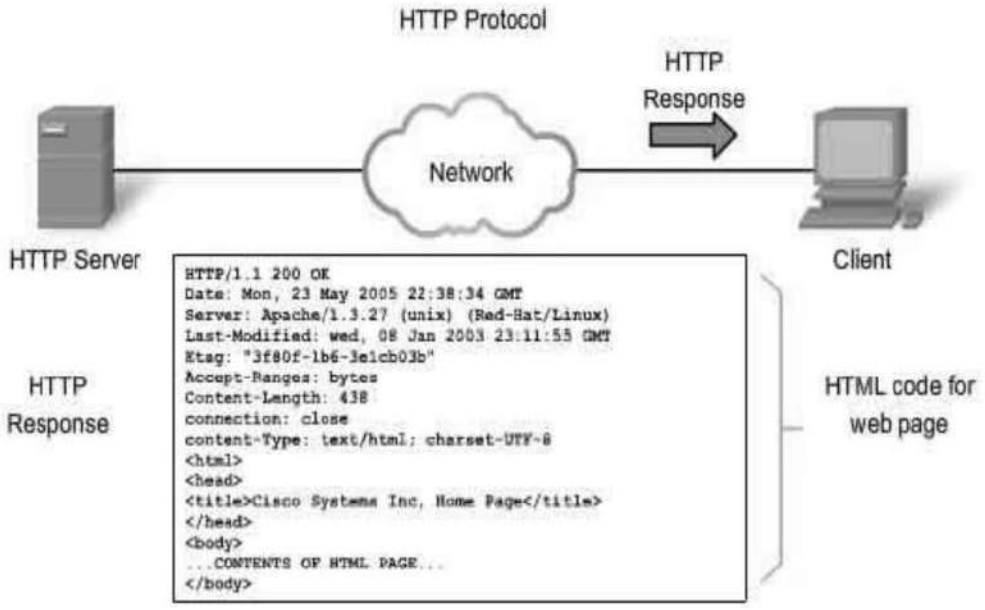
HTTP (Hypertext Transfer Protocol)

Hypertext Transfer Protocol is an algorithm for transferring data on the Web. HTTP essentially publishes and retrieves the HTTP pages on the World Wide Web. HTTP is a language used to contact the browser and the Web server. The information transmitted via HTTP can be audio, video, text, images, and hypertext.

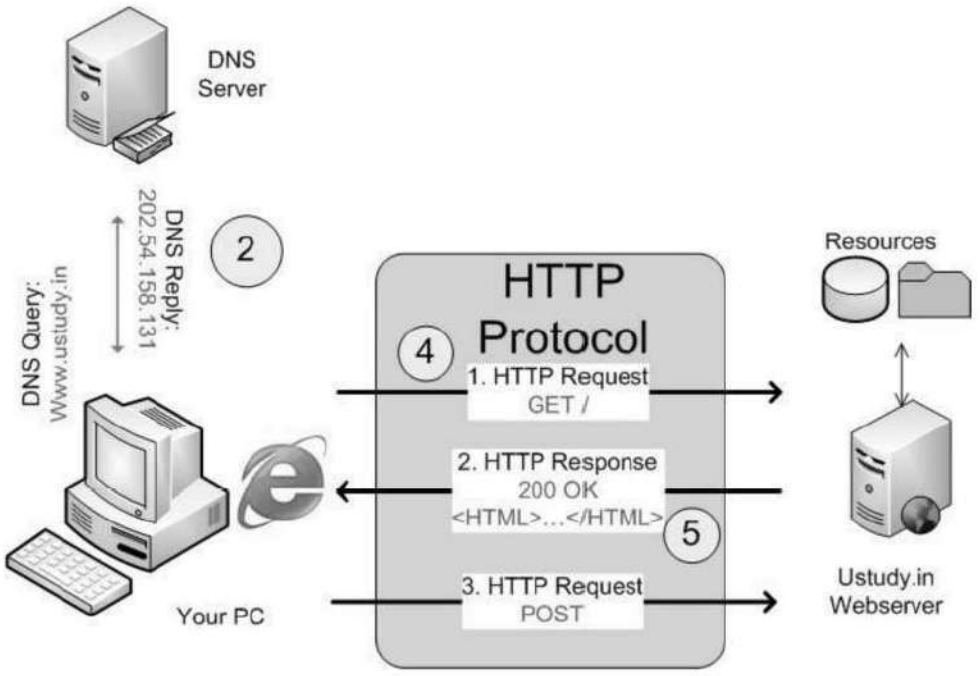
Many proxies are available between the Web browser (client) and server (Web server).

An HTTP client requests to establish a TCP connection to a specific port on the remote host (usually 80 or 8080).

An HTTP server listens to that port and sends a request message to the client. The application server returns a 200 OK message, the user message, an error message, or any other message.



In response to the request, the HTTP server returns code for a web page.



1. The Address Resolution Protocol (ARP) is a network protocol that maps an IP address to its corresponding Media Access Control (MAC)

address on a local network.

2. *ARP operates at the data link layer of the OSI model and is essential for communication between devices within the same network.*
3. *When a device wants to send data to another device on the local network, it first checks its ARP cache (a table that stores IP-to-MAC address mappings) to see if it already has the MAC address of the destination device.*
4. *If the MAC address is not found in the ARP cache, the device sends an ARP request broadcast message to the local network, asking for the MAC address associated with the specified IP address.*
5. *The device with the matching IP address in the local network responds with an ARP reply message, providing its MAC address to the requesting device.*
6. *The requesting device then updates its ARP cache with the IP-to-MAC address mapping received in*

the ARP reply message, allowing future communication with the destination device without further ARP requests.

7. ***ARP is crucial for adequately functioning IP-based networks, as it enables devices to dynamically discover and maintain the MAC address associations required for successful data transmission within the local network.***
8. ***However, ARP is susceptible to security risks, such as spoofing or ARP poisoning, where malicious devices provide false MAC address information, leading to network disruptions or unauthorized access. Various security measures, such as ARP cache poisoning detection and protection, can be implemented to mitigate these risks.***

Poe

1. ***The Hypertext Transfer Protocol (HTTP) is used to transmit and receive web-based information over the Internet.***
2. ***HTTP operates at the application layer of the OSI model and is the foundation of data communication for the World Wide Web.***
3. ***HTTP follows a client-server model, where a client (typically a web browser) sends requests to a server, and the server responds with the requested data or performs the requested action.***
4. ***HTTP uses a request-response paradigm, where the client sends an HTTP request message to the server, specifying the desired action (such as retrieving a webpage or submitting a form).***
5. ***The server processes the request and sends back an HTTP response message containing the requested data, along with a status code indicating the success or failure of the request.***

6. ***HTTP relies on Uniform Resource Identifiers (URIs), more commonly known as URLs (Uniform Resource Locators), to identify and locate resources on the web.***
7. ***HTTP supports various methods or verbs, such as GET, POST, PUT, and DELETE, which define the type of action to be performed on the server.***
8. ***HTTP is a stateless protocol, meaning that each request from the client is independent and does not maintain any memory of previous requests.***
9. ***To enable stateful interactions, HTTP introduced cookies, which are small data stored on the client side and sent with each subsequent request to maintain session information.***
10. ***HTTP can be secured using the Hypertext Transfer Protocol Secure (HTTPS), which adds an additional layer of encryption through SSL/TLS protocols, ensuring secure data transmission.***
11. ***HTTP supports various content types,***

including text, images, audio, video, and more, allowing for the transfer of a wide range of data formats.

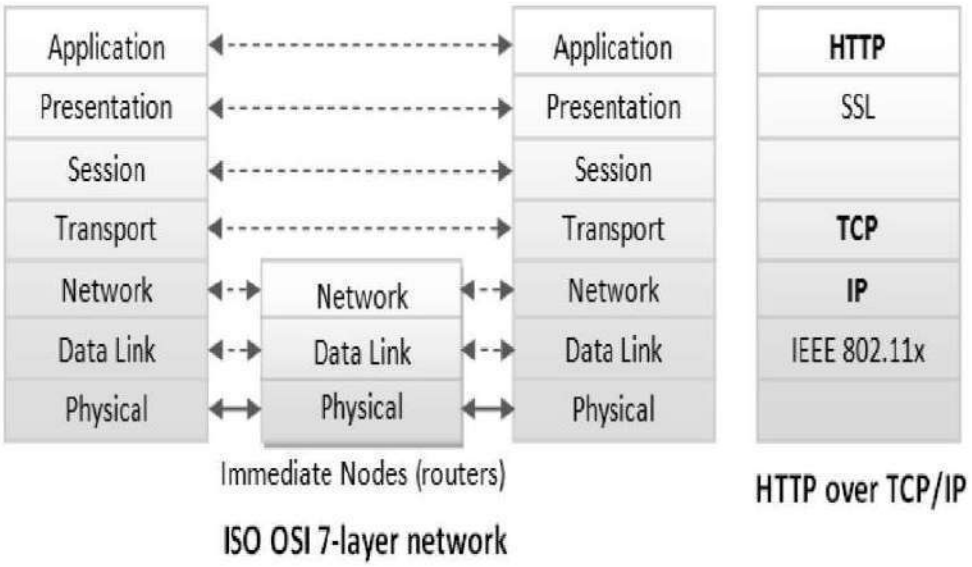
12. *HTTP headers provide additional information about the request or response, such as content type, caching directives, and authentication credentials.*

13. *HTTP supports caching, allowing clients to store and reuse previously fetched resources, reducing the need for repeated requests to the server.*

14. *HTTP supports redirection, allowing servers to redirect clients to a different URL or resource based on certain conditions or rules.*

15. *The continuous development and standardization of HTTP have led to various versions, with HTTP/1.1 and HTTP/2 being the most widely used versions, each introducing performance, security, and efficiency*

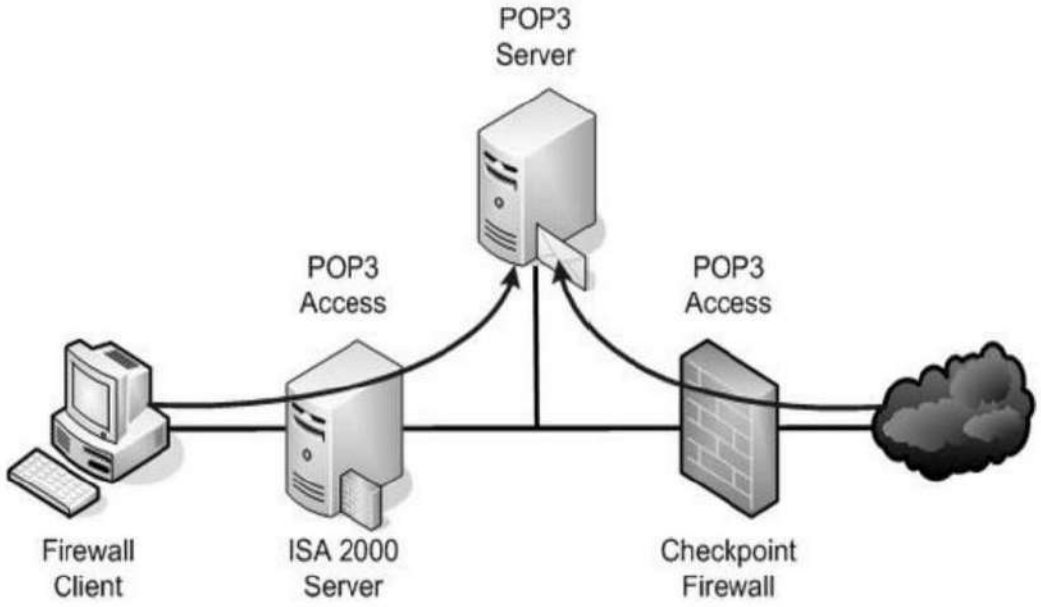
improvements.

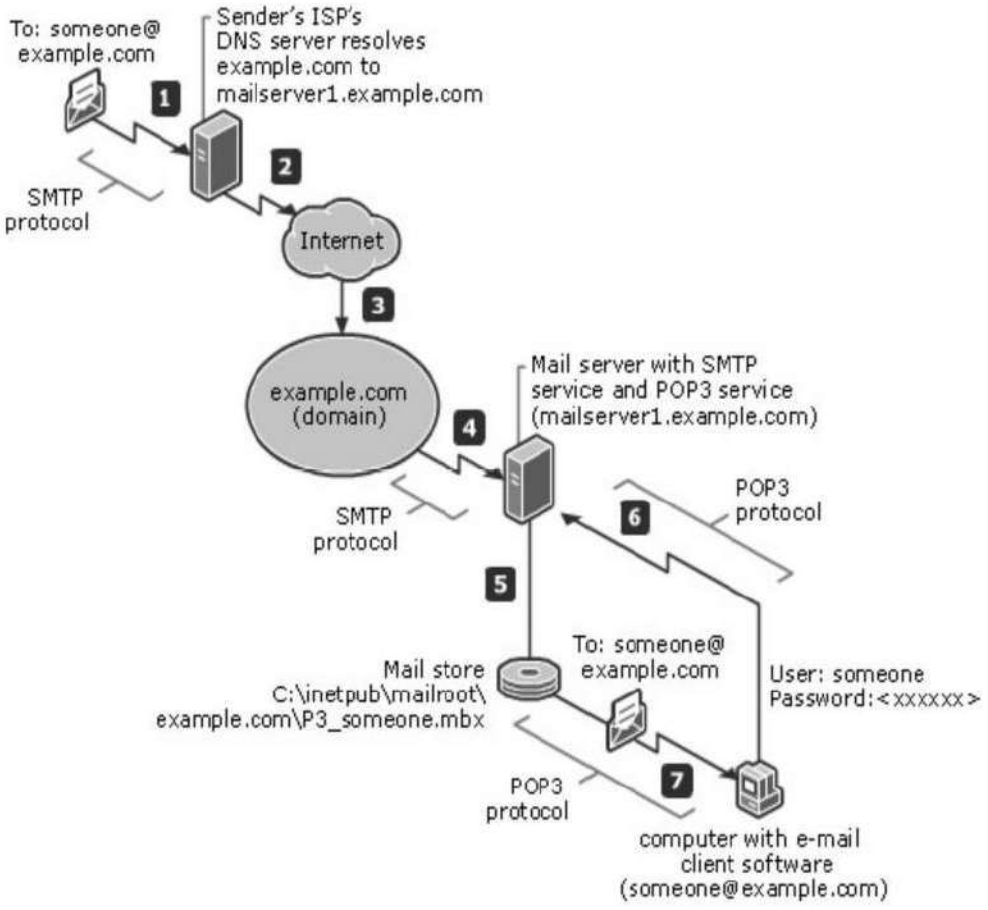


POP3 (Post Office Protocol)

POP3 (Post Office Protocol 3) is a standard protocol for receiving email. POP3 is a client/server protocol in which an Internet server receives email.

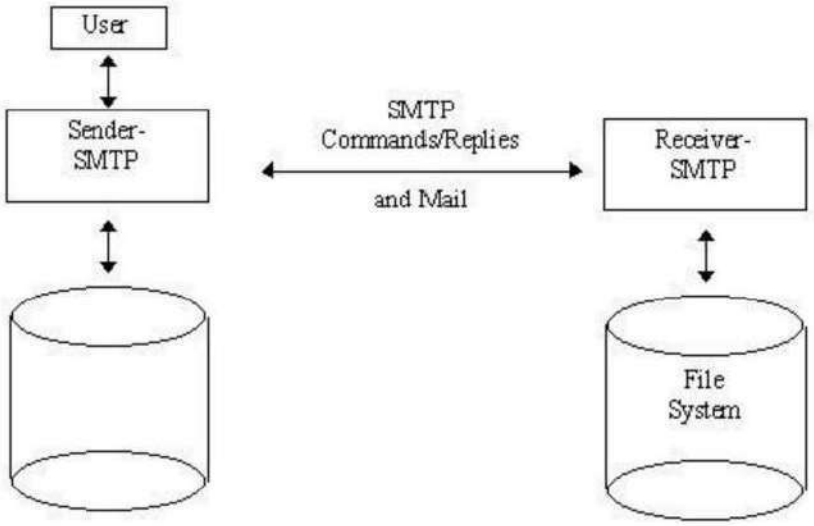
Periodically, the user can receive an email, check the mailbox on the server, and download any mail, probably via POP3. This standard protocol is built into popular email products like Eudora and Outlook Express. It was also incorporated into the Netscape and Microsoft Internet Explorer browsers.


POP3
Server
POP3
Access
POP3
Access
Firewall
Client
ISA 2000
Server
Checkpoint
Firewall


To: someone@
example.com
Sender's ISP's
DNS server resolves
example.com to
mailserver1.example.com
1
2
SMTP
protocol
Internet
3
example.com
(domain)
Mail server with SMTP
service and POP3 service
(mailserver1.example.com)
4
SMTP
protocol
POP3
protocol
6
5
Mail store
C:\inetpub\mailroot\
example.com\P3_someone.mbx
To: someone@
example.com
User: someone
Password:<xxxxxx>
POP3
protocol
7
computer with e-mail
client software
(someone@example.com)

SMTP (Simple Mail Transfer Protocol)

The Simple Mail Transfer Protocol is a protocol for sending email messages between servers. Most email systems and clients use SMTP to send messages from one server to another.



In configuring the e-mail application, the user must configure POP, SMTP, and IMAP in the user's email software. The SMTP protocol is simple and text-based and specifies one or more recipients of the message, and the message is transmitted. The Telnet utility easily verifies the SMTP connection. Default SMTP uses TCP port 25

FTP (File Transfer Protocol)

FTP or file transfer protocol transfers data (upload/download) from one computer to another over the Internet or computer network.

FTP is a communication protocol commonly used for transferring files over the Internet. Typically, two computers are involved in transmitting files from a server and a client.

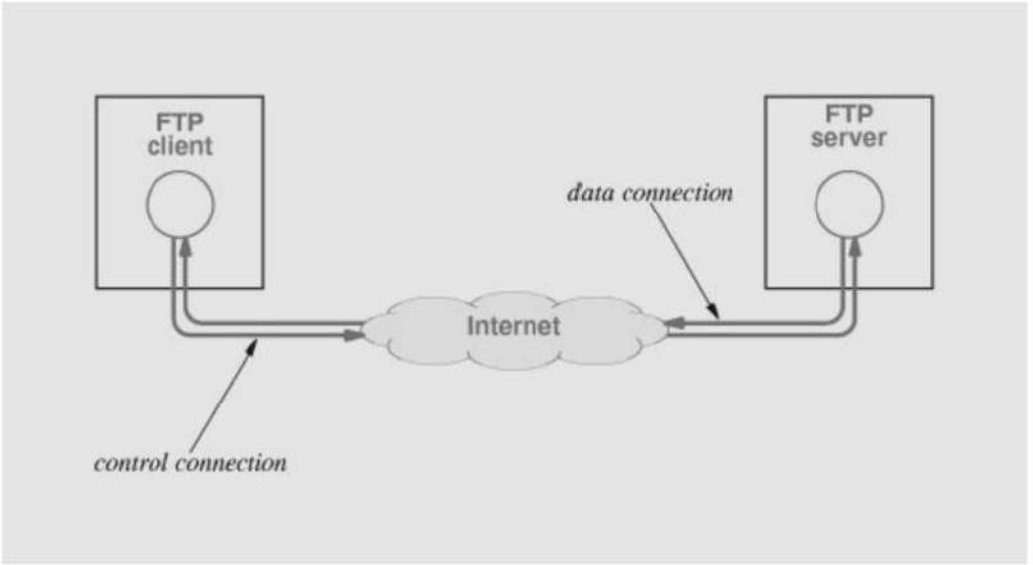
The client computer on which the FTP client software connects to the remote computer (server).

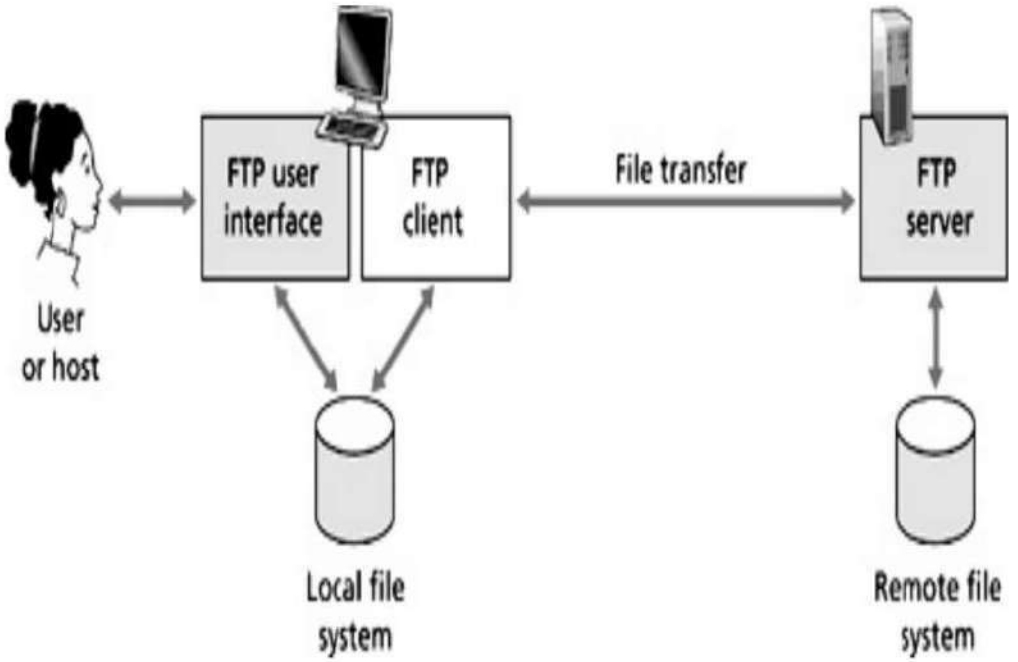
After a successful connection to the server, the client computer may perform a series of operations, such as downloading files, uploading performs, renaming and deleting files, creating new folders, etc. The practical operating system supports FTP protocols.

1. *FTP (File Transfer Protocol) is a widely used network protocol that transfers files between computers on a network.*

2. *It operates on the client-server model, where the client initiates the connection to the server and requests file transfers.*
3. *FTP uses two separate channels for communication: the control channel, which handles commands and responses between the client and server, and the data channel, which is responsible for transferring the actual files.*
4. *It supports various authentication methods, including username and password and anonymous access for public file repositories.*
5. *FTP supports ASCII and binary data transfer modes, enabling the transfer of text-based files and binary files like images or executables.*
6. *It provides features such as directory listing, file renaming, and file deletion, allowing users to manage files on the server remotely.*
7. *While FTP is widely supported, it has some security vulnerabilities, such as transmitting data in plain text.*

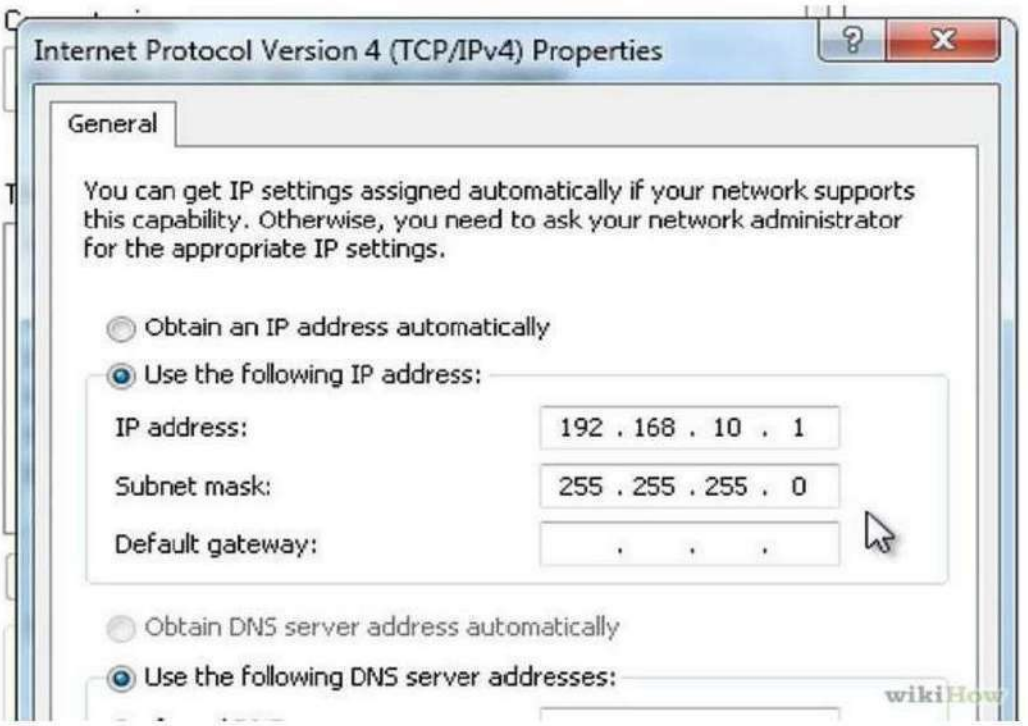
It is recommended to use secure alternatives like FTPS (FTP over SSL) or SFTP (SSH File Transfer Protocol) for encrypted file transfers.





IP (Internet Protocol)

An Internet protocol (IP) is a unique identifier or address of each computer or communications network device and the Internet. Each network device participating computer, such as a router, computer, printer, fax machine, and Internet switch, can have its unique IP address. Each Internet domain must have a unique IP address or a shared IP address.



.

DHCP (Dynamic Host Configuration Protocol)

DHCP or Dynamic Host Configuration Protocol is a set of rules used by a communication device such as a router adapter or computer network, allowing the device to request and obtain a server's IP address with one list of many directions.

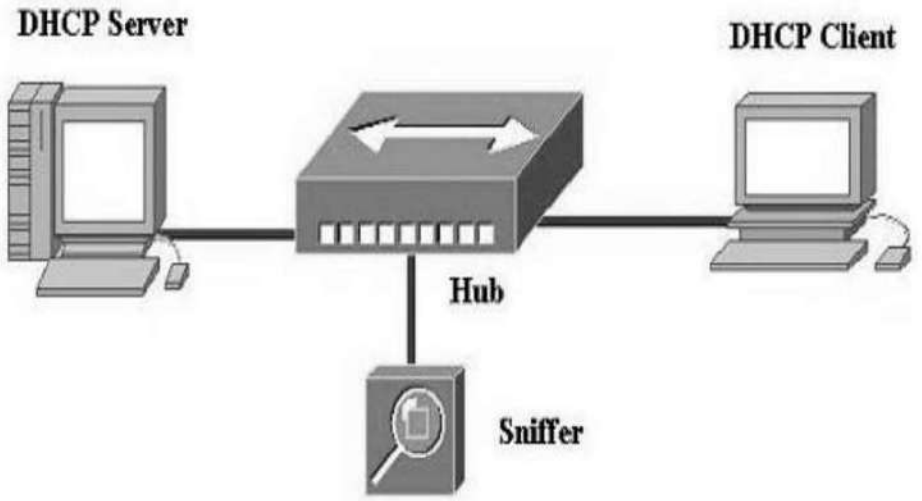
DHCP is a protocol for network equipment to obtain IP addresses and other settings such as a gateway, DNS, and subnet mask of the DHCP server.

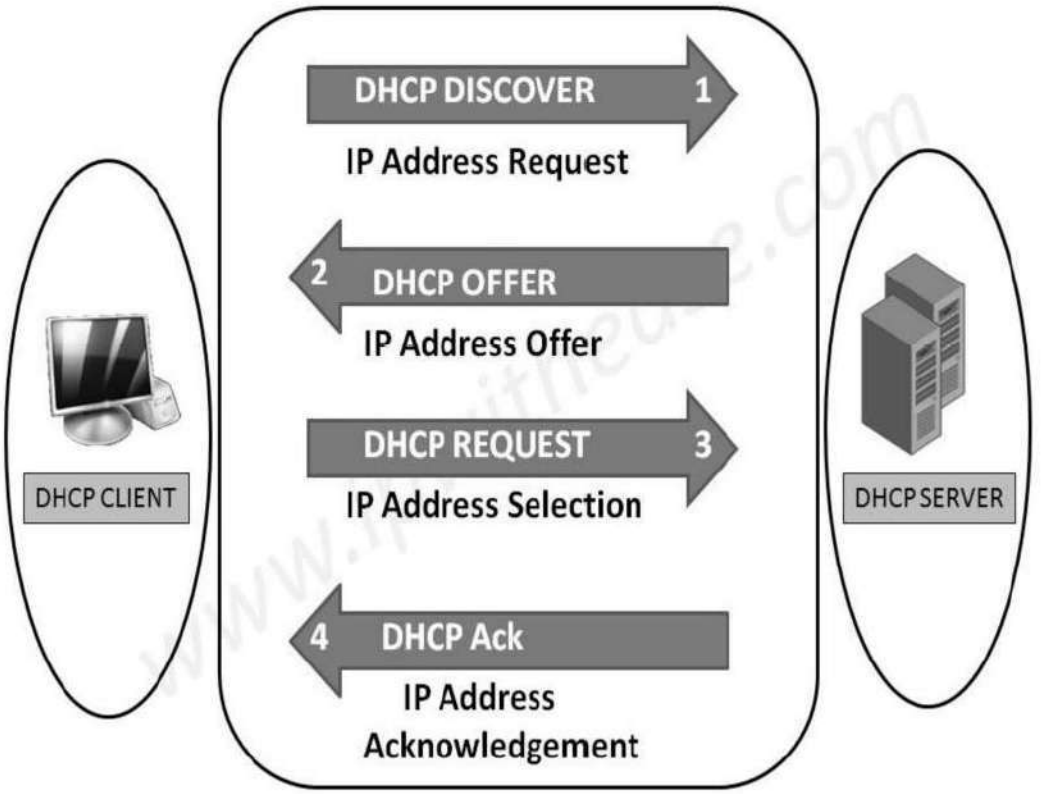
DHCP ensures that all IP addresses are unique and IP address management is performed by the. The allocation of IP addresses expires after a determined time.

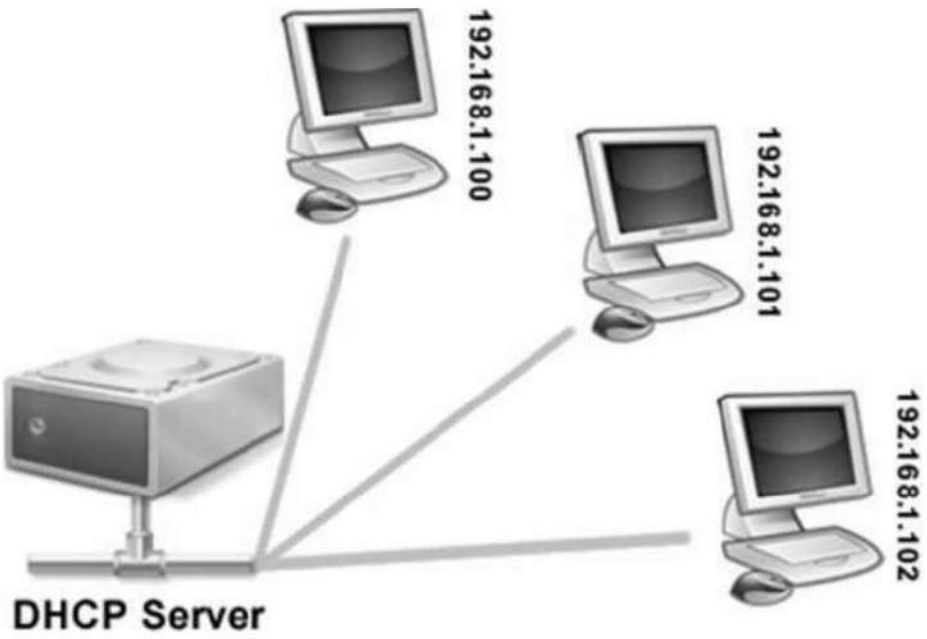
DHCP works in four phases, known as DORA:

1. *Discover*
2. *Observe*
3. *Request*
4. *Authorize*

Network Topology where DHCP Client and Server Reside on Same LAN Segment



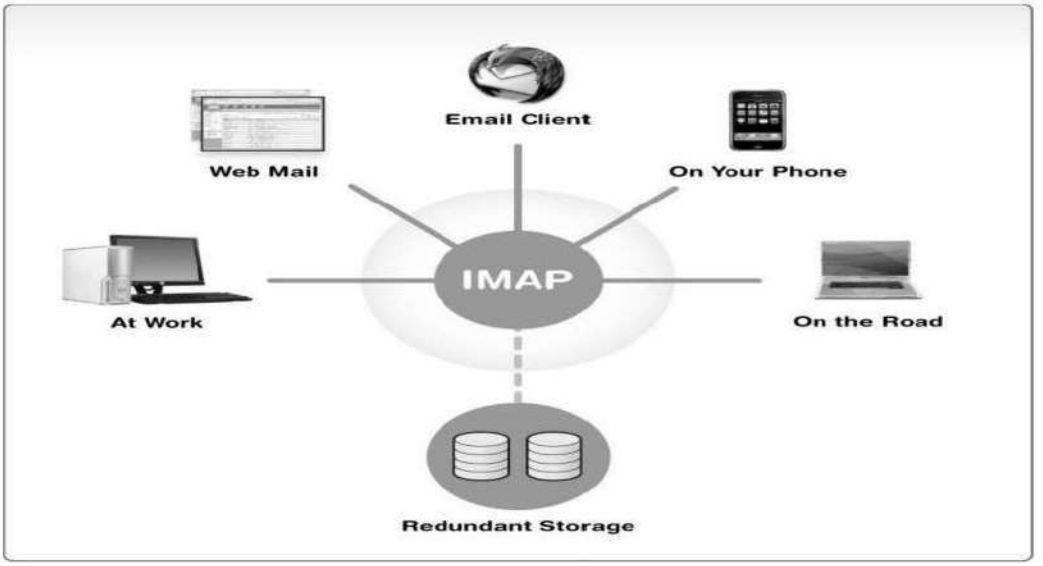


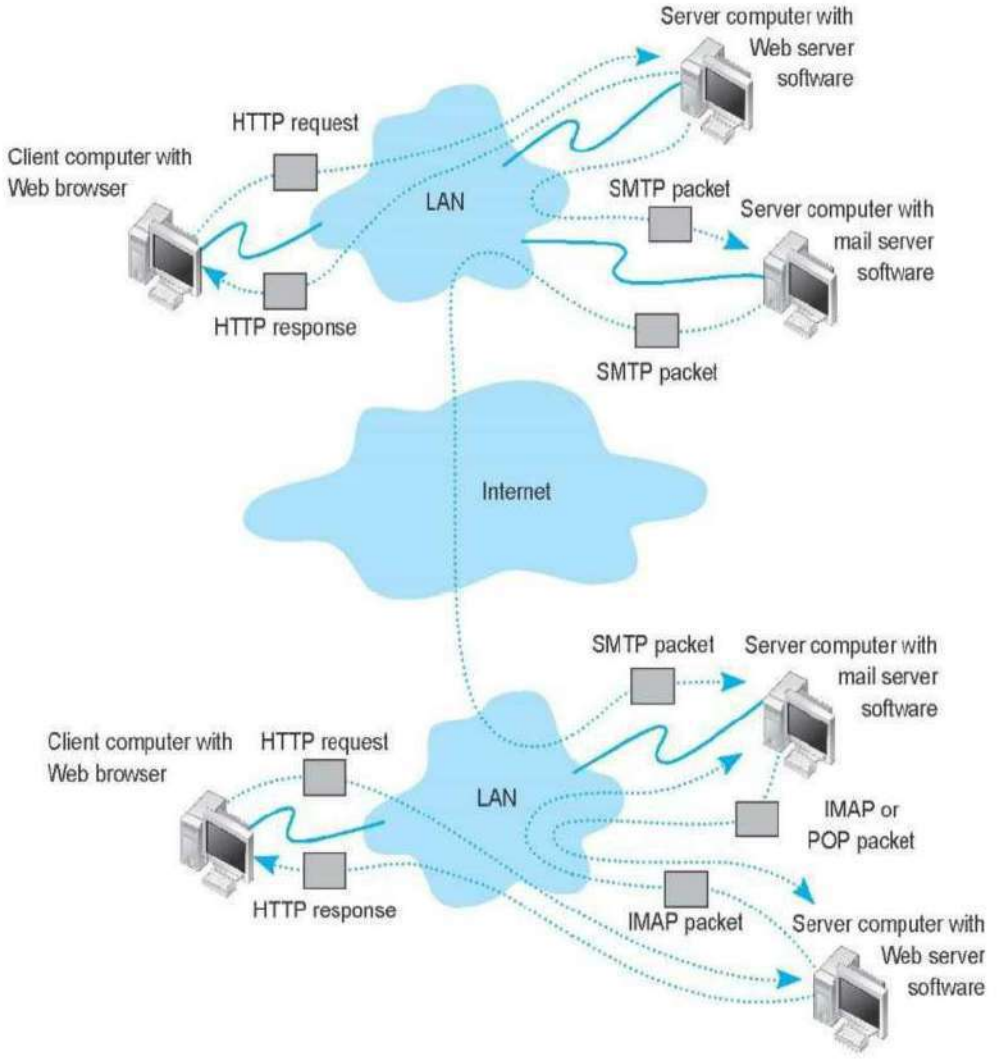


IMAP (The Internet Message Access Protocol)

IMAP works in application layer protocol. It is used to access e-mails on remote servers. POP3 and IMAP protocols are the two most common e-mails used.

The emails are usually stored on the mail server, and users recover these messages using a web browser or email client. IMAP allows users to access their messages immediately on their systems.


Email Client
Web Mail
On Your Phone
IMAP
At Work
On the Road
Redundant Storage


Server computer with Web server software
HTTP request
Client computer with Web browser
LAN
SMTP packet
Server computer with mail server software
HTTP response
SMTP packet
Internet
SMTP packet
Server computer with mail server software
Client computer with Web browser
HTTP request
LAN
IMAP or POP packet
HTTP response
IMAP packet
Server computer with Web server software

ARCNET

ARCNET is a local area network technology with a token bus system to manage the trunk line between workstations. If a device in a network wants to send a message, a token set to 1 is inserted. A target device reads the message, and the token is set to 0 so another device can use the frame.

FDDI

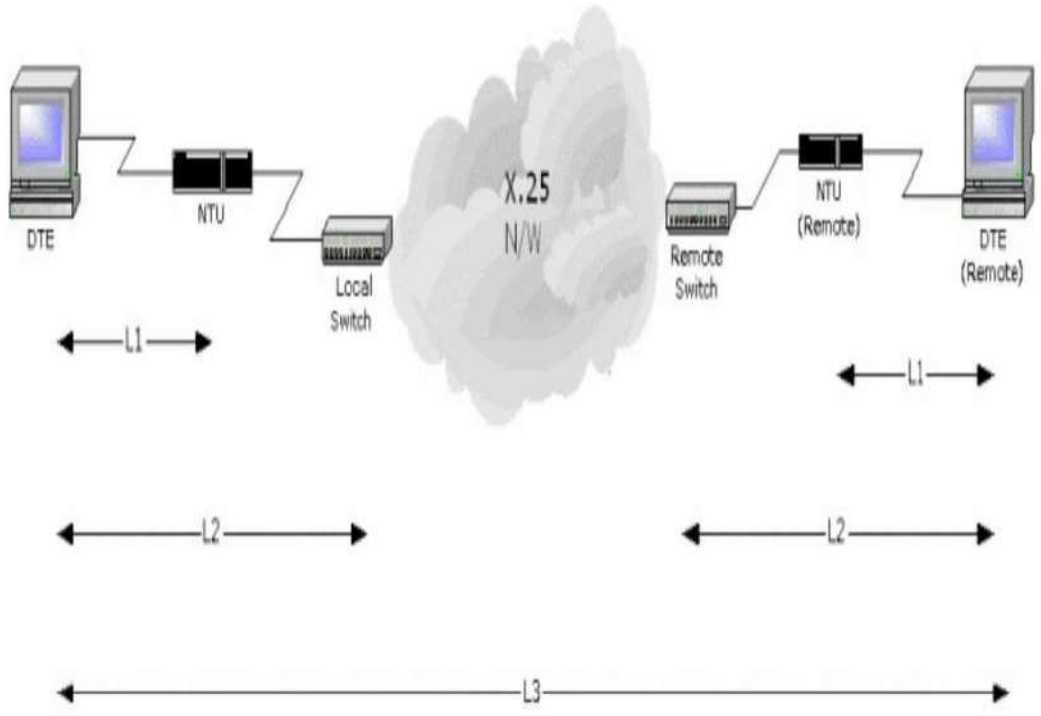
Fiber Distributed Data Interface (FDDI) provides a standard for data transmission in a local area network that can extend a range of 200 kilometers.

The FDDI-ring network protocol is used as a base. The FDDI local area network can support a large number of users and can cover a wide geographic area.

An FDDI network contains two token rings; the main ring has a 100 Mbit / s capacity. FDDI is an ANSI standard network that supports 500 stations at 2 Kilometers.

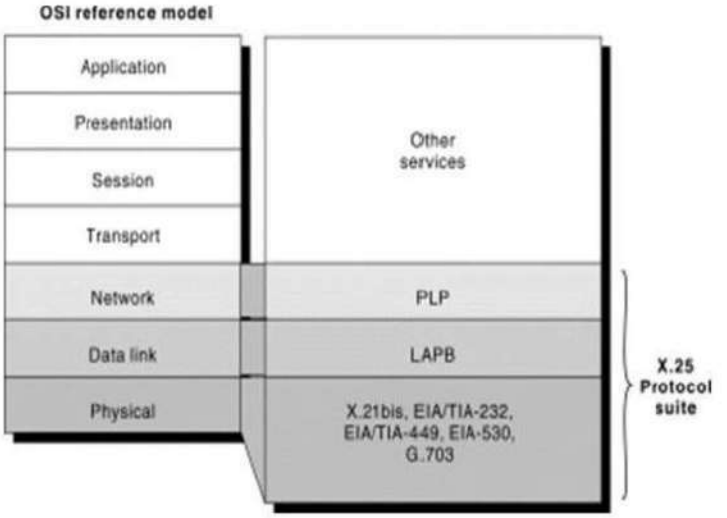
X.25

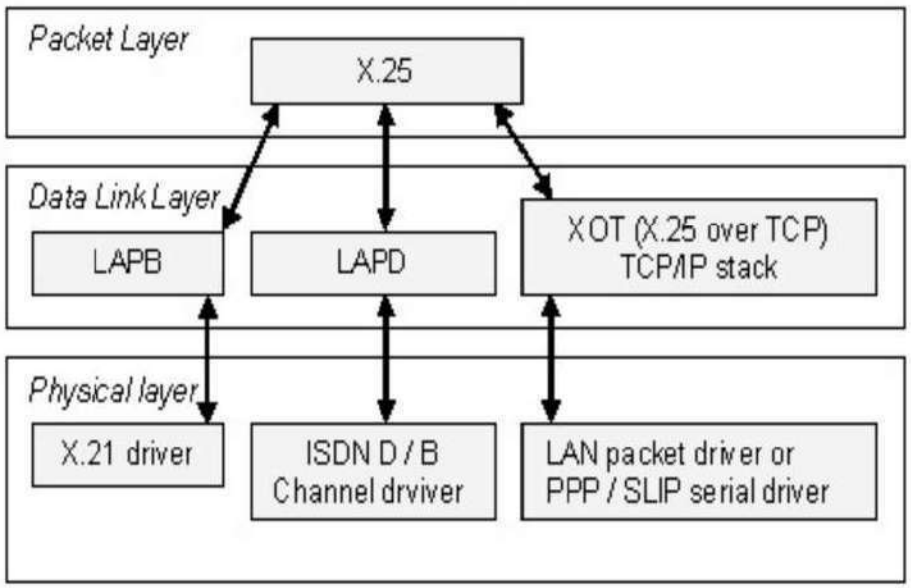
X.25 is a set of standard protocols for wide area networks using a telephone line or ISDN system. The X.25 standard was approved by CCITT now ITU in 1976.



Layer1 - Physical
Layer2 - Data Link
Layer3 - Packet

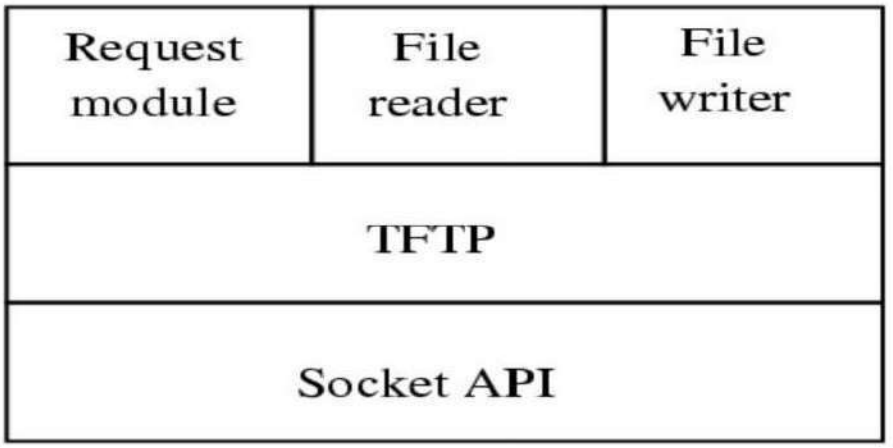
Protocolos do X.25

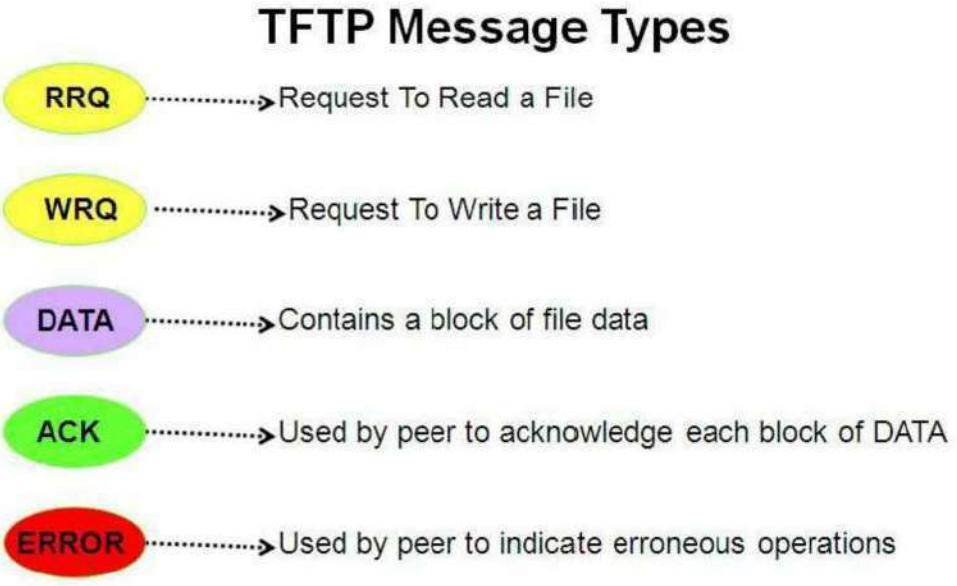




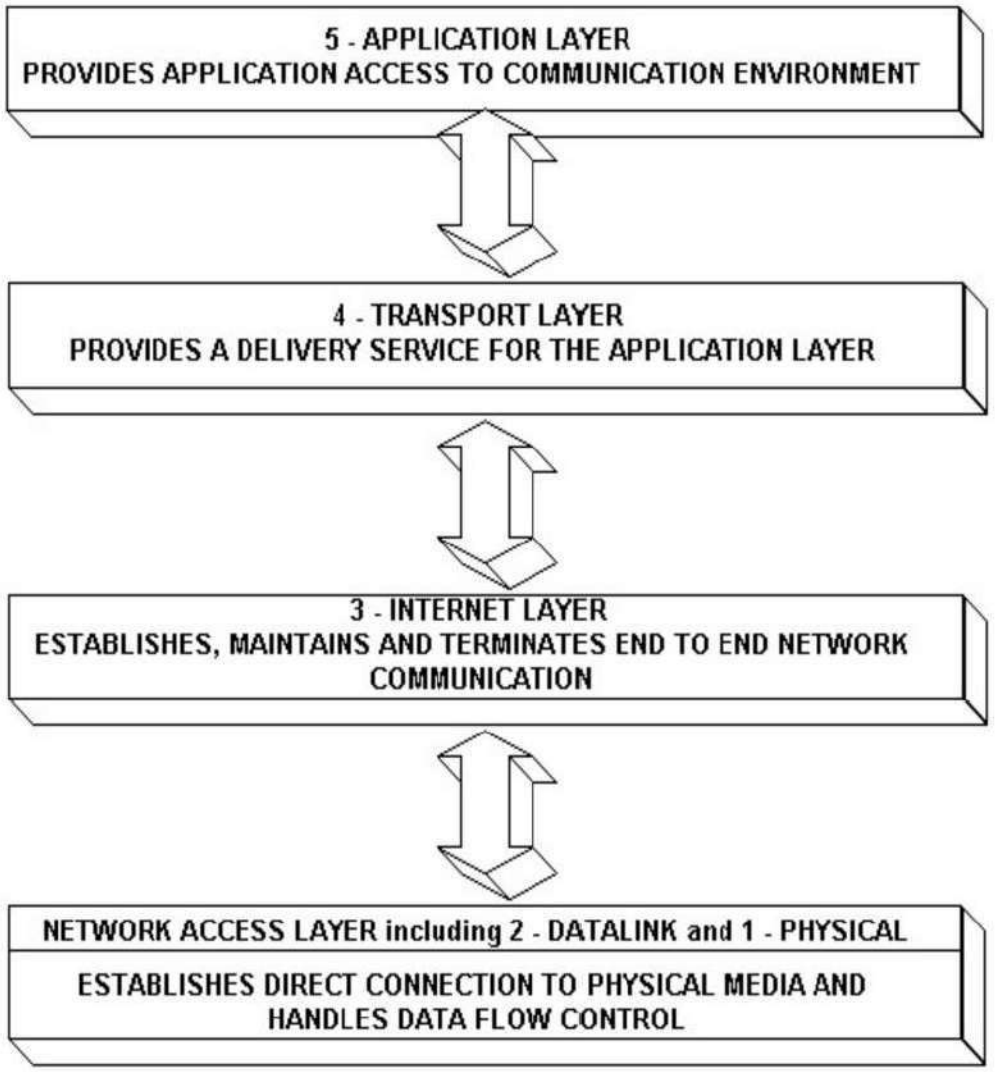
TFTP

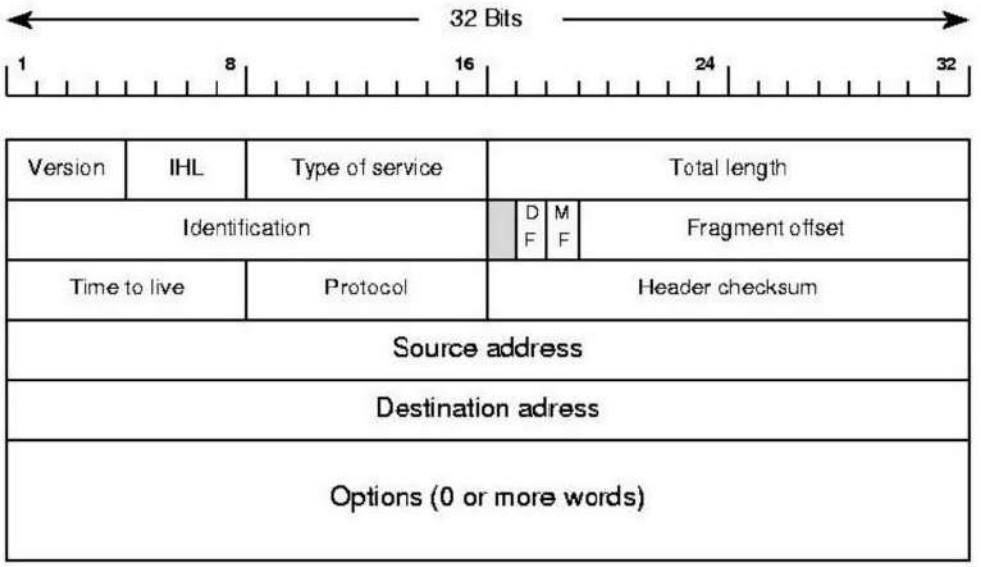
TFTP is an Internet software utility for transferring files. It's easier than File Transfer Protocol (FTP), but has less capability. It is used when required for user authentication and directory visibility. TFTP uses the User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

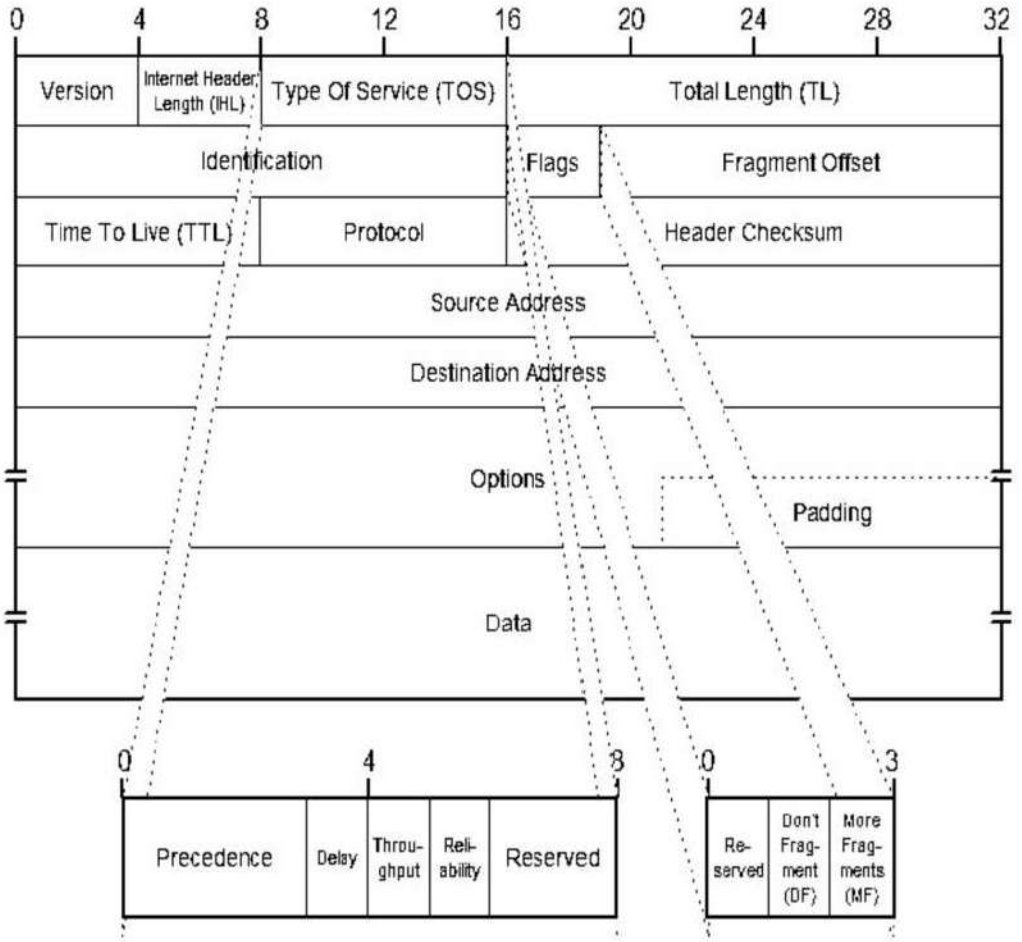




NETWORK LAYER	FUNCTIONS AND PROTOCOLS
Application Layer	Protocol that dictates the method used to send data such as HTTP & FTP (web-based), POP3 & SMTP (Email), SSL & TLS (Security) and SNMP (Network Management)
Transport Layer	Protocol responsible for dictating format of data sent, exactly where it is sent to and maintaining data integrity such as TCP and UDP.
Internet Layer	Purely transports data packets (datagrams) across network boundaries. Possible Internet layer include, IP, ICMP & IGMP.
Physical (Network Interface)	The physical/logical network components used to interconnect hosts or nodes in a network (only on host side). Examples include ISDN, Ethernet, ATM, Wi-Fi.

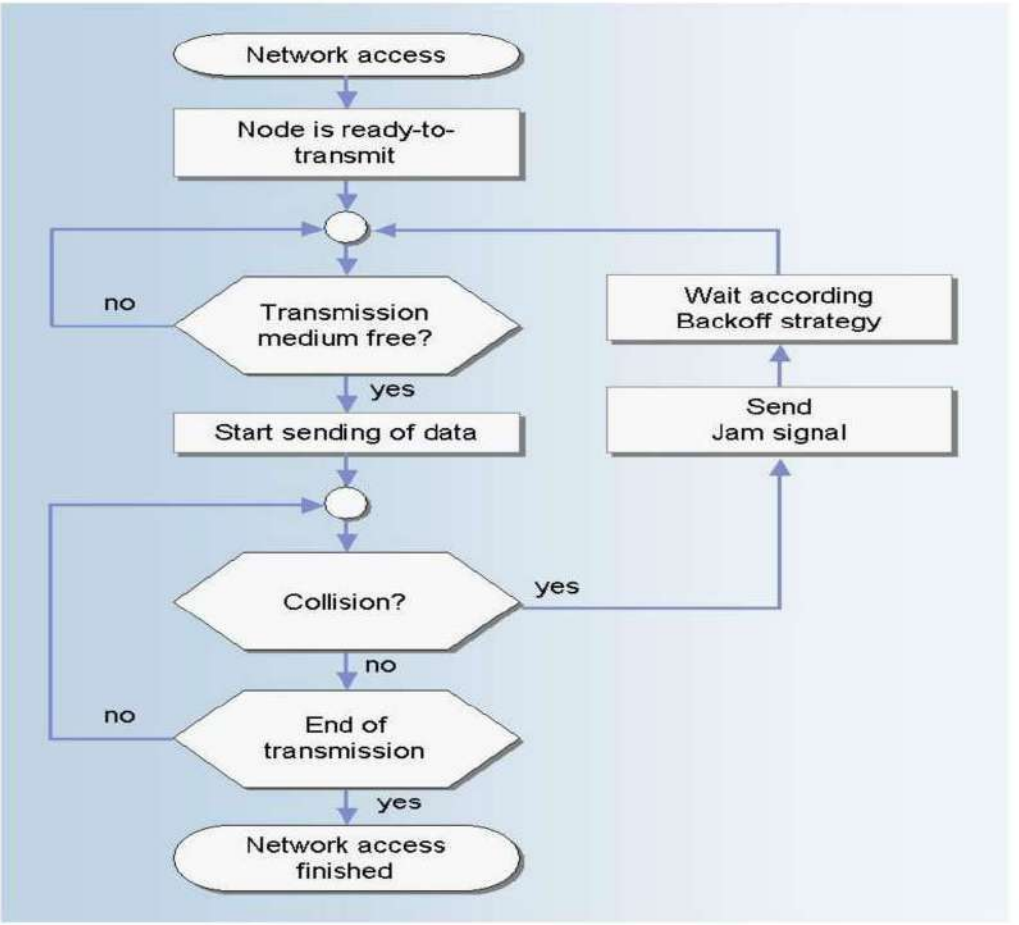


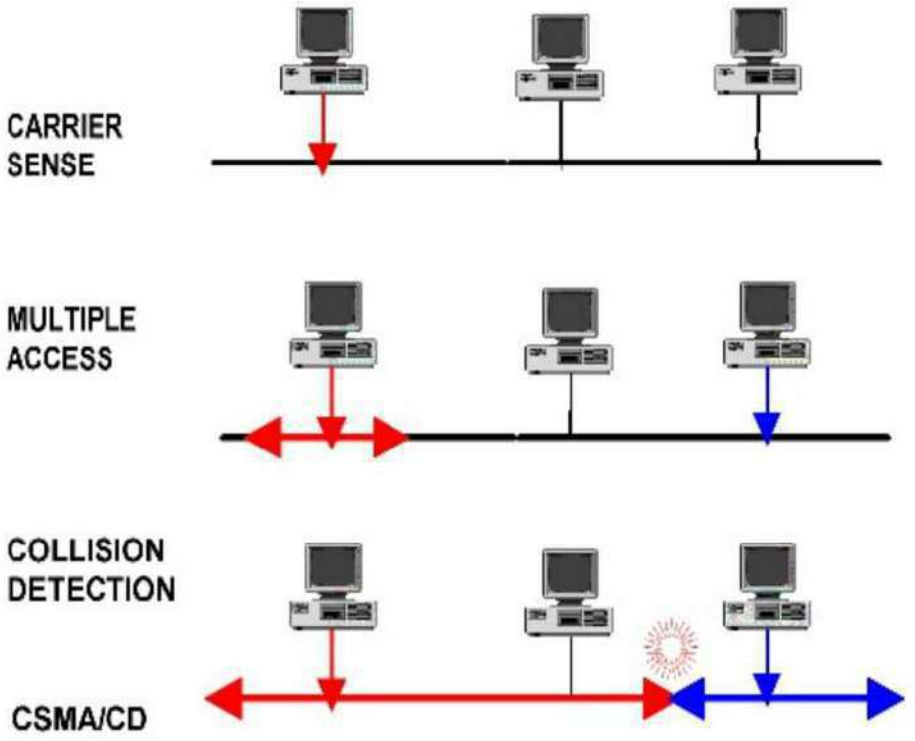

32 Bits
1
8
16
24
32
Version
IHL
Type of service
Total length
Identification
D F
M F
Fragment offset
Time to live
Protocol
Header checksum
Source address
Destination adress
Options (0 or more words)


0
4
8
12
16
20
24
28
32
Version
Internet Header Length (IHL)
Type Of Service (TOS)
Total Length (TL)
Identification
Flags
Fragment Offset
Time To Live (TTL)
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding
Data
0
4
8
Precedence
Delay
Through-ghput
Reli-ability
Reserved
0
3
Re-served
Don't Frag-ment (DF)
More Frag-ments (MF)

The network access layer can be used for Ethernet, Token Ring, FDDI, X.25, Frame Relay, etc.

The most popular LAN architecture is Ethernet. Ethernet depends on an access method called CSMA / CD (Carrier Sense Multiple Access / Collision Detection) to access the media. The access method is interested in how a host places data in the environment.





CSMA / CD access method, each host has equal access to the medium and can send the data to the media when free. When a host wants to put data on the cable, the cable will check to see if another host uses the medium. If traffic is already in the middle, the host will wait and put the data in between if there is no traffic. However, if the user places two sets of data on the environment at the same time, they will collide, destroying data. If the data are destroyed during transmission, the data must be retransmitted. After the

collision, each host will wait a short time interval and broadcast the data again.