Unit-6

Application Layer

Application Layer Function

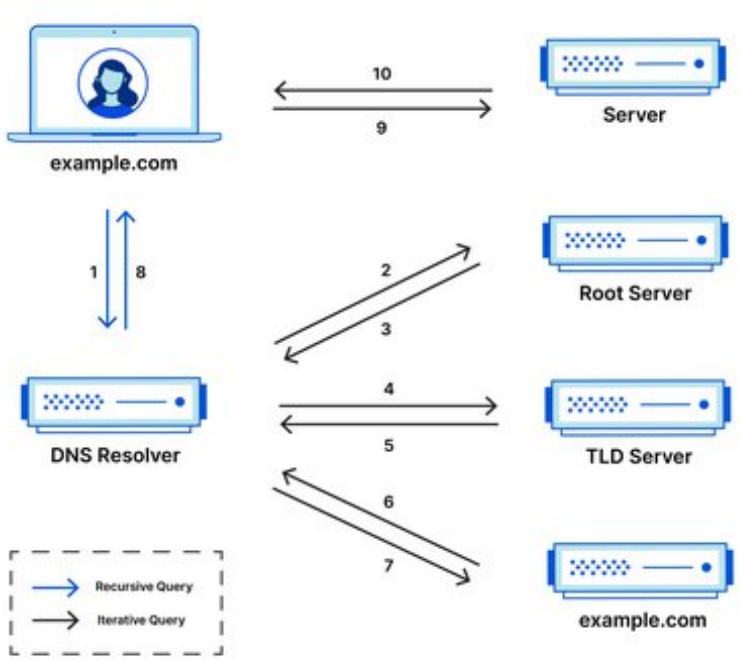
- The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services. Specific services provided by the application layer include the following:
- **Network virtual terminal**. A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.
- **File transfer, access, and management.** This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- **Mail services.** This application provides the basis for e-mail forwarding and storage.
- **Directory services.** This application provides distributed database sources and access to global information about various objects and services.

Web

Web services are information exchange systems that use the Internet for direct application-to-application interaction. These systems can include programs, objects, messages, or documents. A web service is a collection of open protocols and standards used for exchanging data between applications or systems. The World Wide Web (WWW) is a repository of information linked together from points all over the world. The WWW has a unique combination of flexibility, portability, and user-friendly features that distinguish it from other services provided by the Internet. The World Wide Web (WWW), commonly known as the Web, is an information system where documents and other web resources are identified by Uniform Resource Locators (URLs, such as https://www.example.com/), which may be interlinked by hypertext and are accessible over the Internet. The resources of the WWW may be accessed by users by a software application called a web browser. The World Wide Web is what most people think of as the Internet. It is all the Web pages, pictures, videos, and other online content that can be accessed via a Web browser. The Internet, in contrast, is the underlying network connection that allows us to send emails and access the World Wide Web.

DNS

DNS (Domain Name System) is a system that translates human-readable domain names, like www.example.com, into IP addresses, which computers use to identify each other on the internet. The Domain Name System (DNS) is the phonebook of the Internet. When users type domain names such as ‘google.com’ or ‘nytimes.com’ into web browsers, DNS is responsible for finding the correct IP address for those sites.

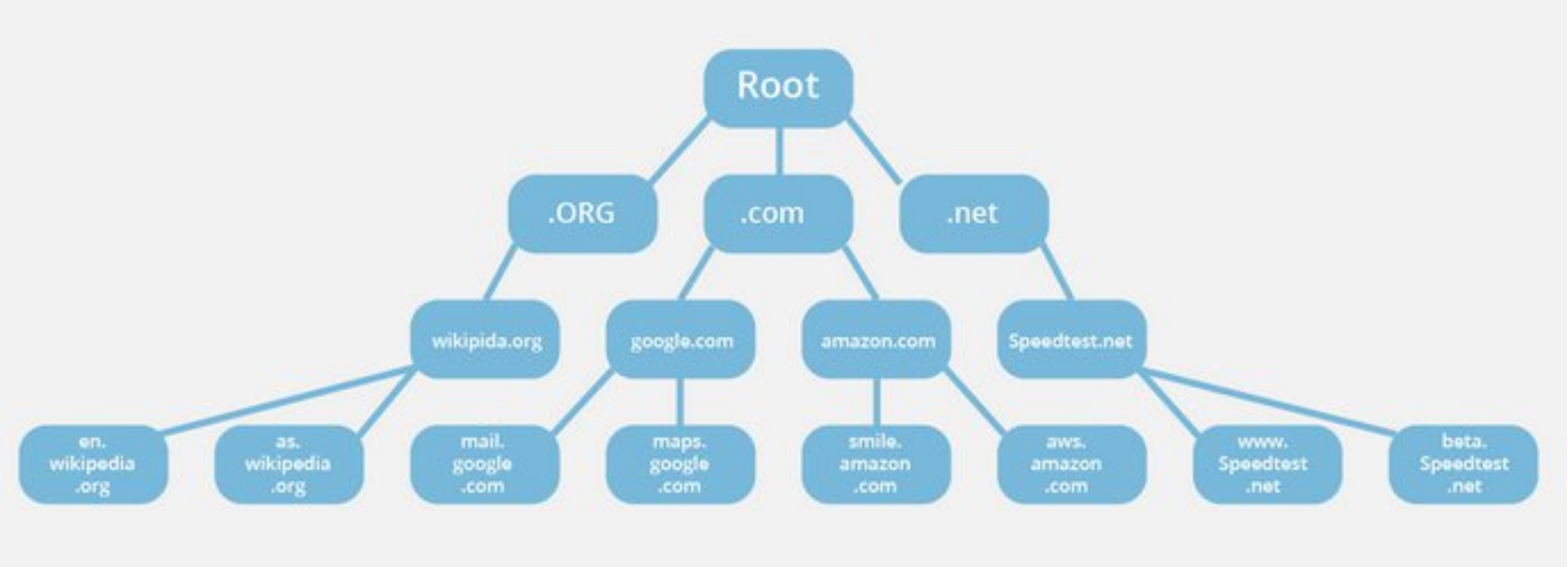


How DNS works?

Here's a simplified explanation of how DNS works:

1. You type a domain name into your web browser (e.g., www.example.com).
2. Your computer sends a query to a DNS resolver (usually provided by your Internet Service Provider (ISP) or a third-party provider like Google DNS), asking for the IP address associated with that domain name.
3. The DNS resolver checks its cache to see if it has the IP address for that domain name. If it does, it returns the IP address to your computer and the process is complete.
4. If the DNS resolver doesn't have the IP address in its cache, it sends a request to a DNS root server, asking for the IP address for the top-level domain (TLD) of the domain name (in this case, .com).
5. The root server responds with a referral to the authoritative server for the .com TLD.
6. The DNS resolver sends a request to the authoritative server for the .com TLD, asking for the IP address for the domain name (e.g., www.example.com).
7. The authoritative server responds with the IP address for the domain name.
8. The DNS resolver caches the IP address for future use and returns it to your computer.
9. Your computer uses the IP address to connect to the web server hosting the website associated with the domain name

How DNS works?



DNS Query Type

There are three types of queries in the DNS system:

Recursive Query

In a recursive query, a DNS client provides a hostname, and the DNS Resolver “must” provide an answer—it responds with either a relevant resource record, or an error message if it can't be found. The resolver starts a recursive query process, starting from the DNS Root Server, until it finds the Authoritative Name Server (for more on Authoritative Name Servers see DNS Server Types below) that holds the IP address and other information for the requested hostname.

Iterative Query

In an iterative query, a DNS client provides a hostname, and the DNS Resolver returns the best answer it can. If the DNS resolver has the relevant DNS records in its cache, it returns them. If not, it refers the DNS client to the Root Server, or another Authoritative Name Server which is nearest to the required DNS zone. The DNS client must then repeat the query directly against the DNS server it was referred to.

DNS Query Type

Non-Recursive Query

A non-recursive query is a query in which the DNS Resolver already knows the answer. It either immediately returns a DNS record because it already stores it in the local cache, or queries a DNS Name Server which is authoritative for the record, meaning it definitely holds the correct IP for that hostname. In both cases, there is no need for additional rounds of queries (like in recursive or iterative queries). Rather, a response is immediately returned to the client.

HTTP

HTTP (Hypertext Transfer Protocol) is a protocol used for transmitting data over the internet. It is the foundation of data communication on the World Wide Web and is responsible for the transfer of data between web servers and clients. HTTP is based on a client-server architecture, where the client (typically a web browser) sends a request to the server, and the server responds with the requested data. An HTTP session is a sequence of network request-response transactions. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a server (typically port 80, occasionally port 8080).

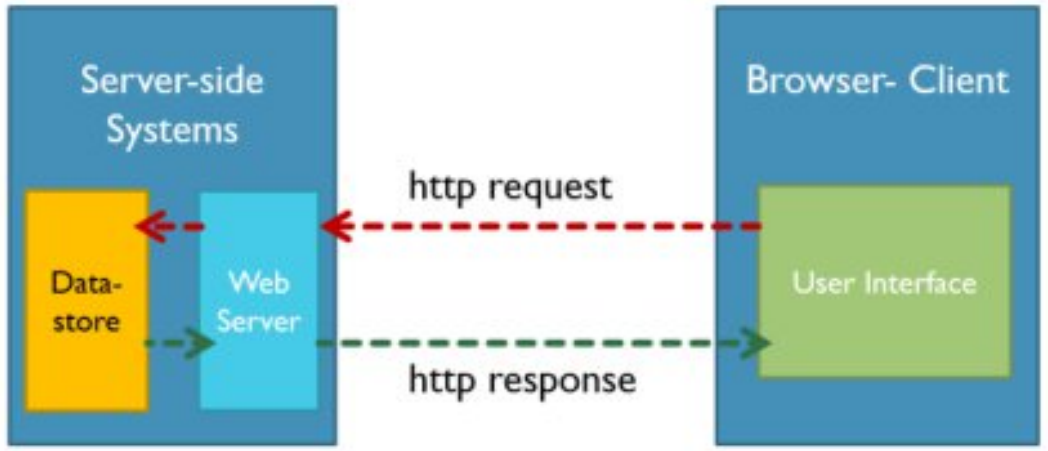
An HTTP server listening on that port waits for a client's request message. Upon receiving the request, the server sends back a status and a message of its own. The body of this message is typically the requested resource, although an error message or other information may also be returned. HTTP is also called a stateless protocol because the sessions between the HTTP browser and the HTTP client are not saved for later reference. The session information is only valid until the session exists.

HTTP

- Here are the main features of HTTP:

1. Stateless Protocol: HTTP is a stateless protocol, which means that each request/response transaction is independent of any other request/response transaction. The server does not maintain any information about previous requests from the same client.
2. Request/Response Model: HTTP follows a request/response model where the client sends a request to the server and waits for a response. The server processes the request and returns a response back to the client.
3. Methods: HTTP defines several methods that are used to request specific actions from the server, such as GET (to retrieve data), POST (to submit data), PUT (to update data), and DELETE (to delete data).
4. Headers: HTTP messages contain headers that provide additional information about the message, such as the content type, cache control directives, and authentication information.
5. Status Codes: HTTP uses status codes to indicate the status of the request/response transaction. For example, a 200 status code indicates that the request was successful, while a 404 status code indicates that the requested resource was not found.

HTTP



HTTP Methods and Their Meaning

Method	Meaning
GET	Read data
POST	Insert data
PUT or PATCH	Update data, or insert if a new id
DELETE	Delete data

HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is a variant of the standard web transfer protocol (HTTP) that adds a layer of security to the data in transit through a secure socket layer (SSL) or transport layer security (TLS) protocol connection. HTTPS enables encrypted communication and secure connection between a remote user and the primary web server. HTTPS is primarily designed to provide an enhanced security layer over the unsecured HTTP protocol for sensitive data and transactions such as billing details, credit card transactions, and user login, etc. HTTPS encrypts every data packet in transition using SSL or TLS encryption techniques to avoid intermediary hackers and attackers to extract the content of the data; even if the connection is compromised. HTTPS is configured and supported by default in most web browsers and initiates a secure connection automatically if the accessed web server requests a secure connection. HTTPS works in collaboration with certificate authorities that evaluate the security certificate of the accessed website.

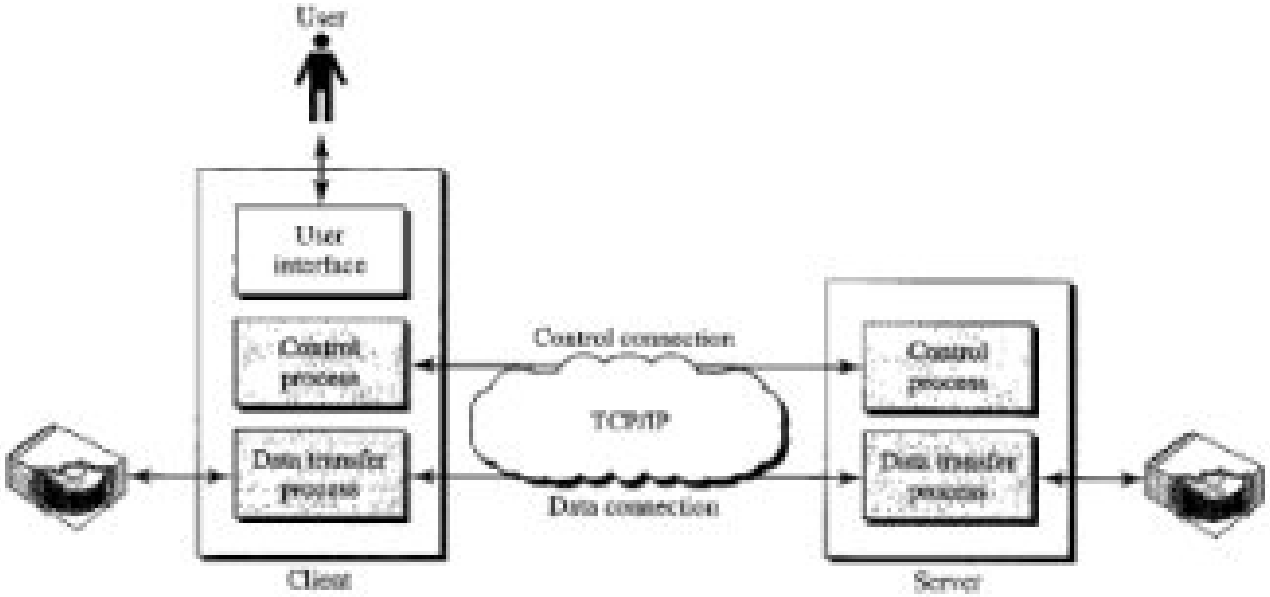
FTP

File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections.

FTP is a client-server protocol that relies on two communications channels between client and server: a command channel for control information (commands and responses) and a data channel for transmitting file content. Clients initiate conversations with servers by requesting to download a file. Using FTP, a client can upload, download, delete, rename, move, and copy files on a server. A user typically needs to log on to the FTP server, although some servers make some or all of their content available without login, also known as anonymous FTP.

FTP uses two well-known TCP ports: Port 21 for the **control connection** and Port 20 for the **data connection**. The control connection remains connected during the entire interactive FTP session. The data connection is opened and then closed for each file transfer. It opens each time commands that involve transferring files are used, and it closes when the file is transferred. In other words, 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


User
User interface
Control process
Data transfer process
Control connection
TCP/IP
Data connection
Control process
Data transfer process
Client
Server

FTP

FTP clients

FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.FTP clients are used to upload, download and manage files on a server. FTP clients include the following:

- **FileZilla.** This is a free FTP client for Windows, macOS and Linux that supports FTP, FTPS and SFTP.
- **Transmit.** This is an FTP client for macOS that supports FTP and SSH.
- **WinSCP.** This is a Windows FTP client that supports FTP, SSH and SFTP.
- **WS_FTP.** This is another Windows FTP client that supports SSH.

How does FTP work?

FTP is a client-server protocol that relies on two communication channels between the client and server: a command channel for controlling the conversation and a data channel for transmitting file content.
Here is how a typical FTP transfer works:
1.A user typically needs to log on to the FTP server, although some servers make some or all of their content available without a login, a model known as *anonymous FTP*.
2.The client initiates a conversation with the server when the user requests to download a file.
3.Using FTP, a client can upload, download, delete, rename, move and copy files on a server.

SFTP

SFTP, which stands for SSH File Transfer Protocol, or Secure File Transfer Protocol, is a separate protocol packaged with SSH that works in a similar way but over a secure connection. The advantage is the ability to leverage a secure connection to transfer files and traverse the filesystem on both the local and remote systems.

In almost all cases, SFTP is preferable to FTP because of its underlying security features and ability to rely on an SSH connection. FTP is an insecure protocol that should only be used in limited cases or on networks you trust.

SSH or Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command line, login, and remote command execution, but any network service can be secured with SSH.

By default, SFTP uses the SSH protocol to authenticate and establish a secure connection. Because of this, the same authentication methods are available that are present in SSH.

SFTP also protects against password sniffing and man-in-the-middle attacks. It protects the integrity of the data using encryption and cryptographic hash functions, and authenticates both the server and the user.

SMTP

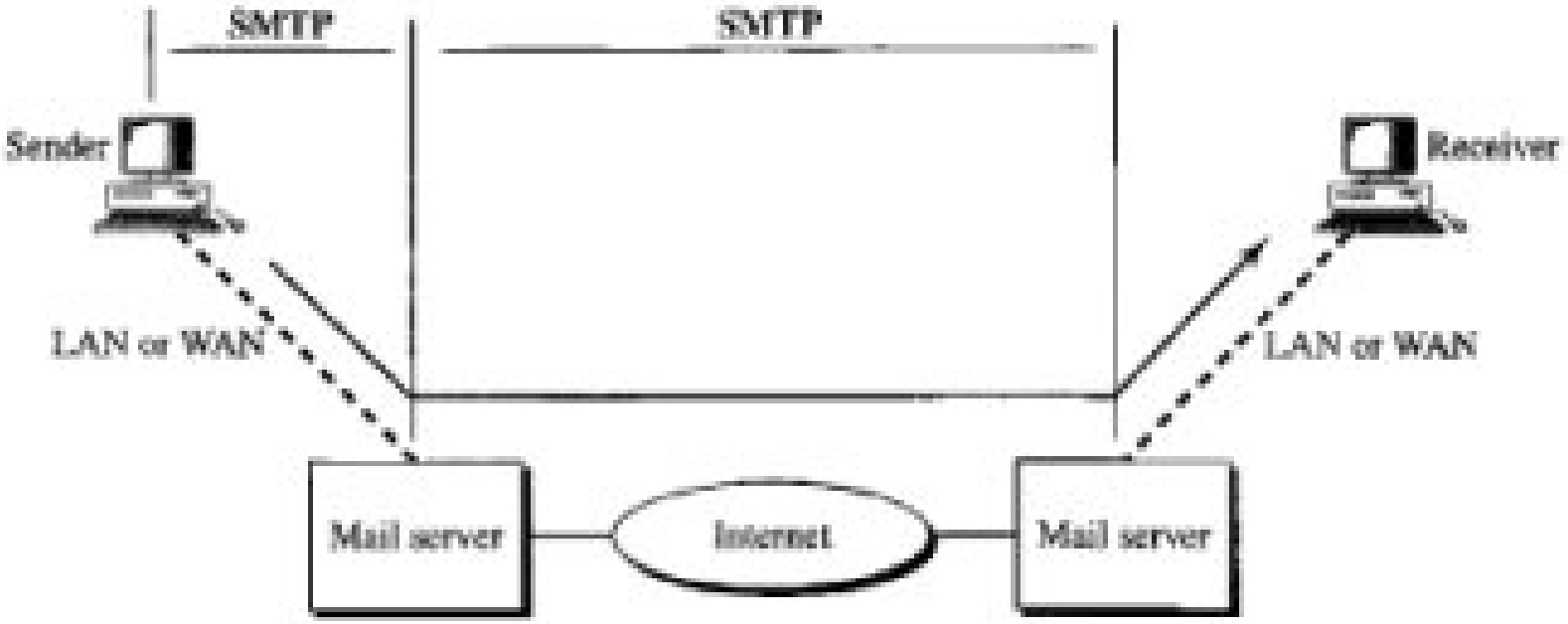
SMTP is a client-server protocol, meaning that it requires a client to initiate communication with a server. The client typically runs on the sender's computer, while the server runs on the recipient's computer.

Here's a simplified overview of how SMTP works:

1. The sender creates an email message and enters the recipient's email address.
2. The sender's mail client (such as Outlook or Gmail) sends the message to the sender's mail server using SMTP.
3. The sender's mail server looks up the recipient's mail server's IP address using DNS and initiates an SMTP session with the recipient's mail server.
4. The sender's mail server sends the email message to the recipient's mail server over the SMTP connection.
5. The recipient's mail server receives the message and stores it in the appropriate mailbox.
6. The recipient's mail client (such as Outlook or Gmail) retrieves the message from the recipient's mail server using a protocol like POP3 or IMAP.

SMTP is a widely used protocol for sending email messages over the internet, and it's used by a variety of email clients and servers. It's a relatively simple protocol, but it's also very powerful and flexible, making it an important component of the Internet’s email infrastructure.

SMTP


SMTP
SMTP
Sender
Receiver
LAN or WAN
LAN or WAN
Mail server
Internet
Mail server

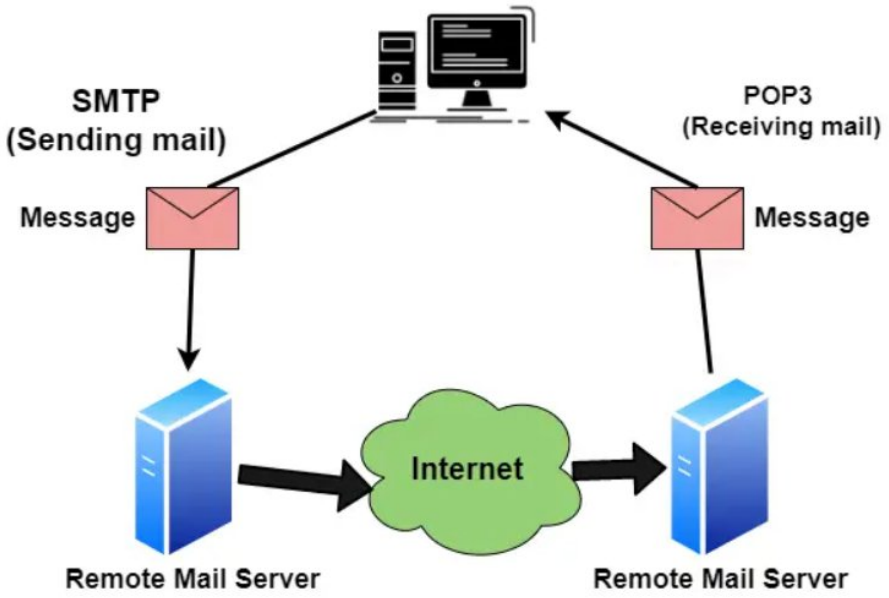
POP

- Post Office Protocol (POP) is a type of computer networking and Internet standard protocol that extracts and retrieves email from a remote mail server for access by the host machine.
- POP is an application layer protocol in the OSI model that provides end users the ability to fetch and receive email.

POP

- All the incoming messages are stored on the POP server until the user login by using an email client and downloads the message to their computer. After the message is downloaded by the user it gets deleted from the server.
- As we know that SMTP is used to transfer the email message from the server to the server, basically POP is used to collect the email with an email client from the server and it does not include means to send messages.
- If any user tries to check all the recent emails then they will establish a connection with the **POP3** at the server-side. The user sends the username and password to the server machine for getting the proper authentication. After getting the connection, users can receive all text-based emails and store them on their local terminal (machine), then finally discard all server copies and then breaks the connection from the server machine.
- In order to retrieve a message from the server following steps are taken;
- Firstly a TCP connection is established by the client using port 110.
- The client identifies itself to the server.
- After that client issues a series of POP3 commands.

POP


SMTP
(Sending mail)
POP3
(Receiving mail)
Message
Message
Internet
Remote Mail Server
Remote Mail Server

IMAP

IMAP stands for **Internet Message Access Protocol**. It is an application layer protocol that is used to receive emails from the mail server. It is the most commonly used protocol like POP3 for retrieving emails. With IMAP accounts, messages are stored on a remote server. Users can log in via multiple email clients on computers or mobile devices and read the same messages. All changes made in the mailbox will be synced across multiple devices and messages will only be removed from the server if the user deletes the email.

- You can be logged in with multiple computers and devices simultaneously.
- Your mail archive is synced and stored on the server for all connected devices to access.
- Sent and received mail is stored on the server until the user permanently deletes it.

Overview of Application Server Concepts:

Application Server is a type of server designed to install, operate, and host applications. An application server is a program that resides on the server side, and it’s a server programmer providing business logic behind any application. This server can be a part of the network or the distributed network. Ideally, server programs are used to provide their services to the client program that either resides on the same machine or lies on a network.

Overview of Application Server Concepts: Proxy Server:

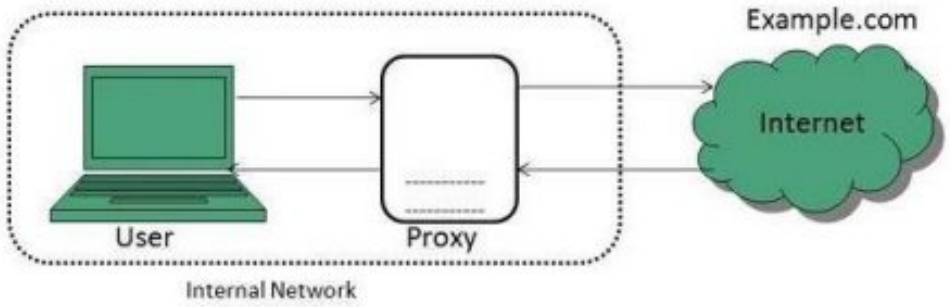
Proxy Server: In computer networks, a proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server. The proxy server evaluates the request as a way to simplify and control its complexity. Thus, a Proxy server is an intermediary server between the client and the internet. Proxy servers allow you to hide, conceal and make your network id anonymous by hiding your IP address.

Functionalities and Benefits of Proxy Servers:

- Firewall, Network data Monitoring, and filtering.
- Network connection sharing
- Data caching, Improving Performance
- Translation of Content
- Accessing Services Anonymously
- Enhanced Security

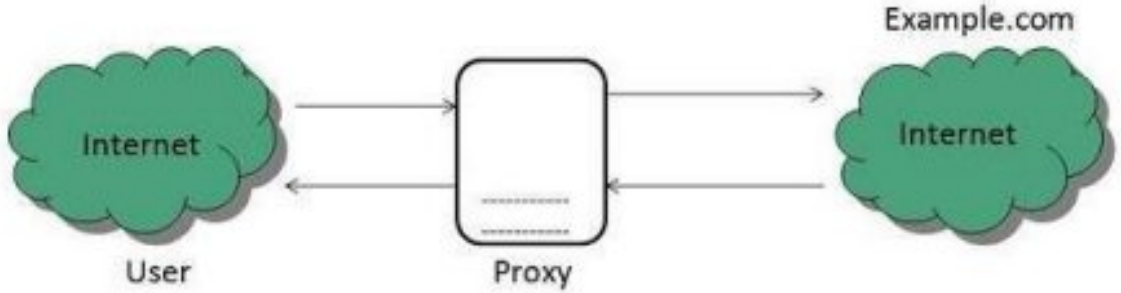
Types of Proxies

1. **Forward Proxies:** In this, the client requests its internal network server to forward to the internet.



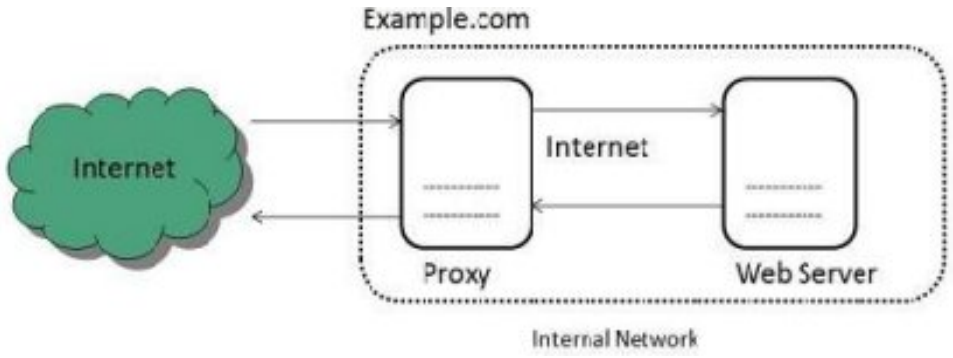
Types of Proxies

2. Open Proxies: Open Proxies helps the clients to conceal their IP address while browsing the web.



Types of Proxies

3. Reverse Proxies: In this, the requests are forwarded to one or more proxy servers, and the response from the proxy server is retrieved as if it came directly from the original Server.

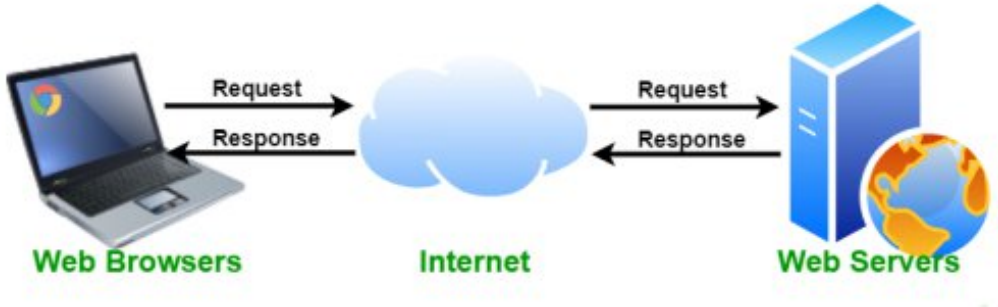


Web Server:

Web server can refer to either the hardware (the computer) or the software (the computer application) that helps to deliver Web content that can be accessed through the Internet. The most common use of web servers is to host websites, but there are other uses such as gaming, data storage or running enterprise applications. The primary function of a web server is to deliver web pages on the request to clients using the Hypertext Transfer Protocol (HTTP). A user agent, commonly a web browser, initiates communication by making a request for a specific resource using HTTP and the server responds with the content of that resource or an error message if unable to do so. The resource is typically a real file on the server's secondary memory, but this is not necessarily the case and depends on how the web server is implemented. While the primary function is to serve content, a full implementation of HTTP also includes ways of receiving content from clients.

Web Server:

Web servers respond to the client request in either of the following two ways: • Sending the file to the client associated with the requested URL. • Generating response by invoking a script and communicating with database.



Key Points:

• When a client sends a request for a web page, the web server search for the requested page if the requested page is found then it will send it to the client with an HTTP response.

• If the requested web page is not found, the web server will send an HTTP response: Error 404 Not found.

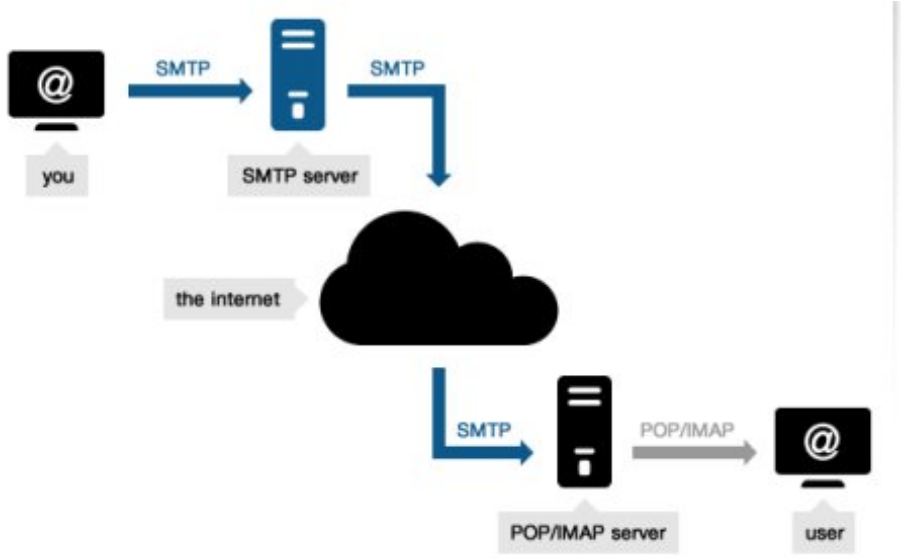
• If the client has requested some other resources then the web server will contact to the application server and data store to construct the HTTP response.

Mail Server:

A mail server (or email server) is a computer system that sends and receives email. In many cases, web servers and mail servers are combined in a single machine. However, large ISPs and public email services (such as Gmail and Hotmail) may use dedicated hardware for sending and receiving emails. In order for a computer system to function as a mail server, it must include mail server software. This software allows the system administrator to create and manage email accounts for any domains hosted on the server. For example, if the server hosts the domain name "example.com," it can provide email accounts ending in "@example.com." Mail servers send and receive email using standard email protocols. For example, the SMTP protocol sends messages and handles outgoing mail requests. The IMAP and POP3 protocols receive messages and are used to process incoming mail. When you log on to a mail server using a webmail interface or email client, these protocols handle all the connections behind the scenes. Webmail: example.com/webmail Email Client: Email applications and interfaces like Gmail, Outlook, Yandex etc.

Mail Server:

Mail servers can be broken down into two main categories: outgoing mail servers and incoming mail servers. • Outgoing mail servers are known as SMTP, or Simple Mail Transfer Protocol, servers. • Incoming mail servers come in two main varieties. o POP3, or Post Office Protocol version 3, servers are best known for storing sent and received messages on PCs' local hard drives. o IMAP, or Internet Message Access Protocol, servers always store copies of messages on servers. Most POP3 servers can store messages on servers, too, which is a lot more convenient.



Network Management: SNMP (Simple Network Management Protocol)

We can define network management as monitoring, testing, configuring, and troubleshooting network components to meet a set of requirements defined by an organization. These requirements include the smooth, efficient operation of the network that provides a predefined quality of service for users.

Network Management Functions:

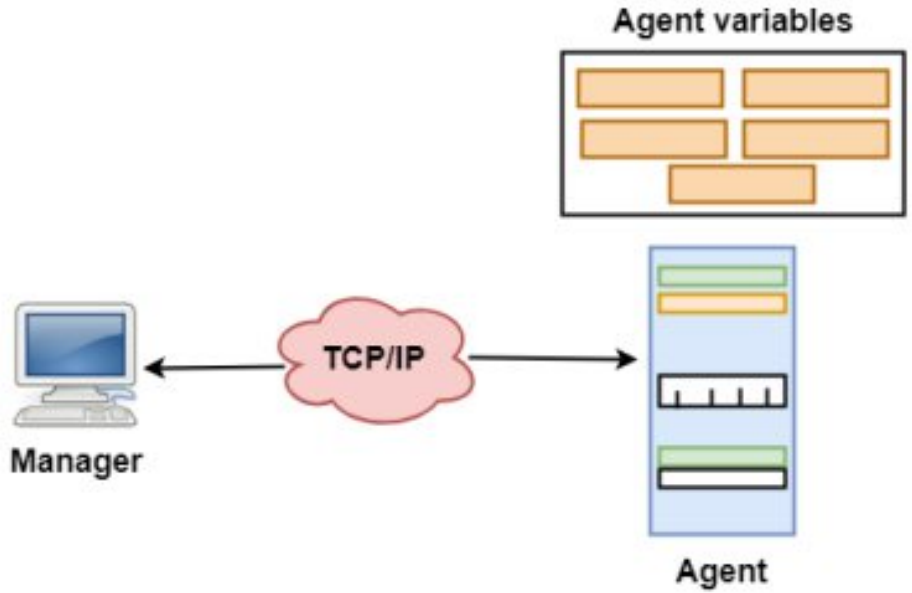
• **Performance management** deals with monitoring and managing the various parameters that measure the performance of the network. Performance management is an essential function that enables a service provider to provide quality-of-service guarantees to their clients and to ensure that clients comply with the requirements imposed by the service provider.

Network Management: SNMP Protocol

- **Fault management** is the function responsible for detecting failures when they happen and isolating the failed component. The network also needs to restore traffic that may be disrupted due to the failure, but this is usually considered a separate function.
- **Configuration management** deals with the set of functions associated with managing orderly changes in a network. The basic function of managing the equipment in the network, connection management, and network adaptation belong to this category.
- **Security management** includes administrative functions such as au authenticating users and setting attributes such as read and write permissions on a per-user basis.

Network Management: SNMP Protocol

Simple Network Management Protocol (SNMP) is the application layer protocol that is used to perform the above-mentioned network management functions. SNMP uses the concept of manager and agent. That is, a manager, usually a host, controls and monitors a set of agents, usually routers. A few manager stations control a set of agents. The protocol is designed at the application level so that it can monitor devices made by different manufacturers and installed on different physical networks.



Network Management: SNMP Protocol

Managers and Agents:

- A manager is a host that runs the SNMP client program while the agent is a router that runs the SNMP server program.
- Management of the internet is achieved through simple interaction between a manager and an agent.
- The agent is used to keep the information in a database while the manager is used to access the values in the database. For example, a router can store the appropriate variables such as the number of packets received and forwarded while the manager can compare these variables to determine whether the router is congested or not.
- Agents can also contribute to the management process. A server program on the agent checks the environment, if something goes wrong, the agent sends a warning message to the manager.