Network Layer

Some basic Concept

Repeater:

Repeater operates is physical layer. This are analog devices that are connected between two cable segment a signal appearing in one of them is reproduce and put on the other. Reapeator don't understand frames, packets or headers they understand only volts repeater is not an amplifier.

Hubs:

Hubs are also operational in physical layer. It has a no. of input lines that it joins electrically. Data arriving on any of the lines are sent out to all the others. The entire hub forms a single collision domain. All the lines in a hub must operate at the same speed,

Bridge:

Bridge operates in data link layer. A bridge connects two or more LANs. When a frame arrive, software in the bridge extracts the destination address from the frame data and looks up in a table to see in which LAN the frame should be forwarded. A bridge may connect different network type at different speed. Each line has its own collision domain. ~~So multi~~

Switches:

Switch are similar to bridge and also operates in datalink layer. The switch is most often use to connect the individual computer rather than LAN. The switch has mode code than the bride for the same region. The switch has buffer to handle the synchronization issues. (Speed mismatch)

Router:

Routers operates in network layer. When the frames comes into the router the header an tailer are cut off and the data in the frame is passed to the routing software this software uses the packet header to choose the output line. The routing software dont care about the frame address or the path from which it came.

Gateway:

Gateway connects two network that uses different protocals. The transport gateway can copy the packets from connection to another by reformatting them. Application Gateway understand the format and the content of the data and translate message from one format to another.

Example, an Email gateway can translate internet messages into SMS messages for mobile phone. Gateway's operates in transport / application layer

IP addressing

Internet Protocal: is an unreliable protocal. The packet in Ip layer is known as datagram ip uses best effort delivery method (No Error checking no tracking). If the sender does't recive any response from the receiver then the datagram is retransmitted. The datagram is transmitted in separate pices each of which may take different root and arrive at different time, so the datagrams are not received in the same order as they were sent. IP is the responsibility to the receiver to reasemble them.

Ip datagram

Version 4 bits	header length 4	service Servu Type 8	Total length (16)	4 byte
identification.		Flag 3	fragmentation offset 13	4
Time to live 8	Protocal 8		Header checksum 16	4
32-bit source Ip address				4
32-bit destination Ip address				4
optional (Routing control, Timing, Management & alignment) (upto 40 byte)				

Every i'p is devided into two parts header and data
The datagram may be of maximum size (2^{16}) bytes.
The size of the header may varied from 20 - 60 bytes.

Version: The binary value of version no of Ip.

Header length: Specifies the length of the header multiple of 4 bytes.

Service type: This specifies the priority of the datagram

Total length: Specifies the total length of Ip datagram.

Identification: This field is used to identify the fragments of the datagram so that it canbe reassemble.

Flags: These bits specifies the fragment type
first fragment / midle fragment / last fragment.

Fragmentation offset: This is specifies the offset value of the fragment.

Time to live: this field sets the amount of time the datagram can stay in the network before it is destroy. It uses a event driven timer.

Protocol: It is defines the upper level protocol who is using the IP. (Example ~~Tcp/UDP~~) TCP/UDP

Header checksum: Header checking field of the header only (data is not check.

Destination address: It is a four byte internet address that specifies the destion.

Source address: It is a four byte internet address specifies the source

optional: It specifies additional options that may be the information related to routing, control, timing, management & alignment.

Mac address / Physical address

Each device connected to the network must have a unique hardware address i.e specified by the device manufacturer. This address is unique and can't be changed. This address is refer as hardware or machine address (Mac address) and is 6 bytes long.

Ip address

The ip address is unique address i.e loggically assign to a device in a network. It is also known as the logical and software address. The IP address can be change from time to time by the network administrator.

Ip Ip address has two field net id and host id.

class A 1st bit 0 ↕ 0000000
0

class B 2nd bit 1 0 ↕ 00·0000
128

class C 1 1 0 ↕ 00000
192

class D 1 1 1 0 ↕ 0000
224

class E 1 1 1 1 0 | 000
240

0 | 1 1 1 1 1 1 1
127

1 0 | 1 1 1 1 1 1
191

1 1 0 ↕ 1 1 1 1
223

1 1 1 0 ↕ 1 1 1 1
239

1 1 1 1 0 | 1 1 1
255

128
63
91

91
128
64

15
128
64
32
15
1

Class A Net id → 8 bit No. of addresses $(255)^3$ - 16581375
Class B Net id → 16 bit No. of addresses $(255)^2$ - 65025
Class C Net id → 24 bit No. of addresses 255

(1) 5.34.200.85 → A
(2) 228.57.58.19 → D
(3) 169.45.17.10 → B
(4) 200.67.9.25 → C

Without Subnet

Subnetting and Supernetting

Sub.

If all the address in a network are not used, Subnetting allows the address to devided among various organization by creating smaller networks. Subnetting is done by using the portion of the host id as subnet id. It is to be remember that Subnating doesn't increase the total no. of Ip's. It only saves the wastage of Ip.

Supernetting

Supernetting was proposed to combine several class a blocks into a large block for those organizations to require more than 256 addresses and are using class C addressing more.

Classless addressing

In this method, variable length blocks are used that belong to no class. The prefix in an address defines the net id and the suffix defines the host. The block must be pow of 2 & the prefix length is variable.

According to CIDR (classless Interdomain routing, the prefix length is added to the address separated by a slash (/). If n is the prefix length

Ip Protocals

Address Resulation Protocol (ARP)

Every Ethernet board manufacturer uses a unique 48 bit ethernet address (also known as MAC address). A Central authority of manufacturer allocates this address to each LAN chip which can't be common to any other chip in the world.

When a chip install in a machine, it gets and ip address from its network. This address may change in network to network. But the ethernet address of the chip always remains the same, since the network doesn't understand the ip address so the ethernet id must be mapped with the corresponding ip address. This is done by the ARP.

The ARP associate with another ip with physical address. when a router need a physicals of a nodes on its network, it sends and ARP packet across the network. The ARP packet contain the ip packet that the router needs to link to a physical address. The node that holds the particular ip, returns its physical address. Once that is known, it is entered in the routing table for future use. When the Sender machine Sending the ARP packet, it also sends its own ip and ethernet address, so that the receiver may note it down in future use

Reverse Address Resulation Protocol (RARP)

A disk less ('dummy') terminal faces the opposit problem. It knowns the ethernet address (as it's built in) but doesn't know its ip address. The Solution used for this purpose is to use RARP. RARP works from the client End. A newly booted dummy terminal broadcast its ethernet address via RARP datagram packets. The server absorbs the RARP and replies the particular device by sending its ip address.

RARP doesn't work if the client and the server is not on the same LAN. As the router don't forward Ethernet broadcast, so another protocol called boot-p (Boot Protocol) is used. This protocol uses UDP messages which is forwarded by the router. However now a days, both the above protocols are substituted by a more superior protocol known as DHCP (Dynamic Host Configuration protocol).

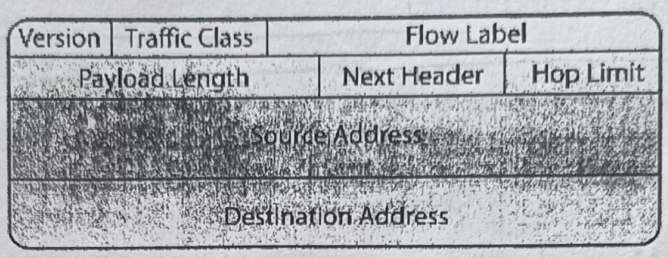
ICMP (Internet Control Message Protocol)

The operation of the internet is closely monitor by the routers. when something unexpected occurs the event is reported by the ICMP. The ICMP messages are as follows-

Message type	Description
1. Destination Unreachable	Packet could not be deliver
2. Time Exceeded	Time to live (TTL) field became zero.
3. Parameter Problem	Invalid header field.
4. Source Quench	choke packet
5. Redirect	Redirects to proper location
6. echo	Ask a machine if it is alive.
7. echo reply	yes i am alive
8. Time-Stamp Require	Same as echo but with time stamp.
9. Time Stamp reply	Same as echo reply but with time stamp.

IPv6

An Internet Protocol version 6 (IPv6) data packet comprises of two main parts: the header and the payload. The first 40 bytes/octets (40x8 = 320 bits) of an IPv6 packet comprise of the header (see Figure 1) that contains the following fields:



Source address (128 bits) The 128-bit source address field contains the IPv6 address of the originating node of the packet. It is the address of the originator of the IPv6 packet.

Destination address (128 bits) The 128-bit contains the destination address of the recipient node of the IPv6 packet. It is the address of the intended recipient of the IPv6 packet.

Version/IP version (4-bits) The 4-bit version field contains the number 6. It indicates the version of the IPv6 protocol. This field is the same size as the IPv4 version field that contains the number 4. However, this field has a limited use because IPv4 and IPv6 packets are not distinguished based on the value in the version field but by the protocol type present in the layer 2 envelope.

Packet priority/Traffic class (8 bits) The 8-bit Priority field in the IPv6 header can assume different values to enable the source node to differentiate between the packets generated by it by associating different delivery priorities to them. This field is subsequently used by the originating node and the routers to identify the data packets that belong to the same traffic class and distinguish between packets with different priorities.

Flow Label/QoS management (20 bits) The 20-bit flow label field in the IPv6 header can be used by a source to label a set of packets belonging to the same flow. A flow is uniquely identified by the combination of the source address and of a non-zero Flow label. Multiple active flows may exist from a source to a destination as well as traffic that are not associated with any flow (Flow label = 0).

The IPv6 routers must handle the packets belonging to the same flow in a similar fashion. The information on handling of IPv6 data packets belonging to a given flow may be specified within the data packets themselves or it may be conveyed by a control protocol such as the RSVP (Resource reSerVation

Protocol).

When routers receive the first packet of a new flow, they can process the information carried by the IPv6 header, Routing header, and Hop-by-Hop extension headers, and store the result (e.g. determining the retransmission of specific IPv6 data packets) in a cache memory and use the result to route all other packets belonging to the same flow (having the same source address and the same Flow Label), by using the data stored in the cache memory.

Payload length in bytes(16 bits) The 16-bit payload length field contains the length of the data field in octets/bits following the IPv6 packet header. The 16-bit Payload length field puts an upper limit on the maximum packet payload to 64 kilobytes. In case a higher packet payload is required, a Jumbo payload extension header is provided in the IPv6 protocol. A Jumbo payload (Jumbogram) is indicated by the value zero in the Payload Length field. Jumbograms are frequently used in supercomputer communication using the IPv6 protocol to transmit heavy data payload.

Next Header (8 bits) The 8-bit Next Header field identifies the type of header immediately following the IPv6 header and located at the beginning of the data field (payload) of the IPv6 packet. This field usually specifies the transport layer protocol used by a packet's payload. The two most common kinds of Next Headers are TCP (6) and UDP (17), but many other headers are also possible. The format adopted for this field is the one proposed for IPv4 by RFC 1700. In case of IPv6 protocol, the Next Header field is similar to the IPv4 Protocol field.

Time To Live (TTL)/Hop Limit (8 bits) The 8-bit Hop Limit field is decremented by one, by each node (typically a router) that forwards a packet. If the Hop Limit field is decremented to zero, the packet is discarded. The main function of this field is to identify and to discard packets that are stuck in an indefinite loop due to any routing information errors. The 8-bit field also puts an upper limit on the maximum number of links between two IPv6 nodes. In this way, an IPv6 data packet is allowed a maximum of 255 hops before it is eventually discarded. An IPv6 data packet can pas through a maximum of 254 routers before being discarded.

In case of IPv6 protocol, the fields for handling fragmentation do not form a part of the basic header. They are put into a separate extension header. Moreover, fragmentation is exclusively handled by the sending host. Routers are not employed in the Fragmentation process.

IPv4	IPv6
IPv4 addresses are 32 bit length.	IPv6 addresses are 128 bit length.
IPv4 addresses are binary numbers represented in decimals.	IPv6 addresses are binary numbers represented in hexadecimals.
IPSec support is only optional.	Inbuilt IPSec support.
Fragmentation is done by sender and forwarding routers.	Fragmentation is done only by sender.
No packet flow identification.	Packet flow identification is available within the IPv6 header using the Flow Label field.
Checksum field is available in IPv4 header	No checksum field in IPv6 header.
Options fields are available in IPv4 header.	No option fields, but IPv6 Extension headers are available.
Address Resolution Protocol (ARP) is available to map IPv4 addresses to MAC addresses.	Address Resolution Protocol (ARP) is replaced with a function of Neighbor Discovery Protocol (NDP).
Internet Group Management Protocol (IGMP) is used to manage multicast group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages.
Broadcast messages are available.	Broadcast messages are not available. Instead a link-local scope "All nodes" multicast IPv6 address (FF02::1) is used for broadcast similar functionality.
Manual configuration (Static) of IPv4 addresses or DHCP (Dynamic configuration) is required to	Auto-configuration of addresses is available.