Computer Network and Data Communication

UNIT 7
Application Layer

Rajan Sharma

Course Outline

7. Application Layer **[5 Hrs]**

7.1. Using & Accessing Network: DNS, DHCP, HTTP, HTTPS

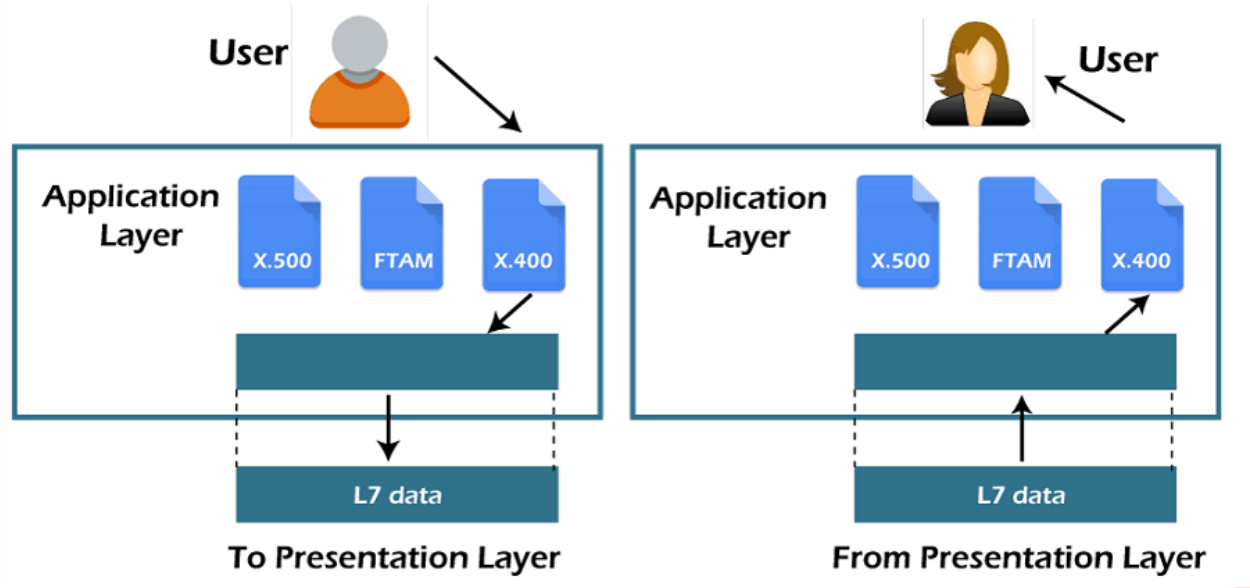
7.2. Email: SMTP, IMAP, POP3

7.3. File Transfer: FTP, FTPS, SFTP

7.4. Network Management & Traffic Analyzer: SNMP, Packet Tracer, Wireshark

7.5. Proxy, Reverse Proxy, Webmail

Application Layer

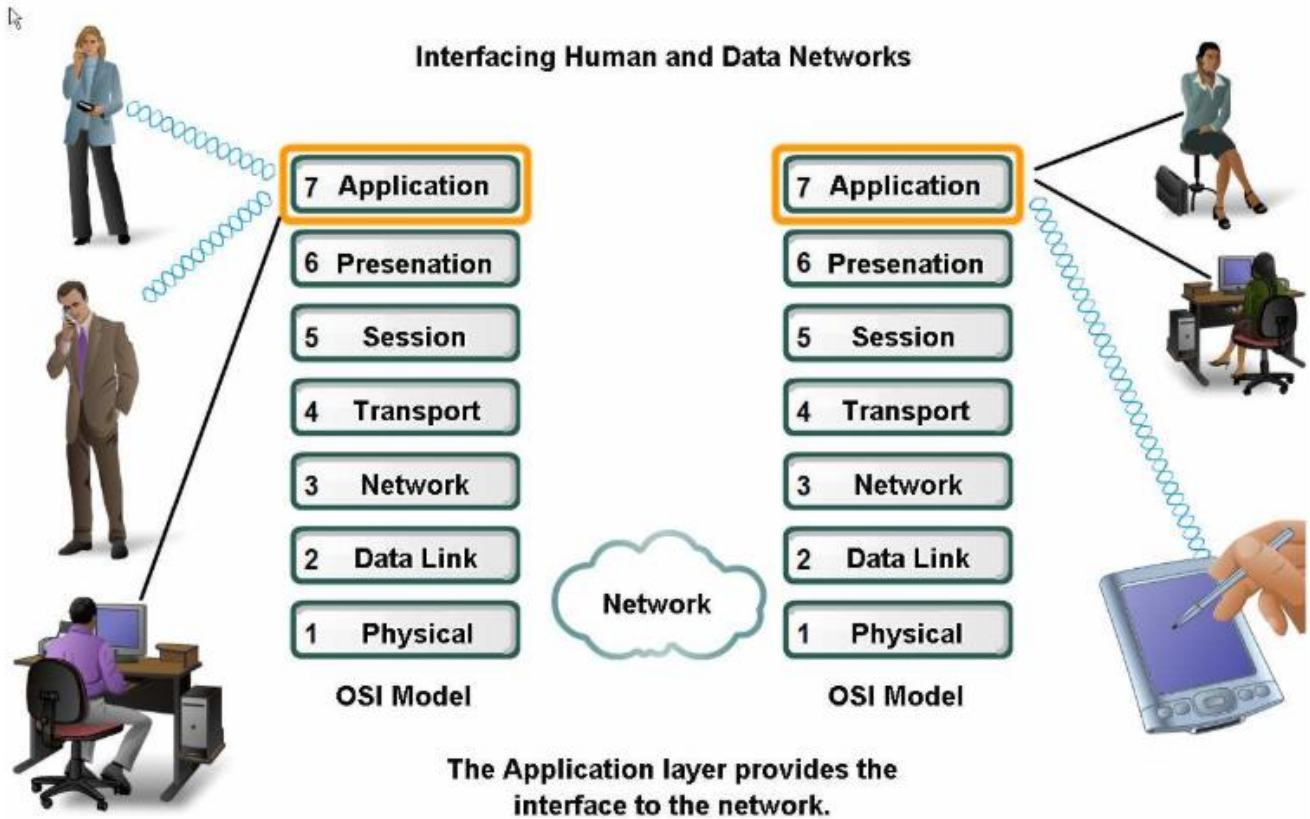


- An application layer serves as a window for users and application processes to access network service.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.

Application Layer

Applications – The Interface Between Human and Data Networks

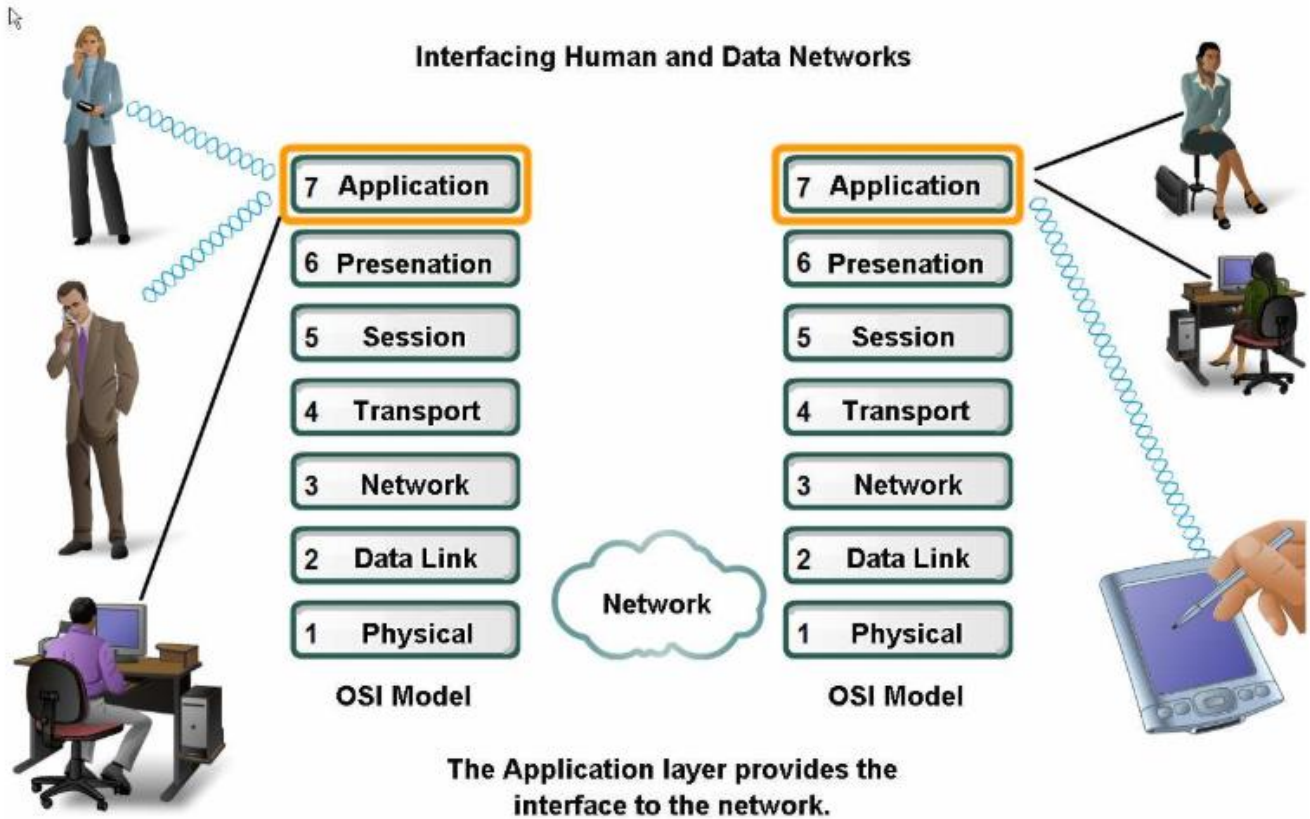
- Applications provide the means for generating and receiving data that can be transported on the network



Application Layer

Applications – The Interface Between Human and Data Networks

- Applications provide the means for generating and receiving data that can be transported on the network



Function of Transport Layer

- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.
- **Directory services**: An application provides the distributed database sources and is used to provide that global information about various objects.
- **Identifying communication partners:** The application layer identifies the availability of communication partners for an application with data to transmit.
- **Determining resource availability:** The application layer determines whether sufficient network resources are available for the requested communication.
- **Synchronizing communication:** All the communications occur between the applications requires cooperation which is managed by an application layer.
- This layer lets users log into a remote host and access any type of application.

Protocols operating at Application Layer

TCP/IP Application layer protocols

- These protocols specify the format and control information necessary for many of the common Internet communication functions. Among these TCP/IP protocols are:

- Domain Name Service Protocol (DNS) is used to resolve Internet names to IP addresses.
- Hypertext Transfer Protocol (HTTP) is used to transfer files that make up the Web pages of the World Wide Web.
- Simple Mail Transfer Protocol (SMTP) is used for the transfer of mail messages and attachments.
- Telnet, a terminal emulation protocol, is used to provide remote access to servers and networking devices. (SSH)
- File Transfer Protocol (FTP) is used for interactive file transfer between systems.

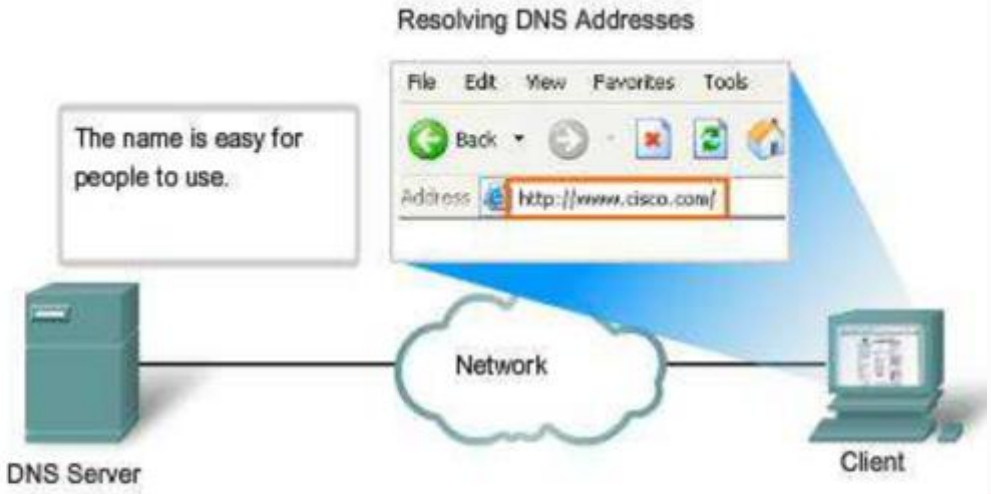
DNS

- DNS (Domain Name System) is a hierarchical distributed naming system used to translate human-readable domain names (e.g., www.example.com) into numerical IP addresses (e.g., 192.0.2.1) required for locating and identifying computer services and devices on the internet or private networks.

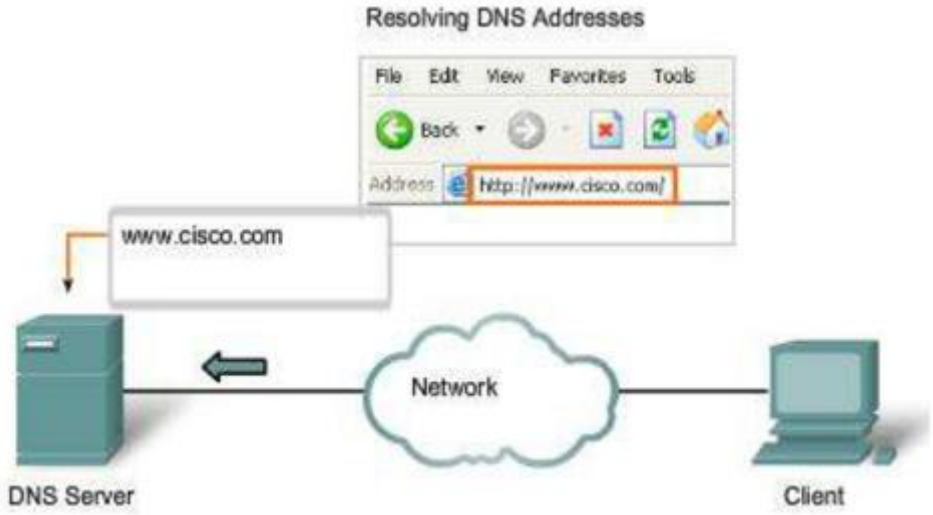
Working of DNS

1. **Domain Name Resolution:**

   - When a user enters a domain name into a web browser or other application, the DNS resolver on the user's device initiates a DNS query to resolve the domain name to an IP address.



   - The DNS resolver first checks its local cache to see if the domain name and corresponding IP address are already stored. If not, it proceeds with the DNS resolution process.



Working of DNS

DNS Hierarchy:

- DNS operates in a hierarchical structure consisting of multiple levels, including the root domain, top-level domains (TLDs), second-level domains, and subdomains each managed by a DNS server.

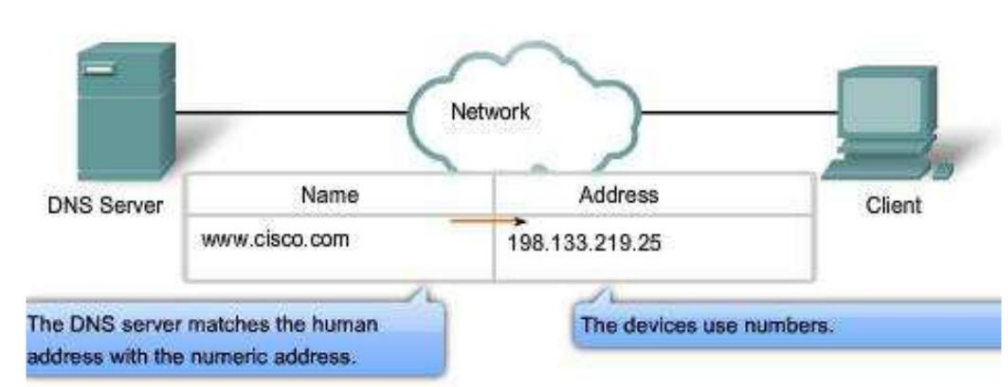
DNS Servers:

- DNS servers are categorized into different types:
  - **Root DNS Servers:** Managed by the Internet Assigned Numbers Authority (IANA), they provide information about the authoritative name servers for TLDs.
  - **Top-Level Domain (TLD) DNS Servers:** Manage domain names within specific TLDs (e.g., .com, .org, .net).
  - **Authoritative DNS Servers:** Managed by domain owners or DNS hosting providers, they hold the authoritative information for specific domain names.
  - **Recursive DNS Servers:** Also known as DNS resolvers, they recursively query other DNS servers until they obtain the IP address associated with the requested domain name.

Working of DNS

2.DNS Resolution Process:

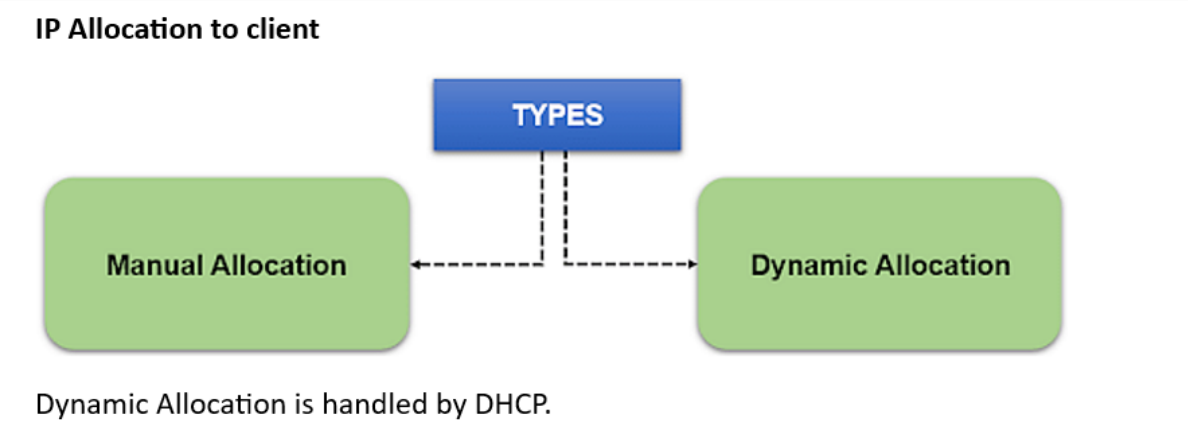
- If the domain name is not found in the local cache, the DNS resolver sends a query to a recursive DNS server, typically operated by the user's ISP or configured in the network settings.
- The recursive DNS server queries the root DNS servers to obtain the IP addresses of the authoritative name servers for the relevant TLD.
- The recursive DNS server then queries the TLD DNS servers to obtain the IP addresses of the authoritative name servers for the requested domain.
- Finally, the recursive DNS server queries the authoritative name servers for the domain to obtain the IP address associated with the requested domain name.
- Once the IP address is obtained, it is returned to the DNS resolver, which caches the result for future use and forwards it to the requesting application.



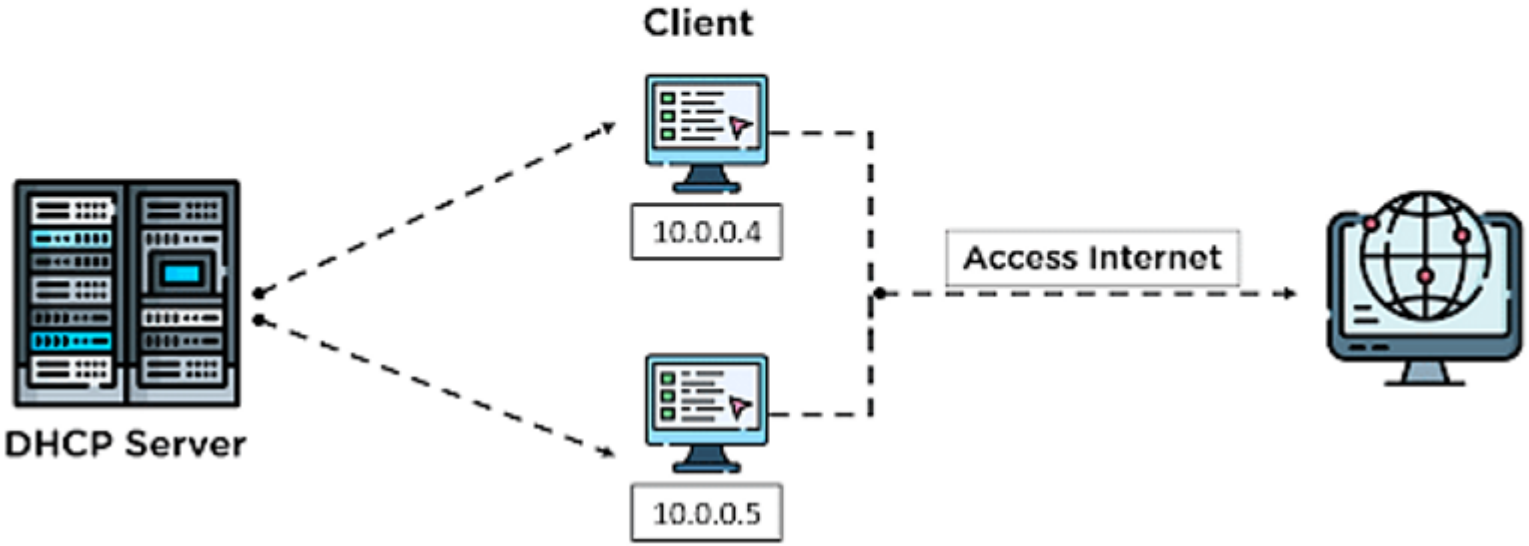
Benefits of DNS

- **Human-Readable Names:** DNS provides a user-friendly naming system that allows users to access websites and services using easily memorable domain names instead of numerical IP addresses.
- **Scalability:** DNS is highly scalable, allowing for efficient resolution of millions of domain names to IP addresses across the internet.
- **Global Reach:** DNS facilitates global communication by providing a unified naming system that enables devices and services to be accessed from anywhere on the internet.

DHCP



- DHCP (Dynamic Host Configuration Protocol) is a network administration protocol that is responsible for the task of assigning an IP address to your system and network device.
- The DHCP network model is based on the client-server architecture, where the connection is established when the client device sends a request message to the server device for providing the system with an IP address.



Working of DHCP

1. The first step is when the client broadcasts the DHCPDISCOVER message over the network channel to establish a network connection with the DHCP server. This message indicates that the client device wants to connect to the internet through the DHCP server.

Working of DHCP

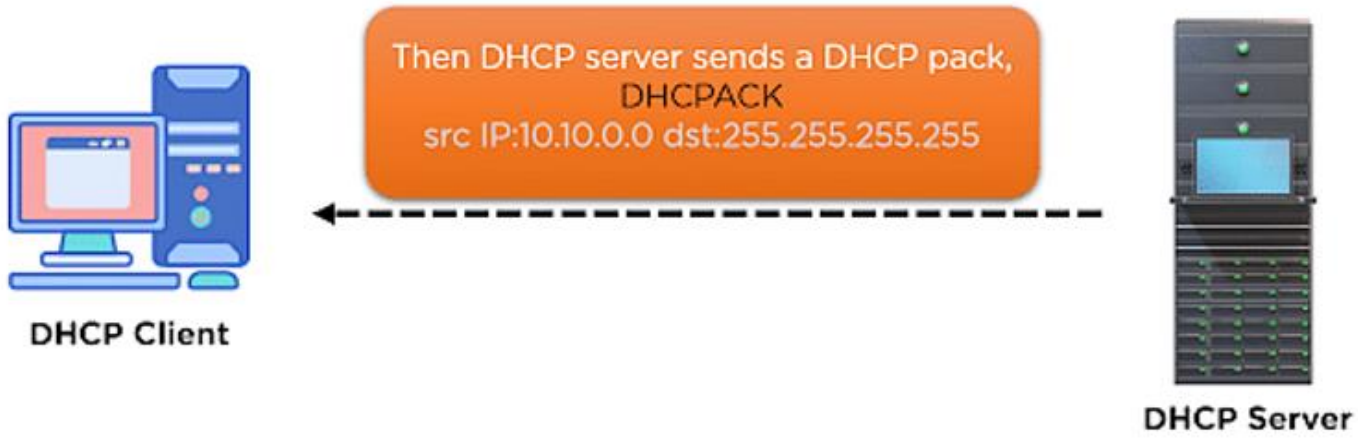
2. The second step is when the DHCP server receives the DHCPDISCOVER message. According to the message, the DHCP server reserves an IP address for the connecting client and other network configuration settings, including subnet-mask default gateway, preferred DNS server, and shares it with the client device through the **DHCPOFFER** message.

Working of DHCP

3. In the third step, the client responds to the DHCP server's DHCPOFFER through a **DHCPREQUEST** message requesting the offered IP address and relevant network configuration sent by the DHCP server for the system.

Working of DHCP

4. In the last step, the server acknowledges the DHCPREQUEST broadcast from the client device and sends the **DHCPACK** packet to the DHCP client, which comprises the required network configuration for the client device



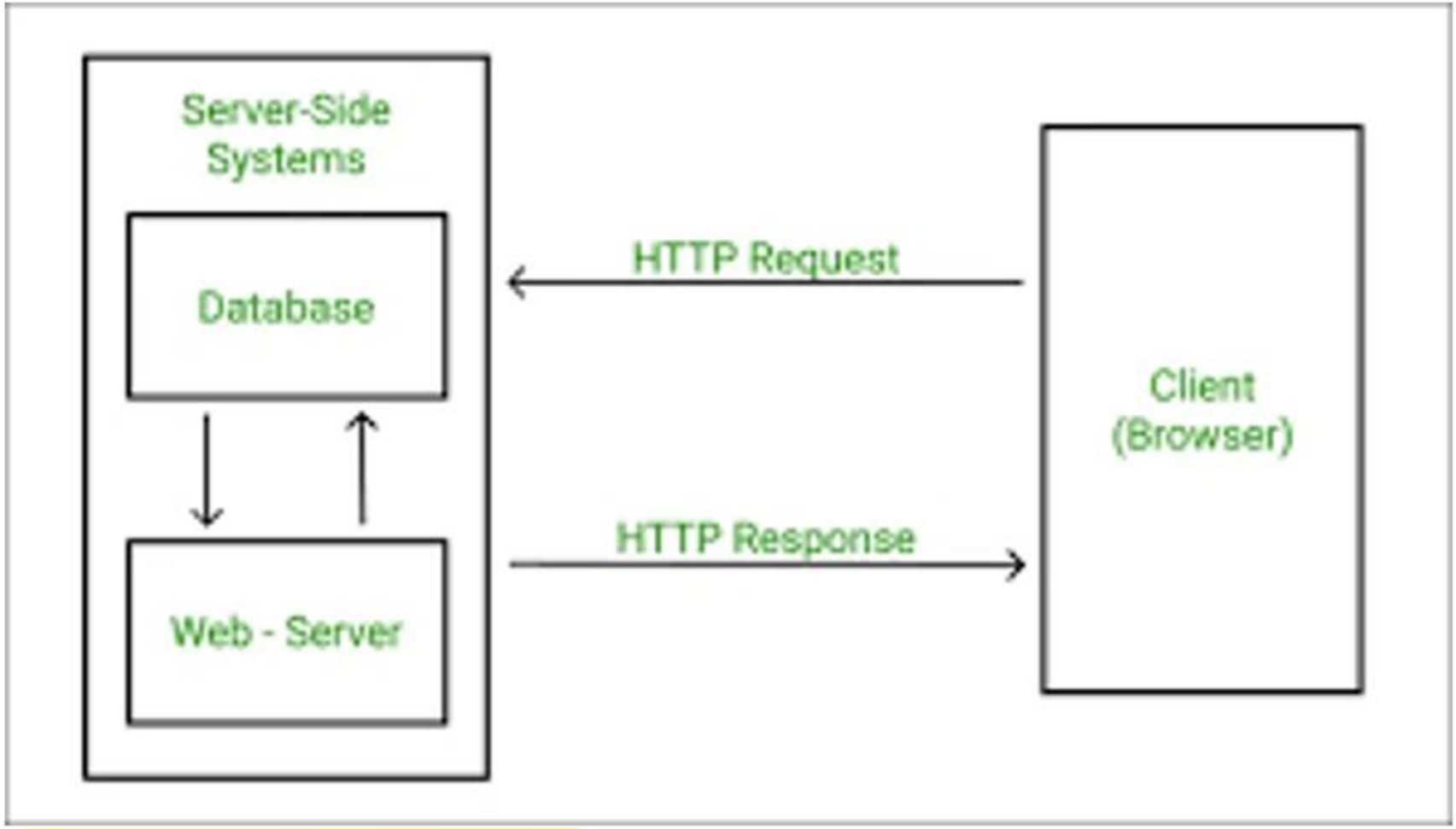
HTTP

- An HTTP stands for Hypertext Transfer Protocol.
- HTTP (Hypertext Transfer Protocol) is an application-layer protocol used for transmitting hypermedia documents, such as HTML files, over the internet.
- It defines the rules and standards for communication between web clients (such as web browsers) and web servers
- When the user makes an HTTP request on the browser, then the webserver sends the requested data to the user in the form of web pages.
- In short, we can say that the HTTP protocol allows us to transfer the data from the server to the client.

HTTP

Client-Server Model:

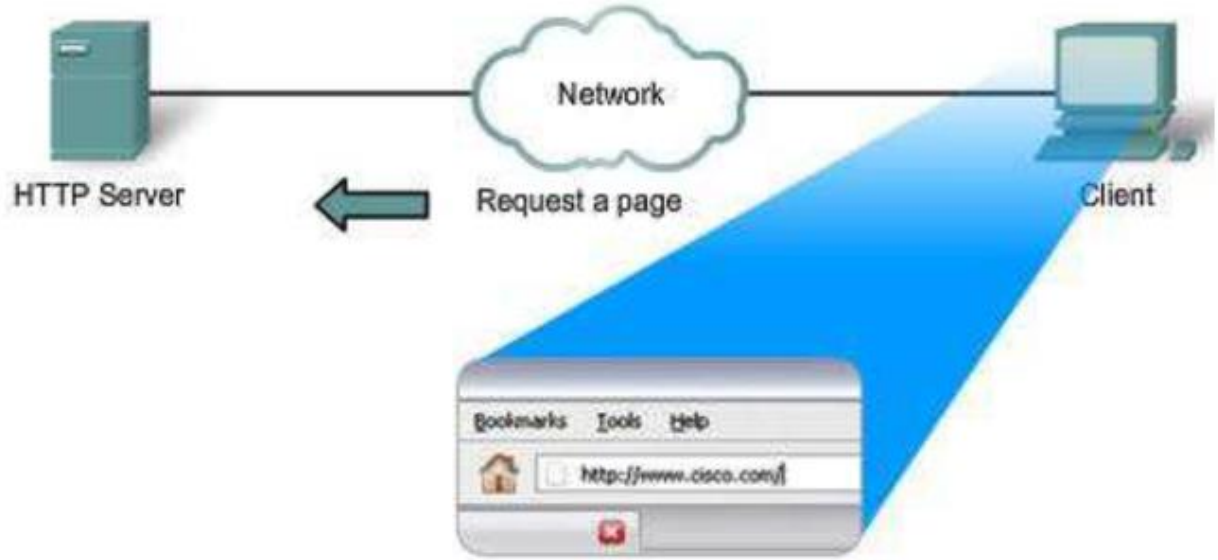
- HTTP operates on a client-server model, where a client (typically a web browser) sends requests to a server (typically a web server) and receives responses in return.



Working of HTTP

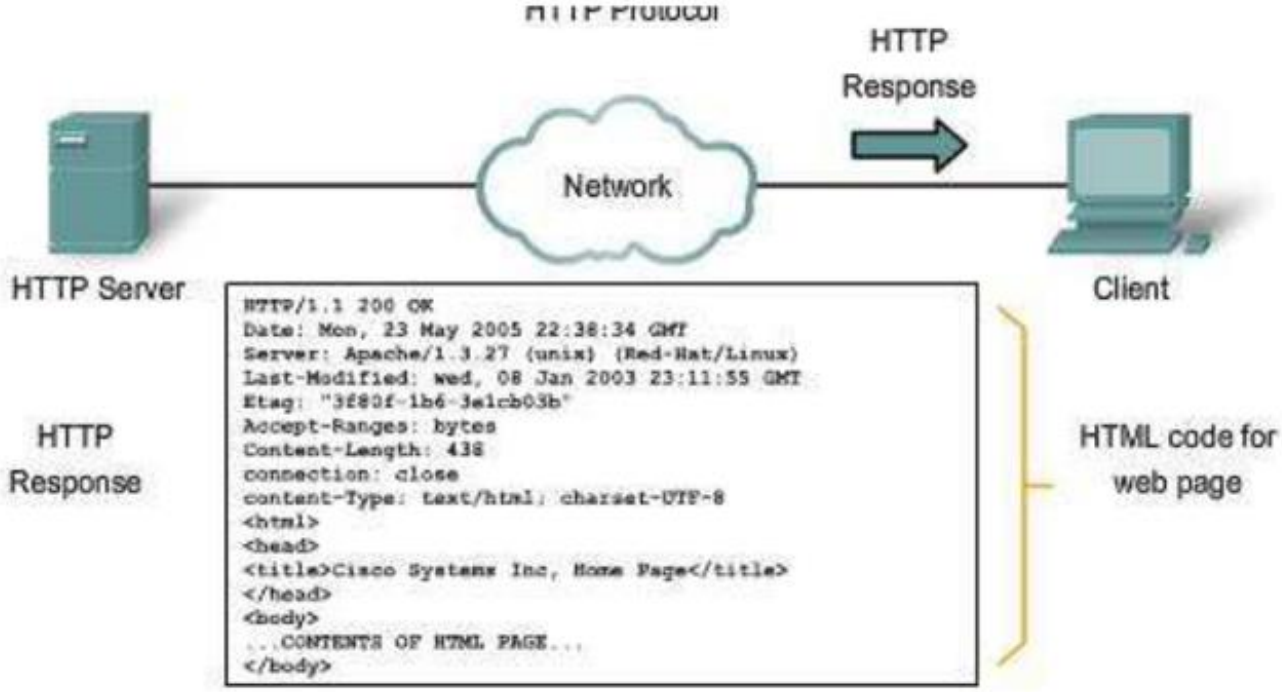
Request-Response Cycle:

- A typical HTTP transaction involves a request-response cycle:
    - **Request:** The client sends an HTTP request to the server, specifying the desired action (e.g., GET to retrieve a resource, POST to submit data).



Working of HTTP

- **Response:** The server processes the request and sends back an HTTP response, which includes a status code indicating the outcome of the request (e.g., 200 for success, 404 for not found) and optionally, the requested data.



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

HTTPS

- The full form of HTTPS is Hypertext Transfer Protocol Secure.
- The HTTP protocol does not provide the security of the data, while HTTP ensures the security of the data.
- Therefore, we can say that HTTPS is a secure version of the HTTP protocol.
- This protocol allows transferring the data in an encrypted form.
- The use of HTTPS protocol is mainly required where we need to enter the bank account details.
- The HTTPS protocol is mainly used where we require to enter the login credentials.
- In modern browsers such as chrome, both the protocols, i.e., HTTP and HTTPS, are marked differently.
- To provide encryption, HTTPS uses an encryption protocol known as Transport Layer Security, and officially, it is referred to as a Secure Sockets Layer (SSL).

Working of HTTPS

1. **SSL/TLS Encryption:**
   - HTTPS uses SSL (Secure Sockets Layer) or its successor, TLS (Transport Layer Security), to encrypt data exchanged between the client and server.
   - Once the connection is established, data transmitted between the client and server is encrypted using symmetric encryption keys negotiated during the SSL/TLS handshake.
2. **Secure Data Transmission:**
   - With HTTPS, all data transmitted between the client and server is encrypted, including HTTP headers, request/response bodies, and any other payload.
   - This encryption prevents eavesdropping, interception, and tampering of sensitive information, such as login credentials, personal data, and financial transactions.

Working of HTTPS

3. Authentication:

- HTTPS provides server authentication, ensuring that the client is communicating with the intended server and not an impostor.
- Digital certificates, issued by trusted Certificate Authorities (CAs), validate the identity of the server and provide assurance to the client that they are connecting to a legitimate website.

4. Data Integrity:

- HTTPS ensures data integrity by using cryptographic hash functions to verify that data has not been altered or corrupted during transmission.
- Any attempt to tamper with the encrypted data would result in a mismatch between the hash values, triggering an error and preventing the client from accepting the modified data.

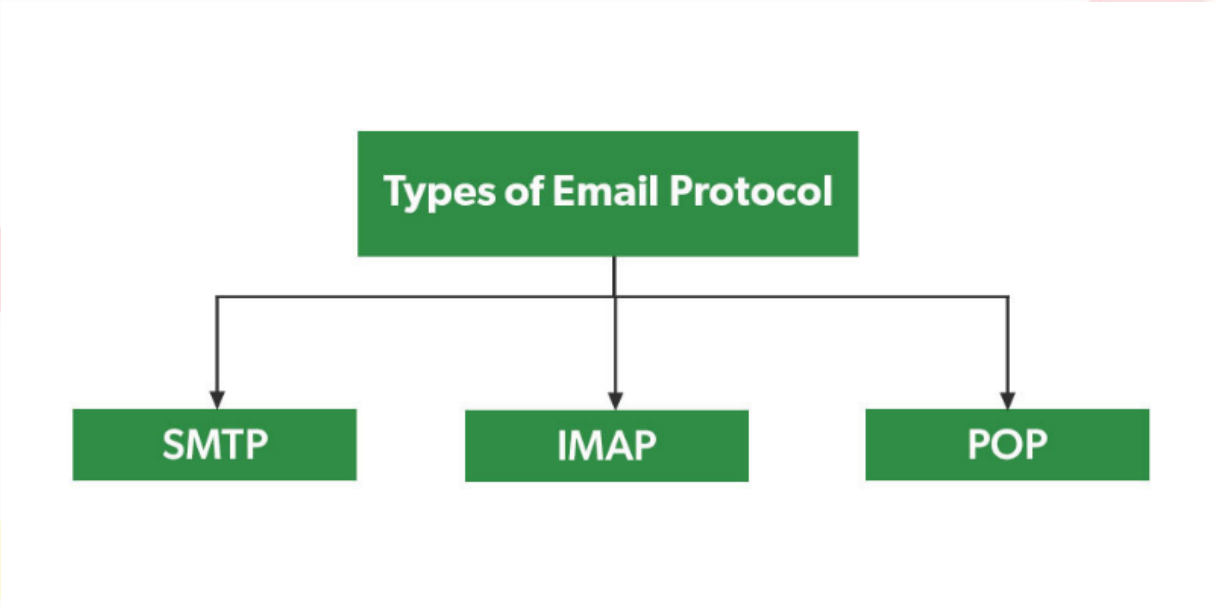
5. Port 443:

- HTTPS typically uses port 443 for communication, whereas HTTP uses port 80. This port separation allows web servers to distinguish between HTTP and HTTPS traffic and enforce security policies accordingly.

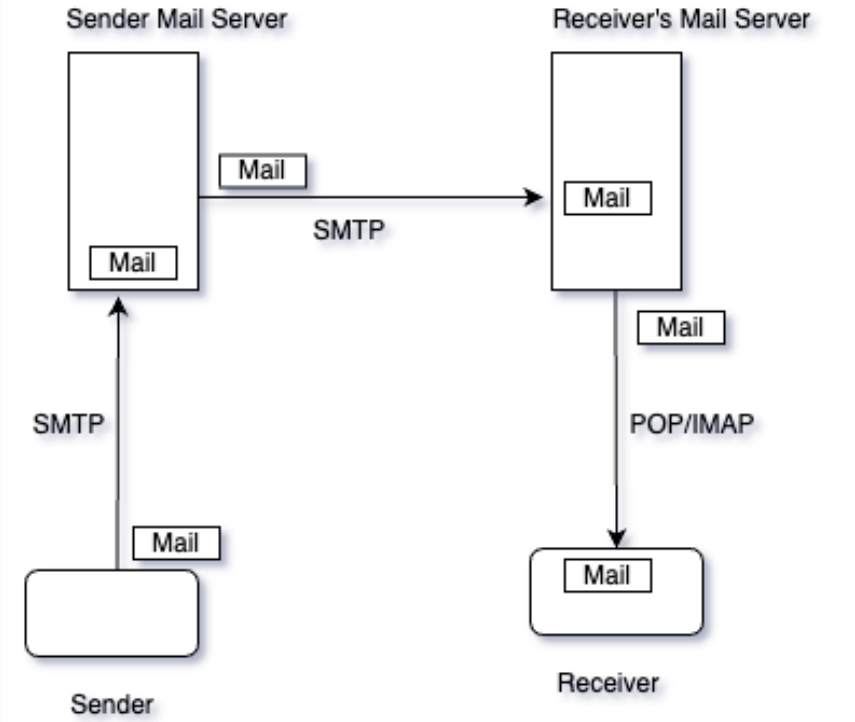
HTTP	HTTPS
The full form of HTTP is the Hypertext Transfer Protocol.	The full form of HTTPS is Hypertext Transfer Protocol Secure.
It is written in the address bar as http://.	It is written in the address bar as https://.
The HTTP transmits the data over port number 80.	The HTTPS transmits the data over port number 443.
It is unsecured as the plain text is sent, which can be accessible by the hackers.	It is secure as it sends the encrypted data which hackers cannot understand.
It is mainly used for those websites that provide information like blog writing.	It is a secure protocol, so it is used for those websites that require to transmit the bank account details or credit card numbers.
It is an application layer protocol.	It is a transport layer protocol.
It does not use SSL.	It uses SSL that provides the encryption of the data.
Google does not give the preference to the HTTP websites.	Google gives preferences to the HTTPS as HTTPS websites are secure websites.
The page loading speed is fast.	The page loading speed is slow as compared to HTTP because of the additional feature that it supports,

Email: SMPT, IMAP, POP3

- Email protocols are a collection of protocols that are used to send and receive emails properly.
- The email protocols provide the ability for the client to transmit the mail to or from the intended mail server.
- Email protocols establish communication between the sender and receiver for the transmission of email.
- There are three basic types of email protocols.



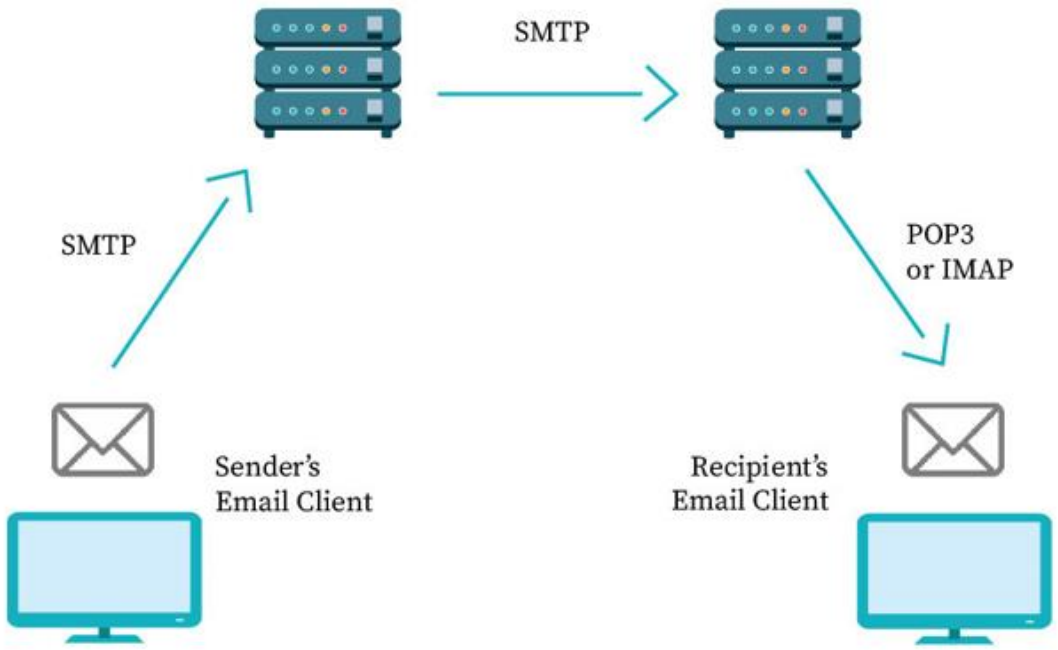
Email: SMPT, IMAP, POP3



- Simple Mail Transfer Protocol or SMTP is the only protocol used for sending emails. SMPT deals with outgoing messages, while two protocols take care of incoming emails.

SMPT

- **SMTP stands for Simple Mail Transfer Protocol**, and it is responsible for sending email messages. This protocol is used by email clients and mail servers to exchange emails between computers.



- A mail client and the SMTP server communicate with each other over a connection established through a particular email port. Both entities are using SMTP commands and replies to process your outgoing emails.

SMTP establishes how the message gets from the sender to the email server. Also, it is used by a mail transfer agent (MTA) to deliver emails between servers.

Working of SMPT

- An SMTP connection begins once you write your email and hit the send button.
- Your email client (a website or app you use to access your emails) will send a request to a mail server and let them know that it wants to establish a connection.
- Then the mail server has to verify the identity of the sender. If that's successful, the server will agree to start the connection
- Once the connection is established, the client will slowly transmit all the data included in the email
- When every component is transmitted, the client will request to terminate the connection.

Working of SMPT

- The communication between the client and the server is conducted using text commands such as HELO, QUIT, DATA, etc.
- SMTP workflow consists of commands sent by the SMTP client and corresponding replies by the SMTP server.
- Default SMTP commands are text-based, such as HELO, MAIL FROM, and others.

Any SMTP conversation consists of three stages:

- **SMTP handshake** – The SMTP client establishes a TCP connection with the SMTP server. Once the server replies with 250, the handshaking starts. The stage ends when the server confirms the recipient's address.
- **Email transfer** – Code 354, as a response to the DATA command, launches the transfer of the email. Once the server gets a final dot, the message is transferred.
- **Termination** – Client and server say goodbye to each other using the command QUIT and code 221, respectively.

POP3

- The POP3 -**Post Office Protocol version 3**, provides access to an inbox stored in an email server.
- Post Office Protocol is used to retrieve email
- POP3 version is the current version of POP used.
- It executes the download and deletes operations for mail.
- Thus, when a POP3 client connects to the mail server, it retrieves all messages from the mailbox. Then it stores them on your local computer and deletes them from the remote server.
- POP3 protocol downloads emails from the server to the local computer, so you can read them even offline.
- The server deletes messages once they are retrieved.
- Modern POP3 clients allow you to keep a copy of your messages on the server if you explicitly select this option.

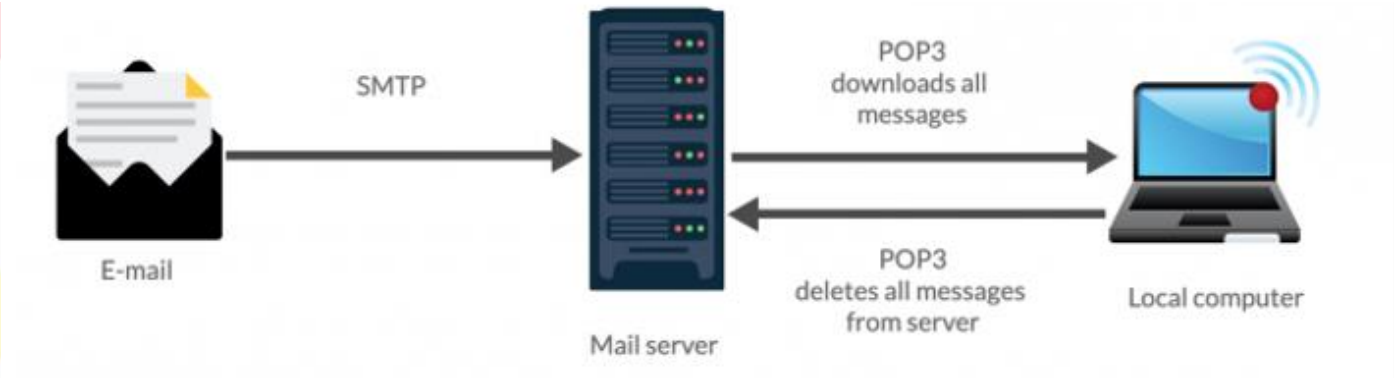
Working of POP3

How POP3 works

- When the client connects to the mail server. The connection is established through TCP port 110. The client authenticates itself by sending username and password information.
- After successful authentication, all new messages stored on the server will be downloaded according to the rules determined by the POP3 protocol.
- When all the messages are retrieved, they get deleted from the server at the end of the session.

POP3 connection consists of four steps:

- The client **connects to the server** (AUTHORIZATION State)
- The client **retrieves new emails** (TRANSACTION State)
- The server **deletes the stored messages** (UPDATE State)
- The client **disconnects from the server**



IMAP

- **The Internet Message Access Protocol (IMAP) allows you to access and manage your email messages on the email server.**

- IMAP stores emails on a remote server and downloads them on demand when the recipient opens them.

- So, the IMAP protocol gets access to the email from any device or location if authorized. This allows for email synchronization, which is why IMAP is the go-to option for most email service providers.

- This protocol permits you to manipulate folders, permanently delete and efficiently search through messages.

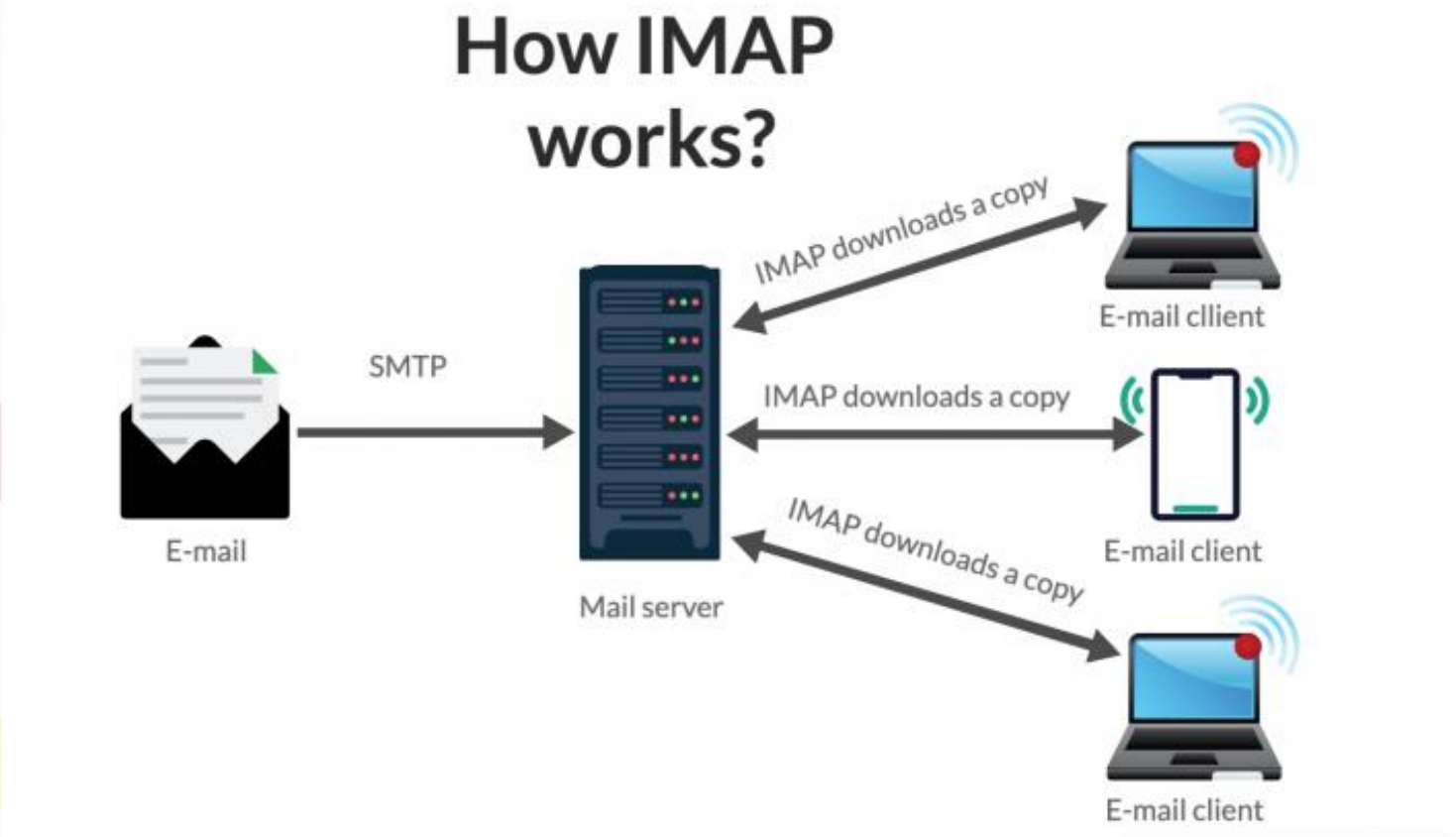
- By default, all messages remain on the server until the user specifically deletes them.

Working of IMAP

How IMAP works

Here is the basic flow of the IMAP client/server interaction:

- A recipient's mail client connects to the server the message is stored on
- The recipient can see the message headers of all the emails on the server
- If the recipient chooses a particular message to read, IMAP downloads it on demand



Comparison Between SMTP vs POP vs IMAP

SMTP	POP	IMAP
Stands for Simple mail transfer protocol	Stands for Post Office Protocol.	Stands for Internet Message Access Protocol.
Used for sending mail.	Used for retrieving mail.	Used for retrieving mail.
it is push protocol.	it is pull protocol.	it is pull protocol.
It work between sender's mail server to receiver's mail server and sender and sender's mail server.	It work between receiver and receiver's mail server.	It works between receiver and receiver's mail server.
It does not store mail on server it just send the mail.	It download all the mail when it connected to internet.	It store all mail on server and download when it get request to download.
Works on TCP port number 25.	Works on TCP port number 110.	Works on TCP port number 143.
Connection oriented protocol.	Connection oriented protocol.	Connection oriented protocol.
It has persistence TCP connection.	It has persistence TCP connection.	It has persistence TCP connection.
Stateless protocol.	Stateful protocol.	Stateful protocol.
It is in band protocol.	It is in band protocol.	It is in band protocol.
Not used at receiver side.	Used at receiver side.	Used at receiver side.

File Transfer: FTP, FTPS, SFTP

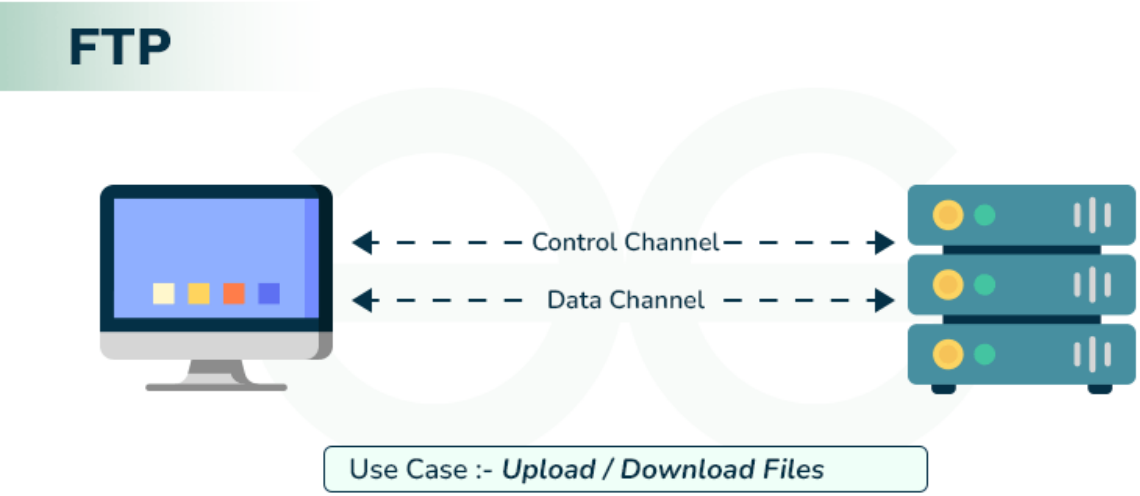
- File transfer refers to the process of transmitting data files from one computer system to another over a network.
- It enables users to share files, documents, multimedia, and other types of data between devices, regardless of their physical location.
- File transfer can be achieved using various protocols and methods, each offering different features, security levels, and performance characteristics.

FTP

- 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 also used for downloading the files from other servers.

- **Objectives of FTP**

- It provides the sharing of files.
- It transfers the data more reliably and efficiently.

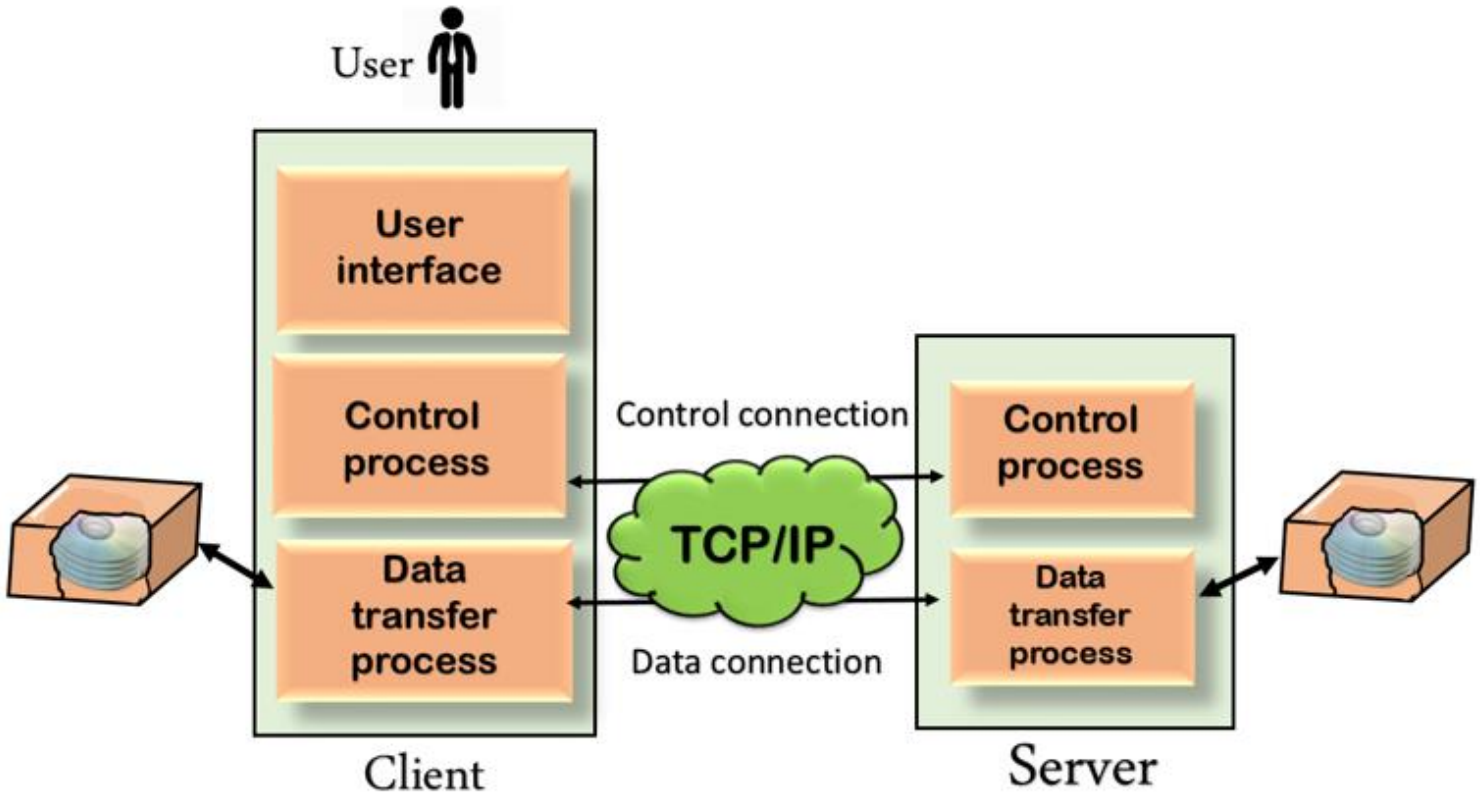


FTP

- **Why FTP is needed ?**
- Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems.
- For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures.
- FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

Working of FTP

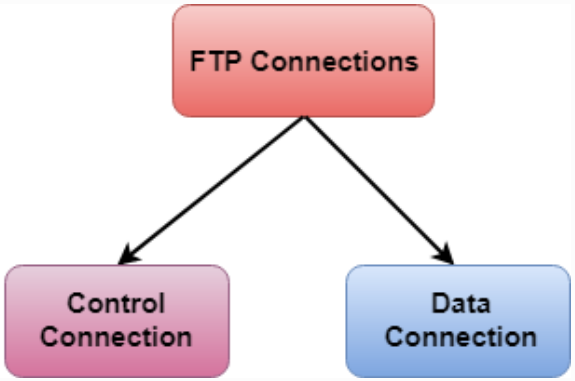
Mechanism of FTP



The above figure shows the basic model of the FTP. The FTP client has three components: the user interface, control process, and data transfer process. The server has two components: the server control process and the server data transfer process.

Working of FTP

- **There are two types of connections in FTP:**



  - **Control Connection:** The control connection uses very simple rules for communication. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.
  - **Data Connection:** The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

Advantages of FTP

- **Speed:** The FTP is one of the fastest way to transfer the files from one computer to another computer.
- **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.
- **Security:** To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.
- **Back & forth movement:** FTP allows us to transfer the files back and forth.

Types of FTP

There are different ways through which a server and a client do a file transfer using FTP. Some of them are mentioned below:

- **Anonymous FTP.** This is the most basic form of FTP. It provides support for data transfers without encrypting data or using a username and password
- **Password Protected FTP:** This type of FTP is similar to the previous one, but the change in it is the use of username and password.
- **FTP Secure (FTPS):** It is also called as FTP Secure Sockets Layer (FTP SSL). It is a more secure version of FTP data transfer. Whenever FTP connection is established, Transport Layer Security (TLS) is enabled.
- **Secure FTP (SFTP):** SFTP is not a FTP Protocol, but it is a subset of Secure Shell Protocol, as it works on port 22.

FTPS

- FTPS is known as FTP SSL which refers to File Transfer Protocol (FTP) over Secure Sockets Layer (SSL) which is more secure from FTP.
- FTPS also called as File Transfer Protocol Secure.
- It refers to basic FTP with security which protects data from any attack by encrypting it so that no one can be able to make use of any information in between transmission at both the ends.
- It implements AES algorithm, Triple DES algorithm, and many other algorithms to encrypt data.
- It enables secure file transfer between a client and server over a network

Working of FTPS

- **SSL/TLS Encryption:**
  - FTPS uses SSL (Secure Sockets Layer) or its successor, TLS (Transport Layer Security), to encrypt data exchanged between the client and server.
  - When establishing a connection, FTPS negotiates SSL/TLS encryption between the client and server to create a secure communication channel.
- **Authentication:**
  - FTPS supports various authentication methods, including username/password authentication and client certificate authentication.
  - Clients authenticate themselves to the server using credentials provided during the connection establishment process.
- **Control and Data Channels:**
  - Similar to FTP, FTPS uses two separate channels for communication: a control channel and a data channel.
  - The control channel is used for sending commands, such as file transfer commands.
  - The data channel is used for transferring actual file data between the client and server.

Benefits of FTPS

- **Data Security:** FTPS encrypts data in transit, protecting it from eavesdropping and interception by unauthorized parties.

- **Authentication:** FTPS supports various authentication methods, ensuring secure access control to the server.

- **Compatibility:** FTPS clients and servers are widely available for different platforms, making it suitable for interoperability between systems.

- **Flexibility:** FTPS can operate in Implicit or Explicit modes, allowing organizations to choose based on their security requirements.

SFTP

- SFTP known is known as SSH FTP which refers to File Transfer Protocol (FTP) over Secure Shell (SSH) which encrypts both commands and data while in transmission.
- SFTP also called as Secure File Transfer Protocol.
- SFTP is a secure file transfer protocol that provides encrypted communication between a client and server over a network.
- It is built on top of SSH (Secure Shell) protocol, leveraging SSH's encryption and authentication mechanisms to ensure secure data transmission.
- It works as an extension to SSH. It encrypts files and data then sends them over a secure shell data stream.
- This protocol allows to remotely connect to other systems and executing commands from the command line.
- Like FTPS it also implements AES algorithm, Triple DES algorithm, and many other algorithms to encrypt data.

Working of SFTP

- **SSH Encryption:**
  - SFTP uses SSH encryption to secure the communication between the client and server.
  - SSH provides encryption for both data and control channels, protecting the confidentiality and integrity of transmitted data.
- **Authentication:**
  - SFTP clients authenticate themselves to the server using SSH key pairs (public and private keys) or username/password credentials.
- **Port 22:**
  - SFTP operates over SSH, typically using port 22 for communication.
  - Since SSH is a single port protocol, SFTP connections can pass through firewalls and network address translation (NAT) devices easily

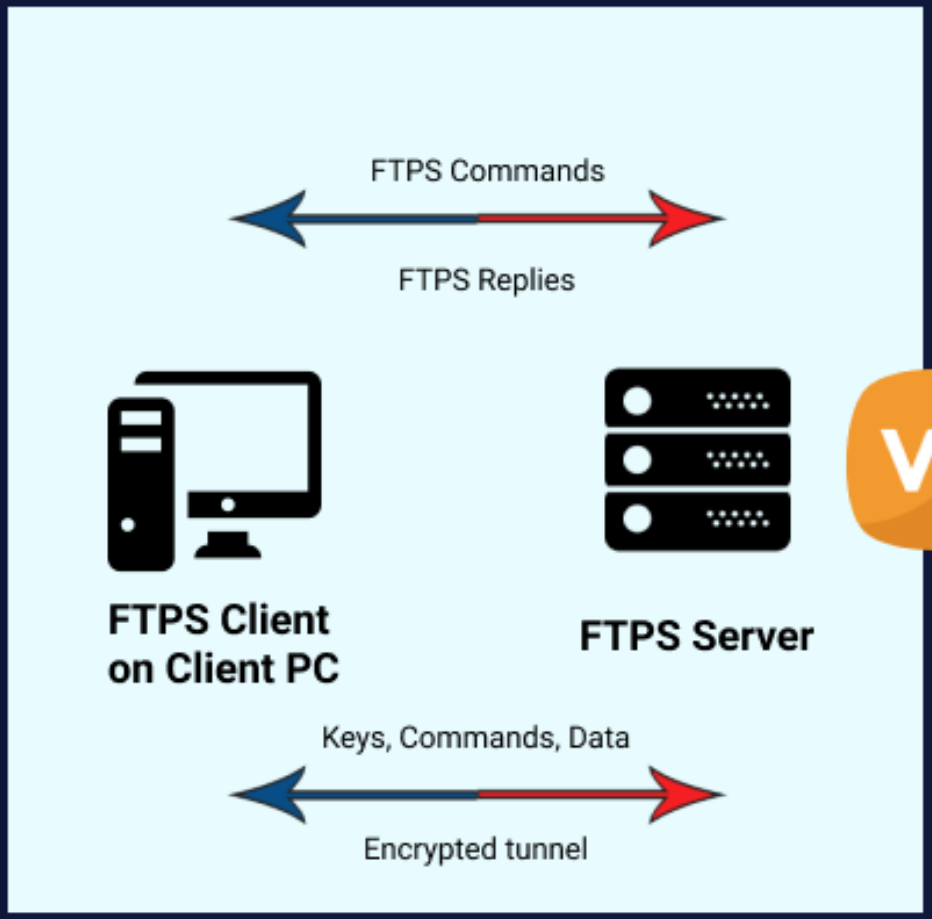
Working of SFTP

- **File Access and Permissions:**
  - SFTP supports various file operations, including file uploads, downloads, deletions, and directory listings.
  - File access and permissions are controlled by the server's filesystem permissions, ensuring that clients can only access authorized files and directories.
- **Error Handling and Status Codes:**
  - SFTP provides error handling mechanisms and status codes to inform clients about the outcome of file transfer operations.
  - Clients receive status codes indicating success, failure, or specific error conditions during file transfer operations.

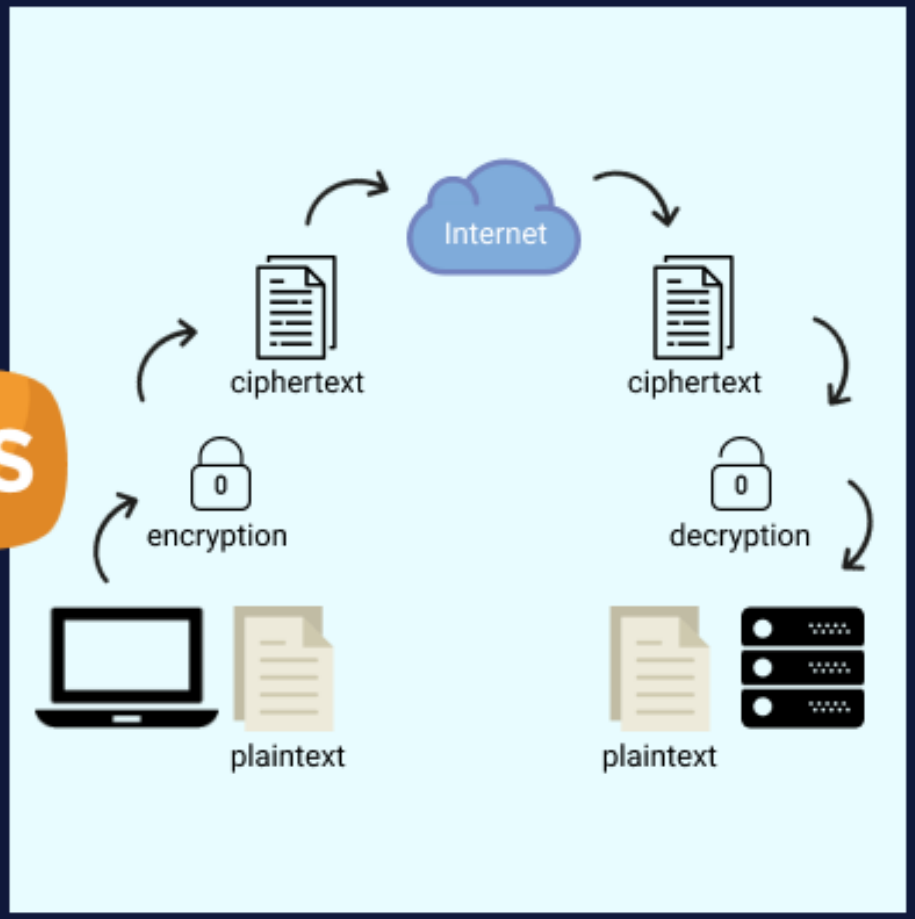
Benefits of SFTP

- **Security:** SFTP encrypts data in transit, protecting it from eavesdropping and interception by unauthorized parties.
- **Authentication:** SFTP supports robust authentication mechanisms, including public key authentication, ensuring secure access control to the server.
- **Data Integrity:** SFTP verifies data integrity using cryptographic hash functions, ensuring that transferred files remain intact and unaltered during transmission.
- **Platform Independence:** SFTP clients and servers are available for various operating systems.

FTPS vs SFTP



VS



FTPS vs. SFTP

	FTPS	SFTP
01.	FTPS refers to File Transfer Protocol with SSL.	SFTP refers to SSH File Transfer Protocol.
02	It is also known as File Transfer Protocol (FTP) over Secure Sockets Layer (SSL).	It is also known as File Transfer Protocol (FTP) over Secure Shell (SSH).
04.	Key based authentication is not supported.	SSH keys can be used to authenticate SFTP connections.
05.	In this certificates are supported.	In this certificates are not supported.
06.	It uses multiport numbers. Each time a file transfer request is made another port number needs to be opened for the data channel.	SFTP needs only a single port number for all SFTP communications and makes it easy to secure and provide greater protection.
07.	It is most commonly used due to its ubiquitous legacy.	But now a days it is more common in recent devices and software.
08.	Authentication is performed via x.509 certificates.	Authentication is performed via SSH keys.
09.	It has separate connection for command and file data.	It has no separate connection for command and file data.

Network Management and Traffic Analyzer

Network Management:

- Network management involves the administration, monitoring, and maintenance of computer networks to ensure their smooth operation and efficiency.
- It encompasses various tasks and processes aimed at managing network resources, diagnosing issues, and implementing solutions.

Components of Network Management

1. Configuration Management:

- Managing network configurations to ensure consistency and compliance with organizational policies.
- This includes **configuration backups, version control, and configuration auditing**.

2. Performance Monitoring:

- Continuously monitoring network performance metrics such as bandwidth utilization, latency, packet loss, and throughput

3. Fault Management:

- Detecting, isolating, and resolving network faults or failures to minimize downtime and maintain network availability.
- This involves proactive monitoring, fault detection algorithms, and automated alerting systems.

Components of Network Management

4.Security Management:

- Implementing security measures to protect network assets from unauthorized access, malware, and cyber threats.
- This includes access control, encryption, intrusion detection/prevention systems, and security policy enforcement.

5.Accounting and Billing:

- Tracking network resource usage for accounting and billing purposes.
- This involves monitoring user activity, data consumption, and service usage to ensure fair allocation of resources and billing accuracy.

6.Change Management:

- Managing changes to network infrastructure, configurations, and policies in a controlled and documented manner to minimize disruptions and maintain stability.

Traffic Analysis

Traffic analysis involves the examination and analysis of network traffic patterns, behaviors, and characteristics to gain insights into network performance, usage, and security.

It helps network administrators understand how traffic flows through the network, identify anomalies, and make informed decisions about network optimization and security enhancements

Components of Traffic Analysis

1. **Traffic Monitoring:**
   - Capturing and monitoring network traffic using packet sniffing tools, network probes, or monitoring software.
   - This includes analyzing traffic volumes, protocols, and sources/destinations.
2. **Traffic Profiling:**
   - Profiling network traffic to identify normal traffic patterns and behaviors.
   - This involves categorizing traffic by application, protocol, user, device, or other attributes
3. **Anomaly Detection:**
   - Detecting abnormal or suspicious network activity that may indicate security threats, performance issues, or policy violations.
   - This includes identifying anomalies such as unusual traffic spikes, protocol deviations, or unauthorized access attempts.

Components of Traffic Analysis

4. Bandwidth Management:

- Managing and optimizing bandwidth usage to ensure efficient resource allocation and QoS (Quality of Service).
- This involves prioritizing critical traffic, implementing traffic shaping/policing, and managing congestion

5. Forensic Analysis:

- Investigating security incidents or network breaches by analyzing historical traffic data.
- This includes reconstructing network events, identifying attack vectors, and gathering evidence for incident response and remediation.

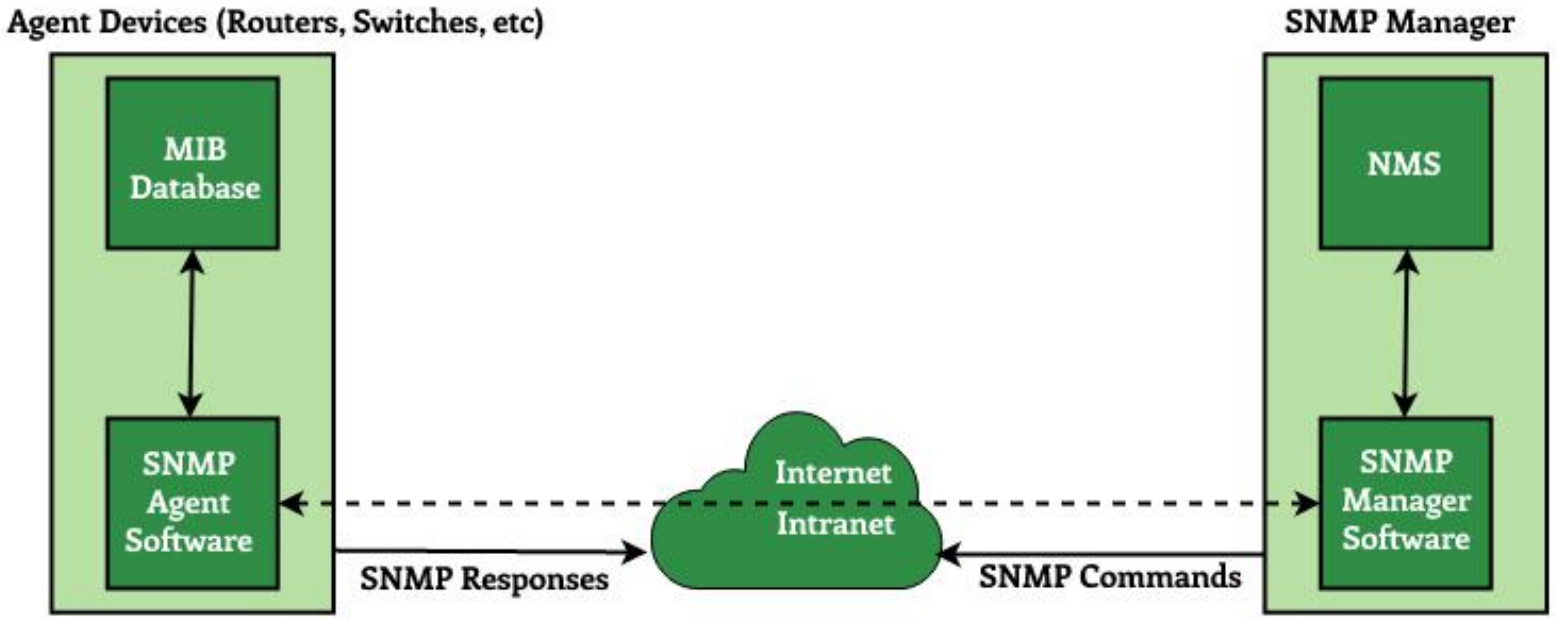
6. Capacity Planning:

- Planning and forecasting network capacity requirements based on traffic analysis data.
- This involves predicting future traffic growth, resource demands, and infrastructure upgrades to meet evolving business needs.

SNMP

- SNMP stands for **Simple Network Management Protocol**.
- SNMP is a framework used for managing devices on the internet.
- It provides a set of operations for monitoring and managing the internet.
- SNMP has major 3 components
  - **SNMP Manager**
  - **SNMP Agent**
  - **Management Information Base**

SNMP Architecture



Management with SNMP has three basic ideas:

- A manager checks the agent by requesting the information that reflects the behavior of the agent.
- A manager also forces the agent to perform a certain function by resetting values in the agent database.
- An agent also contributes to the management process by warning the manager regarding an unusual condition.

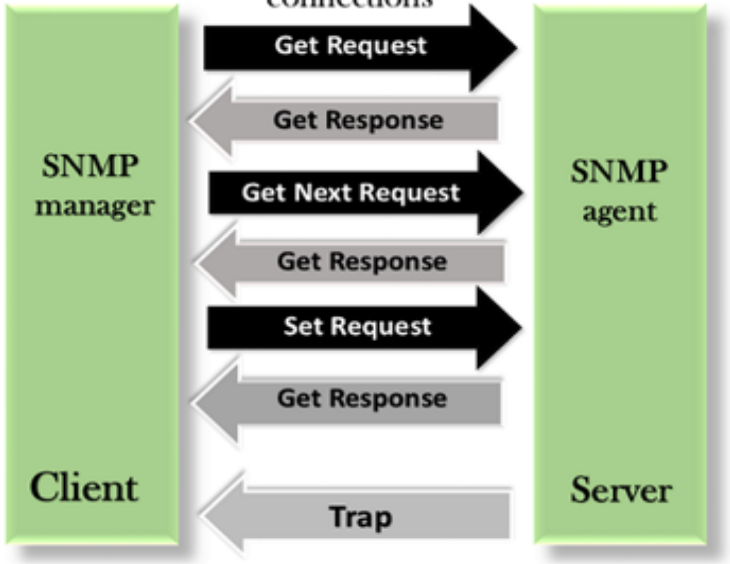
SNMP Architecture

Components of SNMP

There are mainly three components of SNMP:

1. **SNMP Manager**
    - It is a centralized system used to monitor the network. It is also known as a Network Management Station (NMS).
    - The manager is a host that controls and monitors a set of agents such as routers.
2. **SNMP agent**
    - It is a software management software module installed on a managed device.
    - A router that runs the SNMP server program is called an agent
3. **Management Information Base**
    - MIB consists of information on resources that are to be managed. This information is organized hierarchically.
    - It consists of objects instances which are essentially variables.
    - The manager accesses the values stored in the database, whereas the agent maintains the information in the database.

SNMP Messages



Get Request:

- The Get Request message is sent from a manager to the agent to retrieve the value of a variable.

Get Next Request:

- The Get Next Request message is sent from the manager to agent to retrieve the value of a variable. This type of message is used to retrieve the values of the entries in a table.

Get Response:

- The Get Response message is sent from an agent to the manager in response to the Get Request and Get Next Request message.

Set Request:

- The Set Request message is sent from a manager to the agent to set a value in a variable.

Trap:

- The Trap message is sent from an agent to the manager to report an event.
- For example, if the agent is rebooted, then it informs the manager as well as sends the time of rebooting.

Packet Tracer

- Packet Tracer is a network simulation and visualization tool developed by Cisco Systems.
- It is used for teaching, learning, and practicing networking concepts, protocols, and configurations in a virtual environment.

Features of Packet Tracer:

1. **Network Simulation:**
   - Packet Tracer simulates network devices, such as routers, switches, PCs, servers, and IoT devices,
2. **Device Interactions:**
   - Users can interact with simulated devices by configuring settings, connecting devices with cables, and running various network protocols and services.
3. **Protocols and Services:**
   - Packet Tracer supports a wide range of networking protocols and services, including TCP/IP, UDP, DHCP, DNS, HTTP, SSH, VLANs, OSPF, EIGRP, and more.

Packet Tracer

4.Packet Capture and Analysis:

- Users can capture and analyze network traffic within the simulated environment, helping to troubleshoot network issues, debug configurations, and understand protocol behaviors.

5. Activity Wizard:

- Packet Tracer includes an Activity Wizard that provides guided tutorials and interactive exercises for learning networking concepts and configurations step-by-step.

6. Assessment and Evaluation:

- Instructors can create assessments and evaluations using Packet Tracer to test students' understanding of networking concepts and configurations.

7. Device Customization:

- Users can customize device configurations, interfaces, and properties to simulate real-world network scenarios and deployments.

8. Real-Time Mode:

- Packet Tracer includes a real-time mode that allows users to observe network behaviors and packet transmissions in real time as they configure and interact with devices.

Uses of Packet Tracer

1. **Networking Education:**
   - Packet Tracer is widely used in academic institutions, vocational schools, and training centers for teaching networking courses
2. **Network Design and Testing:**
   - Engineers and network administrators use Packet Tracer to design, prototype, and test network configurations before deploying them in production environments.
3. **Self-Study and Practice:**
   - Students and professionals use Packet Tracer for self-study and practice
4. **Demonstrations and Presentations:**
   - Packet Tracer is used by instructors and presenters to demonstrate networking concepts, conduct workshops, and deliver technical presentations in a virtual environment.

Wireshark

- Wireshark is a popular network protocol analyzer that allows users to capture and analyze network traffic in real-time.
- Developed by the Wireshark development team, it is an open-source software available for various operating systems, including Windows, macOS, and Linux.

Features of Wireshark:

1. **Packet Capture:**
    - Wireshark can capture network traffic from wired and wireless interfaces in real-time. It supports a wide range of network protocols and media types, including Ethernet, Wi-Fi, Bluetooth, and more.
2. **Protocol Decoding:**
    - Wireshark dissects captured packets and decodes them into human-readable format, allowing users to analyze the contents of each packet, including headers, payloads, and protocol-specific information.
3. **Powerful Filtering:**
    - Wireshark provides powerful filtering capabilities to focus on specific network traffic based on criteria such as IP address, port number, protocol type, packet size, and more. Filters help users isolate relevant traffic and troubleshoot issues efficiently.

Features of Wireshark

4. **Protocol Support:**
    - Wireshark supports a vast array of network protocols, including common protocols like TCP/IP, UDP, HTTP, DNS, DHCP, as well as more specialized protocols used in various applications and industries.
5. **Colorized Packet Display:**
    - Wireshark colorizes packets based on various criteria, such as packet type, protocol, and severity of issues. Color-coded packet display makes it easier to identify important packets and potential problems.
6. **Packet Analysis Tools:**
    - Wireshark provides built-in tools for analyzing network traffic, including statistics, conversations, protocol hierarchy, packet details, and more. These tools help users gain insights into network behavior and diagnose performance issues.
7. **Export and Save Data:**
    - Wireshark allows users to export captured packets and analysis results in various formats, such as plain text, CSV, XML, or pcap (Packet Capture) files. Exported data can be shared with colleagues or used for further analysis.

Uses of Wireshark

1. **Network Troubleshooting:**
    - Wireshark is commonly used by network administrators and engineers to troubleshoot network issues, diagnose connectivity problems, and identify the root cause of performance issues.
2. **Security Analysis:**
    - Security professionals use Wireshark for analyzing network traffic for signs of malicious activity, such as intrusion attempts, malware infections, or data breaches. It can help detect and mitigate security threats.
3. **Protocol Development:**
    - Developers and protocol engineers use Wireshark for developing and testing network protocols, validating protocol implementations, and debugging protocol interactions.
4. **Education and Training:**
    - Wireshark is used in academic institutions and training programs for teaching networking concepts, protocol analysis, and hands-on network troubleshooting skills.
5. **Application Performance Monitoring:**
    - Wireshark can be used to monitor and analyze application-level protocols to diagnose performance bottlenecks, optimize application behavior, and ensure efficient data transfer.

Proxy

- A forward proxy, often called a proxy, proxy server, or web proxy, is a server that sits in front of a group of client machines.
- When those computers make requests to sites and services on the Internet, the proxy server intercepts those requests and then communicates with web servers on behalf of those clients, like a middleman.

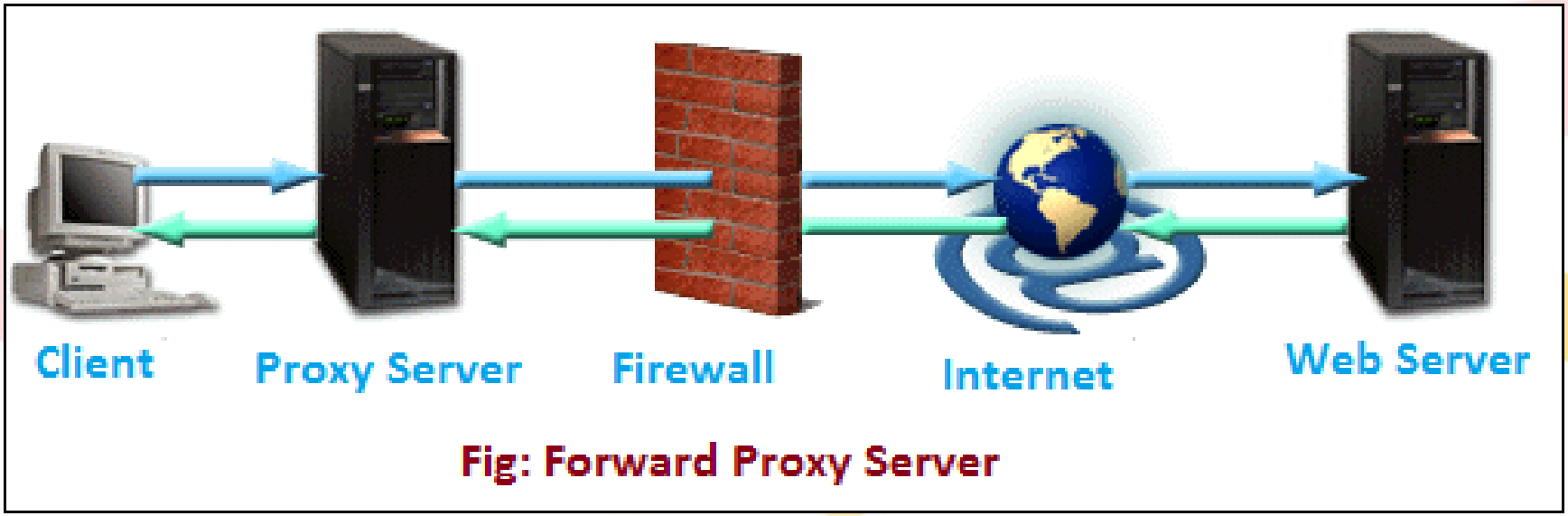
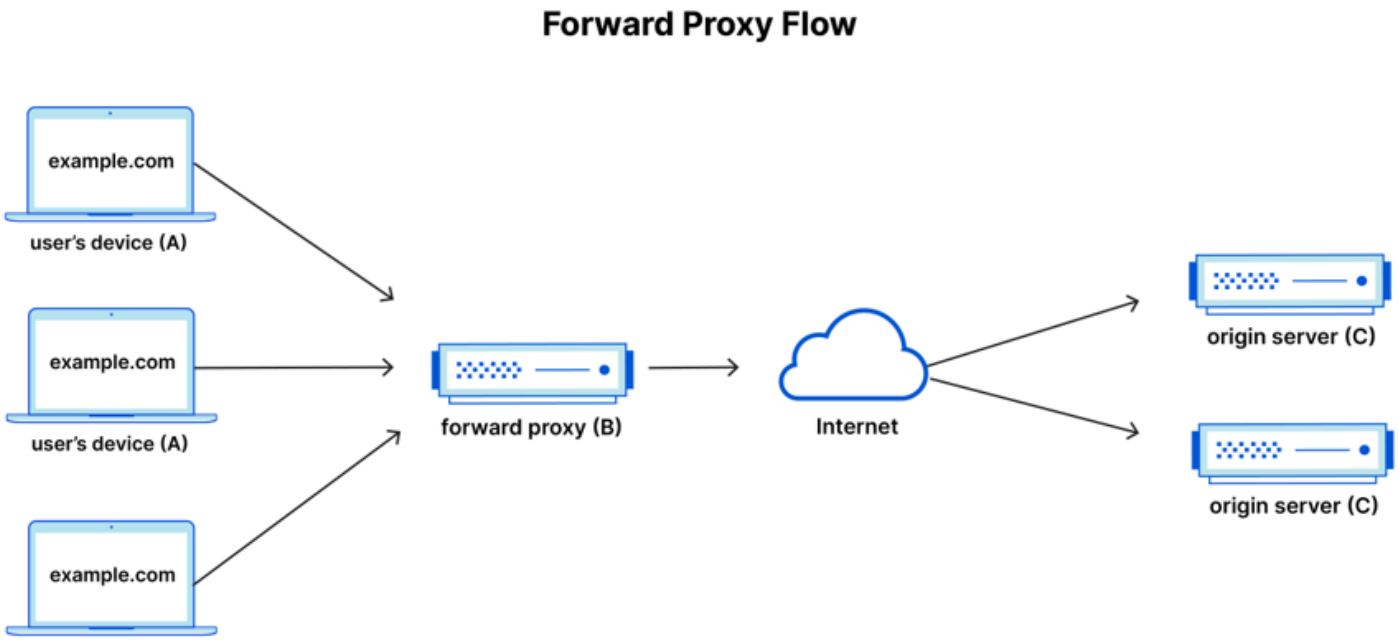


Fig: Forward Proxy Server

Working of Proxy

For example, let's name 3 computers involved in a typical forward proxy communication:

- A: This is a user's home computer
- B: This is a forward proxy server
- C: This is a website's origin server (where the website data is stored)



- In a standard Internet communication, computer A would reach out directly to computer C, with the client sending requests to the origin server and the origin server responding to the client.
- When a forward proxy is in place, A will instead send requests to B, which will then forward the request to C. C will then send a response to B, which will forward the response back to A.

Need of Proxy

- **To block access to certain content** - proxies can be set up to block a group of users from accessing certain sites. For example, a school network might be configured to connect to the web through a proxy which enables content filtering rules, refusing to forward responses from Facebook and other social media sites.
- **To protect their identity online** - In some cases, regular Internet users simply desire increased anonymity online, but in other cases, Internet users live in places where the government can impose serious consequences to political dissidents.
- **It improves the security and enhances the privacy of the user.**
- **It hides the identity (IP address) of the user.**
- **It controls the traffic and prevents crashes.**
- **Saves bandwidth by caching files and compressing incoming traffic.**
- **Protect network from malware.**

Reverse Proxy

- A reverse proxy is a server that sits in front of one or more web servers, intercepting requests from clients.
- This is different from a forward proxy, where the proxy sits in front of the clients.
- With a reverse proxy, when clients send requests to the origin server of a website, those requests are intercepted at the network edge by the reverse proxy server.
- The reverse proxy server will then send requests to and receive responses from the origin server.

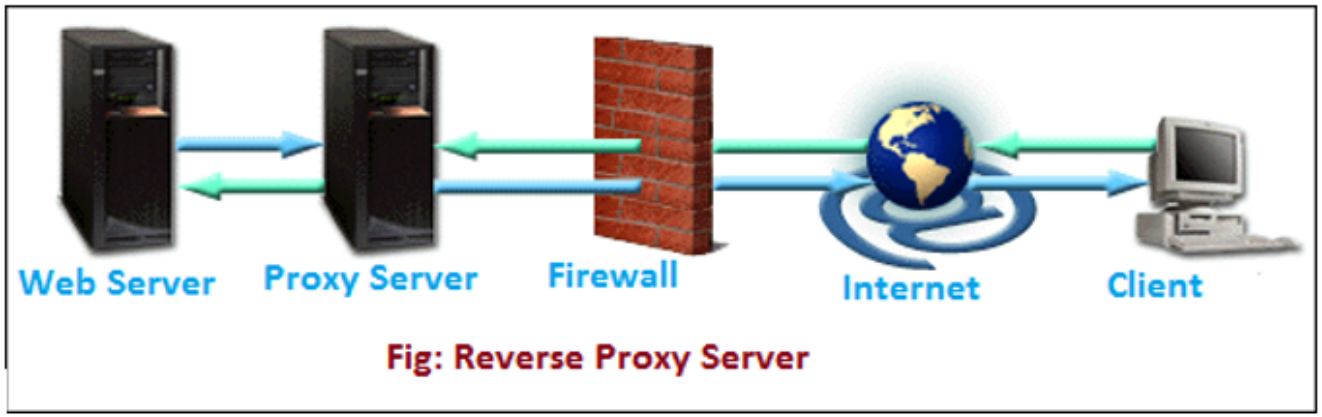
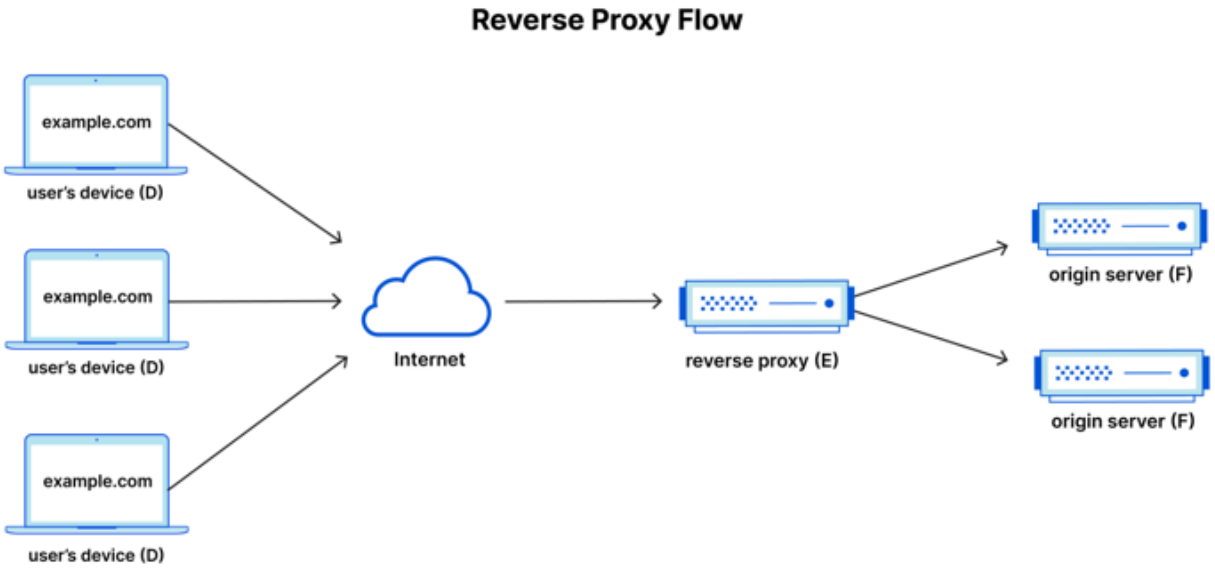


Fig: Reverse Proxy Server

Working of Reverse Proxy

Once again, let's illustrate by naming the computers involved:

- D: Any number of users' home computers
- E: This is a reverse proxy server
- F: One or more origin servers



- Typically all requests from D would go directly to F, and F would send responses directly to D. With a reverse proxy, all requests from D will go directly to E, and E will send its requests to and receive responses from F. E will then pass along the appropriate responses to D.

Need of ReverseProxy

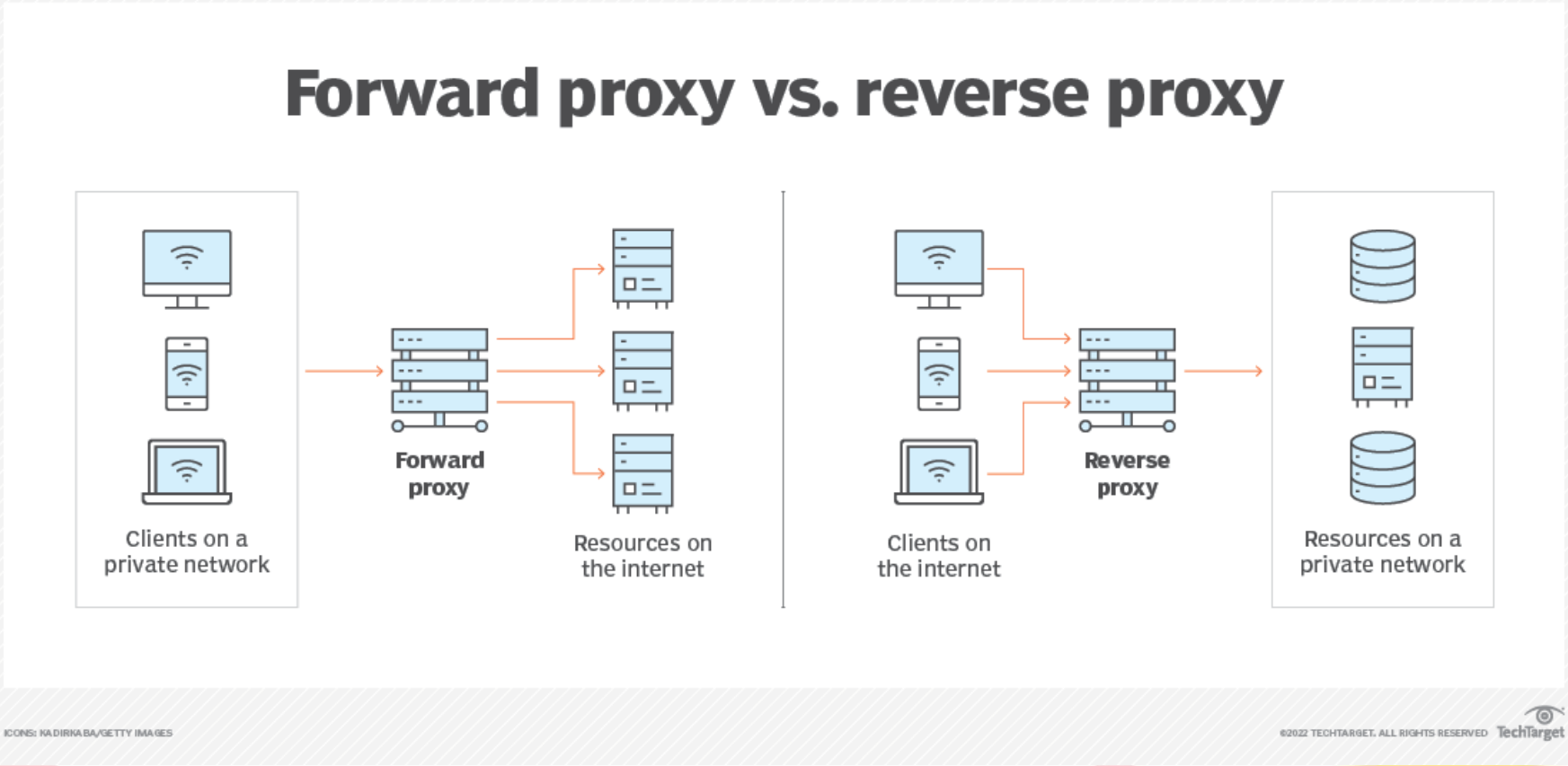
- **Load balancing** -
  - A popular website that gets millions of users every day may not be able to handle all of its incoming site traffic with a single origin server. Instead, the site can be distributed among a pool of different servers
  - Reverse proxy can provide a load balancing solution which will distribute the incoming traffic evenly among the different servers to prevent any single server from becoming overloaded.

Protection from attacks -

- With a reverse proxy in place, a web site or service never needs to reveal the IP address of their origin server(s).
- This makes it much harder for attackers to leverage a targeted attack against them, such as a DDoS attack.

Need of ReverseProxy

- **Caching** -
  - A reverse proxy can also cache content, resulting in faster performance
- **SSL encryption** -
  - Encrypting and decrypting SSL (or TLS) communications for each client can be computationally expensive for an origin server.
  - A reverse proxy can be configured to decrypt all incoming requests and encrypt all outgoing responses, freeing up valuable resources on the origin server.



- Forward proxy sits in front of a client and ensures that no origin server ever communicates directly with that specific client.
- On the other hand, a reverse proxy sits in front of an origin server and ensures that no client ever communicates directly with that origin server.

Webmail

- Webmail refers to email services that are accessed through a web browser rather than through a dedicated email client software installed on a computer or mobile device.
- With webmail, users can access their email accounts from any device with an internet connection and a web browser. Here's an overview of webmail:

Examples of Webmail Services:

- **Gmail:** Google's web-based email service, known for its intuitive interface, powerful search capabilities, and integration with other Google services.
- **Outlook.com:** Microsoft's webmail service, offering features such as integration with Office Online, calendar, contacts, and Skype integration.
- **Yahoo Mail:** Yahoo's web-based email service, providing features such as customizable themes, disposable email addresses, and integration with Yahoo Calendar and Yahoo Messenger.

Features of Webmail

1. **Access Anywhere, Anytime:**
    - Webmail allows users to access their email accounts from any device with an internet connection and a web browser, such as computers, smartphones, and tablets.
2. **No Installation Required:**
    - Unlike traditional email clients that require installation and configuration, webmail services are accessed directly through a web browser, eliminating the need for software installation.
3. **Platform Independence:**
    - Webmail is platform-independent, meaning it can be accessed from any operating system, including Windows, macOS, Linux, iOS, and Android.
4. **Integrated Features:**
    - Webmail services often include integrated features such as contact management, calendar, task lists, and file attachments, providing a comprehensive communication and productivity solution.
5. **Customization Options:**
    - Users can customize their webmail interfaces, including themes, layouts, and settings, to suit their preferences and workflow.

Features of Webmail

6. **Security Measures:**
    - Webmail providers implement security measures such as encryption, authentication, spam filtering, and virus scanning to protect users' email accounts and data.
7. **Search and Organization:**
    - Webmail services typically include search and organization features to help users find and manage their emails efficiently, including folders, labels, and filters.

END of UNIT 6

Thank You.