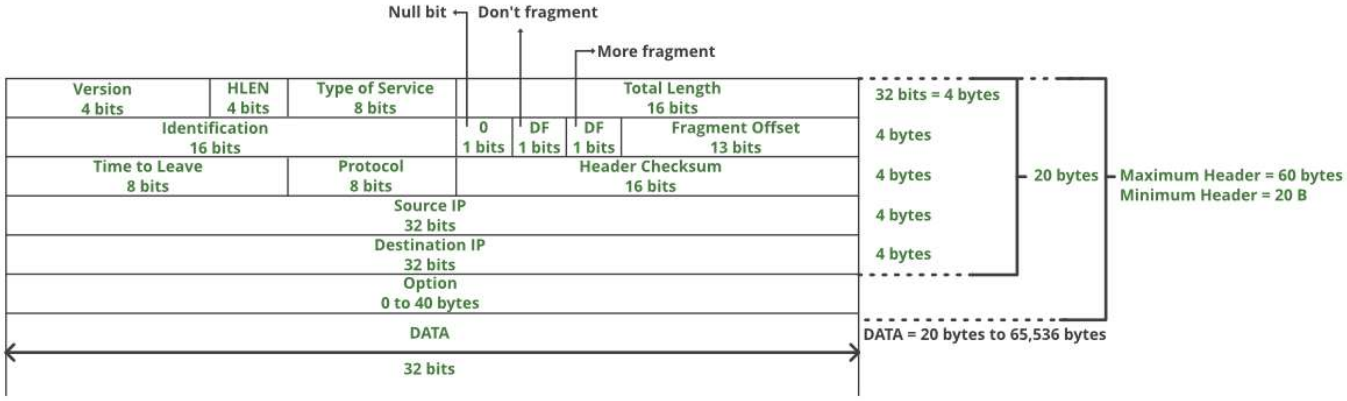
18CSC302J – COMPUTER NETWORKS
IMPORTANT QUESTIONS

UNIT-1

IP Header:

IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet. It provides a logical connection between network devices by providing identification for each device.

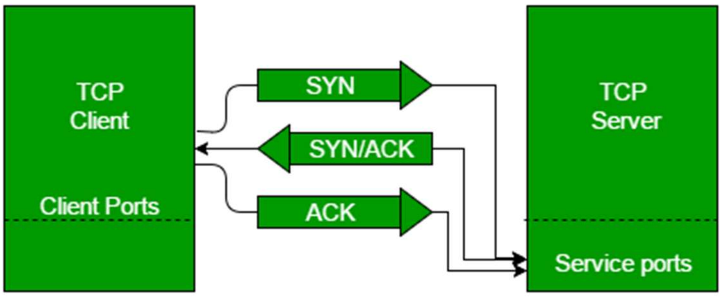


Component	Bits Used	Description
VERSION	4	Version of the IP protocol.
HLEN	4	IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.
Type of Service	8	Low Delay and Reliability
Total Length	16	Length of header + Data, which has a minimum value 20 bytes and the maximum is 65,535 bytes.
Identification	16	Unique Packet ID for identifying the group of fragments of a single IP datagram.
Flags	3	3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)
Fragment Offset	13	Represents the number of Data Bytes ahead of the particular fragment in the particular datagram.
Time to Live	8	It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the destination.
Protocol	8	Name of the protocol to which the data is to be passed.
Header Checksum	16	For checking errors in the datagram header.
Source IP address	32	32 bits IP address of the sender
Destination IP address	32	Destination IP address: 32 bits IP address of the receiver
Option	0 - 40	Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.

TCP & UDP:

Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram-oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast types of network transmission.
TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
An acknowledgment segment is present.	No acknowledgment segment.
Sequencing of data is done in TCP.	Sequencing of data is not done in UDP.
TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.
Retransmission of lost packets is possible in TCP.	Retransmission of lost packets is not possible in UDP.
TCP has a (20-60) bytes variable length header.	UDP has an 8 bytes fixed-length header.
TCP is heavy-weight.	UDP is lightweight.
TCP doesn't support Broadcasting.	UDP supports Broadcasting.
TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet.	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.
The TCP connection is a byte stream.	UDP connection is message stream.
Low overhead but higher than UDP.	Very low overhead.

Three-Way Handshake Protocol:



TCP provides reliable communication with something called Positive Acknowledgement with Re-transmission(PAR). The Protocol Data Unit(PDU) of the transport layer is called a segment. Now a device using PAR resend the data unit until it receives an acknowledgement.

Step 1 (SYN): In the first step, the client wants to establish a connection with a server, so it sends a segment with SYN(Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts segments with.

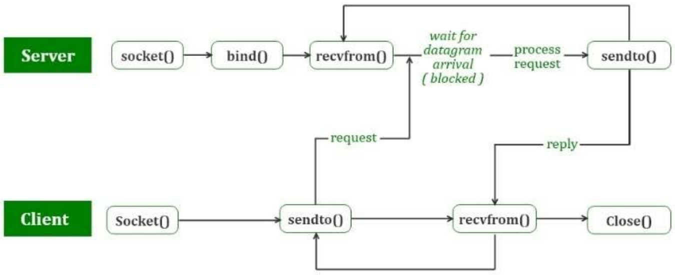
Step 2 (SYN + ACK): Server responds to the client request with SYN-ACK signal bits set. Acknowledgement (ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with.

Step 3 (ACK): In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer.

UNIT-2

UDP Server-Client implementation:

There are two major transport layer protocols to communicate between hosts: TCP and UDP.
In UDP, the client does not form a connection with the server like in TCP and instead just sends a datagram. Similarly, the server need not accept a connection and just waits for datagrams to arrive. Datagrams upon arrival contain the address of the sender which the server uses to send data to the correct client.



The entire process can be broken down into the following steps :
UDP Server :

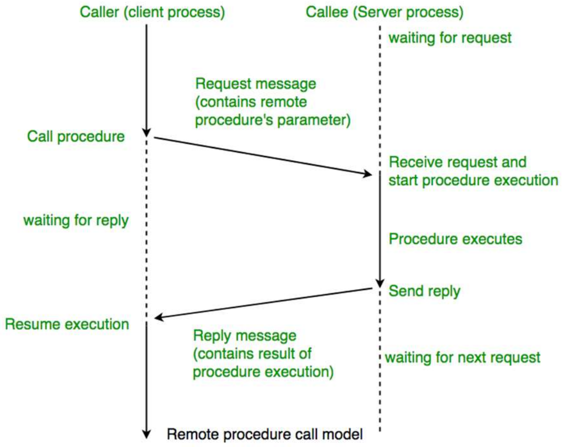
- Create a UDP socket.
- Bind the socket to the server address.
- Wait until the datagram packet arrives from the client.
- Process the datagram packet and send a reply to the client.
- Go back to Step 3.

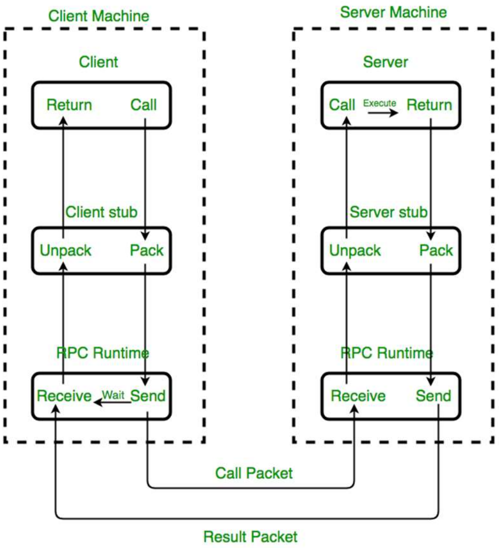
UDP Client :

- Create a UDP socket.
- Send a message to the server.
- Wait until response from the server is received.
- Process reply and go back to step 2, if necessary.
- Close socket descriptor and exit.

Remote Procedure Call (RPC):

RPC is a powerful technique for constructing distributed, client-server based applications. It is based on extending the conventional local procedure calling so that the called procedure need not exist in the same address space as the calling procedure. The two processes may be on the same system, or they may be on different systems with a network connecting them.


Caller (client process)
Callee (Server process)
waiting for request
Request message (contains remote procedure's parameter)
Call procedure
Receive request and start procedure execution
waiting for reply
Procedure executes
Send reply
Resume execution
Reply message (contains result of procedure execution)
waiting for next request
Remote procedure call model



Implementation of RPC mechanism

Stream Control Transmission Protocol (SCTP):

It is a connection- oriented protocol in computer networks which provides a full-duplex association i.e., transmitting multiple streams of data between two end points at the same time that have established a connection in network. A telephonic conversation requires transmitting of voice along with other data at the same time on both ends, SCTP protocol makes it easier to establish reliable connection.

Characteristics of SCTP:

- It is a point-to-point protocol which can use different paths to reach end host.
- It uses SACK and checksums to detect damaged, corrupted, discarded, duplicate and reordered data. It is similar to TCP but SCTP is more efficient when it comes to reordering of data.
- Each message can be framed and we can keep order of data stream and tabs on structure. For this, in TCP, we need a different layer for abstraction.
- It can establish multiple connection paths between two end points and does not need to rely on IP layer for resilience.
- In SCTP, resource allocation for association establishment only takes place following cookie exchange identification verification for the client.

Advantages of SCTP :

- It is a full- duplex connection i.e. users can send and receive data simultaneously.
- It allows half- closed connections.
- The message’s boundaries are maintained and application doesn’t have to split messages.
- It has properties of both TCP and UDP protocol.
- It doesn’t rely on IP layer for resilience of paths.

Disadvantages of SCTP :

- One of key challenges is that it requires changes in transport stack on node.
- Applications need to be modified to use SCTP instead of TCP/UDP.
- Applications need to be modified to handle multiple simultaneous streams.

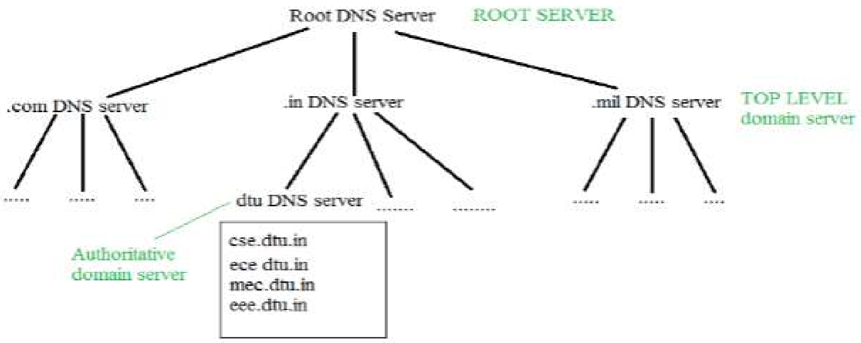
UNIT-3

Domain Name System (DNS):

DNS is a hostname for IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

Every host is identified by the IP address but remembering numbers is very difficult for the people also the IP addresses are not static therefore a mapping is required to change the domain name to the IP address. So, DNS is used to convert the domain name of the websites to their numerical IP address.

Generic domain: .com(commercial) .edu(educational) .mil(military) .org(non-profit organization) .net(similar to commercial) all these are generic domain.
Country domain: .in, .us, .uk, etc.
Inverse domain: If we want to know what is the domain name of the website. IP to domain name mapping.



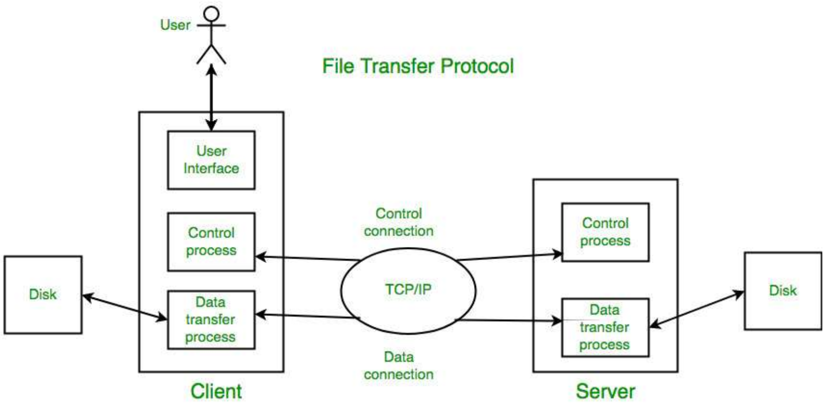
File Transfer Protocol(FTP):

File Transfer Protocol(FTP) is an application layer protocol that moves files between local and remote file systems. It runs on the top of TCP, like HTTP. To transfer a file, 2 TCP connections are used by FTP in parallel: control connection and data connection.

FTP allows three types of data structures :
File Structure: In file structure, there is no internal structure and the file is considered to be a continuous sequence of data bytes.
Record Structure: In record structure, the file is made up of sequential records.
Page Structure: In page structure, the file is made up of independent indexed pages.

USER	This command sends the user identification to the server.
PAS	This command sends the user password to the server.
CW	This command allows the user to work with a different directory or dataset for file storage or retrieval without altering his login or accounting information.

RMD	This command causes the directory specified in the path name to be removed as a directory.
MKD	This command causes the directory specified in the pathname to be created as a directory.
PWD	This command causes the name of the current working directory to be returned in the reply.
RETR	This command causes the remote host to initiate a data connection and to send the requested file over the data connection.
STOR	This command causes to store of a file into the current directory of the remote host.
LIST	Sends a request to display the list of all the files present in the directory.
ABOR	This command tells the server to abort the previous FTP service command and any associated transfer of data.
QUIT	This command terminates a USER and if file transfer is not in progress, the server closes the control connection.



Advantages of FTP:

- Speed is one of the advantages of FTP(File Transfer Protocol).
- File sharing also comes in the category of advantages of FTP in this between two machines' files can be shared on the network.
- Efficiency is more in FTP.

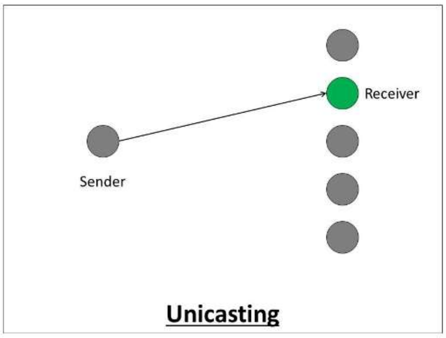
Disadvantages of FTP:

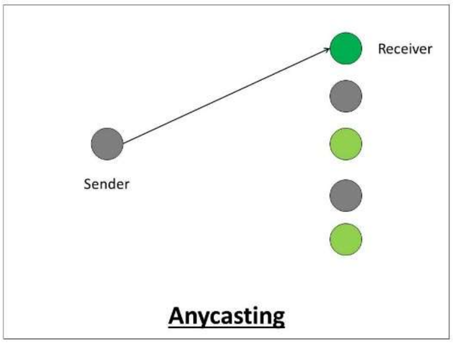
- File size limit is the drawback of FTP only 2 GB size files can be transferred.
- Multiple receivers are not supported by the FTP.
- FTP does not encrypt the data this is one of the biggest drawbacks of FTP.
- FTP is unsecured we use login IDs and passwords but they can be attacked by hackers.

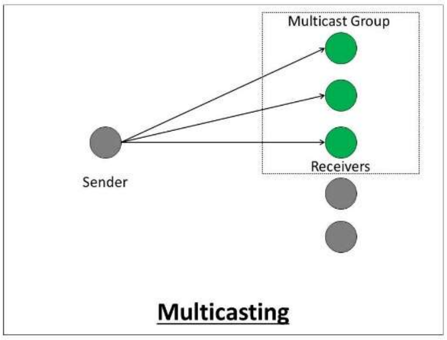
UNIT-4

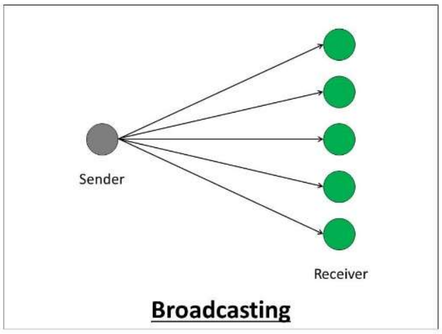
IPv6 Addressing:

IPv6 addresses are 128-bits long and are identifiers for individual interfaces and sets of interfaces. IPv6 addresses of all types are assigned to interfaces, not nodes (hosts and routers). Because each interface belongs to a single node, any of that node's interfaces' unicast addresses can be used as an identifier for the node. A single interface can be assigned multiple IPv6 addresses of any type.









Transmission Type	Transmission Method	Description
Unicast	One – to – One	It is the most common form of packet or data transmission across a network.
Anycast	One – to – Any	Transmitted from a single source to any destination device (mostly the nearest device).
Multicast	One – to – Many	It is used to transfer to some specific hosts but not all the hosts in a network.
Broadcast	One – to – All	It is also a common form of data transmission across network as it is use in LAN (Local Area Network).

IPv4 & IPv6:

IPv4	IPv6
IPv4 has a 32-bit address length.	IPv6 has a 128-bit address length.
In IPv4 end to end, connection integrity is unachievable.	In IPv6 end to end, connection integrity is achievable.
It can generate 4.29×10^{9} address space.	It can generate 3.4×10^{38} address space.
Address representation of IPv4 is in decimal.	Address Representation of IPv6 is in hexadecimal.
Packet flow identification is not available.	Packet flow identification is available.
Checksum field is available.	Checksum field is not available.

It has a broadcast message transmission scheme.	It has anycast message transmission schemes.
Header of 20-60 bytes.	Header of 40 bytes fixed.
Consists of 4 fields which are separated by dot (.)	Consists of 8 fields, which are separated by colon (:)
IP addresses are divided into five different classes: Class A , Class B, Class C , Class D , Class E.	No classes of IP address.
Supports VLSM.	Does not support VLSM.
Example: 66.94.29.13	Example: 2001:0000:3238:DFE1:0063:0000:0000:FEFB

Mobility in IPv6:

When a host is connected to a link or network, it acquires an IP address and all communication take place using that IP address on that link. As soon as, the same host changes its physical location, that is, moves into another network, its IP address changes accordingly, and all the communication taking place on the host using old IP address, goes down.

IPv6 mobility provides a mechanism for the host to roam around different links without losing any communication/connection and its IP address.

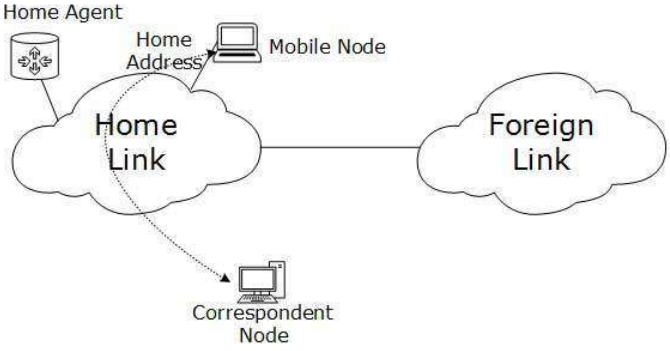
Multiple entities are involved in this technology:

Mobile Node	The device that needs IPv6 mobility.
Home Link	This link is configured with the home subnet prefix and this is where the Mobile IPv6 device gets its Home Address.
Home Address	This is the permanent address of the Mobile Node.
Home Agent	Home Agent is connected to Home Link and maintains information about all Mobile Nodes, their Home Addresses, and their present IP addresses.
Foreign Link	Any other Link that is not Mobile Node’s Home Link.
Care-of Address	Multiple Care-of addresses can be assigned to a Mobile Node, but at any instance, only one Care-of Address has binding with the Home Address.
Correspondent Node	Any IPv6 enabled device that intends to have communication with Mobile Node.

Mobility Operation:

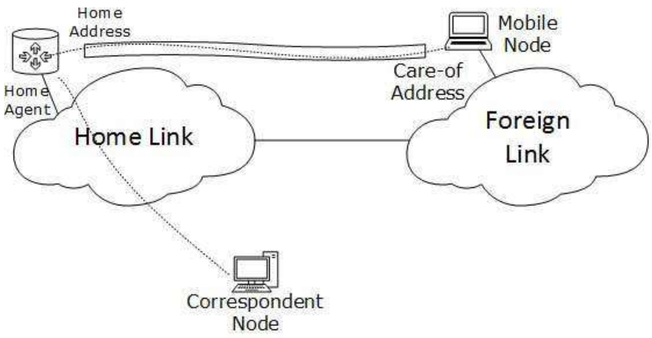
When Mobile Node stays in its Home Link, all communications take place on its Home Address. When a Mobile Node leaves its Home Link and is connected to some Foreign Link, the Mobility feature of IPv6 comes into play.

After getting connected to a Foreign Link, the Mobile Node acquires an IPv6 address from the Foreign Link. This address is called Care-of Address.



Mobile Node connected to Home Link

The Mobile Node sends a binding request to its Home Agent with the new Care-of Address. The Home Agent binds the Mobile Node's Home Address with the Care-of Address, establishing a Tunnel between both. Whenever a Correspondent Node tries to establish connection with the Mobile Node (on its Home Address), the Home Agent intercepts the packet and forwards to Mobile Node's Care-of Address over the Tunnel which was already established.



Mobile Node connected to Foreign Link

Route Optimization:

When a Correspondent Node initiates a communication by sending packets to Mobile the Node on the Home Address, these packets are tunneled to the Mobile Node by the Home Agent. In Route Optimization mode, when the Mobile Node receives a packet from the Correspondent Node, it does not forward replies to the Home Agent. Rather, it sends its packet directly to the Correspondent Node using Home Address as Source Address. This mode is optional and not used by default.

Network Address Translation(NAT):

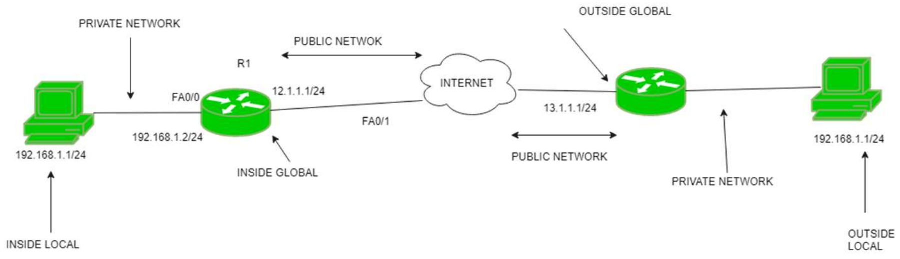
A Network Address Translation (NAT) is the process of mapping an internet protocol (IP) address to another by changing the header of IP packets while in transit via a router. This helps to improve security and decrease the number of IP addresses an organization needs.

How does Network Address Translation work?

A NAT works by selecting gateways that sit between two local networks: the internal network, and the outside network. Systems on the inside network are typically assigned IP addresses that cannot be routed to external networks (e.g., networks in the 10.0.0.0/8 block).

A few externally valid IP addresses are assigned to the gateway. The gateway makes outbound traffic from an inside system appear to be coming from one of the valid external addresses. It takes incoming traffic aimed at a valid external address and sends it to the correct internal system.

This helps ensure security. Because each outgoing or incoming request must go through a translation process that offers the opportunity to qualify or authenticate incoming streams and match them to outgoing requests, for example.



Addresses	Description
Inside Local Address	An IP address that is assigned to a host on the Inside (local) network. These are private IP addresses. This is the inside host seen from the inside network.
Inside Global Address	IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.
Outside Local Address	This is the actual IP address of the destination host in the local network after translation.
Outside Global Address	This is the outside host as seen from the outside network. It is the IP address of the outside destination host before translation.

Static NAT	A single private IP address is mapped with a legally registered public IP address.
Dynamic NAT	An unregistered IP address is translated into a registered public IP address.
NAT Overload	This is known as Port-Address Translation (PAT). In this many private IP addresses can be translated to a single registered IP address.

Transition from IPv4 to IPv6 Address:

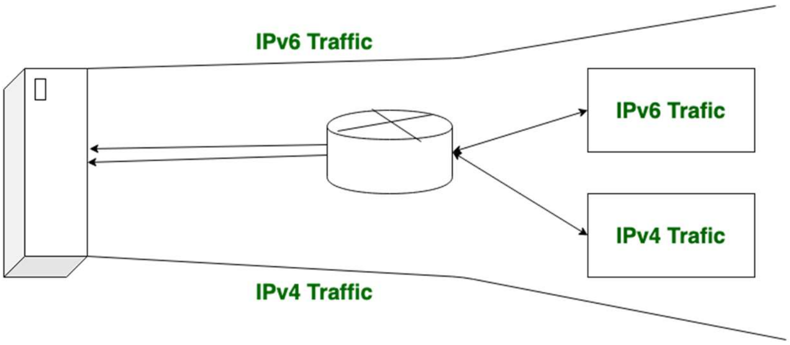
In the current scenario, the IPv4 address is exhausted and IPv6 had come to overcome the limit.
When we want to send a request from an IPv4 address to an IPv6 address, but it isn't possible because IPv4 and IPv6 transition is not compatible. For a solution to this problem, we use some technologies.

The technologies used here are as follows:

- Dual Stack Routers
- Tunneling
- NAT Protocol Translation

Dual-Stack Routers:

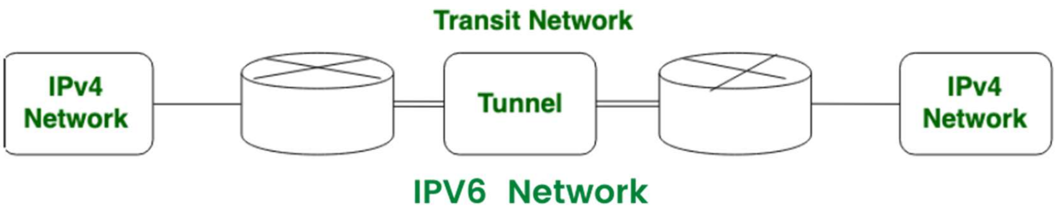
In dual-stack router, A router's interface is attached with IPv4 and IPv6 addresses configured are used in order to transition from IPv4 to IPv6.



In this above diagram, A given server with both IPv4 and IPv6 addresses configured can communicate with all hosts of IPv4 and IPv6 via dual-stack router (DSR). The dual stack router (DSR) gives the path for all the hosts to communicate with the server without changing their IP addresses.

Tunneling:

Tunneling is used as a medium to communicate the transit network with the different IP versions.

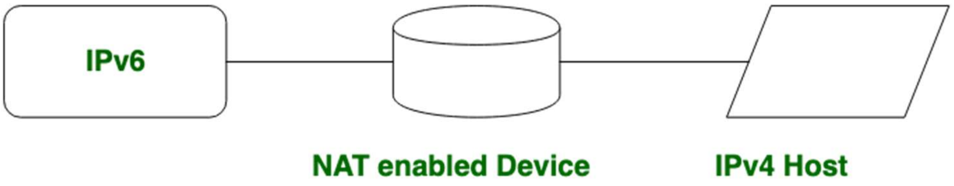


In this above diagram, the different IP versions such as IPv4 and IPv6 are present. The IPv4 networks can communicate with the transit or intermediate network on IPv6 with the help of the Tunnel.
It's also possible that the IPv6 network can also communicate with IPv4 networks with the help of a Tunnel.

NAT Protocol Translation:

With the help of the NAT Protocol Translation technique, the IPv4 and IPv6 networks can also communicate with each other which do not understand the address of different IP version.

Generally, an IP version doesn't understand the address of different IP version, for the solution of this problem we use NAT-PT device which removes the header of first (sender) IP version address and add the second (receiver) IP version address so that the Receiver IP version address understand that the request is sent by the same IP version, and its vice-versa is also possible.

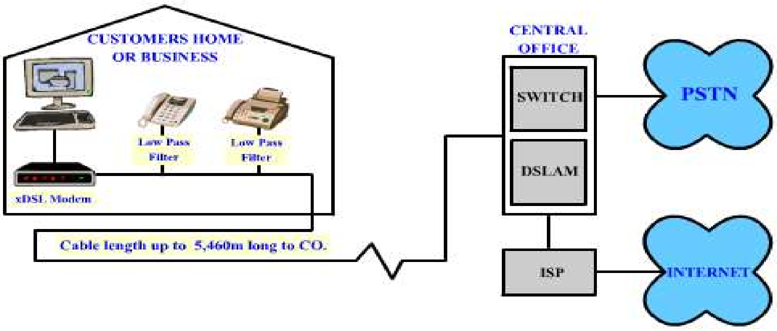


In the above diagram, an IPv4 address communicates with the IPv6 address via a NAT-PT device to communicate easily. In this situation, the IPv6 address understands that the request is sent by the same IP version (IPv6) and it responds.

UNIT-5

Digital Subscriber Line (DSL):

Digital Subscriber Line (DSL) is a communication medium, which is used to transfer internet through copper wire telecommunication line. Along with cable internet, DSL is one of the most popular ways ISPs provide broadband internet access. Its aim is to maintain the high speed of the data being transferred.



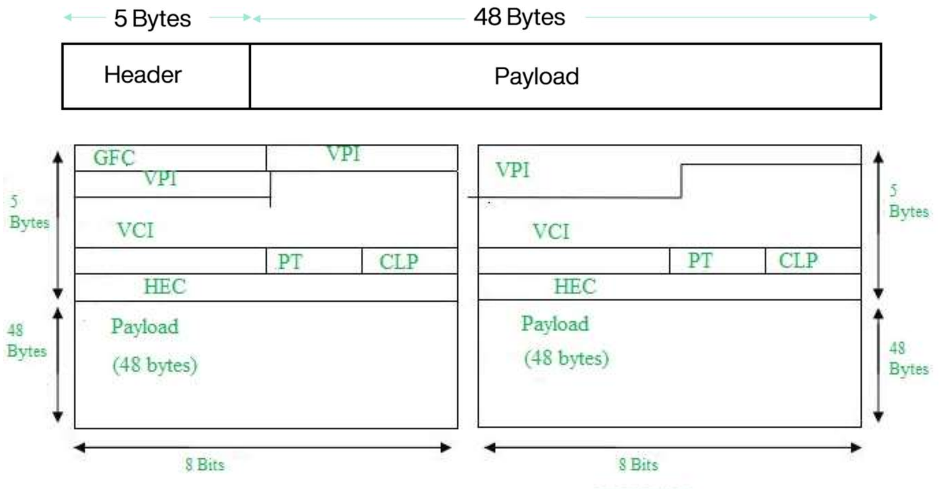
Symmetric DSL	Splits the upstream and downstream frequencies evenly, providing equal speeds to both uploading and downloading data transfer.	2 MB/s upstream 2 MB/s downstream
Asymmetric DSL	Provides a wider frequency range for downstream transfers, which offers several times faster downstream speeds.	20 MB/s downstream 1.5 MB/s upstream

Advantages:

- No Additional Wiring and cost-effective.
- Users can use both telephone lines and the internet at the same time.
- Users can choose between different connection speeds and pricing from various providers.
- Disadvantages:
- DSL Internet service only works over a limited physical distance and remains unavailable in many areas where the local telephone infrastructure does not support DSL technology.
- The service is not available everywhere.
- The connection is faster for receiving data than it is for sending data over the Internet.

Asynchronous Transfer Mode (ATM):

- Destined to replace most existing WAN technologies.
- Improves on performance of Frame Relay.
- 53-byte cells of fixed size = 48-byte data+5 header.
- The standard-sized cells allow switching mechanisms to achieve faster switching rates
- Rates of 155 – 622 MB/s are achieved with theoretical rates up to 1.2 GB/s.
- Compatible with twisted-pair, coax, and fiber.
- ATM uses Asynchronous Time Division Multiplexing.
- Allows any-speed and even variable rate connection.
- ATM standard (defined by CCITT) is widely accepted by common carriers as mode of operation for communication – particularly BISDN.
- ATM is a form of cell switching using small fixed-sized packets.



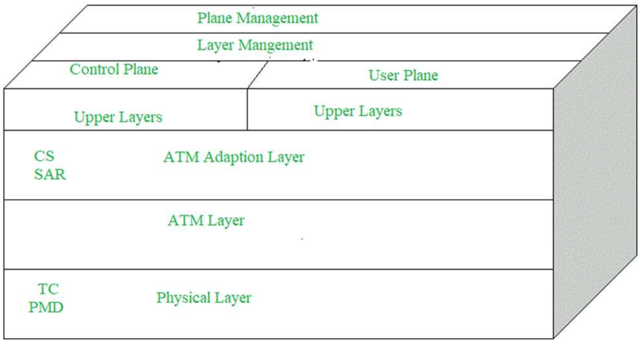
UNI Cell Format

NNI Cell Format

User - Network Interface Header: The UNI Header is used within private networks of ATMs for communication between ATM endpoints and ATM switches. It includes the Generic Flow Control (GFC) field.

Network - Network Interface Header: The NNI is used for communication between ATM switches, and it does not include the Generic Flow Control(GFC) instead it includes a Virtual Path Identifier (VPI) which occupies the first 12 bits.

ATM Layers



TM Adaption Layer (AAL):

It is meant for isolating higher-layer protocols from details of ATM processes and prepares for conversion of user data into cells and segments it into 48-byte cell payloads. AAL protocol excepts transmission from upper-layer services and helps them in mapping applications, e.g., voice, data to ATM cells.

Physical Layer:

It manages the medium-dependent transmission and is divided into two parts physical medium-dependent sublayer and transmission convergence sublayer.

The main functions are as follows:

- It converts cells into a bitstream.
- It controls the transmission and receipt of bits in the physical medium.
- It can track the ATM cell boundaries.
- Look for the packaging of cells into the appropriate type of frames.

ATM Layer:

It handles transmission, switching, congestion control, cell header processing, sequential delivery, etc., and is responsible for simultaneously sharing the virtual circuits over the physical link known as cell multiplexing and passing cells through an ATM network known as cell relay making use of the VPI and VCI information in the cell header.

ATM Applications:

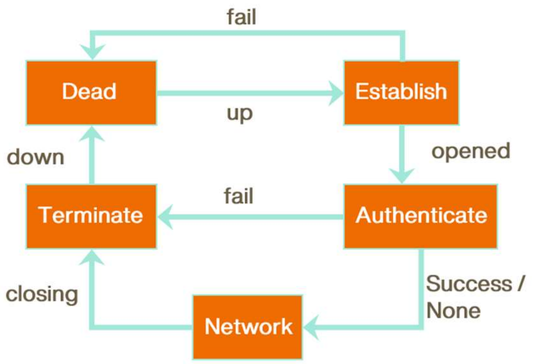
ATM WANs	It can be used as a WAN to send cells over long distances, a router serving as an end-point between ATM network and other networks, which has two stacks of the protocol.
Multimedia VPNs	It helps in managing ATM, LAN, voice, and video services and is capable of full-service virtual private networking, which includes integrated access to multimedia.
Frame Relay Backbone	Frame relay services are used as a networking infrastructure for a range of data services and enabling frame-relay ATM service to Internetworking services.
Residential Broadband Networks	ATM is by choice provides the networking infrastructure for the establishment of residential broadband services in the search of highly scalable solutions.
Carrier infrastructure for telephone and PLNs	To make more effective use of SONET/SDH fiber infrastructures by building the ATM infrastructure for carrying the telephonic and private-line traffic.

Point-to-Point Protocol (PPP):

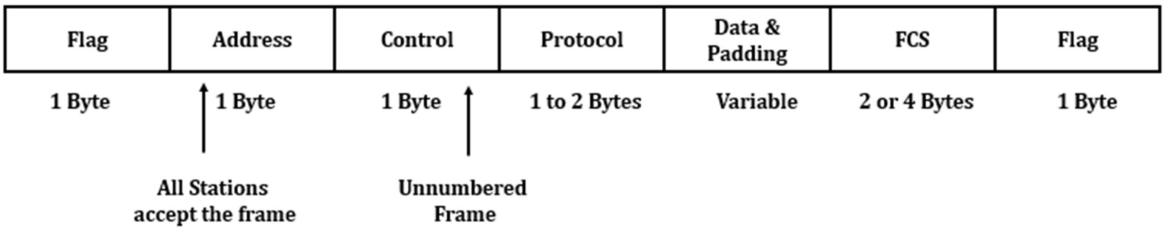
The telephone line or cable companies provide a physical link, but to control and manage the transfer of data, there is a need for a special protocol. The Point-to-Point Protocol (PPP) was designed to respond to this need.

- PPP is comprised of three main components:
- A method for encapsulating multi-protocol datagrams.
- A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.
- Network Control Protocols (NCPs) for establishing and configuring different network – layer protocols.

State Machine of PPP:



Dead	It means that the link is not being used.
Establish	When one of the end machines starts the communication, the connection goes into the establishing state.
Authenticate	The user sends the authenticate request packet & includes the username & password.
Network	The exchange of user control and data packets can start.
Terminate	The users sends this to terminate the link.

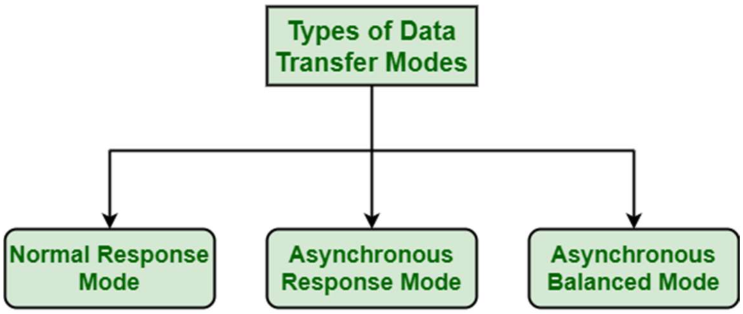


Field Name	Role
Flag Field	The flag field identifies the boundaries of a PPP frame. Its value is 01111110.
Address Field	It uses the broadcast address used in most LANs, 11111111, to avoid a data link address in the protocol.
Control Field	The control field is assigned the value 11000000 to show that, as in most LANs, the frame has no sequence number; each frame is independent.
Protocol Field	The protocol field defines the type of data being carried in the data field: user data or other information.
Data Field	This field carries either user data or other information.
FCS Field	The frame check sequence field is simply a 2-byte or 4-byte CRC used for error detection.

HDLC and its Transfer Modes:

High-Level Data Link Control (HDLC) is basically data link control protocol that is capable of supporting range of various models of operation or data transfer. A mode in HDLC generally represents relationship among two devices that are involved in an exchange.

A mode basically describes who actually controls data link. HDLC communications session uses several modes of data transfer or communications simply to determine or identify how primary and secondary stations actually interact with each other. HDLC basically offers and provides three different modes of operations.

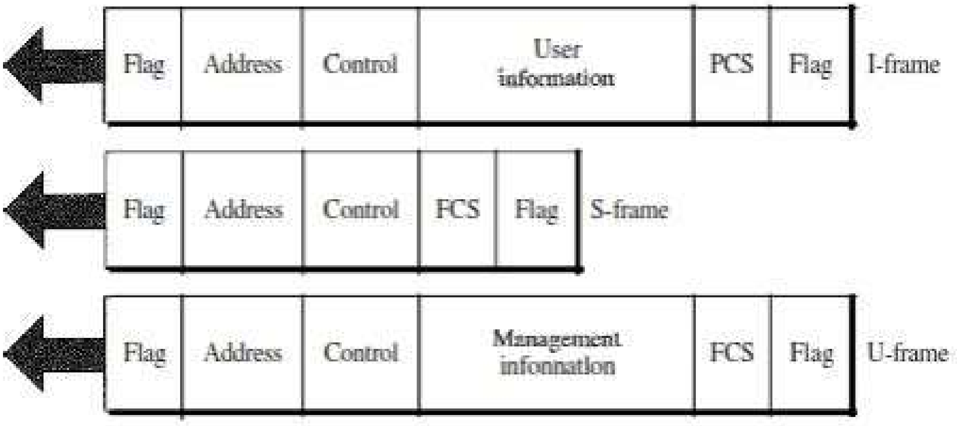

Types of Data Transfer Modes
Normal Response Mode
Asynchronous Response Mode
Asynchronous Balanced Mode

Normal Response Mode (NRM)	Asynchronous Response Mode (ARM)	Asynchronous Balanced Mode (ABM)
Unbalanced configuration.	Unbalanced configuration.	Balanced configuration.
Primary can only initiate transmission.	Primary is responsible for connect, disconnect, error recovery, and initialization.	Either station may initiate transmission without receiving permission.
Secondary may only transmit data in response to command (poll) from primary.	Secondary may initiate transmission without permission form primary.	Either station may initiate transmission without receiving permission.
Used on multi-drop lines.	Rarely used.	Most widely used.

Here, the host computer acts as primary and the terminals as secondary.

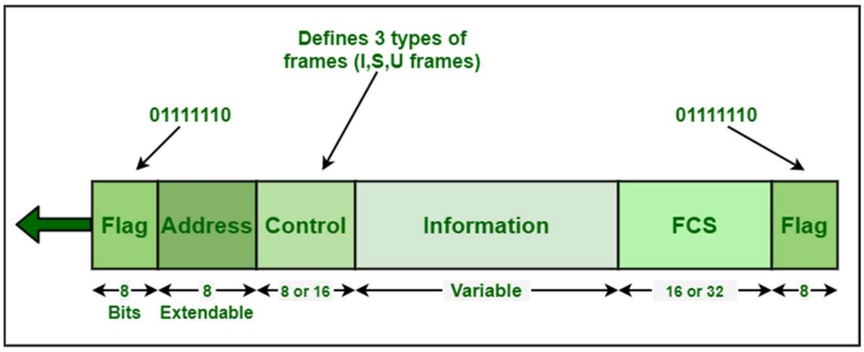
Frame Structure of HDLC:

High-Level Data Link Control (HDLC) generally provides flexibility to simply support all options that are possible in various data transfer modes and configurations. To provide flexibility, HDLC basically uses and explains three different types of frames: Information Frame, Supervisory Frame, Unnumbered Frame.



Frame Structure:

Each and every frame on link should begin and end with Flag Sequence Field (F). Each of frames in HDLC includes mainly six fields. It begins with a flag field, an address field, a control field, an information field, a frame check sequence (FCS) field, and an ending flag field.



Basic Frame Structure

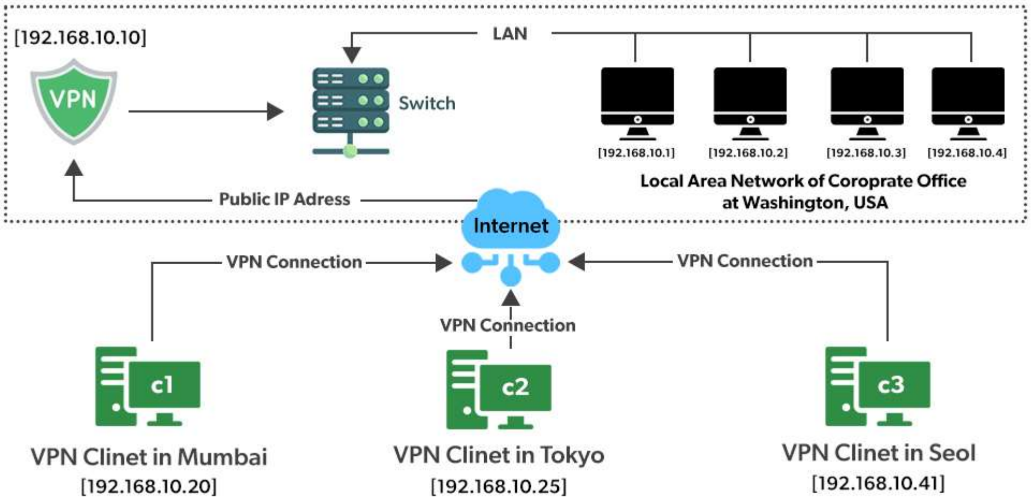
Field Name	Size (bits)	Role
Flag Field	8 bits	Responsible for initiation and termination of error checking.
Address Field	8 bits	It helps to identify secondary station will sent or receive data frame.
Control Field	8 or 16 bits	Used to determine how to control process of communication.
Information Field	Variable	Contains data of users the sender is transmitting to receiver in an I-frame and network layer in U-frame.
FCS Field	16 or 32 bits	Used to confirm and ensure that data frame was not corrupted by medium that is used to transfer frame from sender to receiver.
Closing Flag Field	8 bits	The ending flag field of one frame can serve as beginning flag field of the next frame in multiple-frame transmissions.

Virtual Private Network (VPN):

VPN stands for the virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. A Virtual Private Network is a way to extend a private network using a public network such as the internet. The name only suggests that it is a Virtual “private network” i.e., user can be part of a local network sitting at a remote location. It makes use of tunneling protocols to establish a secure connection.

The situation is described below:

- All 100 hundred computers of the corporate office at Washington are connected to the VPN server(which is a well-configured server containing a public IP address and a switch to connect all computers present in the local network i.e., in US head office).
- The person sitting in the Mumbai office connects to The VPN server using a dial-up window and the VPN server returns an IP address that belongs to the series of IP addresses belonging to a local network of the corporate office.
- Thus, person from the Mumbai branch becomes local to the head office and information can be shared securely over the public internet.
- So, this is the intuitive way of extending the local network even across the geographical borders of the country.



Using VPN is legal in most of the countries. The legality of using a VPN service depends on the country and its geopolitical relations with another country as well. A reliable and secure VPN is always legal if you are not intended to use it for any illegal activities like committing fraud online, cyber theft, or in some countries downloading copyrighted content.

- VPN also ensures security by providing an encrypted tunnel between client and VPN server.
- VPN is used to bypass many blocked sites.
- VPN facilitates Anonymous browsing by hiding your ip address.
- Also, most appropriate Search engine optimization(SEO) is done by analysing the data from VPN providers which provide country-wise stats of browsing a particular product.

China has decided to block all VPN(Virtual private network)s by next year, as per the report of Bloomberg. Many Chinese Internet users use VPNs to privately access websites that are blocked under China’s so-called “great firewall”. This is done to avoid any information leakage to rival countries and so as to tighten the information security.