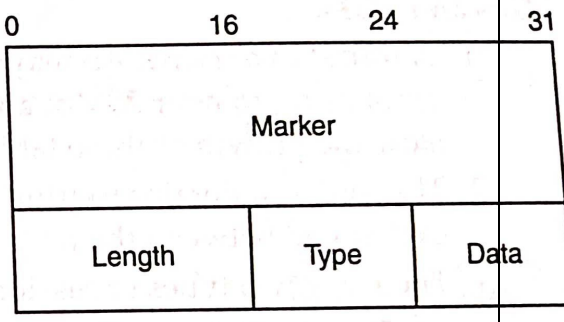


Fig. 9.81. BGP packet header

Marker

Contains an authentication value that the message receiver can predict.

Length

Indicates the total length of the message in bytes. The value of the length field must be betwee 19 and 4096.

Type

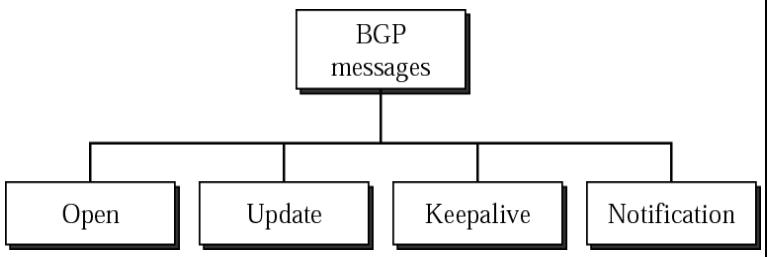
Type specifies the message type as one of the following :

(i) Open
(ii) Update
(iii) Notification
(iv) Keep-alive

Data

Contains the upper layer information in this optional field.

BGP messages - 4 types



❍ OPEN:

- Opens communications between peers
- first message sent by each side after a TCP connection is established
- Authenticates sender

❍ UPDATE:

- provide routing updates to other BGP systems
- Advertises new path (or withdraws old)

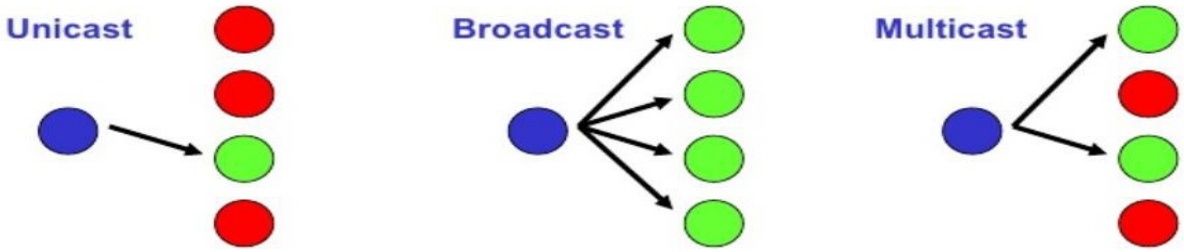
❍ KEEP ALIVE:

- keep BGP connections, ensures neighbours are still alive or active, keep the sessions from expiring

❍ NOTIFICATION:

- notification message is sent when an error condition is detected
- used to Close a connection

- Multicast communications refers to one-to-many communications.



IP Multicasting refers to the implementation of multicast communication in the Internet

Multicast is driven by receivers: Receivers indicate interest in receiving data

- The set of receivers for a multicast transmission is called a **multicast group**
  - A multicast group is identified by a **multicast address**
  - A user that wants to receive multicast transmissions **joins** the corresponding multicast group, and becomes a **member** of that group

- After a user joins, the network builds the necessary routing paths so that the user receives the data sent to the multicast group

Internet Multicasting – IGMP

ICMPv6 :- Internet Control Message Protocol version 6

- Modified version of ICMP.
- This new version follows the same strategy and purposes of version 4.
- ICMPv4 has been modified to make it more suitable for IPv6.
- In addition, some protocols that were independent in version 4 are now part of Internetworking Control Message Protocol (ICMPv6).
- The ARP and IGMP protocols in version 4 are combined in ICMPv6.
- The RARP protocol is dropped from the suite because it was rarely used and BOOTP has the same functionality.

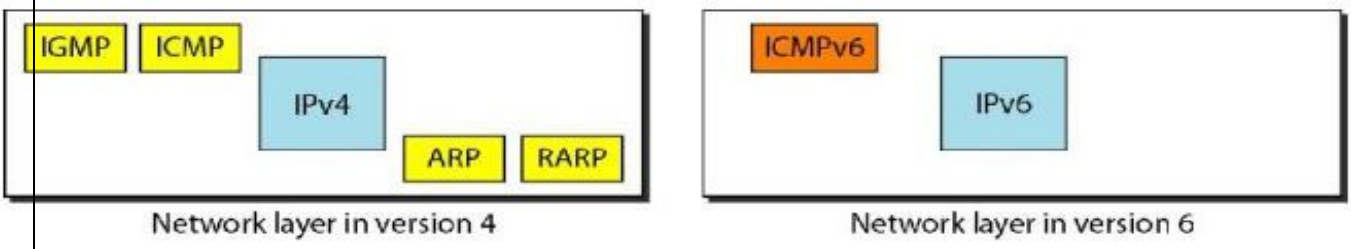


Figure 3.38 Comparison of network layers in version 4 and version 6

ICMPv6 Error Messages

1. "Destination Unreachable" :

- message is generated by the source host or a router when an IPv6 datagram packet cannot be delivered

2. "Packet Too Big" :

- If a router receives a datagram that is larger than the maximum transmission unit (MTU) size of the network through which the datagram should pass, two things happen. First, the router discards the datagram and then an ICMP error packet-a packet-too-big message-is sent to the source.
- MTU (Maximum Transmission Unit) is the size of the largest protocol data unit that is supported over the link.

3. "Time Exceeded" :

- Similar to the Time-to-Live field value in IPv4 datagram header, IPv6 header includes a Hop Limit field.
- The Hop Limit field value in IPv6 header is used to prevent routing loops.
- 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.

4. "Parameter Problem" :

- message is typically related with the problems and mistakes related with IPv6 header itself.
- 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.

5. Redirection

The purpose of the redirection message is the same as described for version 4

❑ **ICMPv6 query messages**

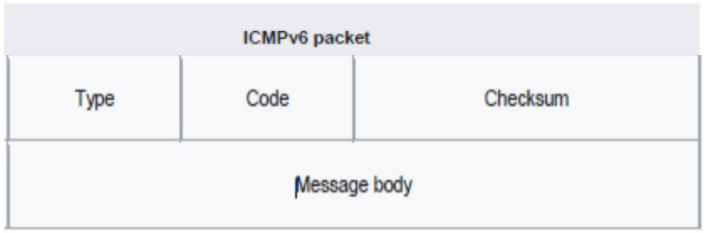
1. **echo request and reply**
2. **router solicitation and advertisement**
3. **neighbor solicitation and advertisement**
   - the network layer in version 4 contains an independent protocol called Address Resolution Protocol (ARP). In version 6, this protocol is eliminated, and its duties are included in ICMPv6. The idea is exactly the same, but the format of the message has changed.
4. **group membership**
   - network layer in version 4 contains an independent protocol called IGMP. In version 6, this protocol is eliminated, and its duties are included in ICMPv6. The purpose is exactly the same

Comparison of query messages in ICMPv4 and ICMPv6

Type of Message	*Version 4*	*Version 6*
Echo request and reply	Yes	Yes
Timestamp request and reply	Yes	No
Address-mask request and reply	Yes	No
Router solicitation and advertisement	Yes	Yes
Neighbor solicitation and advertisement	ARP	Yes
Group membership	IGMP	Yes

Comparison of error-reporting messages in ICMPv4 and ICMPv6

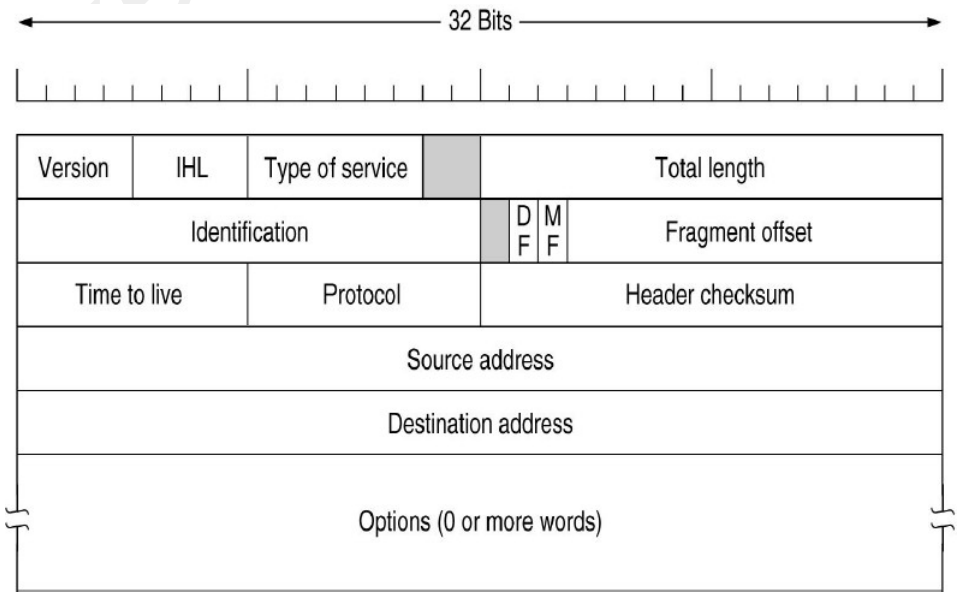
Type of Message	*Version 4*	*Version 6*
Destination unreachable	Yes	Yes
Source quench	Yes	No
Packet too big	No	Yes
Time exceeded	Yes	Yes
Parameter problem	Yes	Yes
Redirection	Yes	Yes



IPv4

- IPv4 address is a 32-bit address
- IPv4 addresses are unique & universal

IP Header format :-



- ✓ **Version:**
  - Defines the IP version used
  - 4 bit long field
- ✓ **IHL (IP Header length):**
  - Defines length of datagram header
- ✓ **Total length**
  - Defines the total length of IP datagram
  - Length of header as well as data field
- ✓ **Type of service field:**
  - to distinguish between different classes of service
- ✓ **Identification field:**
  - Identifies each datagram from others
- ✓ **DF** stands for Do not Fragment
- ✓ **MF** stands for More Fragments.
- ✓ **Fragment offset**
  - Position of fragment w.r.t the whole datagram
  - Identifies the location of the fragment in a packet
- ✓ **Time to Live**
  - Age, lifetime
- ✓ **Protocol**
  - Defines the high level protocol
- ✓ **checksum**
  - For error checking
- ✓ **Source address**
  - Specifies address of sender
- ✓ **Destination address**
  - Specifies address of the receiving node
- ✓ **options**
  - Extra info, support additional options , such as s ecurity

IPv4 addresses

- An IPv4 address is a **32-bit address**
- **IPv4 addresses are unique**
- They are unique in the sense that each address defines one, and only one, connection to the Internet. Two devices on the Internet can never have the same address at the same time
- universally defines the connection of a device (for example, a computer or a router) to the Internet
- if a device operating at the network layer has m connections to the Internet, it needs to have m addresses. We will see later that a router is such a device.
- The **IPv4 addresses are universal** in the sense that the addressing system must be accepted by any host that wants to be connected to the Internet

Address Space

- A protocol such as IPv4 that defines addresses has an address space.
- An address space is the total number of addresses used by the protocol.
- If a protocol uses N bits to define an address, the address space is 2^Nbecause each bit can have two different values

  (0 or 1) and N bits can have 2^N values.
- IPv4 uses 32-bit addresses, which means that the address space is 2^{32} or 4,294,967,296 .

Notations

There are 2 notations to show an IPv4 address:

- binary notation
- dotted-decimal notation.

Limitations of IPv4

- Most obvious limitation is its address field. IP address relies on network layer addresses to identify end points on

  networks, and each networked device has a unique address
- Uses a 32 bit addressing scheme, which gives 4 billion possible addresses.
- Complex host & router configuration
- Non hierarchical addressing
- Difficulty in re-numbering addresses
- Large routing table

To overcome these problems**, IPv6** was proposed

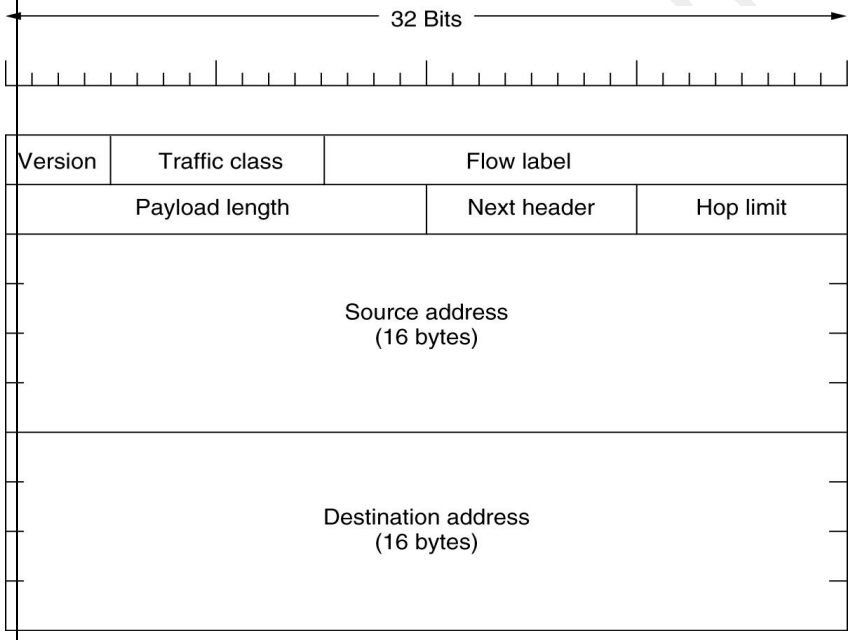
IPv6

- Next generation internet Protocol designed as a successor to IPv4
- Overcoming many of the weakness of IPv4
- 128 bit address space

Advantages

- Larger address space
- Better header format
- New options added to increase the functionality
- Possibility of extension
- More security
- Support to resource allocation
- Plug and play
- Clearer specification & optimization

IPv6 Packet format :



base header :-

✓ **Version :**

- 4 bit field
- Indicates version of IP
- It is always 6 for IPv6

✓ **Traffic Class :**

- 8 bit field
- indicates class or priority of IPv6 packet
- It helps routers to handle the traffic based on priority of the packet.
- If congestion occurs on router then packets with least priority will be discarded.

Each packet consist of a base header which is mandatory followed by the payload. Payload is made up of 2 parts- extension headers & data from an upper layer

✓ **Flow Label :**

- Routers use the value in the flow label field to route the datagram.
- Provide special handling for a particular flow of data

✓ **Payload Length :**

- It is a 16-bit field
- Define total length of IP datagram
- indicates total size of the payload which tells routers about amount of information a particular packet contains in its

  payload.

✓ **Next Header :**

- 8 bit field
- Indicates type of extension header(if present) immediately following the IPv6 base header.
- Whereas In some cases it indicates the protocols contained within upper-layer packet, such as TCP, UDP.

✓ **Hop Limit :**

- This field is same as TTL (Time To Live) in IPv4 packets.
- 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 packet is discarded if value

  decrements to 0.

✓ **Source Address :**

- 128-bit IPv6 address of the original source of the packet.

✓ **Destination Address :**

- 128-bit IPv6 address of the final destination

❖ **Extension header**

- Give more functionality to IP datagram
- Six kinds of extension headers are defined at present

Extension header	Description
Hop-by-hop options	Miscellaneous information for routers
Destination options	Additional information for the destination
Routing	Loose list of routers to visit
Fragmentation	Management of datagram fragments
Authentication	Verification of the sender's identity
Encrypted security payload	Information about the encrypted contents

❑ **IPv6 address**

- An IPv6 address consists of 16 bytes (octets); it is 128 bits long
- To make addresses more readable, IPv6 uses hexadecimal colon notation. In this notation, 128 bits is divided into eight sections, each 2 bytes in length. Two bytes in hexadecimal notation requires four hexadecimal digits. Therefore, the address consists of 32 hexadecimal digits, with every four digits separated by a colon

❑ **IPv6 – 3 different categories of address**

1. *Unicast address*
2. *Multicast address*
3. *Anycast address*

- Unicast address : A unicast address defines a single computer. The packet sent to a unicast address must be delivered to that specific computer
- Multicast address: Multicast addresses are used to define a group of hosts instead of just one. A packet sent to a multicast address must be delivered to each member of the group
- Anycast address: packet destined for an anycast address is delivered to only one of the members of the anycast group, the

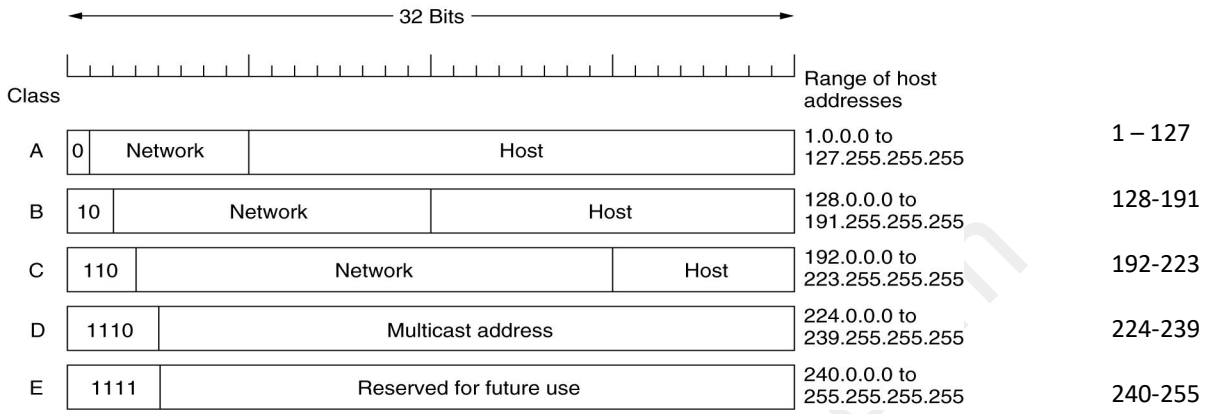
  nearest one (the one with the shortest route)

Comparison :- IPv4 & IPv6

IPv4	IPv6
32 bit address space	128 bit address space
Address Representation in decimal	In hexadecimal
2^{32}possible ways to represent address	2^{128}ways
Packet flow identification : not available	Available and uses flow label field in the header
Checksum Field :Available	Not available
Has 5 different classes of IP address	Does Not contain classes of IP address
End-to-end connection integrity: Unachievable	achievable
Security features: Security is dependent on application	IPsec is inbuilt in the IPv6 protocol
DHCP or manual configuration	Does not require DHCP or manual configuration
Header includes options	All optional data moved to IPv6 extension headers
Not Provide Encryption and Authentication	Provide Encryption and Authentication

IP address

- Every host & router on the internet has a unique IP address
- IP address consist of 2 parts : network number & host number
- IP address is divided into 5 categories. This allocation was called **classful addressing**



Find the class of each address.

a. 00000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

c. 14.23.120.8

d. 252.5.15.111

Solution

a. The first bit is 0. This is a class A address.

b. The first 2 bits are 1; the third bit is 0. This is a class C address.

c. The first byte is 14 (between 0 and 127); the class is A.

d. The first byte is 252 (between 240 and 255); the class is E.