UNIT V – THE APPLICATION LAYER & NETWORK SECURITY

Application layer protocols: HTTP, FTP, SMTP, DNS . Overview of client-server communication and peer-to-peer models . DNS operation and the role of web servers. Security concerns at the network layer: Attacks (DoS, DDoS, MITM). Introduction to Firewalls: Types (packet filtering, stateful inspection, proxy firewalls).VPNs and network security protocols (IPSec, SSL/TLS)., Applications: E-commerce (SSL/TLS), VPNs for remote work, DNS in URL resolution, firewalls in banks and enterprises, cybersecurity practices in web apps.

1. Application layer protocols: HTTP, FTP, SMTP, DNS

1.1 HTTP (HYPERTEXT TRANSFER PROTOCOL)

- The HyperText Transfer Protocol (HTTP) is used to define how the client-server programs can be written to retrieve web pages from the Web.
- It is a protocol used to access the data on the World Wide Web (WWW). The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- HTTP is a stateless request/response protocol that governs client/server communication. An HTTP client sends a request; an HTTP server returns a response.
- The server uses the port number 80; the client uses a temporary port number.
- HTTP uses the services of TCP, a connection-oriented and reliable protocol. HTTP is a text-oriented protocol.
- It contains embedded URL known as links.
- When hypertext is clicked, browser opens a new connection, retrieves file from the server and displays the file.
- Each HTTP message has the general form

START_LINE <CRLF>
MESSAGE_HEADER <CRLF>
<CRLF>MESSAGE_BODY<CRLF>
where <CRLF> stands for carriage-return-line-feed.

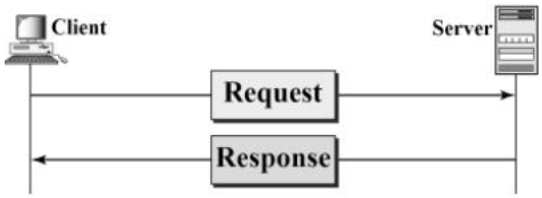
Features of HTTP

- Connectionless protocol: HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.
- Media independent: HTTP protocol is a media independent as data can be sent as long asboth the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.
- Stateless: HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the

client and server do not retain the information between various requests of the web pages.

HTTP REQUEST AND RESPONSE MESSAGES

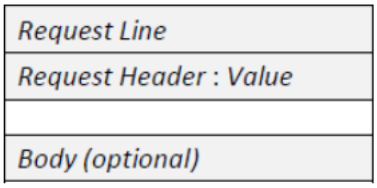
The HTTP protocol defines the format of the request and response messages.



- Request Message: The request message is sent by the client that consists of a request line, headers, and sometimes a body.

- Response Message: The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body

HTTP REQUEST MESSAGE



- The first line in a request message is called a request line.
- After the request line, we can have zero or more request header lines.
- The body is an optional one. It contains the comment to be sent or the file to be published on the website when the method is PUT or POST.

Request Line

- There are three fields in this request line - Method, URL and Version. The Method field defines the request types.
- The URL field defines the address and name of the corresponding web page.
- The Version field gives the version of the protocol; the most current version of HTTP is 1.1.
- Some of the Method types are

Method	*Action*
GET	Requests a document from the server
HEAD	Requests information about a document but not the document itself
PUT	Sends a document from the client to the server
POST	Sends some information from the client to the server
TRACE	Echoes the incoming request
DELETE	Removes the web page
CONNECT	Reserved
OPTIONS	Inquires about available options

Request Header

- Each request header line sends additional information from the client to the server.
- Each header line has a header name, a colon, a space, and a header value. The value field defines the values associated with each header name.
- Headers defined for request message include

Header	*Description*
User-agent	Identifies the client program
Accept	Shows the media format the client can accept
Accept-charset	Shows the character set the client can handle
Accept-encoding	Shows the encoding scheme the client can handle
Accept-language	Shows the language the client can accept
Authorization	Shows what permissions the client has
Host	Shows the host and port number of the client
Date	Shows the current date
Upgrade	Specifies the preferred communication protocol
Cookie	Returns the cookie to the server
If-Modified-Since	If the file is modified since a specific date

Body

- The body can be present in a request message. It is optional.
- Usually, it contains the comment to be sent or the file to be published on the website when the method is PUT or POST.

Conditional Request

- A client can add a condition in its request.
- In this case, the server will send the requested web page if the condition is metor inform the client otherwise.
- One of the most common conditions imposed by the client is the time and datethe web page is modified.
- The client can send the header line If-Modified-Since with the request to tell theserver that it needs the page only if it is modified after a certain point in time.

HTTP RESPONSE MESSAGE

Status Line
Response Header : Value
Body

- The first line in a request message is called a status line.
- After the request line, we can have zero or more response header lines.
- The body is an optional one. The body is present unless the response is an error message

Status Line

- The Status line contains three fields - HTTP version, Status code, Status phrase The first field defines the version of HTTP protocol, currently 1.1.
- The status code field defines the status of the request. It classifies the HTTP result.
- It consists of three digits. 1xx–Informational, 2xx– Success, 3xx–Redirection, 4xx–Client error, 5xx–Server error
- The Status phrase field gives brief description about status code in text form.
- Some of the Status codes are

Code	Phrase	Description
100	Continue	Initial request received, client to continue process
200	OK	Request is successful
301	Moved permanently	Requested URL is no longer in use
404	Not found	Document not found
500	Internal server error	An error such as a crash, at the server site

Response Header

- Each header provides additional information to the client.
- Each header line has a header name, a colon, a space, and a header value.
- Some of the response headers are:

Response Header	Description
Content-type	specifies the MIME type
Expires	date and time up to which the document is valid
Last-modified	date and time when the document was last updated
Location	specifies location of the created or moved document

Body

The body contains the document to be sent from the server to the client.

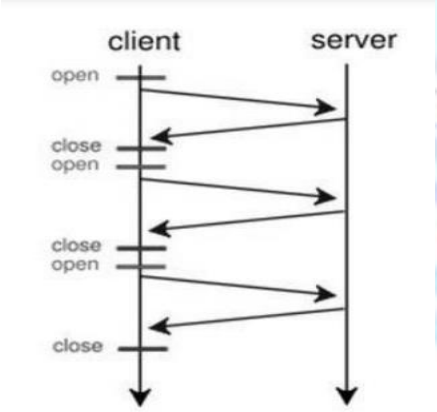
The body is present unless the response is an error message.

HTTP CONNECTIONS

- HTTP Clients and Servers exchange multiple messages over the same TCP connection.
- If some of the objects are located on the same server, we have two choices: to retrieve each object using a new TCP connection or to make a TCP connection and retrieve them all.
- The first method is referred to as a non-persistent connection, the second as a persistent connection.
- HTTP 1.0 uses non-persistent connections and HTTP 1.1 uses persistent connections

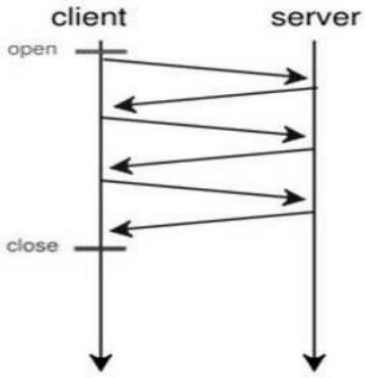
NON-PERSISTENT CONNECTIONS

- In a non-persistent connection, one TCP connection is made for each request/response.
- Only one object can be sent over a single TCP connection
- The client opens a TCP connection and sends a request.
- The server sends the response and closes the connection.
- The client reads the data until it encounters an end-of-file marker.
- It then closes the connection.



PERSISTENT CONNECTIONS

- HTTP version 1.1 specifies a persistent connectionby default. Multiple objects can be sent over a single TCP connection.
- In a persistent connection, the server leaves the connection open for more requests after sending a response.
- The server can close the connection at the request of a client or if a time-out has been reached.
- Time and resources are saved using persistent connections. Only one set of buffers and variables needs to be set for the connection at each site.
- The round-trip time for connection establishment and connection termination is saved.



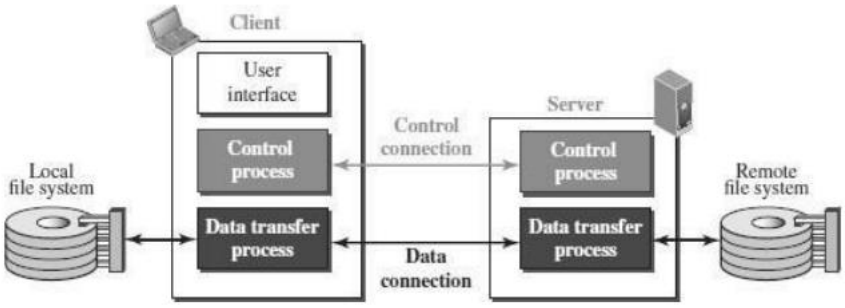
1.2 FTP (FILE TRANSFER PROTOCOL)

- FTP stands for File transfer protocol.
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.
- Although we can transfer files using HTTP, FTP is a better choice to transfer large files or to transfer files using different formats.

FTP OBJECTIVES

- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

FTP MECHANISM

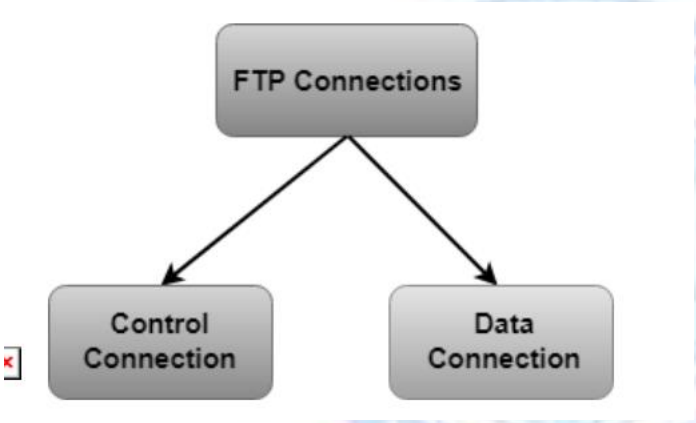


The above figure shows the basic model of the FTP.

- ✧ The FTP client has three components:
  - o user interface, control process, and data transfer process.
- ✧ The server has two components:
  - o server control process and server data transfer process.

FTP CONNECTIONS

- There are two types of connections in FTP -
  Control Connection and Data Connection.
- The two connections in FTP have different lifetimes.
- The control connection remains connected during the entire interactive FTP session.
- The data connection is opened and then closed for each file transfer activity.
- When a user starts an FTP session, the control connection opens. While the control connection is open, the data connection can be opened and closed multiple times if several files are transferred. FTP uses two well-known TCP ports:
- o Port 21 is used for the control connection
- o Port 20 is used for the data connection.



Control Connection:

o The control connection uses very simple rules for communication.
o Through control connection, we can transfer a line of command or lineof response at a time.
o The control connection is made between the control processes.
o The control connection remains connected during the entire interactive FTP session.

Data Connection:

o The Data Connection uses very complex rules as data types may vary. o The data connection is made between data transfer processes.
o The data connection opens when a command comes for transferring the files and closes when the file is transferred.

FTP COMMUNICATION

- FTP Communication is achieved through commands and responses.
- FTP Commands are sent from the client to the server FTP responses are sent from the server to the client.
- FTP Commands are in the form of ASCII uppercase, which may or may not be followed by an argument.

✧ Some of the most common commands are

Command	*Description*
ABOR	Abort the previous command
CDUP	Change to parent directory
CWD	Change to another directory
DELE	Delete a file
LIST	List subdirectories or files
MKD	Create a new directory
PASS	Password
PASV	Server chooses a port
PORT	Client chooses a port
PWD	Display name of current directory
QUIT	Log out of the system
RETR	Retrieve files; files are transferred from server to client
RMD	Delete a directory
RNFR	Identify a file to be renamed
RNTO	Rename the file
STOR	Store files; file(s) are transferred from client to server
STRU	Define data organization (**F**: file, **R**: record, or **P**: page)
TYPE	Default file type (**A**: ASCII, **E**: EBCDIC, **I**: image)
USER	User information
MODE	Define transmission mode (**S**: stream, **B**: block, or **C**: compressed

✧ Every FTP command generates at least one response.
✧ A response has two parts: a three-digit number followed by text.
✧ The numeric part defines the code; the text part defines needed parameter.

Code	*Description*	*Code*	*Description*
125	Data connection open	**250**	Request file action OK
150	File status OK	**331**	User name OK; password is needed
200	Command OK	**425**	Cannot open data connection
220	Service ready	**450**	File action not taken; file not available
221	Service closing	**452**	Action aborted; insufficient storage
225	Data connection open	**500**	Syntax error; unrecognized command
226	Closing data connection	**501**	Syntax error in parameters or arguments
230	User login OK	**530**	User not logged in

FTP FILE TYPE

FTP can transfer one of the following file types across the data connection: ASCII file, EBCDIC file, or image file.

FTP DATA STRUCTURE

✧ FTP can transfer a file across the data connection using one of the following data structure : file structure, record structure, or page structure.

- ✧ The file structure format is the default one and has no structure. It is a continuous stream of bytes.
- ✧ In the record structure, the file is divided into records. This can be used only with text files.
- ✧ In the page structure, the file is divided into pages, with each page having a page number and a page header. The pages can be stored and accessed randomly or sequentially.

FTP TRANSMISSION MODE

- ✧ FTP can transfer a file across the data connection using one of the following three transmission modes: stream mode, block mode, or compressed mode.
- ✧ The stream mode is the default mode; data are delivered from FTP to TCP as a continuous stream of bytes.
- ✧ In the block mode, data can be delivered from FTP to TCP in blocks. In the compressed mode, data can be compressed and delivered from FTP to TCP.

FTP FILE TRANSFER

- ✧ File transfer occurs over the data connection under the control of the commands sent over the control connection.
- ✧ File transfer in FTP means one of three things:

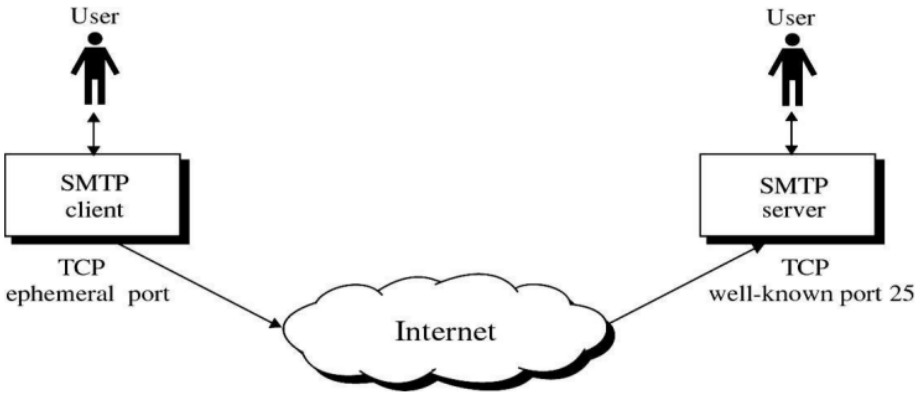
o retrieving a file (server to client)
o storing a file (client to server)
o directory listing (server to client).

FTP SECURITY

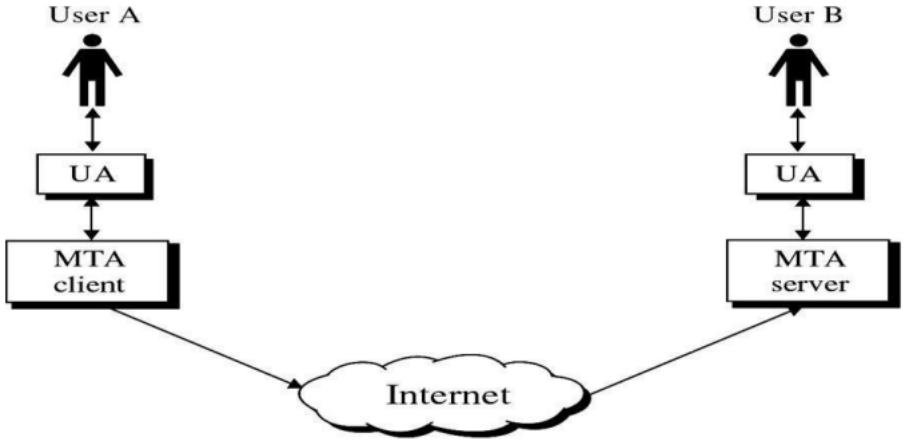
- ✧ FTP requires a password, the password is sent in plaint-ext which is encrypted.
- ✧ This means it can be intercepted and used by an attacker.
- ✧ The data transfer connection also transfers data in plain-text, which is insecure.
- ✧ To be secure, one can add a Secure Socket Layer between the FTP application layer and the TCP layer.
- ✧ In this case FTP is called SSL-FTP.

SMTP-SIMPLE MAIL TRANSFER PROTOCOL

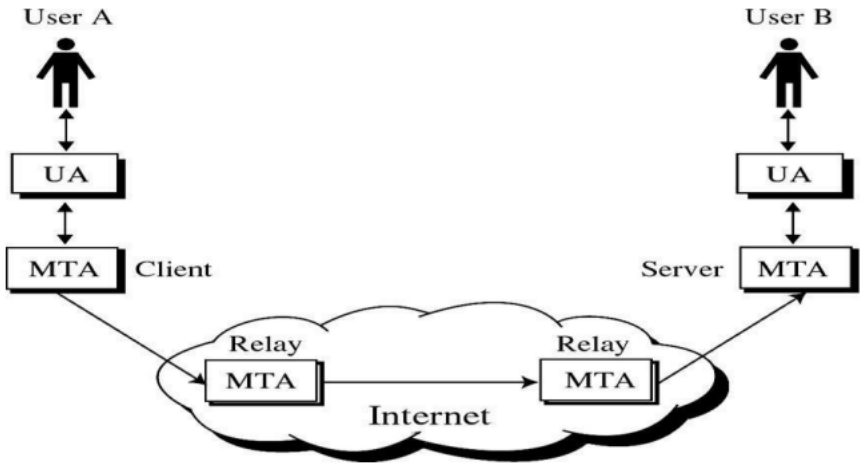
- ✧ SMTP is the standard protocol for transferring mail between hosts in the TCP/IP protocol suite.
- ✧ SMTP is not concerned with the format or content of messages themselves.
- ✧ SMTP uses information written on the envelope of the mail (message header),but does not look at the contents (message body) of the envelope.



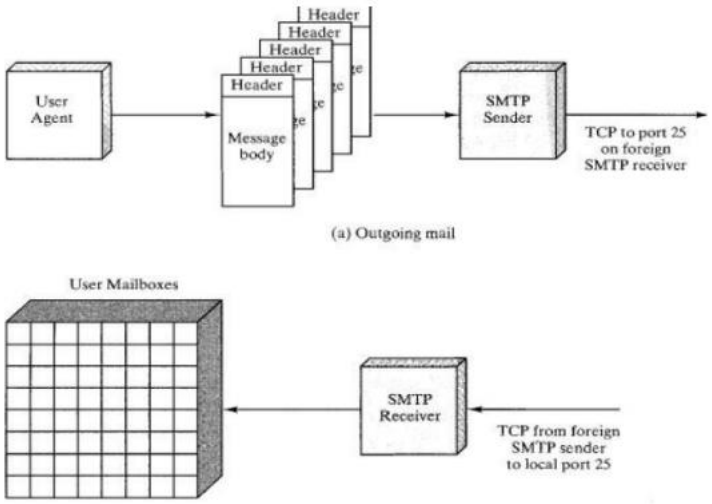
SMTP clients and servers have two main components
o User Agents(UA) – Prepares the message, encloses it in an envelope. o Mail Transfer Agent (MTA) – Transfers the mail across the internet



SMTP also allows the use of Relays allowing other MTAs to relay the mail



SMTP MAIL FLOW



- ✧ To begin, mail is created by a user-agent program in response to user input.
- ✧ Each created message consists of a header that includes the recipient's email address and other information, and a message body containing the message to be sent.
- ✧ These messages are then queued in some fashion and provided as input to an SMTP Sender program.

SMTP COMMANDS AND RESPONSES

- ✧ The operation of SMTP consists of a series of commands and responses exchanged between the SMTP sender and SMTP receiver.
- ✧ The initiative is with the SMTP sender, who establishes the TCP connection. Once the connection is established, the SMTP sender sends commands over the connection to the receiver.
- ✧ The command is from an MTA client to an MTA server; the response is from an MTA server to the MTA client.

SMTP Commands

Commands are sent from the client to the server. It consists of a keyword followed by zero or more arguments. SMTP defines 14 commands.

SMTP commands

Keyword	*Argument(s)*	*Description*
HELO	Sender's host name	Identifies itself
MAIL FROM	Sender of the message	Identifies the sender of the message
RCPT TO	Intended recipient	Identifies the recipient of the message
DATA	Body of the mail	Sends the actual message
QUIT		Terminates the message
RSET		Aborts the current mail transaction
VRFY	Name of recipient	Verifies the address of the recipient
NOOP		Checks the status of the recipient
TURN		Switches the sender and the recipient
EXPN	Mailing list	Asks the recipient to expand the mailing list
HELP	Command name	Asks the recipient to send information about the command sent as the argument
SEND FROM	Intended recipient	Specifies that the mail be delivered only to the terminal of the recipient, and not to the mailbox
SMOL FROM	Intended recipient	Specifies that the mail be delivered to the terminal *or* the mailbox of the recipient
SMAL FROM	Intended recipient	Specifies that the mail be delivered to the terminal *and* the mailbox of the recipient

SMTP Responses

- ✧ Responses are sent from the server to the client.
- ✧ A response is a three-digit code that may be followed by additional textual information.

SMTP Responses

Code	*Description*
	Positive Completion Reply
211	System status or help reply
214	Help message
220	Service ready
221	Service closing transmission channel
250	Request command completed
251	User not local; the message will be forwarded
	Positive Intermediate Reply
354	Start mail input
	Transient Negative Completion Reply
421	Service not available
450	Mailbox not available
451	Command aborted: local error
452	Command aborted; insufficient storage
	Permanent Negative Completion Reply
500	Syntax error; unrecognized command
501	Syntax error in parameters or arguments
502	Command not implemented
503	Bad sequence of commands
504	Command temporarily not implemented
550	Command is not executed; mailbox unavailable
551	User not local
552	Requested action aborted; exceeded storage location
553	Requested action not taken; mailbox name not allowed
554	Transaction failed

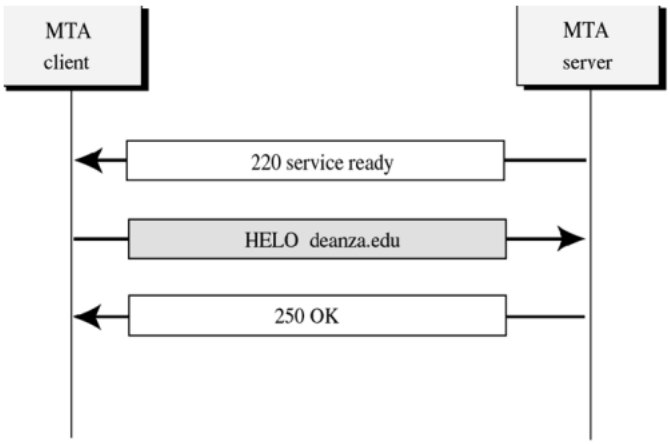
SMTP OPERATIONS

Basic SMTP operation occurs in three phases:
1. Connection Setup
2. Mail Transfer
3. Connection Termination

Connection Setup

- An SMTP sender will attempt to set up a TCP connection with a target host when it has one or more mail messages to deliver to that host.
- The sequence is quite simple:

1. The sender opens a TCP connection with the receiver.
2. Once the connection is established, the receiver identifies itself with "Service Ready".
3. The sender identifies itself with the HELO command.
4. The receiver acceptsthe sender's identification with "OK".
5. If the mail service on the destination is unavailable, the destination host returns a "Service Not Available" reply in step 2, and the process is terminated.

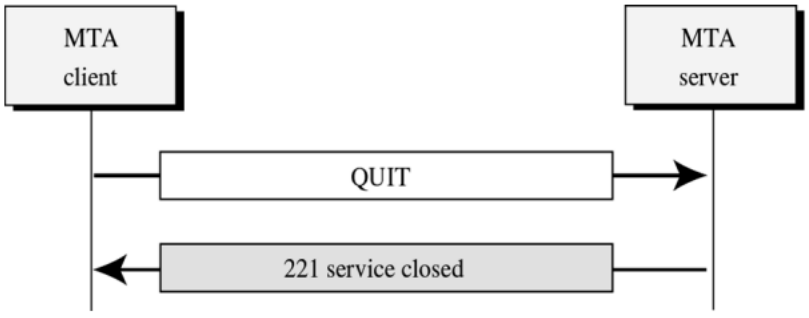


Mail Transfer

- Once a connection has been established, the SMTP sender may send one or more messages to the SMTP receiver.
- There are three logical phases to the transfer of a message:
    1. A MAIL command identifies the originator of the message.
    2. One or more RCPT commands identify the recipients for this message.
    3. A DATA command transfers the message text.

Connection Termination

- The SMTP sender closes the connection in two steps.
- First, the sender sends a QUIT command and waits for a reply.
- The second step is to initiate a TCP close operation for the TCP connection.
- The receiver initiates its TCP close after sending its reply to the QUIT command.



LIMITATIONS OF SMTP

- SMTP cannot transmit executable files or other binary objects.
- SMTP cannot transmit text data that includes national language characters, as these are represented by 8-bit codes with values of 128 decimal or higher, and SMTP is limited to 7-bit ASCII.
- SMTP servers may reject mail message over a certain size.

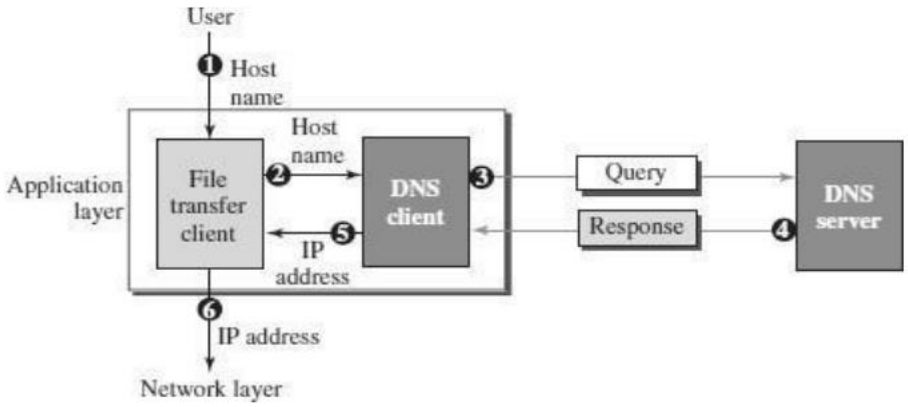
- SMTP gateways that translate between ASCII and the character code EBCDIC do not use a consistent set of mappings, resulting in translation problems.
- Some SMTP implementations do not adhere completely to the SMTP standards defined.
- Common problems include the following:

1. Deletion, addition, or recording of carriage return and linefeed.
2. Truncating or wrapping lines longer than 76 characters
3. Removal of trailing white space (tab and space characters).
4. Padding of lines in a message to the same length. Conversion of tab characters into multiple-space characters

1.4 DOMAIN NAME SYSTEM(DNS)

- Domain Name System was designed in 1984.
- DNS is used for name-to-address mapping.
- The DNS provides the protocol which allows clients and servers to communicate with each other.
- Eg: Host name like www.yahoo.com is translated into numerical IP addresses like 207.174.77.131
- Domain Name System (DNS) is a distributed database used by TCP/IP applications to map between host names and IP addresses and to provide electronic mail routing information.
- Each site maintains its own database of information and runs a server program that other systems across the Internet can query

WORKING OF DNS



The following six steps shows the working of a DNS. It maps the host name to an IP address:

1. The user passes the host name to the file transfer client.
2. The file transfer client passes the host name to the DNS client.
3. Each computer, after being booted, knows the address of one DNS server. The DNS client sends a message to a DNS server with a query that gives the file transfer server name using the known IP address of the DNS server.
4. The DNS server responds with the IP address of the desired file transfer server.
5. The DNS server passes the IP address to the file transfer client. 6. The file transfer client now uses the received IP address to access the file transfer server.

NAME SPACE

- To be unambiguous, the names assigned to machines must be carefully selected from a name space with complete control over the binding between the names and IP address.
- The names must be unique because the addresses are unique.
- A name space that maps each address to a unique name can be organized in two ways: flat (or) hierarchical.

Flat Name Space

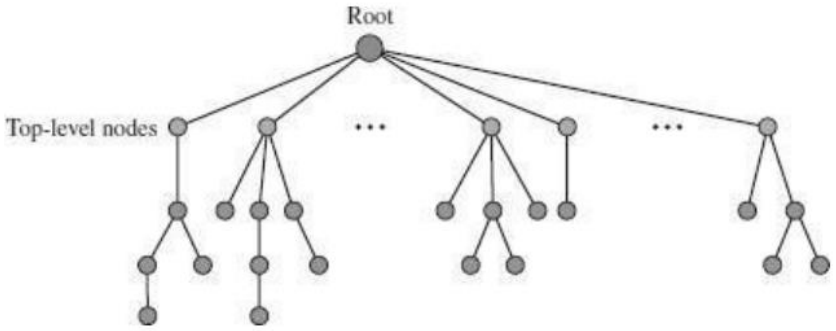
- In a flat name space, a name is assigned to an address.
- A name in this space is a sequence of characters without structure.
- The main disadvantage of a flat name space is that it cannot be used in a large system such as Internet because it must be centrally controlled to avoid ambiguity and duplication.

Hierarchical Name Space

- In a hierarchical name space, each name is made of several parts. The first part can define the organization, the second part can define the name,the third part can define departments, and so on.
- In this case, the authority to assign and control the name spaces can be decentralized.
- A central authority can assign the part of the name that defines the nature of the organization and the name.
- The responsibility for the rest of the name can be given to the organization itself.
- Suffixes can be added to the name to define host or resources. The management of the organization need not worry that the prefix chosen fora host is taken by another organization because even if part of an address is the same, the whole address is different.
- The names are unique without the need to be assigned by a central authority.
- The central authority controls only part of the name, not the whole name.

DOMAIN NAME SPACE

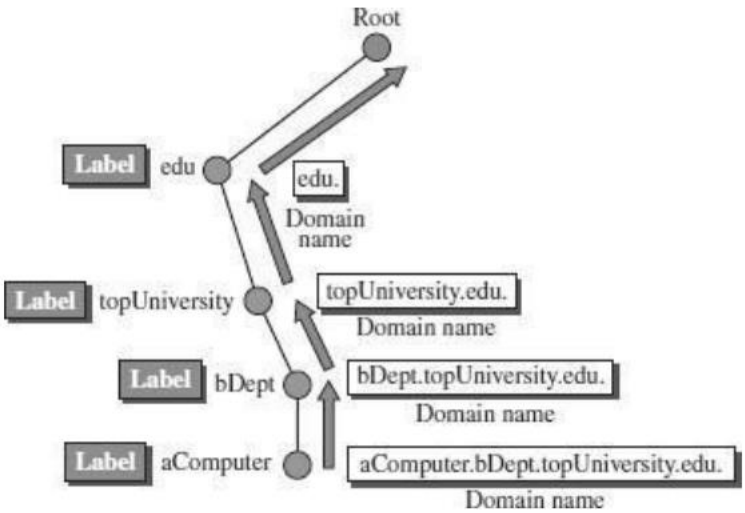
- To have a hierarchical name space, a domain name space was designed. In this design, the names are defined in an inverted-tree structure with the root at the top.
- Each node in the tree has a label, which is a string with a maximum of 63 characters.
- The root label is a null string.
- DNS requires that children of a node have different labels, which guarantees the uniqueness of the domain names.



- Each node in the tree has a label, which is a string with a maximum of 63 characters.
- The root label is a null string (empty string). DNS requires that children of a node (nodes that branch from the same node) have different labels, which guarantees the uniqueness of the domain names.

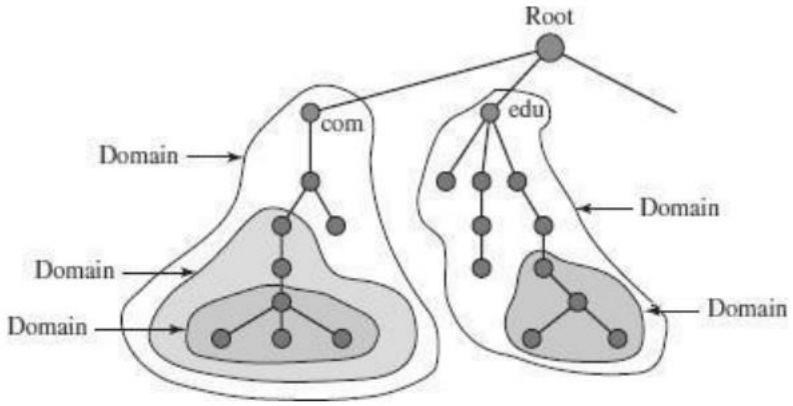
Domain Name

- Each node in the tree has a label called as domain name.
- A full domain name is a sequence of labels separated by dots (.)
- The domain names are always read from the node up to the root.
- The last label is the label of the root (null).
- This means that a full domain name always ends in a null label, which means the last character is a dot because the null string is nothing.
- If a label is terminated by a null string, it is called a fully qualified domainname (FQDN).
- If a label is not terminated by a null string, it is called a partially qualified domain name (PQDN).



Domain

- A domain is a subtree of the domain name space.
- The name of the domain is the domain name of the node at the top of the sub-tree.
- A domain may itself be divided into domains.

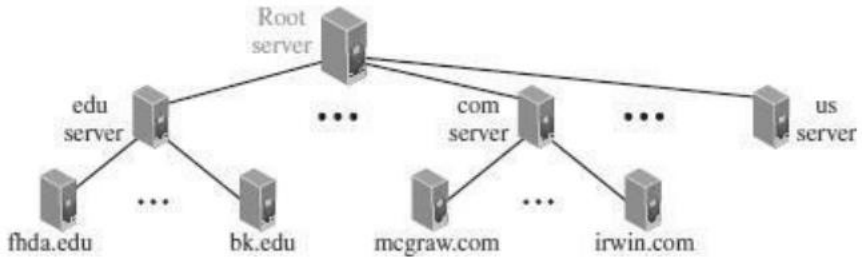


DISTRIBUTION OF NAME SPACE

- The information contained in the domain name space must be stored.
- But it is very inefficient and also not reliable to have just one computer store such a huge amount of information.
- It is inefficient because responding to requests from all over the world, places a heavy load on the system.
- It is not reliable because any failure makes the data inaccessible.
- The solution to these problems is to distribute the information among many computers called DNS servers.

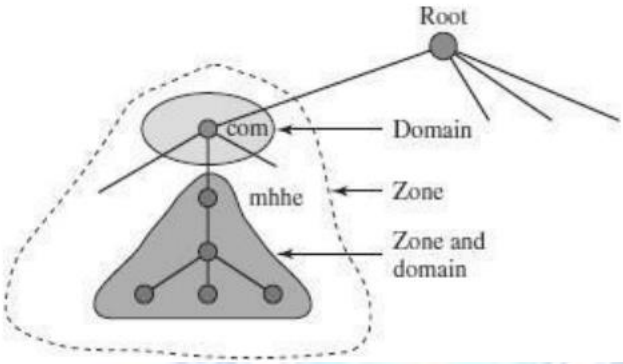
HIERARCHY OF NAME SERVERS

- The way to distribute information among DNS servers is to divide the whole space into many domains based on the first level.
- Let the root stand-alone and create as many domains as there are first level nodes.
- Because a domain created this way could be very large, DNS allows domains to be divided further into smaller domains.
- Thus, we have a hierarchy of servers in the same way that we have a hierarchy of names



ZONE

- What a server is responsible for, or has authority over, is called a zone.
- The server makes a database called a zone file and keeps all the information for every node under that domain.
- If a server accepts responsibility for a domain and does not divide the domains into smaller domains, the domain and zone refer to the same thing.
- But if a server divides its domain into sub domains and delegates parts of its authority to other servers, domain and zone refer to different things.
- The information about the nodes in the sub domains is stored in the servers at the lower levels, with the original server keeping some sort of references to these lower-level servers.
- But still, the original server does not free itself from responsibility totally.
- It still has a zone, but the detailed information is kept by the lower level servers.



ROOT SERVER

- A root sever is a server whose zone consists of the whole tree.
- A root server usually does not store any information about domains but delegates its authority to other servers, keeping references to those servers.
- Currently there are more than 13 root servers, each covering the whole domain name space.
- The servers are distributed all around the world.

PRIMARY AND SECONDARY SERVERS

- DNS defines two types of servers: primary and secondary.
- A Primary Server is a server that stores a file about the zone for which it is an authority.
  - Primary Servers are responsible for creating, maintaining, and updating the zone file. □
  - Primary Server stores the zone file on a local disc.
- A secondary server is a server that transfers the complete information about a zone from another server (Primary or Secondary) and stores the file on its local disc.
- If updating is required, it must be done by the primary server, which sends the updated version to the secondary.

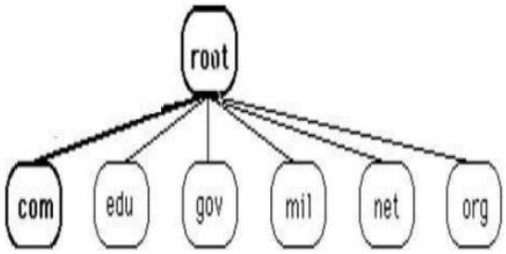
- A primary server loads all information from the disk file; the secondary server loads all information from the primary server.

DNS IN THE INTERNET

- DNS is a protocol that can be used in different platforms.
- In the Internet, the domain name space (tree) is divided into three different sections - Generic domains, Country domains, and Inverse domain.

Generic Domains

- The generic domains define registered hosts according to their generic behavior.
- Each node in the tree defines a domain, which is an index to the domain name space database.
- The first level in the generic domains section allows seven possible three character levels. These levels describe the organization types as listed in following table



.COM	Commercial Organizations
.EDU	Educational institutions
.GOV	Government institutions
.MIL	Military groups
.NET	Major network support centers
.INT	International Organizations
.ORG	Nonprofit Organizations

Country Domains

- The country domains section follows the same format as the generic domains but uses two characters for country abbreviations
- E.g.; in for India, us for United States etc) in place of the three character organizational abbreviation at the first level.
- Second level labels can be organizational, or they can be more specific,national designation.
- India for example, uses state abbreviations as a subdivision of the country domain us. (e.g., ca.in.)

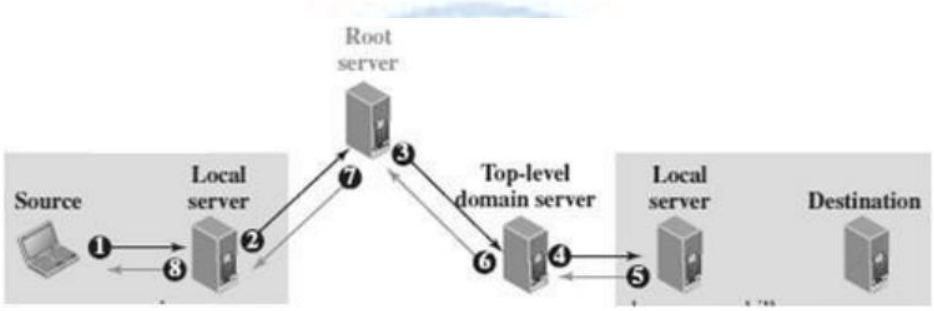
Inverse Domains

- Mapping an address to a name is called Inverse domain.
- The client can send an IP address to a server to be mapped to a domain name and it is called PTR(Pointer) query.
- To answer queries of this kind, DNS uses the inverse domain

DNS RESOLUTION

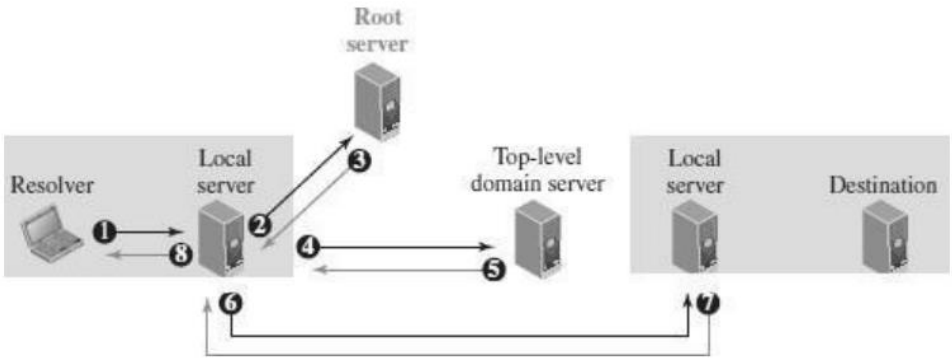
- Mapping a name to an address or an address to a name is called name address resolution.
- DNS is designed as a client server application. A host that needs to map an address to a name or a name to an address calls a DNS client named a Resolver.
- The Resolver accesses the closest DNS server with a mapping request.
- If the server has the information, it satisfies the resolver; otherwise, it either refers the resolver to other servers or asks other servers to provide the information.
- After the resolver receives the mapping, it interprets the response to see if it is areal resolution or an error and finally delivers the result to the process that requested it.
- A resolution can be either recursive or iterative.

Recursive Resolution



- The application program on the source host calls the DNS resolver (client) to find the IP address of the destination host. The resolver, which does not know this address, sends the query to the local DNS server of the source (Event 1)
- The local server sends the query to a root DNS server (Event 2)
- The Root server sends the query to the top-level DNS server (Event 3)
- The top-level DNS server knows only the IP address of the local DNS server at the destination. So, it forwards the query to the local server, which knows the IP address of the destination host (Event 4)
- The IP address of the destination host is now sent back to the top-level DNS server (Event 5) then back to the root server (Event 6), then back to the source DNS server, which may cache it for the future queries (Event 7), and finally back to the source host (Event 8).

Iterative Resolution



- In iterative resolution, each server that does not know the mapping, sends theIP address of the next server back to the one that requested it.
- The iterative resolution takes place between two localservers. The original resolver getsthe final answer from the destination localserver.
- The messages shown by Events 2, 4, and 6 contain the same query.
- However, the message shown by Event 3 contains the IP address of the top-level domain server.
- The message shown by Event 5 contains the IP address of the destination local DNS server
- The message shown by Event 7 contains the IP address of the destination.
- When the Source local DNS server receives the IP address of the destination, it sends it to the resolver (Event 8).

DNS CACHING

- Each time a server receives a query for a name that is not in its domain, it needsto search its database for a server IP address.
- DNS handles this with a mechanism called caching. When a server asks for a mapping from another server and receives the response, it stores this information in its cache memory before sending it to the client.
- If the same or another client asks for the same mapping, it can check its cache memory and resolve the problem. However, to inform the client that the response is coming from the cache memory and not from an authoritative source, the server marks the response as unauthoritative.
- Caching speeds up resolution. Reduction of this search time would increase efficiency, but it can also be problematic.
- If a server caches a mapping for a long time, it may send an outdated mapping to the client.
- To counter this, two techniques are used.
  - ✓ First, the authoritative server always adds information to the mapping called time to live (TTL).It defines the time in seconds that the receiving server can cache the information. After that time, the mapping is invalid and any query must be sent again to the authoritative server.
  - ✓ Second, DNS requires that each server keep a TTL counter for each mapping it caches. The cache memory must be searched periodically and those mappings with an expired TTL must be purged.

DNS RESOURCE RECORDS (RR)

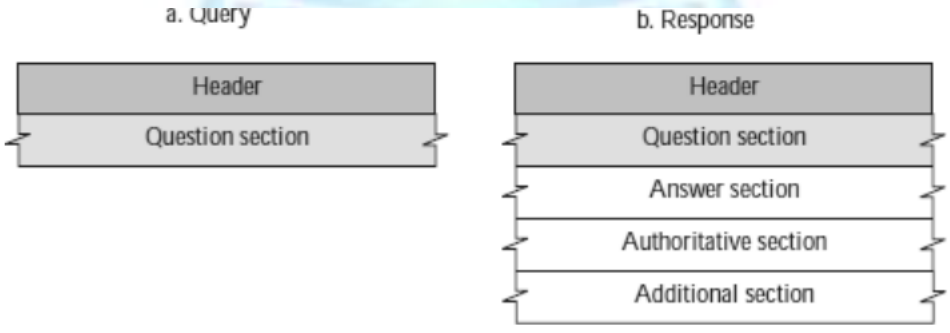
- The zone information associated with a server is implemented as a set of resource records.
- In other words, a name server stores a database of resource records.
- A resource record is a 5-tuple structure
  (Domain Name, Type, Class, TTL, Value)
- The domain name identifies the resource record.
- The type defines how the value should be interpreted.
- The value defines the information kept about the domain name.
- The TTL defines the number of seconds for which the information is valid.
- The class defines the type of network

Types of Resource Records

Type	*Interpretation of value*
A	A 32-bit IPv4 address
NS	Identifies the authoritative servers for a zone
CNAME	Defines an alias for the official name of a host
SOA	Marks the beginning of a zone
MX	Redirects mail to a mail server
AAAA	An IPv6 address

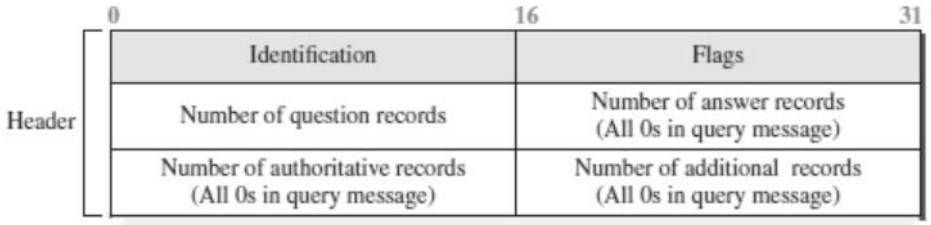
DNS MESSAGES

- DNS has two types of messages: query and response.
- Both types have the same format.
- The query message consists of a header and question section.
- The response message consists of a header, question section, answer section, authoritative section, and additional section



Header

- Both query and response messages have the same header format with some fields set to zero for the query messages.
- The header fields are as follows:



- The identification field is used by the client to match the response with the query.
- The flag field defines whether the message is a query or response. It also includes status of error.
- The next four fields in the header define the number of each record typein the message.
- Question Section
  - The question section consists of one or more question records. It is present in both query and response messages.
- Answer Section
  - The answer section consists of one or more resource records. It ispresent only in response messages.
- Authoritative Section
  - The authoritative section gives information (domain name) about one ormore authoritative servers for the query.
- Additional Information Section
  - The additional information section provides additional information thatmay help the resolver.

DNS CONNECTIONS

- DNS can use either UDP or TCP.
- In both cases the well-known port used by the server is port 53.
- UDP is used when the size of the response message is less than 512 bytes because most UDP packages have a 512-byte packet size limit.
- If the size of the response message is more than 512 bytes, a TCP connection isused.

DNS REGISTRARS

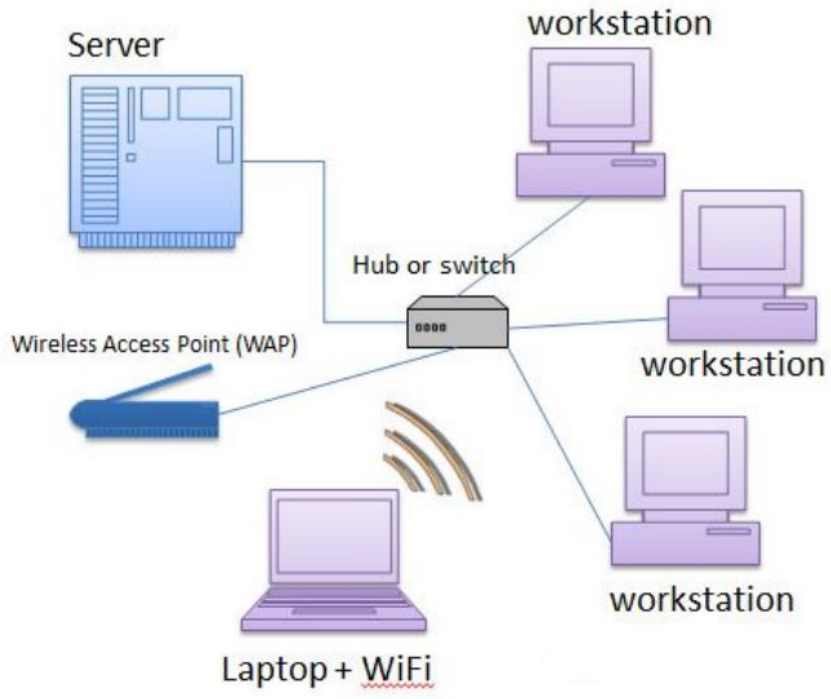
- New domains are added to DNS through a registrar. A fee is charged.
- A registrar first verifies that the requested domain name is unique and thenenters it into the DNS database.
  - Today, there are many registrars; their names and addresses can be found at http://www.intenic.net
- To register, the organization needs to give the name of its server and the IP address of the server.
- For example, a new commercial organization named wonderful with a server named ws and IP address 200.200.200.5, needs to give the following information to one of the registrars:
  - Domain name: ws.wonderful.com IP address: 200.200.200.5

2. OVERVIEW OF CLIENT-SEVER COMMUNICATION AND PEER TO PEER MODEL

CLIENT-SERVER NETWORK

- With a client server network the files will not be stored on the hard drive of each workstation.Instead they will be stored on a computer which is known as a server

- If you are using a client server network then you will have a user account and you will have to log on with a user name and password.



- The first is to identify you to the server so that it knows which files belong to yo u and it can fetch them for you.
- The second is so that the security systems can check that you are actually who you say you are and that the account belongs to you.
- On a large network there may be more than just the file server.
- There might also be an email server which deals with the internal email system.

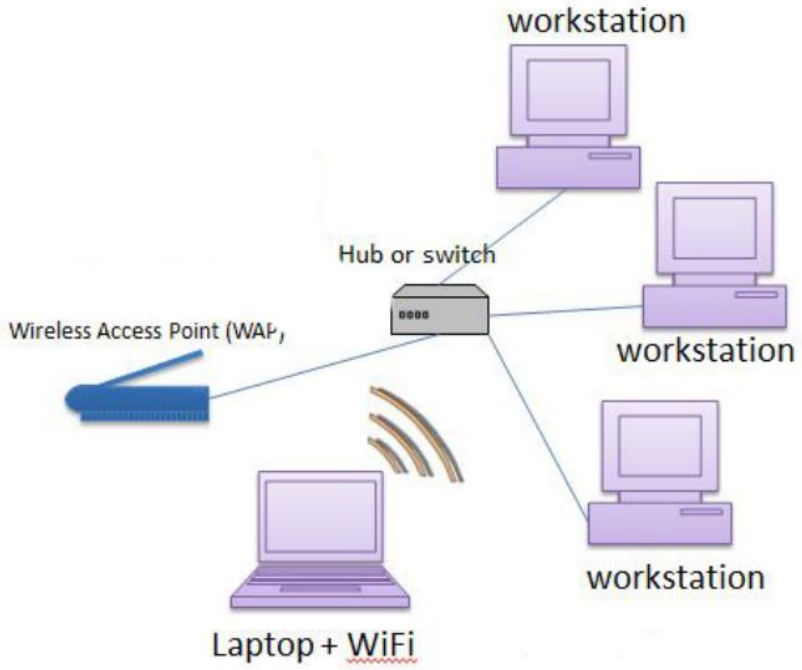
- A web server controls access to the Internet and blocks access to any unsuitable s ites and a print server which deals with all of the printing requests.
- So that is the 'server' part of the client server network.
- The 'client' part is the workstations that are connected to the network.
- The 'clients' rely on servers to store and fetch networked files provide services that the users require
- manage network peripherals that the user wants to access.

Client- Server Networks

Advantages	Disadvantages
Files can be are stored in a central location (although each workstation can have its own files as well)	A specialist network operating system is needed
Network peripherals are controlled centrally	The server is expensive to purchase
Backups and network security is controlled centrally	Specialist staff such as a network manager is often needed
Users can access shared data which is centrally controlled	If key parts of the network fail such as the server or the switch, a lot of disruption can occur
Software licenses and installation for each workstation can be controlled centrally	

PEER TO PEER NETWORK (P2P)

- This type of network is where two or more computers are connected together with out needing a file server to be part of the network.
- A peer to peer network can be as simple as two people in the same room temporar ily connecting their computers via a Universal Serial Bus to enable them to transf er or share files directly with one another.
- It can also include a more permanent network where say half- a- dozen computers in a small office are connected together via a hub or switch.



- This type of network means that every PC, once connected to the network is actin g both as a server and a client. There is no need for a special network operating s ystem. Access rights to files, folders and data is controlled by setting the sharing permissions on individual machines. So for example, if User A wants to access s ome files from User B's computer, User B must set their permissions to allow thi s. Otherwise, User A won't be able to see or access any of User B's work.

- Permissions can be set to allow complete access to every file, folder and documen t stored on your system or just for particular things - perhaps a music library if a t home. This also works with a Wi-Fi connected laptop as long as the Wireless Access Point is also connected to the hub. In home networking systems, the hub / switch / WAP / ADSL modem are

- all built into one unit that an ISP (Internet Service Provider) supplies. For exampl e; BT supplies a 'Home Hub' unit for its customers that acts as a switch, WAP an d a modem.

Peer- to- Peer Networks

Advantages	Disadvantages
No need for a network operating system	Because each computer might be being accessed by others it can slow down the performance for the user
Does not need an expensive server because individual workstations are used to access the files	Files and folders cannot be centrally backed up
No need for specialist staff such as network technicians because each user sets their own permissions as to which files they are willing to share.	Files and resources are not centrally organized into a specific 'shared area'. They are stored on individual computers and might be difficult to locate if the computer's owner doesn't have a logical filing system.
Much easier to set up than a client-server network - does not need specialist knowledge	Ensuring that viruses are not introduced to the network is the responsibility of each individual user
If one computer fails it will not disrupt any other part of the network. It just means that those files aren't available to other users at that time.	Although it is often the case that a password protected user account is set up on a machine, this does not have to be the case and so security is not as robust as a client server model.

DNS OPERATION AND THE ROLE OF WEB SERVERS

DNS (Domain Name System) operations translate human-friendly domain names (like google.com) into computer-readable IP addresses, acting as the internet's phonebook, while web servers host the actual website content; DNS resolution finds the correct IP address, allowing a user's browser to connect to the specific web server hosting the site, making browsing intuitive and functional. Web servers store website files, and when a browser gets the IP via DNS, it sends an HTTP request to that server to fetch the page.

DNS OPERATIONS (THE LOOKUP PROCESS)

1. **User Request:** You type a domain name (e.g., www.example.com) into your browser.
2. **Recursive Resolver:** Your computer asks a recursive DNS resolver (often your ISP's server) to find the IP address.
3. **Caching:** The resolver checks its cache; if the IP is found, it's returned instantly.
4. **Root Servers:** If not cached, the resolver asks a root server, which directs it to the Top-Level Domain (TLD) server (e.g., for .com).
5. **TLD Servers:** The TLD server points to the Authoritative Nameserver for that domain.
6. **Authoritative Nameserver:** This server holds the official DNS records (like A records, which map names to IPs) and provides the final IP address.
7. **Connection:** Your browser receives the IP address and connects to the web server hosting the site.

ROLE OF WEB SERVERS

- **Hosting Content:** Web servers store all website files (HTML, CSS, images, videos).
- **Responding to Requests:** They listen for HTTP/HTTPS requests from browsers (once the IP is found via DNS) and send back the requested page data.
- **Serving Data:** They are the destination for DNS lookups, making the actual website accessible.

VIRTUAL PRIVATE NETWORK - VPN

A Virtual Private Network (VPN) is a network security technology that establishes an encrypted tunnel between a user's device and a remote VPN server over the public internet. It masks the user's IP address, protects data from unauthorized access, and ensures secure and private communication, especially when using untrusted networks.

- **Privacy Protection:** A VPN hides the user's real IP address and encrypts internet traffic, preventing Internet Service Providers (ISPs), advertisers, and third parties from monitoring browsing activities.
- **Security on Public Networks:** VPN encryption protects sensitive data such as passwords and personal information when connected to unsecured public Wi-Fi networks like those in airports or cafes.
- **Bypassing Geo-Restrictions:** By routing traffic through servers in different locations, a VPN enables access to region-restricted websites, streaming services, and online platforms.
- **Prevention of Bandwidth Throttling:** Since ISPs cannot inspect encrypted VPN traffic, intentional speed throttling during activities like streaming or gaming can be reduced or avoided.
- **Secure Remote Access:** VPNs allow employees and remote workers to securely access private organizational networks and internal resources over the internet.

WORKING OF VPN

A VPN operates by establishing a secure, encrypted tunnel between a user's device and a remote VPN server, ensuring that all data transmitted over the public internet remains confidential and protected from unauthorized access.

Step-by-Step Working of a VPN

- **Connection Establishment:** When the VPN is activated, the client software authenticates the user and establishes a secure connection with a VPN server operated by the service provider.
- **Data Encryption:** All outgoing data is encrypted using cryptographic algorithms, making it unreadable to hackers, ISPs, or any third party attempting to intercept the traffic.
- **Traffic Redirection:** The encrypted data is routed through the VPN server, which replaces the user's real IP address with its own, thereby masking the user's identity and location.
- **Data Decryption and Forwarding:** At the VPN server, the data is decrypted and forwarded to the intended destination (websites or online services). The response is then sent back to the user through the same encrypted tunnel.
- **End-to-End Protection:** This secure tunnelling ensures data privacy, integrity, and anonymity throughout the communication process.

TYPES OF VPN

VPNs can be classified based on their usage scenarios and underlying tunneling protocols, each designed to meet specific requirements ranging from individual remote access to large-scale enterprise connectivity.

A. VPN Types Based on Usage

- **Remote Access VPN:** Allows individual users to securely connect to a private network over the internet, commonly used by employees accessing organizational resources from remote locations.
- **Site-to-Site VPN:** Establishes a secure connection between two or more geographically separated networks, enabling seamless and protected communication between branch offices.
- **Mobile VPN:** Designed for mobile devices, it maintains a stable VPN connection even when the device switches between networks such as Wi-Fi and cellular data.
- **MPLS VPN (Multiprotocol Label Switching VPN):** Used primarily by large enterprises, MPLS VPNs provide efficient, scalable, and reliable network connectivity with traffic prioritization, though they rely on service provider infrastructure rather than encryption.

B. VPN Types Based on Protocols

- **PPTP (Point-to-Point Tunnelling Protocol):** An early VPN protocol that offers high speed but weak security, making it largely obsolete and suitable only for legacy systems.
- **L2TP/IPsec (Layer 2 Tunnelling Protocol with IPsec):** Combines tunneling and encryption to provide better security than PPTP, but with moderate performance overhead.
- **OpenVPN:** An open-source and highly secure VPN protocol that uses SSL/TLS for encryption and is widely adopted due to its flexibility and strong security.
- **IKEv2/IPsec (Internet Key Exchange v2 with IPsec):** A fast and secure protocol optimized for mobile users, known for its ability to reconnect when network conditions change automatically.

VPN PROTOCOLS

VPN protocols are standardized methods that define how data is securely tunneled, encrypted, transmitted, and authenticated between a user's device and a VPN server over a public network.

Common VPN Protocols

1. OpenVPN

- OpenVPN is an open-source VPN protocol that uses SSL/TLS for secure authentication and encryption, providing a highly configurable and versatile solution.
- It can operate over UDP for faster performance or TCP for reliability, making it suitable for different network environments.
- Supports strong cryptographic ciphers such as AES-256 and ChaCha20, ensuring data confidentiality and integrity.
- Compatible with most operating systems and capable of bypassing most firewall and NAT restrictions.
- Widely used for general-purpose secure remote access, privacy protection, and bypassing censorship.

2. WireGuard

- WireGuard is a modern VPN protocol designed to be lightweight, with a small codebase for reduced attack surface and high performance.
- Operates primarily over UDP, using a fixed set of modern cryptographic primitives such as ChaCha20 for encryption, Poly1305 for authentication, and BLAKE2s for hashing.
- Its simplicity and efficiency make it very fast and suitable for latency-sensitive applications such as streaming and online gaming.
- Ideal for mobile devices due to low overhead and rapid reconnection after network changes.

3. IKEv2/IPSec

- IKEv2 is a key exchange protocol that negotiates and establishes secure tunnels, usually paired with IPSec for encryption and data integrity.
- Offers automatic session re-establishment when the network connection changes, making it highly suitable for mobile devices that frequently switch between Wi-Fi and cellular networks.
- Uses strong encryption algorithms such as AES-256 and supports Perfect Forward Secrecy, ensuring that past sessions cannot be decrypted even if keys are compromised.
- Commonly used for remote access and secure connections in enterprise environments.

4. L2TP/IPSec

- L2TP creates a tunneling layer at the data link level, while IPSec provides encryption, authentication, and integrity of the transmitted data.
- Provides better security than PPTP but introduces double encapsulation, which can reduce network throughput.
- Compatible with a wide range of platforms, making it suitable for legacy systems and cross-platform VPN connectivity.
- Often used when other modern protocols are not supported, although it is slower than newer protocols.

5. PPTP

- PPTP (Point-to-Point Tunneling Protocol) is an older VPN protocol that establishes a tunnel for data transmission but uses weak encryption algorithms.
- It is very fast due to minimal overhead but is highly vulnerable to cryptographic attacks.
- No longer recommended for secure communications or sensitive data, but it may still be used in legacy environments where speed is prioritized over security.

6. SSTP

- SSTP (Secure Socket Tunneling Protocol) is a Microsoft-developed VPN protocol that encapsulates VPN traffic within SSL/TLS over TCP port 443, allowing it to traverse most firewalls.

- Provides robust encryption and authentication comparable to modern VPN protocols, primarily on Windows platforms.
- Especially useful for bypassing strict firewall restrictions where other VPN protocols may be blocked.
- Less widely supported on non-Windows operating systems.

HOW TO CHOOSE THE RIGHT VPN FOR YOUR NEEDS?

Choosing the right VPN involves evaluating security, performance, compatibility, and service reliability to ensure safe, efficient, and uninterrupted internet access based on individual or organizational requirements.

Factors to Consider When Selecting a VPN

- **Security Features:** Select a VPN that offers strong encryption standards (such as AES-256), secure protocols like OpenVPN or IKEv2/IPsec, and a strict no-logs policy to ensure data privacy.
- **Performance and Speed:** For activities like streaming, gaming, or video conferencing, choose a VPN with high-speed servers and low latency to avoid performance degradation.
- **Server Locations:** A wide range of global server locations improves connectivity options and enables access to geographically restricted content.
- **Device and Platform Compatibility:** Ensure the VPN supports all required operating systems and devices, including Windows, macOS, Android, iOS, and routers if needed.
- **Customer Support and Reliability:** Opt for a VPN provider with responsive customer support, clear documentation, and reliable uptime to resolve technical issues efficiently.

DRAWBACKS OF USING VPN

While VPNs enhance security and privacy, they also introduce certain limitations related to performance, accessibility, cost, and configuration that users should consider before adoption.

- **Reduced Internet Speed:** Encryption overhead and routing traffic through remote VPN servers can increase latency and reduce overall connection speed.
- **Variation in VPN Quality:** Not all VPN providers offer the same level of security; some may log user data or use weak encryption, compromising privacy.
- **VPN Blocking and Restrictions:** Certain websites, streaming platforms, and countries actively block VPN traffic, which may prevent access to specific services.
- **Configuration Complexity:** Manual VPN setup and advanced configurations may require technical knowledge, particularly in enterprise or custom environments.
- **Cost Considerations:** Free VPN services often have limitations, while premium VPNs involve recurring subscription costs in exchange for better performance and security.

NETWORK SECURITY PROTOCOLS (IPSec, SSL/TLS)

IPSec(IP Security)

What is IP Security (IPSec)

IP Security (IPSec) refers to a collection of communication rules or protocols used to establish secure network connections. Internet Protocol (IP) is the common standard that controls how data is transmitted across the internet. IPSec enhances the protocol security by introducing **encryption** and **authentication**. IPSec encrypts data at the source and then decrypts it at the destination. It also verifies the source of the data.

Importance of IPSec

IPSec (Internet Protocol Security) is important because it helps keep your data safe and secure when you send it over the Internet or any network. Here are some of the important aspects why IPSec is Important:

- IPSec protects the data through Data Encryption.
- IPSec provides Data Integrity.
- IPSec is often used in Virtual Private Networks (VPNs) to create secure, private connections.
- IPSec protects from Cyber Attacks.

Features of IPSec

- **Authentication:** IPSec provides authentication of IP packets using digital signatures or shared secrets. This helps ensure that the packets are not tampered with or forged.
- **Confidentiality:** IPSec provides confidentiality by encrypting IP packets, preventing eavesdropping on the network traffic.
- **Integrity:** IPSec provides integrity by ensuring that IP packets have not been modified or corrupted during transmission.
- **Key management:** IPSec provides key management services, including key exchange and key revocation, to ensure that cryptographic keys are securely managed.
- **Tunneling:** IPSec supports tunneling, allowing IP packets to be encapsulated within another protocol, such as GRE (Generic Routing Encapsulation) or L2TP (Layer 2 Tunneling Protocol).
- **Flexibility:** IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.
- **Interoperability:** IPSec is an open standard protocol, which means that it is supported by a wide range of vendors and can be used in heterogeneous environments.

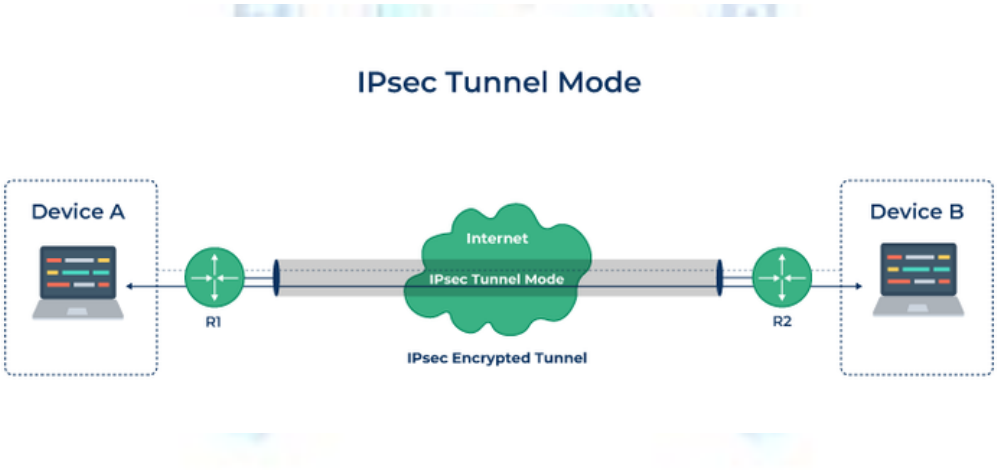
How Does IPSec Work

IPSec (Internet Protocol Security) is used to secure data when it travels over the Internet. IPSec works by creating secure connections between devices, making sure that the information exchanged is kept safe from unauthorized access. IPSec majorly operates in two ways i.e. **Transport Mode** and **Tunnel Mode**.

To provide security, IPSec uses two main protocols: **AH (Authentication Header)** and **ESP (Encapsulating Security Payload)**. Both protocols are very useful as **Authentication Header** verifies the data that whether it comes from a trusted source and hasn't been changed, and **ESP** has the work of performing authentication and also encrypts the data so that it becomes difficult to read.

For Encryption, IPSec uses cryptographic keys. It can be created and shared using a process called **IKE (**Internet Key Exchange**)**, that ensures that both devices have the correct keys to establish a secure connection.

When two devices communicate using IPSec, the devices first initiate the connection by sending a request to each other. After that, they mutually decide on protection of data using **passwords** or digital certificates. Now, they establish the secure tunnel for communication. Once the tunnel is set up, data can be transmitted safely, as IPSec is encrypting the data and also checking the integrity of the data to ensure that data has not been altered. After the communication is finished, the devices can close the secure connection. In this way, the IPSec works.



IPSec Connection Establishment Process

IPSec is a protocol suite used in securing communication using the Internet Protocol such that each packet communicated in the course of a particular session is authenticated and encrypted. The process of establishing an IPSec connection involves two main phases:

Phase 1: Establishing the IKE (Internet Key Exchange) Tunnel

In phase 1, the main aim is to establish the secure channel the IKE tunnel, which is used to further negotiations. Phase 1 can operate in one of two modes:

- **Main Mode:** Main Mode is a six-message exchange procedure that is more secure than Basic Mode, although at the cost of a longer session, since identity information is transmitted during negotiations.
- **Aggressive Mode:** Aggressive Mode takes lesser time with the exchange of three messages and is less secure since more information like identity is disclosed during the course of negotiation.

Phase 2: Establishing the IPSec Tunnel

Phase 2 is called Quick Mode and its aim is to negotiate the IPSec Security Associations after the construction of a secure IKE tunnel has been made. There are two modes in Phase 2.

- **Tunnel Mode:** This mode encapsulates the whole of the original IP packet including the header and data. It is mostly deployed in the site to site VPNs.
- **Transport Mode:** By this mode, only the actual data to be transmitted is encrypted and the header part of the IP packets remain unaltered. It is mainly employed in end to end communication between hosts.

Difference Between IPSec Tunnel Mode and IPSec Transport Mode

- The IPSec tunnel mode is appropriate for sending data over public networks because it improves data security against unauthorised parties. The computer encrypts all data, including the payload and header, and adds a new header to it.
- IPSec transport mode encrypts only the data packet's payload while leaving the IP header unchanged. The unencrypted packet header enables routers to determine the destination address of each data packet. As a result, IPSec transport is utilized in a closed and trusted network, such as to secure a direct link between two computers.

Protocols Used in IPSec

It has the following components:

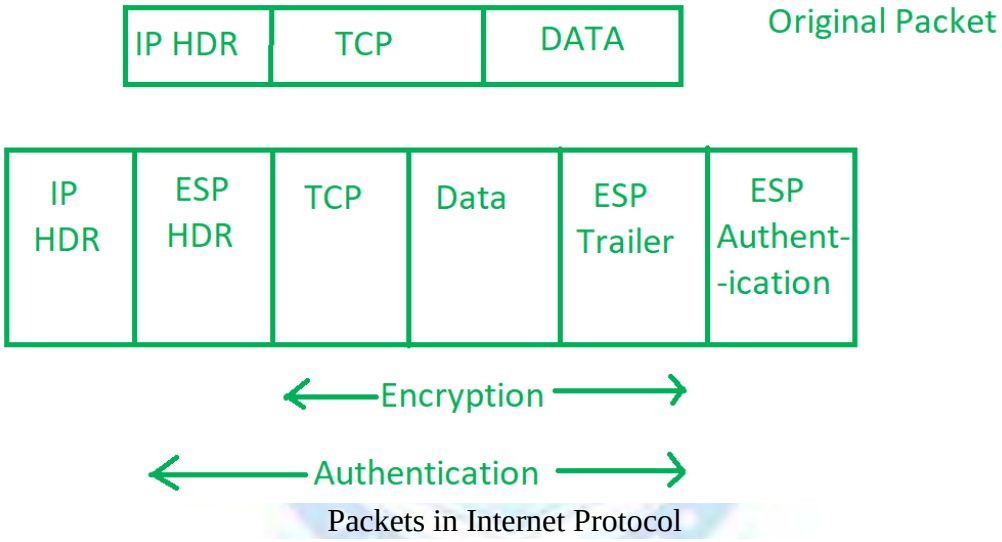
- Encapsulating Security Payload (ESP)
- Authentication Header (AH)
- Internet Key Exchange (IKE)

1. Encapsulating Security Payload (ESP): It provides data integrity, encryption, authentication, and anti-replay. It also provides authentication for payload.

2. Authentication Header (AH): It also provides data integrity, authentication, and anti-replay and it does not provide encryption. The anti-replay protection protects against the unauthorized transmission of packets. It does not protect data confidentiality.

IP Header

3. Internet Key Exchange (IKE): It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association provides a framework for authentication and key exchange. ISAKMP tells how the setup of the Security Associations (SAs) and how direct connections between two hosts are using IPsec. Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP sec users produce a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets that are not authorized are discarded and not given to the receiver.



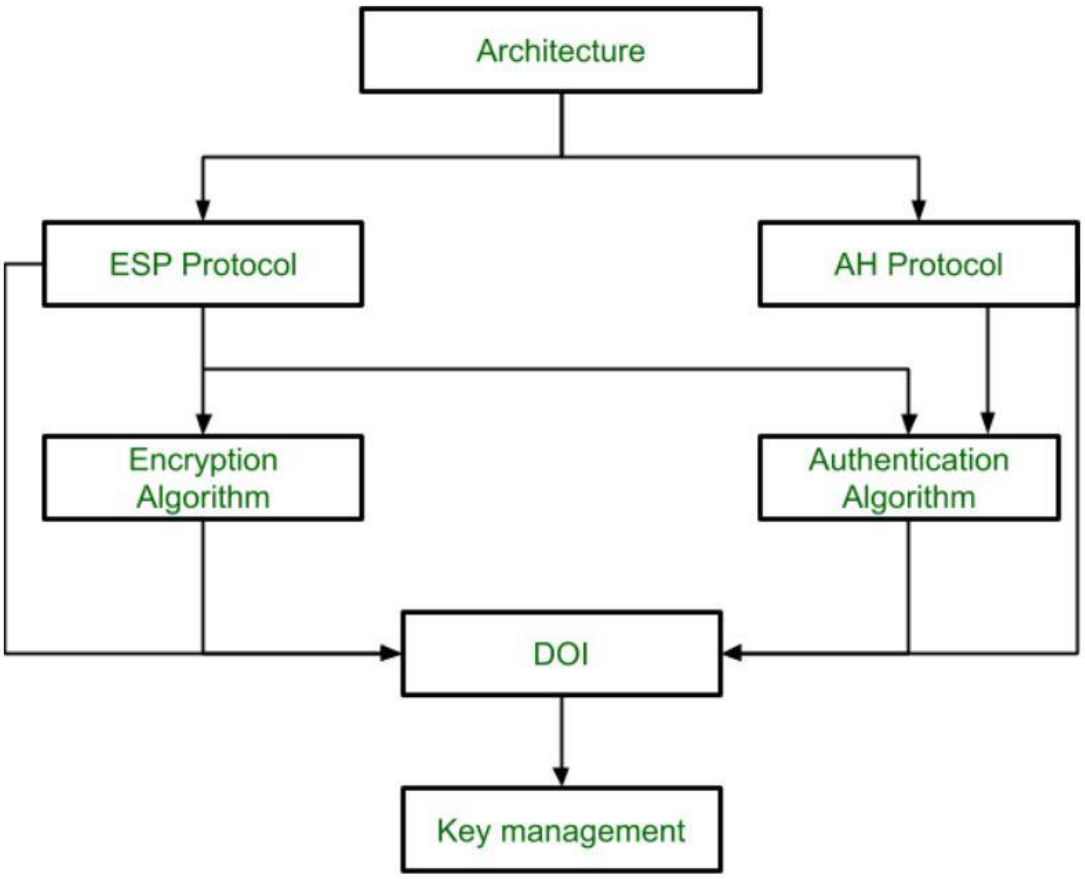
Packets in Internet Protocol

IP Security Architecture

IPSec (IP Security) architecture uses two protocols to secure the traffic or data flow. These protocols are

- ESP (Encapsulation Security Payload)
- AH (Authentication Header)

IPSec Architecture includes protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services such as Confidentiality, Authenticity and Integrity.



IP Security Architecture

IPSec Encryption

IPSec encryption is a software function that encrypts data to protect it from unauthorized access. An encryption key encrypts data, which must be decrypted. IPSec supports a variety of encryption algorithms, including AES, Triple DES etc. IPSec combines asymmetric and symmetric encryption to provide both speed and security during data transmission. In asymmetric encryption, the encryption key is made public, while the decryption key remains private. Symmetric encryption employs the same public key to encrypt and decrypts data. IPSec builds a secure connection using asymmetric encryption and then switches to symmetric encryption to speed up data transmission.

IPSec VPN

VPN(Virtual Private Network) is a networking software that enables users to browse the internet anonymously and securely. An IPSec VPN is a type of VPN software that uses the IPSec protocol to establish encrypted tunnels over the internet. It offers end-to-end encryption, which means that data is broken down at the computer and then collected at the receiving server.

Uses of IP Security

IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

Advantages of IPSec

- **Strong security:** IPSec provides strong cryptographic security services that help protect sensitive data and ensure network privacy and integrity.
- **Wide compatibility:** IPSec is an open standard protocol that is widely supported by vendors and can be used in heterogeneous environments.
- **Flexibility:** IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.
- **Scalability:** IPSec can be used to secure large-scale networks and can be scaled up or down as needed.
- **Improved network performance:** IPSec can help improve network performance by reducing network congestion and improving network efficiency.

Disadvantages of IPSec

- **Configuration Complexity:** IPSec can be complex to configure and requires specialized knowledge and skills.
- **Compatibility Issues:** IPSec can have compatibility issues with some network devices and applications, which can lead to interoperability problems.
- **Performance Impact:** IPSec can impact network performance due to the overhead of encryption and decryption of IP packets.
- **Key Management:** IPSec requires effective key management to ensure the security of the cryptographic keys used for encryption and authentication.
- **Limited Protection:** IPSec only provides protection for IP traffic, and other protocols such as ICMP, DNS, and routing protocols may still be vulnerable to attacks.

SSL/TLS

SSL (Secure Socket Layer) and TLS (Transport Layer Security) are like bodyguards for websites, making sure that when information is sent over the internet, it stays safe and can't be messed with by sneaky people. They use a special code to lock up the data and keep it private.

Think of TLS as the upgraded version of SSL. It's like when you get a new and improved phone with better features. TLS is on its third version, called TLS 1.3, and it's more secure than SSL, which is kind of like the older version.

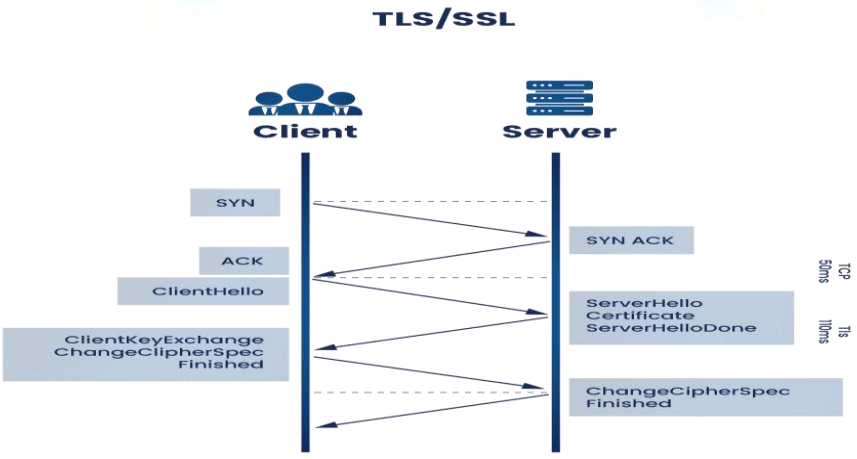
Even though SSL is outdated and not used in modern systems anymore, people still use the term "SSL" when talking about both protocols. For example, they might say "SSL certificate."

When you see "HTTPS" in your web browser's address bar, it means that the website is using TLS to protect your connection. It's like a green light that tells you it's safe.

TLS doesn't just protect websites; it also keeps things like emails and calls safe from prying eyes. It's like a superhero for your online conversations!

Secure Socket Layer (SSL)

HOW DOES IT WORK?



When two systems employing TLS attempt to establish a connection, they go through a process known as the TLS handshake. During this handshake, both parties verify each other's support for TLS and agree on parameters like TLS version, encryption algorithm, and cipher suite. Once the TLS handshake is successful, a secure line is established for data exchange.

Encryption and decryption in TLS rely on keys, where public keys encrypt information, and private keys decrypt it. This asymmetric cryptography involves two different keys for security.

The TLS handshake typically follows these steps, considering a scenario where a client (browser) connects to a server hosting a website:

1. The client requests the server to open a secure line, and the server responds by presenting a list of compatible TLS versions and cipher suites. Once they agree on common parameters, the handshake begins.
2. The server sends its public key, attached to a digital certificate, to the client. The client verifies the certificate to ensure the server's legitimacy before proceeding.
3. Using the server's public key and its private key, the client encrypts a 'session key.' This session key is used by both parties for encrypting and decrypting information during the session and becomes invalid upon connection termination.
4. Both parties test the connection by sending encrypted messages to each other. If the other party can successfully decrypt these messages using the session key, the connection is secured.

SSL PROTOCOLS

SSL consists of several protocols, each handling a different aspect of secure communication

1. SSL Record Protocol

SSL Record Protocol

- Provides confidentiality and message integrity.
- Application data is divided into fragments, optionally compressed and appended with a Message Authentication Code (MAC).
- The data is then encrypted and transmitted with an SSL header.

2. Handshake Protocol

Establishes SSL sessions and authenticates clients and servers.

SSL Handshake Protocol Phases diagrammatic representation

Four phases:

- Client and server exchange hello packets, protocol versions and cipher suites.
- Server sends its certificate and server key information.
- Client responds with its certificate and key exchange.
- Change Cipher Spec finalizes the handshake, activating secure communication.

3. Change-Cipher Spec Protocol.

Change Cipher Spec Protocol

- Signals that pending cryptographic parameters from the handshake should now become active.
- Consists of a single 1-byte message.

4. Alert Protocol

Alert Protocol

- Communicates SSL-related warnings or errors.
- **Warning alerts (level 1):** Non-critical issues, such as expired or unsupported certificates.
- **Fatal alerts (level 2):** Critical errors, such as handshake failures, bad record MAC or illegal parameters, which terminate the connection.

Versions of SSL/TLS

Version	Release Year	Notes
SSL 1	Never released	Insecure
SSL 2	1995	First public release
SSL 3	1996	Improved security
TLS 1.0	1999	Successor to SSL 3.0
TLS 1.1	2006	Improved encryption and security
TLS 1.2	2008	Widely adopted, strong encryption
TLS 1.3	2018	Modern, efficient, secure protocol

SSL CERTIFICATES

SSL certificates are digital certificates issued by trusted Certificate Authorities (CAs) to secure and verify websites.

Key Features

- **Encryption:** Protects sensitive information during transmission.
- **Authentication:** Confirms the identity of the website or service.
- **Integrity:** Ensures transmitted data is not altered.
- **Non-repudiation:** Prevents denial of transmitted messages.
- **Public-key cryptography:** Facilitates secure key exchange.
- **Session management:** Allows resumption of secure sessions after interruptions.

Types of SSL Certificates

1. **Single-Domain:** Secures one domain.
2. **Wildcard:** Secures one domain and all its subdomains.
3. **Multi-Domain:** Secures multiple unrelated domains in one certificate.

Validation Levels

- **Domain Validation (DV):** Confirms domain ownership.
- **Organization Validation (OV):** Confirms the organization's identity.
- **Extended Validation (EV):** Rigorous verification, highest trust level, often indicated by a green address bar.

APPLICATIONS: E-COMMERCE (SSL/TLS), VPNS FOR REMOTE WORK, DNS IN URL RESOLUTION, FIREWALLS IN BANKS AND ENTERPRISES, CYBERSECURITY PRACTICES IN WEB APPS.

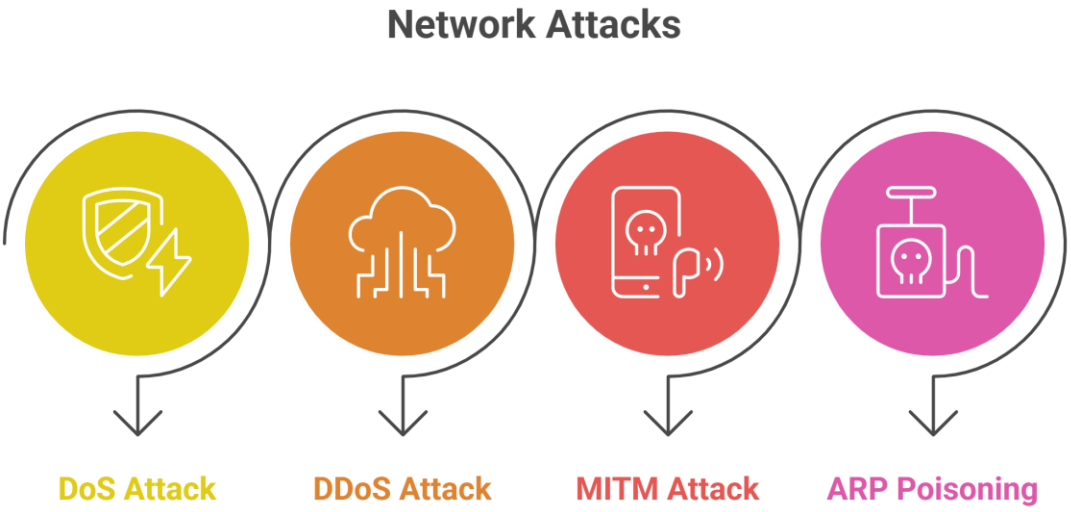
The following applications illustrate the fundamental role of networking protocols and security measures in modern technology:

- **E-commerce (SSL/TLS)**: Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS), are essential for e-commerce. They establish encrypted links between a web server and a client (browser), ensuring that sensitive data such as credit card numbers and login credentials remain private and secure during online transactions. This is often indicated by "HTTPS" in the URL bar and a padlock icon.

- **VPNs for Remote Work**: Virtual Private Networks (VPNs) create a secure, encrypted "tunnel" over the public internet, allowing remote workers to securely connect to their company's internal network. This protects corporate data from interception and unauthorized access, effectively extending the secure boundary of the enterprise network to the remote employee's location.
- **DNS in URL Resolution**: The Domain Name System (DNS) is a critical protocol that acts as the internet's phonebook. When a user types a URL (e.g., www.example.com) into a browser, DNS translates this human-readable domain name into a machine-readable IP address, which directs the browser to the correct server hosting the website.
- **Firewalls in Banks and Enterprises**: Firewalls are security systems that monitor and control incoming and outgoing network traffic based on predefined security rules. Financial institutions and large enterprises use firewalls to create a barrier between their trusted internal networks and untrusted external networks (like the internet), preventing unauthorized access and cyber threats.
- **Cyber security Practices in Web Apps**: Web applications employ various cyber security practices to protect against attacks. These include input validation to prevent SQL injection and cross-site scripting (XSS) attacks, using secure coding principles (like the guidance from the OWASP Foundation), regular security audits, and employing Web Application Firewalls (WAFs) to filter malicious traffic.

SECURITY CONCERNS AT THE NETWORK LAYER: ATTACKS (DOS, DDOS, MITM AND ARP POISONING).

Network layer security concerns involve attacks like **DoS/DDoS**, overwhelming services with traffic (e.g., flooding with requests) to cause outages, and **Man-in-the-Middle (MitM)**, where attackers intercept and alter communication between two parties, often by spoofing addresses (like ARP poisoning) to eavesdrop, steal data, or hijack sessions, disrupting confidentiality and integrity. These attacks target network protocols and infrastructure, making data unavailable or untrustworthy.



1. DoS (Denial of Service) Attack

A DoS attack is one of the simplest yet most dangerous types of network attacks. In a DoS attack, the attacker tries to make a server, website, or network unavailable to users. This is done by overwhelming the system with too many requests, causing it to slow down or crash.

Example: Imagine a shop that can only serve 50 customers at a time. A group of people intentionally blocks the entrance, so real customers cannot enter. In the digital world, the "shop" is a website, and the "people blocking the entrance" are the fake requests from the attacker.

Signs of a DoS attack:

- Websites or services become slow or unreachable.
- Servers may crash or restart frequently.
- Network traffic spikes abnormally.

How to prevent it:

- Use firewalls and intrusion detection systems.
- Limit requests from a single IP.
- Employ content delivery networks (CDNs) to absorb traffic.

2. DDoS (Distributed Denial of Service) Attack

A DDoS attack is similar to a DoS attack but more powerful. Instead of one computer, the attacker uses multiple computers or devices (often part of a botnet) to send overwhelming traffic to the target.

Example: Think of the previous shop scenario. This time, not just one group, but thousands of people from different cities block the shop. Naturally, real customers cannot enter, and the shop loses business.

Types of DDoS attacks:

- **Volume-based attacks:** Flood the network with traffic.
- **Protocol attacks:** Exploit weaknesses in network protocols like TCP or HTTP.
- **Application layer attacks:** Target specific applications, like web servers or login pages.

How to prevent it:

- Use DDoS protection services like Cloudflare or AWS Shield.
- Monitor traffic patterns for unusual spikes.
- Scale resources to handle temporary traffic surges.

3. MITM (Man-in-the-Middle) Attack

A MITM attack happens when an attacker secretly intercepts communication between two parties. The attacker can eavesdrop, modify, or steal data without the users knowing.

Example: Imagine sending a letter to your friend, but someone secretly opens it, reads it, and even changes its content before it reaches your friend. In digital terms, the "letter" can be emails, chat messages, or website data.

How attackers perform MITM attacks:

- **Wi-Fi eavesdropping:** Setting up fake Wi-Fi networks to capture data.
- **Packet sniffing:** Intercepting data packets in transit.
- **SSL stripping:** Replacing secure HTTPS connections with HTTP to capture data.

How to prevent it:

- Always use HTTPS websites.
- Avoid public Wi-Fi or use a VPN.
- Enable two-factor authentication (2FA) on accounts.
- Keep software and devices updated.

4. ARP Poisoning (Address Resolution Protocol Poisoning)

ARP poisoning is a network attack where the attacker spoofs the MAC address of a device to intercept data on a local network. It allows attackers to redirect traffic, steal sensitive information, or launch other attacks like MITM.

How it works:

- Every device on a local network has an IP and a MAC address.
- Devices use ARP (Address Resolution Protocol) to match IPs to MAC addresses.
- Attackers send fake ARP messages, tricking devices into sending data to the attacker instead of the correct destination.

Example: Imagine sending a parcel to your friend, but the delivery man is tricked into giving it to a stranger. That stranger can open it, read the contents, and even send it to your friend afterward.

How to prevent ARP poisoning:

- Use static ARP entries for critical devices.
- Deploy network security tools that detect ARP anomalies.
- Enable packet filtering and encryption to protect sensitive data.

Signs That Your Network Might Be Under Attack

Recognizing the signs of network attacks can help you respond faster:

- Slow network or unresponsive websites.
- Frequent system crashes or application failures.
- Unusual network traffic spikes.
- Unknown devices connected to your network.
- Unexpected login attempts or alerts from security systems.

General guidelines to Protect Your Network

- **Keep systems updated** – Security patches fix known vulnerabilities.
- **Use strong passwords** and change them regularly.
- **Enable firewalls and antivirus software** on all devices.
- **Segment your network** – Separate critical systems from public-facing networks.
- **Monitor logs and network traffic** for unusual activity.
- **Educate users** about phishing and safe browsing practices.

INTRODUCTION TO FIREWALLS: TYPES (PACKET FILTERING, STATEFUL INSPECTION, PROXY FIREWALLS

A firewall is a network security system, available as hardware or software, that monitors and controls incoming and outgoing traffic based on predefined rules. It acts like a security guard, filtering data packets to either:

- **Accept:** Allow the traffic.
- **Reject:** Block with an error response.
- **Drop:** Block silently without response.

Importance of Firewalls

A firewall is the first line of defense in cybersecurity, acting as a security barrier between internal systems and external networks. It forces all traffic through a single checkpoint, where data packets are monitored, filtered, and either allowed or blocked based on predefined rules. Firewalls are essential because they:

- **Prevent Unauthorized Access:** Like a locked door with a guard, only trusted users and traffic are allowed through.
- **Block Malicious Traffic:** Harmful data such as viruses, phishing attempts, or denial-of-service (DoS) attacks are stopped before reaching the system.
- **Protect Sensitive Information:** Safeguards personal and business data from theft or accidental leaks.
- **Control Network Usage:** Enforces policies such as parental controls, workplace restrictions, or government filtering.
- **Mitigate Insider Risks:** Detects suspicious applications or data exfiltration attempts from within the network.

By combining prevention, monitoring, and control, firewalls provide customizable and comprehensive protection against both external and internal threats.

Working of Firewall

A firewall inspects all incoming and outgoing traffic and decide whether to allow or block it.

1. All data packets entering or leaving the network must first pass through the firewall.
2. The firewall examines each packet against predefined security rules set by the organization.
3. If the packet matches safe rules, it is allowed; if it is suspicious, blacklisted, or contains malicious content, it is blocked.
4. Blocked or unusual traffic is recorded in logs, and real-time alerts may be generated for serious threats.
5. Since it is not possible to define every rule, the firewall applies a default policy (accept, reject, or drop). Setting the default policy to drop or reject is considered best practice to prevent unauthorized access.

TYPES OF NETWORK FIREWALLS

Here are the main types of network firewalls, organized by how they function and where they're deployed:

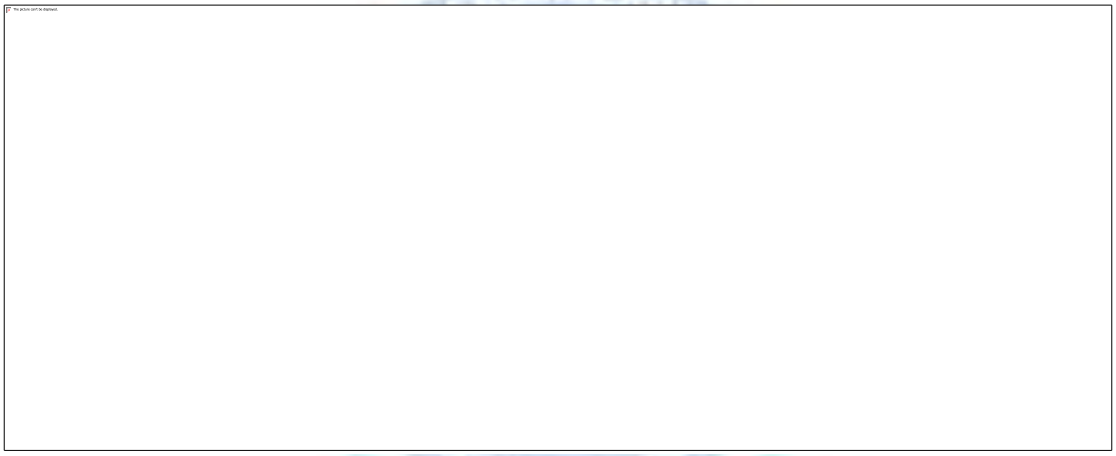
1) Based on Function (How They Filter Traffic)

Network Security is the process of protecting networks, systems, and data from unauthorized access, attacks, and damage.

a. Packet Filtering Firewall

A basic firewall that checks packet headers like IP, port, and protocol.

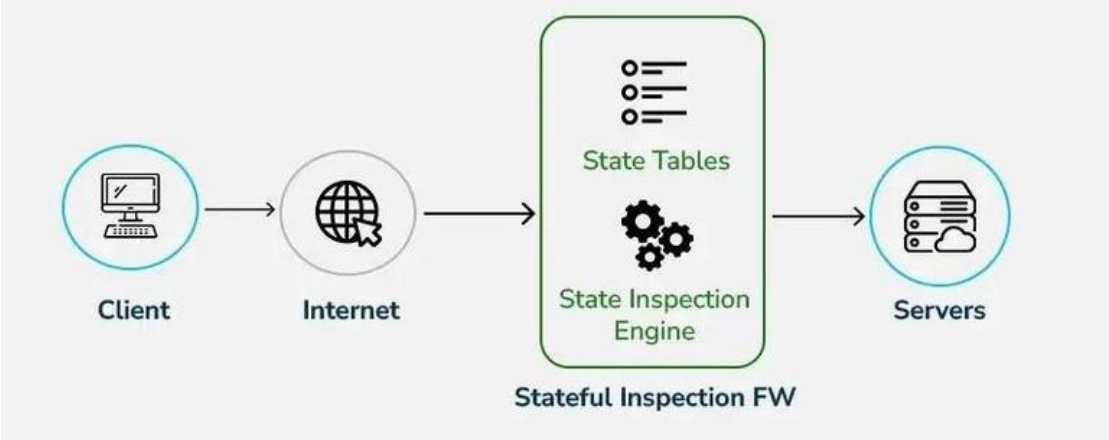
- Very fast and lightweight
- Does not inspect data inside packets
- Provides basic security only



b. Stateful Inspection Firewall

Tracks active connections and makes decisions based on traffic context.

- More secure than packet filtering
- Remembers past traffic (state table)
- Blocks suspicious or unexpected packets



c. Proxy (Application-Level) Firewall

Acts as a middleman between user and destination server.

- Filters data at the application layer
- Hides internal network details
- Can block malicious content before it reaches the user