**NETWORK LAYER PROTOCOLS**

Each computer in a network has unique IP address from which it can be identified from the network .IP address is assigned in layer 3 (network layer) . IP address can vary at different instance.

**ADDRESS RESOLUTION PROTOCOL (ARP)**

Duringtransmission the source needs the MAC address of the destination machine which belonging to the same network. MAC address is physically burnt into the Network interface card of the machine by the manufacturer and it is fixed can’t be changed.

On the other side , the IP address on the public domain is not fixed can be changed. If the NIC is changed due to some faults then the MAC address can be changed. To know the MAC address of the remote source on a broadcast domain, the machine which is interested to initiate a connection will send ARP broadcast message asking who have this particular IP address , since it is a broadcast all the machines in the network will receive the packet request and process it.ARP packet contains the IP address of the destination , the sources wishes to communicate. When the destination receives the ARP packet destined to it, it answers the request with its own MAC address.

Once the source gets the MAC address of the destination, it can communicate with the source using data link layer protocol. This MAC address to IP address mapping is stored in to ARP cache of both transmitting and receiving hosts.

Next time if they want to communicate they can directly refer to their respective ARP cache.

**REVERESE ADDRESS RESOLUTION PROTOCOL(RARP)**

Reverse address resolution protocol is a mechanism where source knows the MAC address of the source but required to know the IP address of the destination to transmit the data packets.

**INTERNET CONTROL MESSAGE PROTOCOL(ICMP)**

ICMP is network diagnostic and error reporting protocol. ICMP belongs to IP protocol suite and uses IP as carrier protocol. After generating ICMP packet , it is encapsulated in IP packet since IP is a best effort non reliable protocol.

Any feedback about the network is sent back to the originating host. If some error in the network occurs, it is reported by means of ICMP . ICMP contains dozens of diagnostic and error reporting messages.

ICMP echo and ICMP echo reply are the most commonly used ICMP messages to know the reachability of end to end hosts . when a source receives an ICMP echo request it is bound to send back an ICMP echo reply. If there is any problem in the transmission network, ICMP will report the problem.

**IPv4**

IPv4 is 32 bit addressing mechanism used as TCP/IP host addressing mechanism. IP addressing gives unique identity to every host in a network .it provides hierarchical addressing scheme which helps it to divide the single network into sub networks.

**CLASS A** uses first three octets for network addressing and last three addresses for host addressing

**CLASS B** uses first two octets for network addressing and last two addresses for host addressing.

**CLASS C** uses first three octets for network addressing and last one addresses for host addressing.

**CLASS D** it provides flat IP addressing scheme in contrast to hierarchial structure for above three.

**CLASS E** is used as experimental.

IPv4 has well defined address spaces to be used as private addresses which can not be routable on internet, public addresses which can be routable on internet.

IP is not a reliable one, but it provides best effort delivery mechanism.

**INTERNET PROTOCOL VERSION (IPv6)**

Ipv4 address gave birth to next generation internet protocol version 6.IPv6 address has 128bit addressing providing more address space.

IPv6 has introduced anycast addressing but removed broadcast addressing.

IPv6 enables devices to self acquire an IPv6 address and can communicate with in that subnet .this auto configuration removes the DHCP service. Even when the DHCP server on that subnet is down the host can communicate with each other.

IPv6 provides mobility. Mobile IPv6 equipped machines can roam around without the need of changing their IP address. It is still in the transition phase and is expected to replace IPv4 completely in coming years. At present there are few networks which runs using IPv6. There are some transition mechanism available for IPv6 enabled networks to speak and roam different networks easily on IPv4.

* Dual stack implementation
* Tunnelling
* NAT-PT

**TRANSMISSION CONTROL PROTOCOL**

* It provides reliable transmission between the source and destination.
* It is one of important protocol of internet protocol suit. It is the most widely used protocol for data communication in the internet.
* TCP is a reliable protocol which means the destination always sends either positive or negative acknowledgement about the data packet to the source, so that the source always has the clear idea about whether the data packet is reached successfully to the destination or to be resend.
* TCP ensures that the data reached the destination is in same sequence of data send by the source.
* TCP is connection oriented protocol. TCP requires connection between two remote host has to be established before transmitting the data.
* TCP provides error checking and recovery mechanism.
* TCP provides end to end communication. TCP provides flow control and quality of service.
* TCP operates in source/destination point to point mode.
* TCP provides full duplex service that is it can perform both receiving sending the data simultaneously.
* The length of the TCP varies from 20bytes to 60bytes.

**Source port(16bits):**

It identifies the source port of the application process on the source machine.

**Destination port(16-bits):**

It identifies the destination port of the application process on the destination device.

**Sequence number(32-bits):**

Sequence number of the data bytes of the packets in a session.

**Acknowledgement number(32 bits):**

When the acknowledgement flag is set. This number contains the next sequence number of the data byte expected and works as the acknowledgement of the previous data packets received.

**Data offset(4-bits):**

This field says about both the size of the TCP header and the offset of the data in the current packet in the whole TCP segment.

**Reserved(3-bits):**

Reserved for future use and all are set to 0 by default.

**Flags(1-bit each):**

**NS:** nonce sum bit is used by explicit congestion notification signalling process.

**CWR:**

When a host receives the packets with the ECE bit set, it set congestion windows reduced to acknowledged that ECE received.

**ECE**:

If SYN bit is clear to 0 then ECE means that IP packets its congestion experience bit set.

If SYN bit is set 1, then the EWCE means that he device is ECT capable.

**URG:**

It indicates that urgent pointer field has significant data and should be processed.

**ACK:**

It indicates that acknowledgement field has significance.

If ACK is cleared to 0, it indicates that the packets does not contain any acknowledgement.

**PSH:**

When PSH is set, it is a request to the destination to push data as soon as it comes to the receiving application without any buffer.

**RST:**

Reset flag has the following features;

* It is used to refuse an incoming connection.
* It is used to reject a segment.
* It is used to restart the connection.

**SYN:**

This flag is used to setup the connection between the source and the destination.

**FIN:**

This flag is used to release the connection between the source and the destination. And ensures that no more data transfer happens thereafter, because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.

**Windows size:**

This field is used for flow control between the source and the destination and indicates the buffering in the destination.

**Checksum:**

This field contains the check sum of header data, and pseudo headers.

**Urgent point:**

It points to the urgent data bytes if the flag is set to 1.

**UDP**-**USER DATAGRAM PROTOCOL:**

it is the simplest transport layer protocol available TCP IP protocol suit. It is set to be unreliable protocol but it is uses IP services which provides best effort delivery mechanism.

**FEATURES:**

* UDP is used when the acknowledgement of data hold any significant.
* UDP is a good protocol for data flowing in one direction.
* UDP is simple and suitable for query based application.
* It is not connection oriented protocol.
* It does not provide congestion control mechanism.
* UDP does not guarantee ordered delivery of the data.
* UDP does not says any information about the previous processed data i.e, stateless.
* UDP is suitable protocol for streaming application.

**UDP HEADER:**

**Source port;**

This the sixteen bit information used to identify the source port of the packet.

**Destination port;**

This the sixteen bit information used to identify the destination port of the packet.

**Length;**

This field tells about the entire length of the UDP packet including the header.

It is the sixteen bit field and the minimum value is eight byte.

**Checksum;**

This field stores the checksum value generated by the source before transmitting.

IPv4 has this field as an optional when the checksum field does not contain any value it is cleared to zero and all its bits are cleared to zero.

**SIMPLE MAIL TRANSFER PROTOCOL:**

It is used to transfer email from one user to the another.

This task is done by means of email client software the user is using.user agent help the user to type,format,store the mail until the internet is available.when the email is submitted to send. The sending process if handled by the message transfer agent which is in built in the email clients software.

Message transfer agent uses SMTP to forward the email to the other message transfer agent while the SMTP is used by end user to only send the emails and server uses the SMTP to both send and receive the mails.

Client software users internet access protocol or pop to receive mails.

**FILE TRANSFER PROTOCOL**:

FTP is widely used protocol for file transfer over the networks.FTP uses TCP/IP for communication and it works on TCP port 21. FTP works on client server model where the client request for file from the server and the server sends the requested file back to the clients. FTP uses out of band controlling.

FTP uses TCP port 20 for exchanging control information.the actual data is sent over TCP port 21. The clients sends the request for a file. Then the server receives the request for a file. It opens the TCP connection for the client and transfers the file.

After the completion of the file transfer, the server closes the connection. For the second file transfer anew TCP connection is established between the client and the server.

**POST OFFICE PROTOCOL (POP):**

It is the simple mail retrieval protocol used by the user agent to retrieve the main from the server. When the clients needs to retrieve the mail from a server it establishes the connection with the server using TCP port110 user can then access the mail and download them to the local machine.

It works on two modes;

Common mode and delete mode is to delete the emails from the server after they are downloaded to the local computer.

Keep mode;

It does not delete the email from the server gives an opportunity to the client to access the email later.

**HTTP:**

It is the foundation of world wide web. It works on client server model. When client wants to access any HTTP page on the internet the client machine at the user end establishes a TCP connection between the server and client on port 80.

When the server accepts the client request, the client gets the authorization to access the web page.

The client uses the web browsers to access the web page which is responsible for establishing maintaining and terminating the TCP connection. It is the stateless protocol which means the server does not store any information about the previous request by the clients.

**HTTP VERSION**:

HTTP 1.0- non persistent HTTP. Single object can be transfer over a single TCP connection.

HTTP 1.1- persistent HTTP. Many object can be transferred over a single TCP connection.