KTU NOTES

The learning companion.

KTU STUDY MATERIALS | SYLLABUS | LIVE NOTIFICATIONS | SOLVED QUESTION PAPERS

Module V

Internet Control Protocols

Internet control protocols

Internet protocol (IP) provides unreliable and connectionless datagram delivery which means it has no error-reporting or error correcting mechanism.

ie, Ip protocol has no built in mechanism to notify or correcting error. when error happens, router must discard the datagram

∴ In addition to IP, Internet control protocols are used in Network layer for flow control & error control. by the use of Internet control protocol we can make a relaliable data delivery.

- Important Internet control protocols are.

1) ICMP (Internet control Message protocol)
2) ARP (Address Resolution protocol)
3) RARP (Reverse address Resolution protocol)
4) BOOTP (Bootstrap protocol)
5) DHCP (Dynamic Host Configuration protocol)

ICMP (Internet control Message protocol)

The Internet control Message protocol has been designed to compensate deficiencies of Internet protocol (IP).

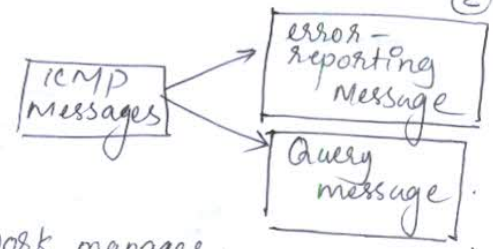
- Defficiencies of IP
  1) Ip protocol has no error-reporting or error correcting Mechanism.
  2) Ip protocol also lacks a mechanism for host and management queries.

∴ ICMP is a companion to the IP protocol.

- when something unexpected occure, the event is reported by ICMP, which is also used to test the Internet.
- ICMP messages are divided into two broaid categories.
  1) error-reporting Message.
  2) Query Message.

(2)

* Error-reporting Message report problems that a router or a host (destination) may meet unexpected when it processes an I/p packet.



* The Query messages, help a host or a network manager to get specific information from a router or another host.

Eg:- Query messages are used, if ~~need~~ a node need redirect it message.

Error reporting

- One of the main responsibility of ICMP is to report errors.
- ICMP does not correct error - it simply reports them (Error correction can be done by high-level protocols).
- ICMP always reports error messages to the Orginal source.
- Five types of errors are handled by ICMP.
  1) Destination unreachable 2) Source Quench
  3) time exceeds 4) parameter problem 5) Redirection.

Message type	Description
Destination unreachable	Packet could not be delivered
Source quench	Choke packet
time exceeds	Time to live field bit '0'
Parameter problem	Invalid Header field
Redirection	Teach a router about geography

Note:-

1) No ICMP error message will be generated in response to a datagram carrying an ICMP error message.

2) No ICMP error message will be generated for a fragmented datagram that is not the first fragment

3) No ICMP error message will be generated for a datagram having a multicast address.

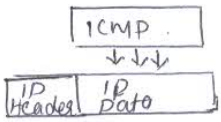
4) No ICMP error message will generated for a datagram having a special address such as 127.0.0.0 or 0.0.0.0.

Query message

In addition to error reporting, ICMP can diagnose some network problems. This is accomplished through the Query messages.
- a group of four diffrent pairs of messages are used for Query messaging.

1) Echo request & reply.
2) Timestamp request & Reply.
3) Address-mask request & Reply.
4) Router solicitation & advertisement.

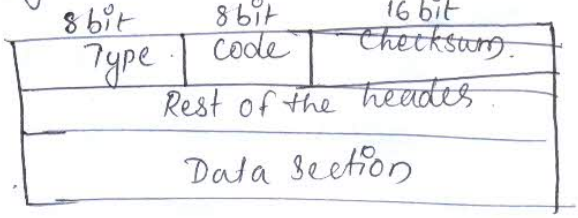
- In query message, a node send a message to destination and a answer message in a specific format by destination to source.
- A query message is encapsulated in an IP packet. (for Transmission)



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

Message-frame-format

An ICMP message has an 8-byte header and variable-size data section.



type:- define the type of message.

Type 3 :- Destination unreachable
Type 4 :- Source quench
Type 11 :- Time exceeded
Type 12 :- parameter problem
Type 5 :- Redirection.

Type 8 and 0 :- Echo request & Reply
Type 13 and 14 :- Timestamp request & Reply
Type 17 and 18 :- Address-mask request and reply
Type 10 and 9 :- Router solicitation and advertisement.

Code :- The code field specifies the reason for the particular message type.
Checksum :- error calculation, In ICMP the checksum is calculated over the entire message (header and data).
Rest of the header :- depends on diffrent messages, (specific for each message type)
The data section :- The data section in error message carries information for finding the orginal packet that had the error. In query messages the data section carries extra information based on the type of query.

* ARP (The address resolution Protocol)

An Internet is made of a combination of physical Network connected by internetworking devices such as routers. A packet starting from a source host may pass through several diffrent physical networks before finally reaching the destination host. The host and routers are recognized at the network level by their logical address (IP).
- every machine on the Internet has one (or more) IP address. these cannot actually be used for sending packet because the data link layer hardware does not understand Internet address (IP address)

two type of address for Computer Network
- IP address (logical address)
- MAC address (physical address)

- At the physical level, the IP address is not useful but the hosts and routers are recognized by their MAC address.
- A Mac address is a local address.
- The IP and MAC address are two diffrent identifiers and both of them are need
- A example of physical address is the 48-bit MAC address in the Ethernet protocol, which is imprinted on the NIC in the host or router

- The physical address and the logical address are two diffrent identifiers we need both because in Internet we deal with data link layer protocols and Network layer protcol. (data link layer protocol use physical address & Network layer use logical address)

Eg:- Ethernet (or LAN) can have two diffrent protocols. at network layer IP and data link layer Ethernet protocol

- This means that delivery of a packet to a host or router require two level of addressing, logical & physical addressing
  - we need to able to map a logical address to its corresponding physical address and vice versa.

Address mapping < static mapping / Dynamic mapping.

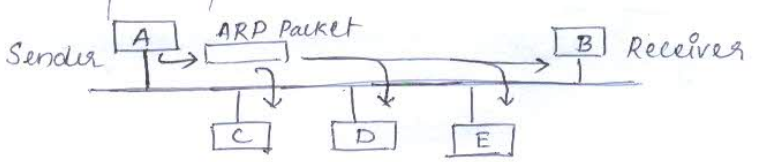
* Static mapping:- A table is created and stored in each machine This table is associates an ip address with a MAC address.
  - If a machine know ip address of another machine then it can search for corresponding MAC address in its table.
  - The limitation of statical mapping is that the MAC address can change.
  - TO implement statical mapping, the static mapping table need to be updated periodically.

* Dynamic mapping :- In dynamic mapping technique, a protocol is used for finding the other address. If one type of address is known.
  - There are two protocols designed to perform the dynamic mapping.
    1) ARP (address resolution protocol)
    2) RARP (Reverse address resolution protocol)

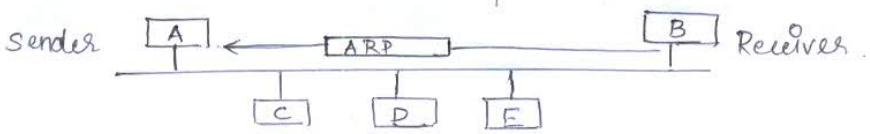
Mapping logical to physical address: (ARP)

ARP is used to mapping logical to physical address mapping.

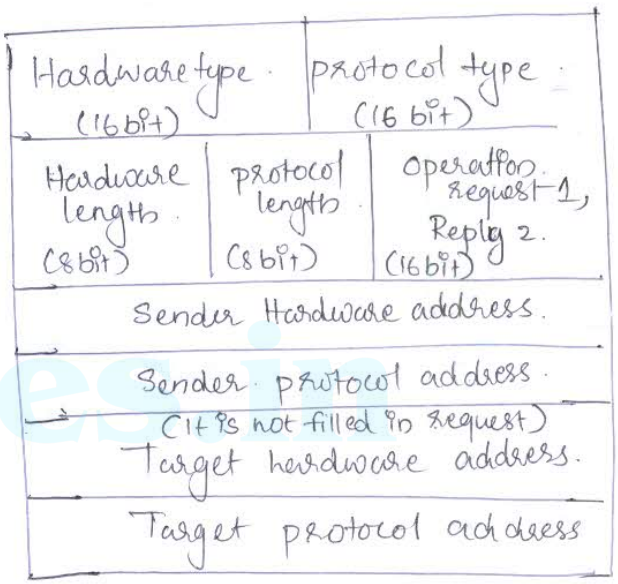
- The router or host, who wants to find the MAC address of some other router, sends an ARP request packet.
  - ARP request packet consist of IP and MAC address of sender and ip address of receiver/destination.
- The request packet is broadcasted over the network.



- Every hosts and router on the network receives and processes the ARP request packet. But only the intended receiver recognize its IP address in the request packet and send back an ARP response packet.
- ARP response packet contains the IP and physical address of the receiver
- ARP response packet is delivered only to sender (unicast) using A's physical address in the ARP request packet.



ARP packet format



Hardware type (16 bit field)
- defining the type of the network on which ARP run.
- ARP can run on any physical N/w.

protocol type (16 bit field)
- defining the protocol using ARP
- ARP can be used with any higher-level protocol.

Hardware length (8 bit field)
- used to defining the length of physical address in bytes.
  Eg:- value is 6 for Ethernet.

Protocol length (8 bit field)
- define the length of the IP address in bytes. Eg:- IPV4 — 4

Operation (16 bit field)
- define the type of packet.
- The possible type of packets are 1) ARP request & 2) ARP reply.

Sender Hardware address
- defining the physical address of the sender. The length of this field is variable.

Sender protocol address
- defining the logical address of sender. the length is variable.

Target Hardware address
- define the physical address of the target. It is a variable length field
- for ARP request packet the field contains all zeros because the sender does not know the receivers physical address.

Target protocol address.
- define the logical address of the target. It is a variable length field.

* An ARP packet (request or reply) is encapsulated directly into the data link-frame in the Data field. and the type field of data link layer frame indicate that data carried by the frame is an ARP request or reply packet.

Operation of ARP on Internet

The services of ARP can be used under the following working conditions when it is being operated on Internet

1. The sender is a host and wants to send a packet to another host on the same network.
2. The Sender is a host and wants to send a packet to another host on another network.
3. The sender is a router which has received a datagram destined for a host on another network.
4. The Sender is a router that has received a datagram destined for a host in the same network.

Operation

Step ① :- The sender know the IP address of the target & Internet protocol asks ARP to create an ARP request message

Step ② :- The message is passed to the data link layer where it is encapsulated in a frame by using the physical address of the sender as the source address and the physical broadcast address as the destination address

Step ③ :- Every host or router receives the frame, The target machine only accept the packet (frame) because it can only recognize its IP address.

Step ④ :- The target machine replies with an ARP reply message that contains its physical address. This message is unicast

Step ⑤ :- The sender receives the reply message. It now know the physical address of the target machine.

Step (6) :- The IP datagram, which carries data for the target machine is now encapsulated a frame and is unicast to the destination.

* Mapping physical to Logical address : RARP, BOOTP and DHCP

There are occasions in which a host knows its physical address and unknow its logical address. This may happen in two case.

1) A diskless station is just booted. The station can find its physical address by checking its interface, but it does not know its IP address.

2) An organization does not have enough IP address to assign to each stations; it needs to assign IP addres on demand. The station can send its physical address and ask for a short time lease.

RARP (Reverse address Resolution protocol).

RARP finds the logical address for a machine that knows only its physical address.

- The IP address of a machine is usually read from its configuration file stored on a disk file.
- a diskless machine is usually booted from ROM, which has minimum booting information. The ROM is installed by the manufacture. It can't include the IP address because IP address on a network are assigned by the network administrator.

* The machine can get its physical address, which is unique locally (by reading its NIC). It can then use the physical address to get the logical address by using the RARP protocol.

- A RARP request is created and broadcast on the local network.
- Another machine on the local network that knows all the Ip addresses will respond with a RARP reply.
- The requesting machine must be running a RARP client program and the responding machine must be running a RARP server program.

Problem of RARP.

Broadcasting is done at the data link layer. The physical broadcast address, (all 1's in the case of Ethernet) does not pass the boundaries of network. This means that

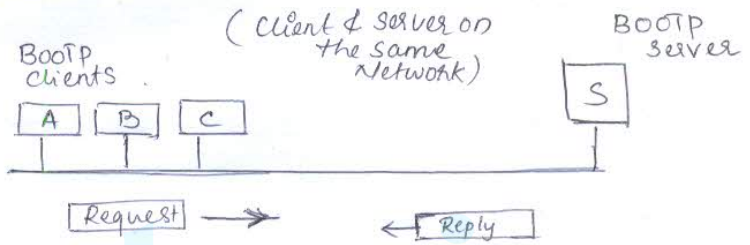
If an administrator has several networks or several subnets. It need to assign a RARP server for each network or subnet.

- This is the Reason that RARP is almost out dated

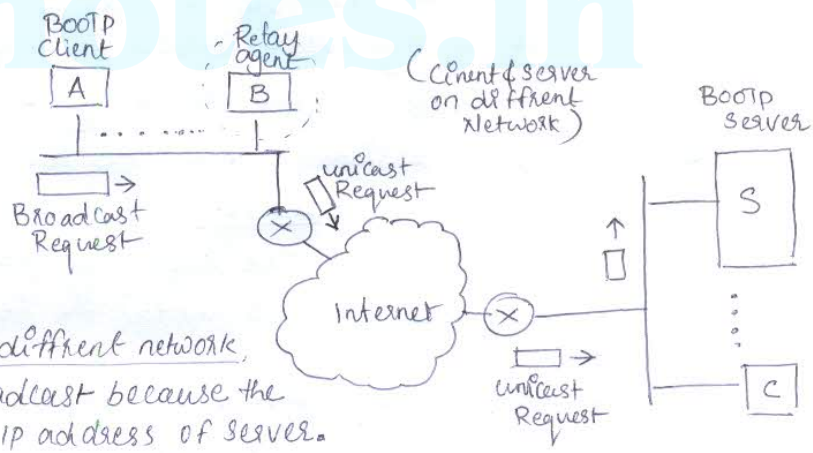
- Two protocols are commonly used for replacing RARP,
  1) BOOTP 2) DHCP.

* BOOTP (Bootstrap protocol)

- The Bootstrap protocol (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 diffrent 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 use all 0s as the source address and all 1s as the destination address.



* One of the advantage of BOOTP over RARP is that the client and server are application layer processes.



- In client and server on diffrent network, The BOOTP request is bradcast because the client does not know the IP address of server. A broadcast IP datagram cannot pass through any router, so there is a need for an intermediary. One of the host can be used as a relay (Relay agent) The Relay agent know the unicast address of BOOTP server.
  - When Relay agent receives BOOTP request packet, it encapsulate the message in a unicast datagram and send 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.

DHCP (Dynamic Host configuration protocol)

BOOTp is not a dynamic configuration protocol. ~~BOOTP Server~~. when a client request it 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 client already exist. The binding is predetermind.

* The Dynamic Host configuration protocol (DHCP) has been devised to provide static and dynamic address allocation that can be done by manual or automatic.

Static address allocation :- In this case DHCP acts as BOOTp does.
- a host running client can request a static address from a DHCP server
- A DHCP server has a database that statically binds the physical address to Ip addersses.

Dynamic Address allocation :- DHCP has a second database with a pool of available Ip addresses. This second data base make DHCP dyneumic.
- when a DHCP client request a temporeary Ip address, the DHCP server goes the pool of available (unused) Ip addresses and assign an Ip address for a negotiable period of time.
  - DHCP provide temporeary Ip addresses for a limited time.
- The address assigned from the pool are temporeary addresses. The DHCP server issue a **Lease** for a specific time.
  - when the lease expires, the client must either stop using the Ip address. or renew the lease.

* DHCP allow both manual and automatic configurations.

Static address are created manually.
dynamic address are created automatically

Internet Multicasting

The Ip protocol can be involved in two types of communication
1) unicasting 2) Multicasting.

unicasting is the communication between one sender and one receiver. (one-to-one communication).
Multicasting; send the same message to a large number of receivers simultaneously. (one-to-many communication)

Examples of multicasting application, 1) Multiple Stockbrokers can simultaneously be informed of change in stock price. 2) Travel agents can be informed of plane cancellation. 3) distance learning 4) Video-on-demand etc.

* Ip support multicasting, using class D addresses.
Two kind of group address are supported.
1) permanent 2) Temporary.

- The Internet Group Mangement Protocol (IGMP) is one of the necessary, but not sufficient Protocol that is involved in multicasting
- IGMP is a companion to the Ip protocol.

* Multicasting environment uses multicast packets. Hence, in an internet, we need the router which are able to route multicast packets.
The routing tables of these routers should be updated using a multicasting routing protocols.
  - IGMP is not a multicast routing protocol
  - IGMP ~~manages~~ Manages the group membership.

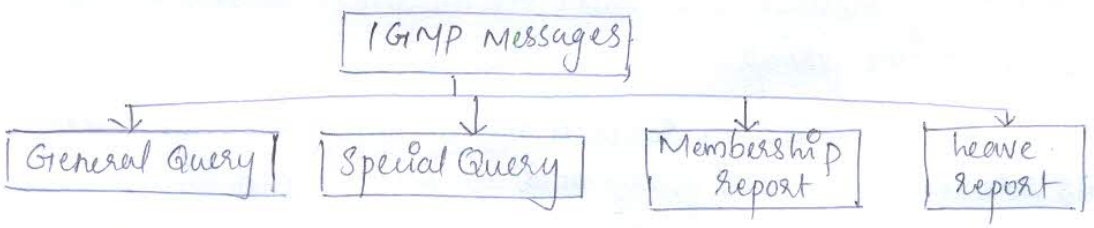
* IGMP is group Mangement protocol. It helps a multicast router to create and update a list of loyal members related to each router interface.

IGMp Messages.

IGMp has two versions < IGMPv1, IGMPv2 (Commonly used)

In IGMPv2 has three type of messages
1) Query 2) Membership Report 3) Leave ~~Leave~~ Report

There are two type of Query messages < 1) general Query, 2) Special Query



IGMp Message Format

(8bit) Type	Maximum Response time (8bit)	Checksum (16 bit)
Group address in membership and leave reports and special query all 0s in general Query		

Type :- (8 bit field) defines the type of message

Maximum Response Time (8 bit)
- field define the amount of time in which a query must be answered.
- The value is in tenths of a second.
  Eg:- 100 value – 10s
- Non zero value in Query messages & set zero in Membership report & leave report message type

Type	value
General or Special Query	– 00010001
Membership Report	– 00010110
leave Report	– 00010111

Checksum (16 bit)
field carrying the checksum. The checksum is calculated ove the 8-byte messages.

Group address.
- The value of this field is '0' for 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.

Operation of IGMP
In IGMP operation, Multicast router has a list of multicast addresses of the groups for which the router distributes packets. The packet 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.

* A host or a router can join a group by the use of Membership report message, the membership report need to be sent twice one after the other within a few moments, so that even if the first one is lost or damaged the second one can be used.

* A host or a router can leave a Group by the use of leave report message. On receiving the leave report, the multicast router sends a Special Query message and insert the multicast address or group ID related to the group.

* The router periodically sends a general Query message after every 125 seconds. The general query field is set 0.0.0.0 and the router will expect an answer from each group in its list. general Query message is used for monitoring membership. The maximum response time allowed for this message is 10sec.

Exterior Gatway Routing Protocol

the Internet is made up of a large number of autonomous system (or subnet). A routing algorithm within an autonomous system (AS) is called Interior gatway protocol and an algorithm for routing between ASes is called Exterior Gatway Routing protocol

- Example for Interior gatway protocol is OSPF (Open Shortest path First) and Example for Exterior Gatway Routing protocol is BGP (Border Gatway protocol)

BGP (The Exterior Gatway Routing Protocol)

BGP → Border Gatway protocol.

Routing between Autonomous Systemes (ASes), BGP is used.

- Goals of an Interior and exterior routing are not same. All an Interior gatway protocol has to do is move packet as effecienty as possible from the source to destination. It does not have politics.

Exterior gatway protocol routers have to worry about politics. Exterior gatway protocols in general and BGP in particular have been designed to allow many kind of routing policies to be create inter AS traffic.

- Typical policies involve political, security or economic consideration.

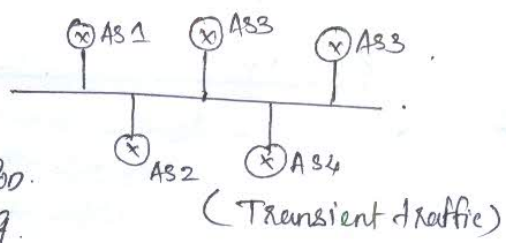
Eg:- Traffic starting or ending at IBM should not transit Microsoft.

type of autonomous systems (used in BGP) divide into three categories. 1) Stub 2) Multihomed 3) Transit

Stub AS. :- A stub AS has only one connection to another AS.

Multihomed :- A multihomed AS has more than one connection to other ASs,

Transit AS :- A transit As is a multihomed AS that also allows transient traffic.



* Pair of BGP routers communicate with each other by establishing Tcp connection. Operating this way provide reliable communication and hides all the details of the network being passed through.
* BGP is fundamentally a distance vector protocol, but quite different from most other DVP.
  - BGP router tells its neighbors the exact path it is using

- The exchange of routing information between two router using BGP take place in a session : — BGP session.
- BGP can have two type type of sessions.

BGP session < External BGP (E-BGP)
Internal BGP (I-BGP)

E-BGP session is used to exchange information between two speaker nodes belonging to two diffrent autonomous system. (Speaker node – Gateway)

I-BGP session, is used to exchange routing information between two routers inside an autonomos system.

IPv6 (Internet protocol version 6.)

- IPv6 is the next generation Internet protocol designed as a successor of the IP version 4.
- IPv6 was designed to enable hig-performance, scalable Internet. This was achieved by overcoming many of weaknesses of IPv4 protocol and adding several new features.

Advantages of IPv6

1) Larger address space : IPv6 has 128-bit address space. (4 times wider in bits in compared to IPv4)
2) Better Header Format
3) New options : IPv6 to increase the functionality.
4) possibility of Extension :
5) More Security : IPv6 includes encryption of packet and authentication of sender of packets.
6) Support to Resource Allocation.
7) Plug and play
8) Clearer specification and optimization.

An IPv6 Packet Format

* The IPv6 packet consists of a base header which is mandatory followed by the payload.

- payload is made up of two parts.
  1) optional extension header and
  2) Data from an upper layer.
- The base header is 40 byte length whereas the extension header and data from upper layer contain upto 65,535 bytes of information.

VER (version) (4 bit field) field defines the version of IP such as IPv4 or IPv6, For IPv6 the value is 6

PRI (Priority) (4bit) field)
- fied define the priority of the packet which is important in connection with the traffic congestion. Sometimes this field is called Traffic class.

Flow Label (24 bit – 3 byte)
fied which is designed for providing special handling for a particular flow of data. (special treatment packet)

Payload length (2 byte)
field is used to define the total length of the IP datagram excluding the base header.

Nent Header (8 bit)
define the header which follow the base header in the datagram.
- Nent header tell which transport protocol handler (Eg:- TUP & UDP) to pass the packet to.

Hop Limit (8 bit)
field which has the same purpose as time to live in IPv4

Source address (16 byte - 128 bit)
identifies the original source of datagram.

Destination address (16 byte - 128 bit)
Identifies the final destination of datagram.

Extension Headers.

The length of the base header is fined at 40 byte. to provide greater functionality to the Ip datagram base header can be used.

* base header can be followed by up to six extension headers (many of these headers are option in IPV4)

Code	Nent Header
0	— hop by hop option.
2	— ICMP
6	— TCP
17	— UDP
43	— source Routing
44	— fragmentation
50	— Encrypted Security Payload
51	— Authentication.
59	— Null (no next header)
60	— Destination option.

Hop-by-Hop-option

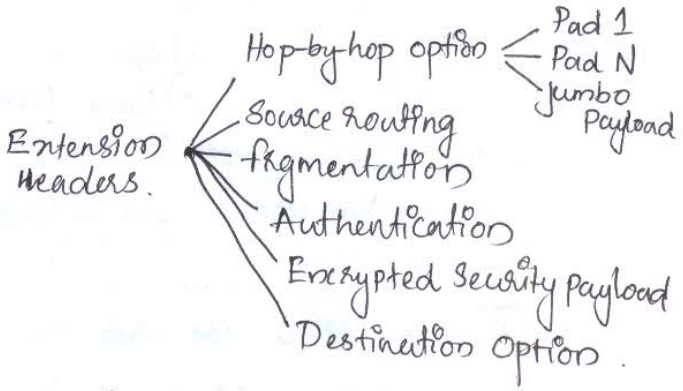
* used when the source needs to pass informations to all routers visited by the datagram

Three option is defined in.

Hop-by-Hop option

1) Pad 1 2) Pad N

3) Jumbo payload.



The pad1 option is 1 byte long and is designed for alignment purpose. PadN is similar in concept to Pad1. The difference is that PadN is used when 2 or more bytes is needed for alignment. The Jumbo payload option is used to define a payload longer than 65,535 bytes.

Source routing

The source routing extension header combines the concepts of the strict source route and loose source route optins of IPV4

Fragmentation

The concept of fragmentation is the same as that of IPV4. In IPV4, the source or a router is required to fragment if the size of the datagram is larger than the MTU (Maximum transfer unit) of the network over which the datagram travels.

In IPv6, Only the orginal source can fragment. A source must use a path MTU discovery technique to find the smallest MTU supported by any network on the path. The source then fragments using this knowledge.

Authentication

The authentication extension header has a dual purpose:

1) it validate the message sender and 2) Ensure the integrity of data.

Encrypted Security Payload

is an extension that provides confidentiality and guard aganist eavesdropping (Secretly listen to a conversation)

Destination option :- is used when the source need to pass information to the destination only. Intermediate routers are not permitted access to this information.

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

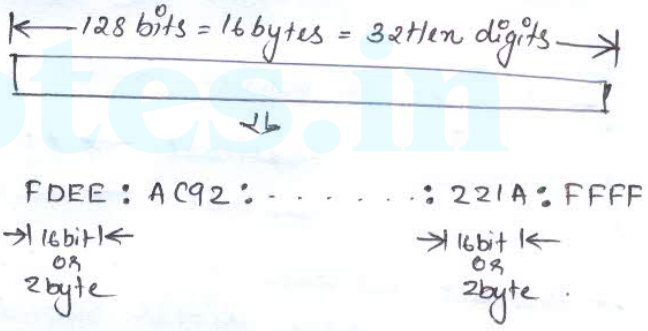
IPv6 addresses

IPv6 address consists of 16 bytes (octets) = 128 bits long.

Hexadecimal Colon Notation

128 bits are divided into 8 sections, each one is 2 bytes long. (16 bits). we need 4 hexadecimal ~~notations~~ digits for represent one section.

ie, IPv6 address consists of 32 hex digits and every group of 4 digits is separated by a colon



Note:-
Only about 15% of the address space is initally allocated, the remaining 85% being reserved for future use.

Eg:- Unabbrevated address: AC81 : 9840 : 0086 : 3210 : 000A : BBFF : 0000 : FFFF

Drop Drop Drop

Abbreviated address: AC81 : 9840 : 86 : 3210 : A : BBFF : 0 : FFFF

Eg:- Abbreviated address: AC81 : 0 : 0 : 0 : 0 : BBFF : 0 : FFFF

Replace by double semicolons.

further abbreviated: AC81 : : BBFF : 0 : FFFF

IPV6 define three different types of addresses.

IPV6 → unicast address, Multicast address, Anycast address.

1) Unicast
A unicast address defines a single computer. A packet sent to a unicast address is delivered to that specific computer.

2) Anycast
This is a type of address which defines a group of computers with addresses which have same prefix. A packet sent to an anycast address must be delivered to exactly one of the member of the group which is the closest of the most easily accessible

3) Multicast
A multicast address defines a group of computers which may or may not share the same prefix and may or may not be connected to same physical Network. A packet sent to a multicast address must be delivered to each member of the group.

* There are no broadcast address in IPv6, because multicast address can perform the same function.

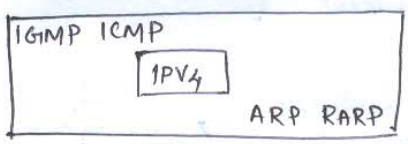
- The type of address define by leading bits.
  Multicast → FF (1111 1111)
  unicast → all other addressess.

- Anycast address are assigned from unicast address space and they do not have differ syntactically from unicast addresses.

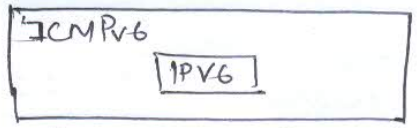
ICMPv6

modified version of ICMP is ICMPv6
ICMPv4 is modified to make it more suitable for IPv6

* 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.



Network layer in version 4



Network layer in version 6

ICMP Messages divided into two categories < Error reporting / Query.

Error reporting

One of the main responsibilities of ICMP is to error reporting.

* Five types of error are handled,
  1) Destination unreachable. 2) packet too big.
  3) time exceeded. 4) parameter problems.
  5) redirection.

ICMPv6 forms an error packet which is encapsulated in an IP datagram. This is delivered to the original source of the failed datagram.

Type of Message	version 4	version 6
Destination unreachable	— Yes	— Yes.
Source quench	— Yes.	— No.
Packet to big	— No	— Yes.
Time exceedes	— Yes	— Yes.
Parameter problem	— Yes	— Yes.
Redirection	— Yes	— Yes.

Packet to Big

This is a new type of message added to version 6. If a router receives a datagram that is larger than the maximum transmission unit (MTU) size of the network through which the data gram should pass, two things happen.

1) The router discard the datagram.
2) Then an ICMP error packet - a packet too-big Message - is sent to the source.

Query

In addition to error reporting, ICMP can diagnose some network problems. ~~by~~ through the query Messages.

different groups of Query messages

1) Echo request & reply
2) Solicitation & advertisement.
3) Neighbor solicitation & advertisment
4) group Membership

Type of message	Version 4	Version 6
Echo request & Reply	Yes	Yes
Timestamp request & Reply	Yes	No
Address-mask request & Reply	Yes	No.
Router solicitation & advertisement	Yes	Yes
Neighbor solicitation & advertisment	ARP	Yes
Group Membership	IGMP	Yes

Neighbor solicitation and advertisement

The Network Layer in version 4 contains an independent protocol called Address Resolution protocol (ARP). In version 6, the protocol is eliminated and its duties are included in ICMPv6. The idea is same as ARP. by the frame format is changed to ICMPv6.

Group Membership

the 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 same.

* Echo request and Reply & Router solicitation and advertisment both use the same idea and format as in version 4.