Unit 6: Application Layer

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 for 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.

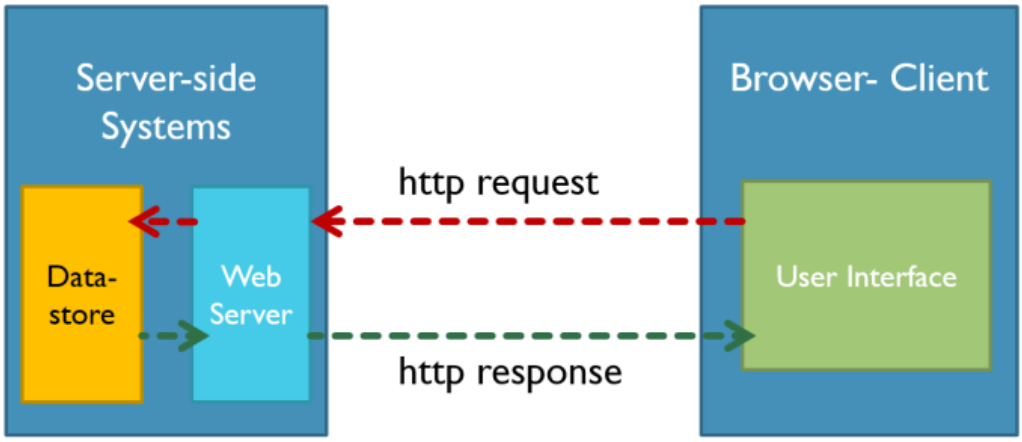
The World Wide Web (WWW), commonly known as the Web, is an information system where documents and other web resources are identified by Uniform Resource Locators (URLs, such as https://www.example.com/), which may be interlinked by hypertext, and are accessible over the Internet. The resources of the 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 email and access the World Wide Web.

HTTP:

The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser.

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 stateless protocol because the sessions between the HTTP browser

and HTTP client are not saved for later reference. The session is information is only valid until the session exists.



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

lynda.com

HTTPS:

Hypertext Transfer Protocol Secure (HTTPS) is a variant of the standard web transfer protocol (HTTP) that adds a layer of security on 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 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 technique to avoid intermediary hackers and attackers to extract the content of the data; even if the connection is compromised.

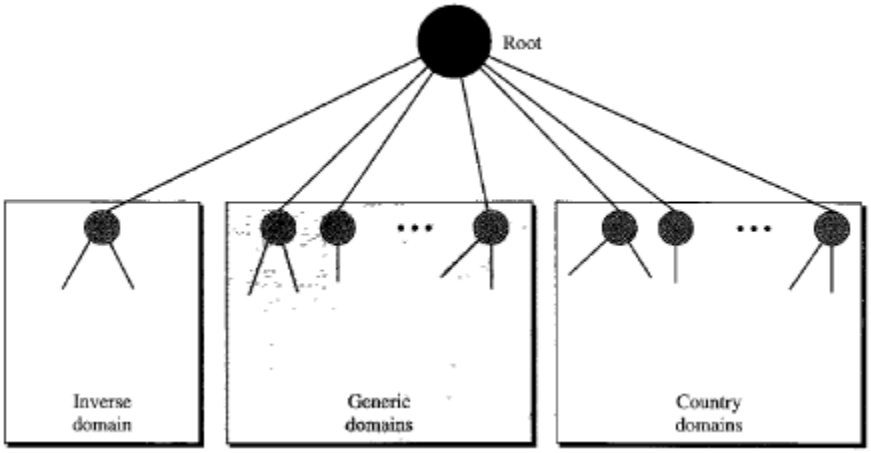
HTTPS is configured and supported by default in most web browsers and initiates a secure connection automatically if the accessed web server requests secure connection. HTTPS works in collaboration with certificate authorities that evaluates the security certificate of the accessed website.

Domain Naming System (DNS):

The domain name system (DNS) is a naming database in which internet domain names are located and translated into internet protocol (IP) addresses. The domain name system maps the name people use to locate a website to the IP address that a computer uses to locate a website. For example, if someone types example.com into a web browser, a server behind the scenes will map that name to the corresponding IP address. Facebook.com will be mapped to 66.220.144.0. Web browsing and most other internet activities rely on DNS to quickly provide the information necessary to connect users to remote hosts.

Although it's possible to enter an IP address into a web browser into order to get to a website, it's a lot easier to enter its domain name instead. However, computers, servers and other devices are unable to make heads or tails of domain names - they strictly rely on binary identifiers. The DNS's job, then, is to take domain names and translate them into the IP addresses that allow machines to communicate with one another. Every domain name has at least one IP address associated with it.

Figure 25.8 *DNS used in the Internet*



Generic domain labels

Com-commercial organizations

Gov- Government institutions

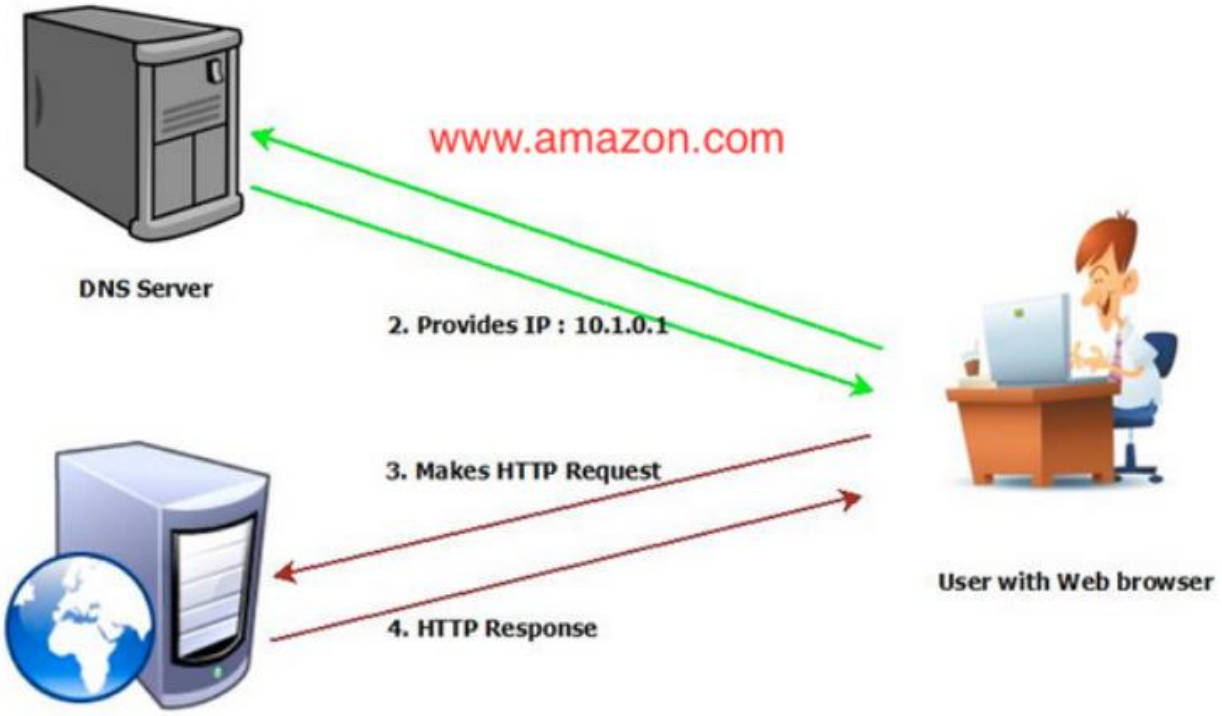
Net- network support centers

Org- nonprofit organizations

Name- personal names (individual) etc.

Inverse Domain: Used to map an ip address to a domain name.

Country Domains: .np, .in, .jp, .au, .uk, etc



There are three types of queries in the DNS system:

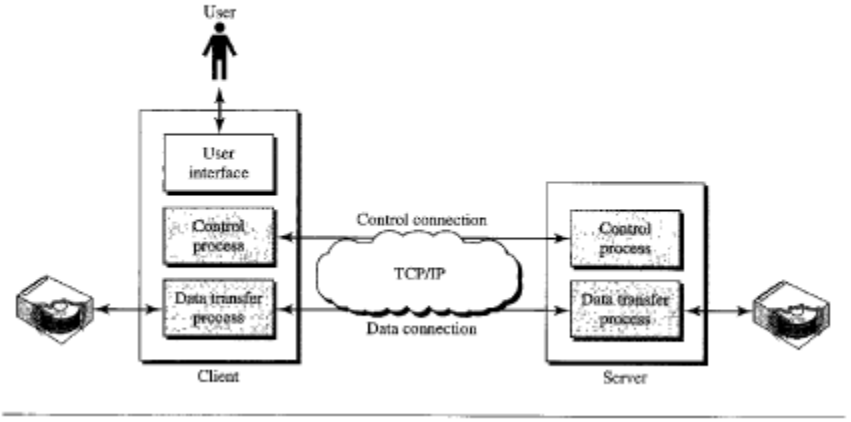
- **Recursive Query**
  In a recursive query, a DNS client provides a hostname, and the DNS Resolver "must" provide an answer—it responds with either a relevant resource record, or an error message if it can't be found. The resolver starts a recursive query process, starting from the DNS Root Server, until it finds the Authoritative Name Server 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.
- **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 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.

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 control connection and Port 20 for the data connection.

Figure 26.21 *FTP*



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.

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 system.

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.

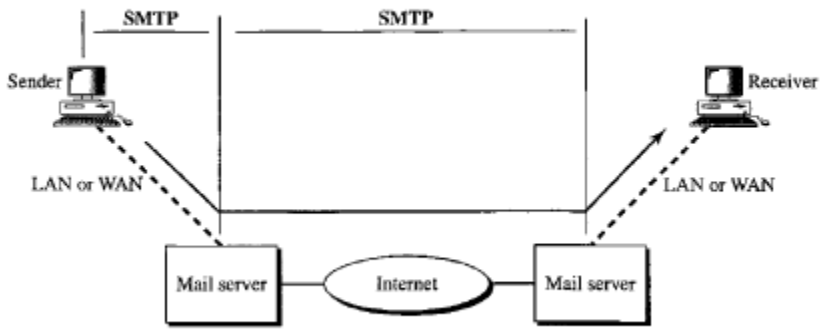
By default, SFTP uses the SSH protocol to authenticate and establish a secure connection. Because of this, the same authentication methods are available that are present in SSH.

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.

Simple Mail Transfer Protocol (SMTP):

It is a standard protocol used for sending e-mail efficiently and reliably over the internet.

Figure 26.16 *SMTP range*



Key Points:

- SMTP is application level protocol.
- SMTP is connection-oriented protocol.
- SMTP is text-based protocol.
- It handles exchange of messages between e-mail servers over TCP/IP network.
- Apart from transferring e-mail, SMTP also provides notification regarding incoming mail.
- When you send e-mail, your e-mail client sends it to your e-mail server which further contacts the recipient mail server using SMTP client.
- In case, message cannot be delivered, an error report is sent to the sender which makes SMTP a reliable protocol.

S.N.	Command Description
1	**HELLO** This command initiates the SMTP conversation.

2	**EHELLO** This is an alternative command to initiate the conversation. ESMTP indicates that the sender server wants to use extended SMTP protocol.
3	**MAIL FROM** This indicates the sender's address.
4	**RCPT TO** It identifies the recipient of the mail. In order to deliver similar message to multiple users this command can be repeated multiple times.
5	**SIZE** This command let the server know the size of attached message in bytes.
6	**DATA** The **DATA** command signifies that a stream of data will follow. Here stream of data refers to the body of the message.
7	**QUIT** This command is used to terminate the SMTP connection.
8	**VERFY** This command is used by the receiving server in order to verify whether the given username is valid or not.
9	**EXPN** It is same as VRFY, except it will list all the users name when it used with a distribution list.

IMAP:

IMAP stands for Internet Message Access Protocol. It is a standard protocol for accessing e-mail from the local server. IMAP is a client/server protocol in which e-mail is received and held by the Internet server. As this requires only a small data transfer, this works well even over a slow connection. Only if we request to read a specific email, message will it be downloaded from the server. We can also create and manipulate folders or mailboxes on the server, delete messages etc.

Key Points:

- IMAP allows the client program to manipulate the e-mail message on the server without downloading them on the local computer.

- The e-mail is hold and maintained by the remote server.
- It enables us to take any action such as downloading, delete the mail without reading the mail. It enables us to create, manipulate and delete remote message folders called mail boxes.
- IMAP enables the users to search the e-mails.
- It allows concurrent access to multiple mailboxes on multiple mail servers.

POP:

POP stands for Post Office Protocol. It is generally used to support a single client. There are several versions of POP but the POP 3 is the current standard.

Key Points

- POP is an application layer internet standard protocol.
- Since POP supports offline access to the messages, thus requires less internet usage time.
- POP does not allow search facility.
- In order to access the messages, it is necessary to download them.
- It allows only one mailbox to be created on server.
- It is not suitable for accessing non-mail data.

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.

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 their complexity.

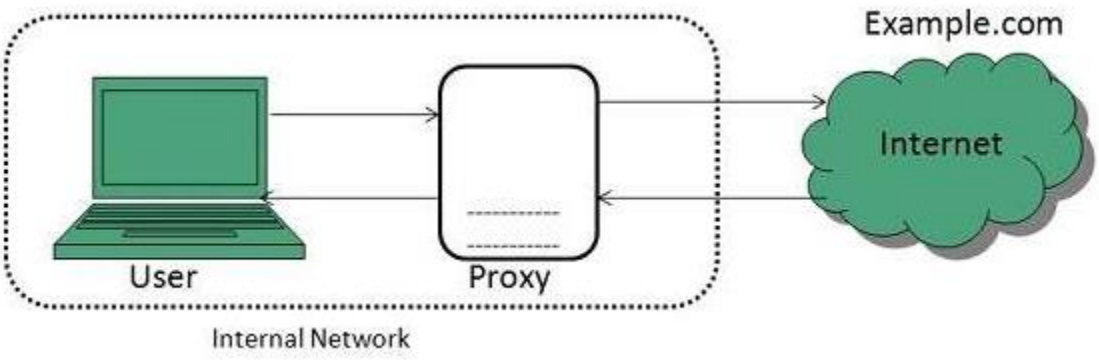
Thus, Proxy server is an intermediary server between client and the internet. Proxy servers allow to hide, conceal and make your network id anonymous by hiding your IP address.

Functionalities and Benefits of Proxy Servers:

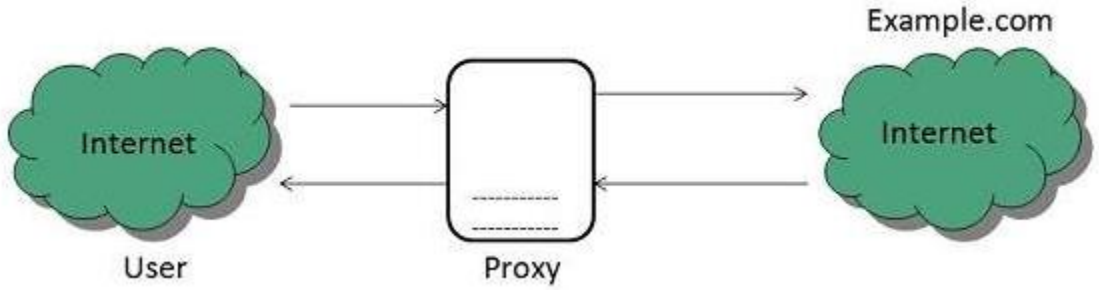
- Firewall, Network data Monitoring and filtering.
- Network connection sharing
- Data caching, Improving Performance
- Translation of Content
- Accessing Services Anonymously
- Enhanced Security

Types of Proxies:

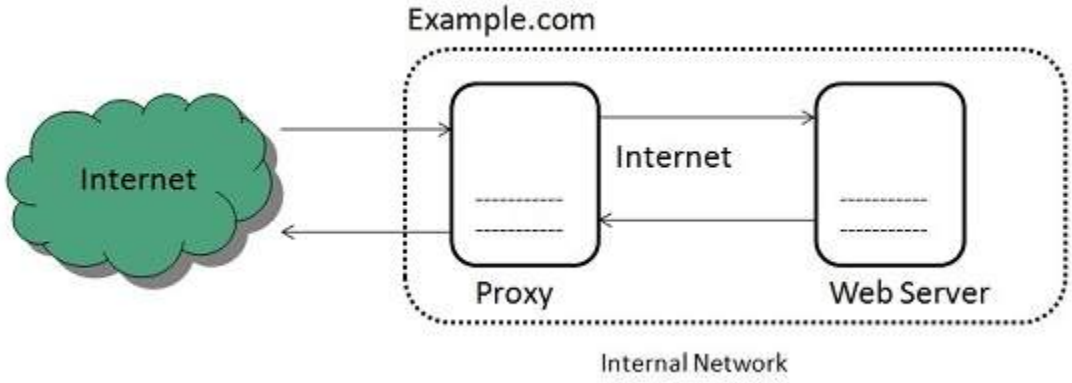
1. Forward Proxies: In this the client requests its internal network server to forward to the internet.



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



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:

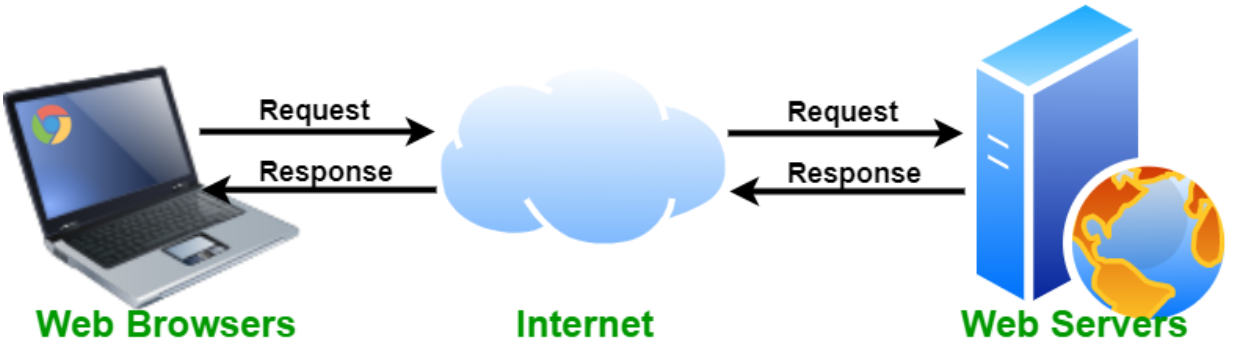
Web server can refer to either the hardware (the computer) or the software (the computer application) that helps to deliver Web content that can be accessed through the Internet. The most common use of web servers is to host websites, but there are other uses such as gaming, data storage or running enterprise 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 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



ƏG

Key Points:

- When client sends request for a web page, the web server search for the requested page if requested page is found then it will send it to client with an HTTP response.
- If the requested web page is not found, web server will the send an HTTP response: Error 404 Not found.
- If client has requested for 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 email.

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."

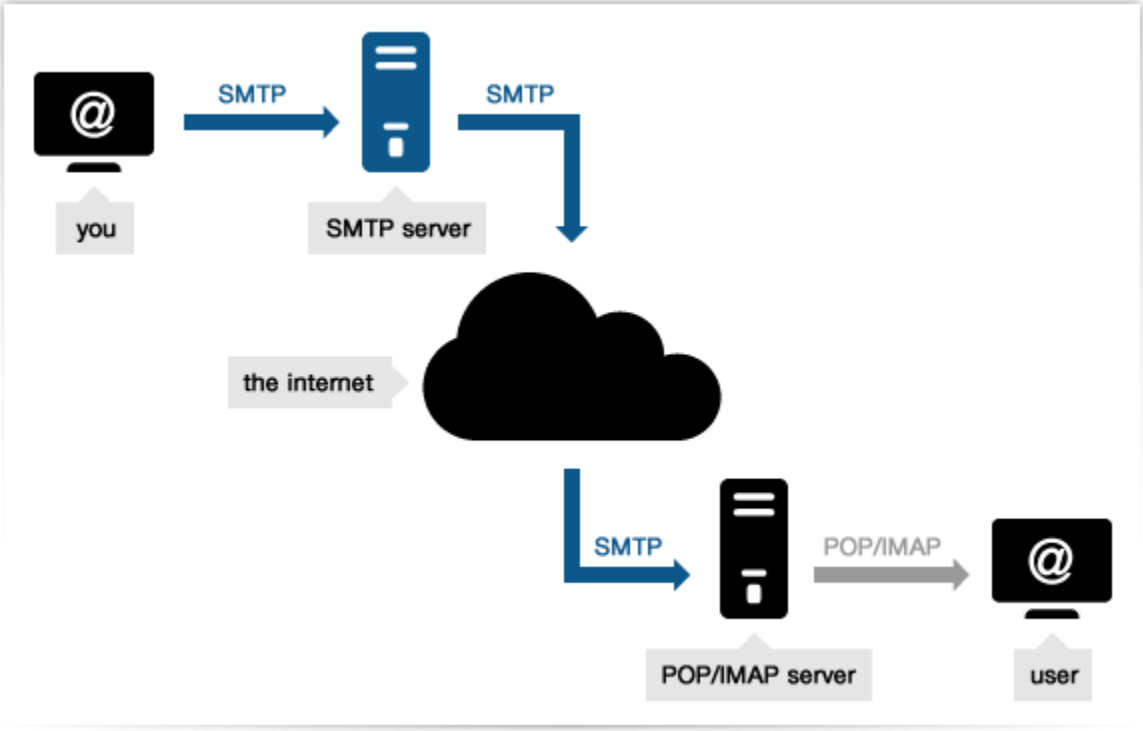
Mail servers send and receive email using standard email protocols. For example, the SMTP protocol sends messages and handles outgoing mail requests. The IMAP and POP3 protocols receive messages and are used to process incoming mail. When you log on to a mail server using a webmail interface or email 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 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.
    - POP3, or Post Office Protocol version 3, servers are best known for storing sent and received messages on PCs' local hard drives.
    - 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

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 the predefined quality of service for users.

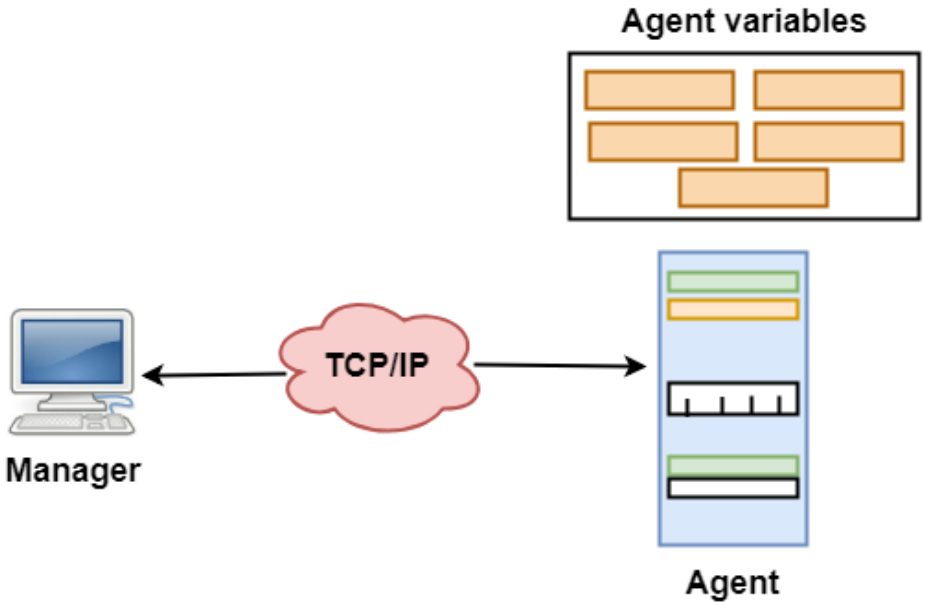
Network Management Functions:

- **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.

- **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, network adaptation belongs to this category.
- **Security management** includes administrative functions such as authenticating users and setting attributes such as read and write permissions on a per-user basis

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.



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 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 a 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 manage.