

Computer Networks

BE Computer 7th Semester

Er. Anuj Sherchan

Assistant Professor

Unit 8:Application Layer

- Outline:
- 11.1.DNS ,ARP and RARP, Mail protocol (SMTP, POP, IMAP), DHCP, Web services (WWW, HTTP, HTTPS, FTP), telnet, DHCP.
- 11.2.Client server and P2P application
- 11.3.Relation between Application layer and Transport layer.

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,
 - file access and transfer,
 - access to system resources,
 - surfing the world wide web, and
 - network management.

Application Layer

- **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.

Domain Name System(DNS)

- Although it's possible to enter an IP address into a web browser in 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.

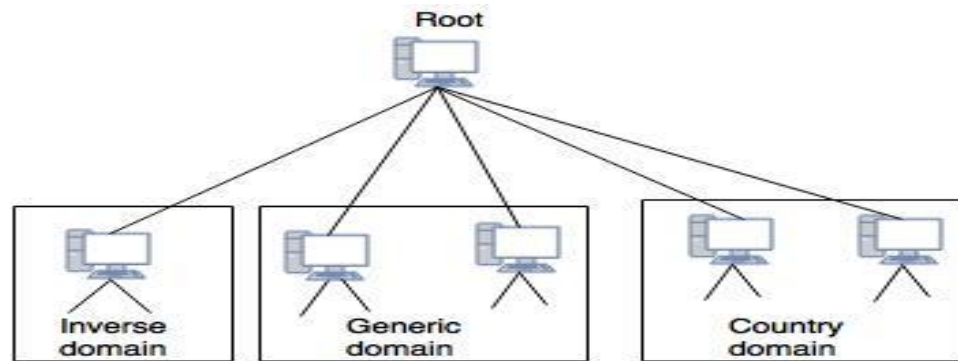
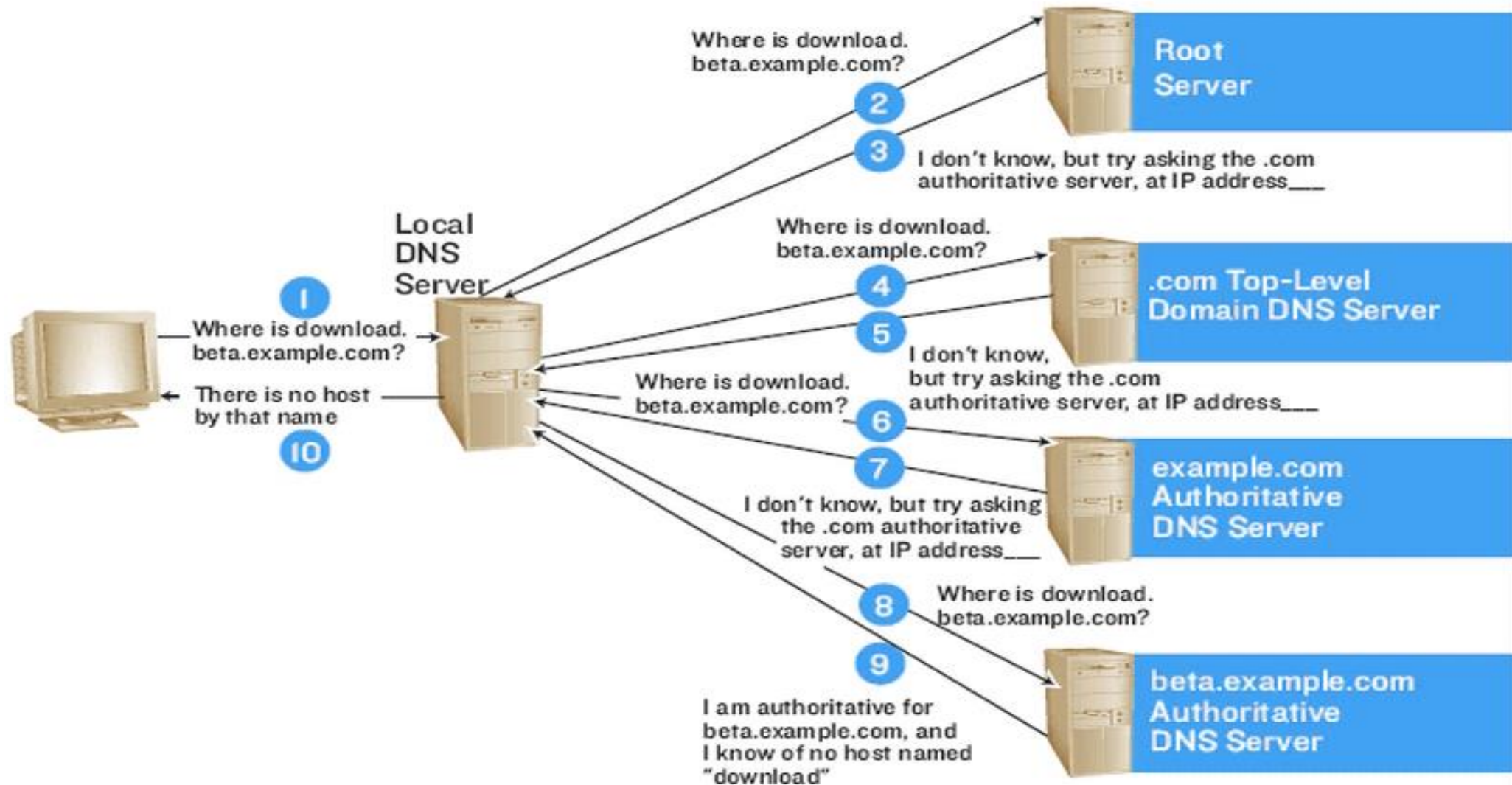


Fig. : DNS in the Internet

Domain Name System(DNS)

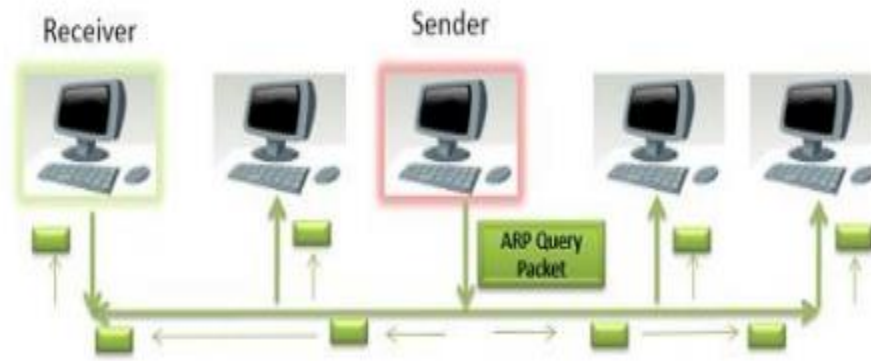
- Generic domain labels
- Com-commercial organizations
- Gov- Government institutions
- Net- network support centers
- Org- nonprofit organizations
- Name- personal names (individual) etc.
- Inverse Domain: Used to map an ip address to a domain name.

HOW DNS WORKS

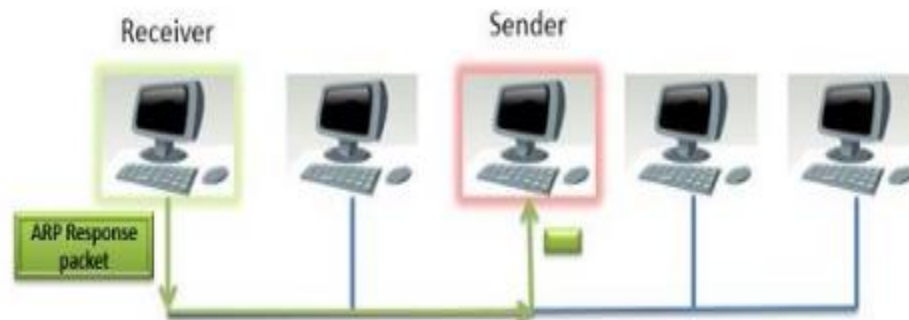


Address Resolution Protocol and Reverse Address Resolution Protocol (ARP & RARP)

- ARP and RARP both are the Network layer protocol.
- Whenever a host needs to send an IP datagram to another host, the sender requires both the logical address and physical address of the receiver.
- The dynamic mapping provides two protocols ARP and RARP.
- The basic difference between ARP and RARP is that ARP when provided with the logical address of the receiver it obtains the physical address of the receiver whereas in RARP when provided with the physical address of the host, it obtains the logical address of the host from the server.
- ARP maps 32-bit logical (IPv4) address to a 48-bit physical address of the receiver. On the other hand, RARP maps 48-bit physical address to 32-bit logical address of the receiver.

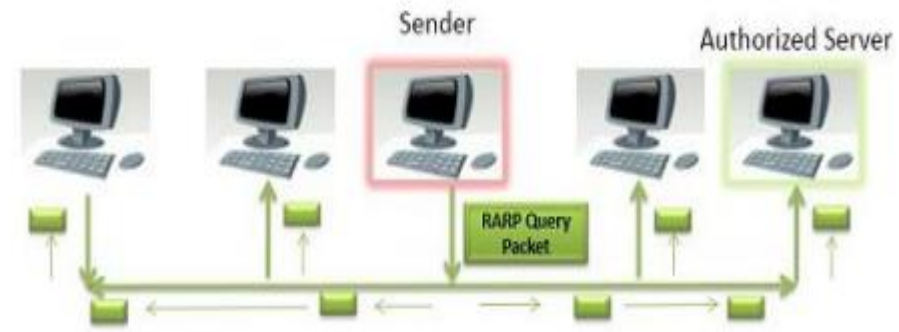


(a)

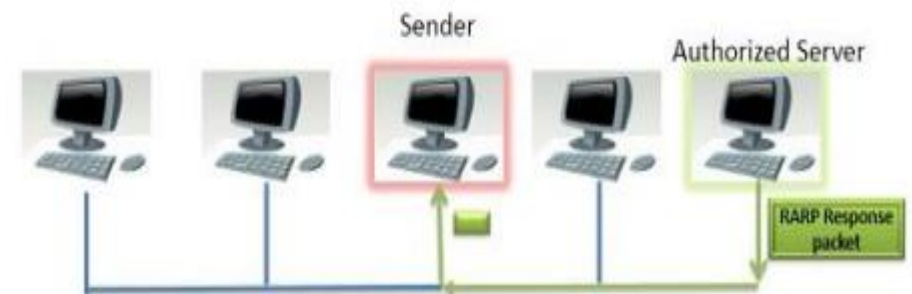


(b)

Address Resolution Protocol



(a)



(b)

Reverse Address Resolution Protocol

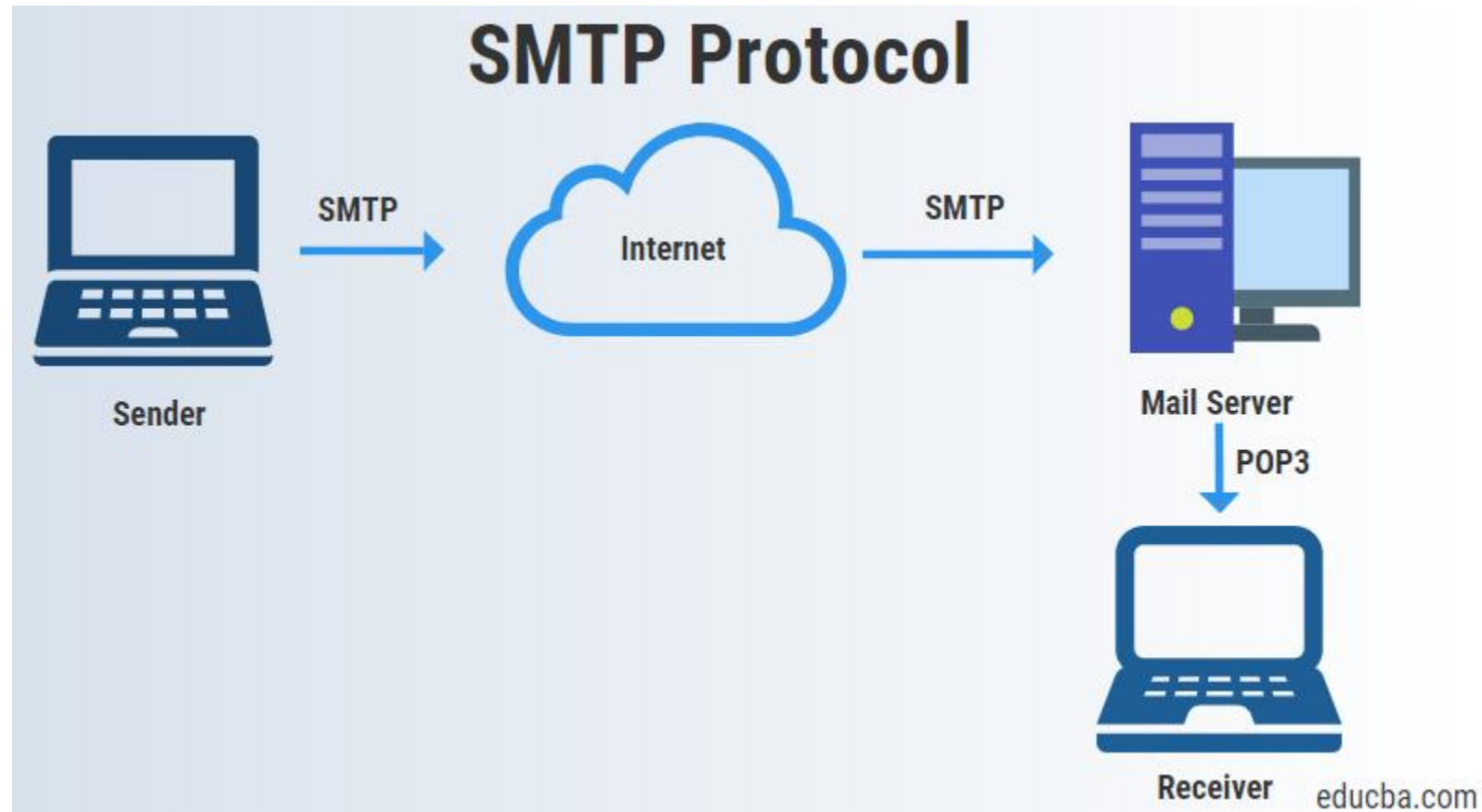
Mail Protocols

- Mail Protocols are set of rules that help the client to properly transmit the information to or from the mail server.
- Major protocols for mail services are SMTP, POP, and IMAP.
- **Simple Mail Transfer Protocol (SMTP)**
- It is a standard protocol used for sending e-mail efficiently and reliably over the internet
- SMTP is application level protocol.
- SMTP is connection-oriented protocol.
- SMTP is text-based protocol.

Simple Mail Transfer Protocol (SMTP)

- 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.

Simple Mail Transfer Protocol (SMTP)



Simple Mail Transfer Protocol (SMTP)

- **Commands used in SMTP Protocol**
- **HELLO** :This command initiates the SMTP conversation.
- **EHELLO** :This is an alternative command to initiate the conversation. ESMTP indicates that the sender server wants to use extended SMTP protocol.
- **MAIL FROM** :This indicates the sender's address.
- **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.
- **SIZE** :This command let the server know the size of attached message in bytes.
- **DATA** :The DATA command signifies that a stream of data will follow. Here stream of data refers to the body of the message.

Simple Mail Transfer Protocol (SMTP)

- QUIT :This command is used to terminate the SMTP connection.
- VRFY: This command is used by the receiving server in order to verify whether the given username is valid or not.
- EXPN: It is same as VRFY, except it will list all the users name when it used with a distribution list.

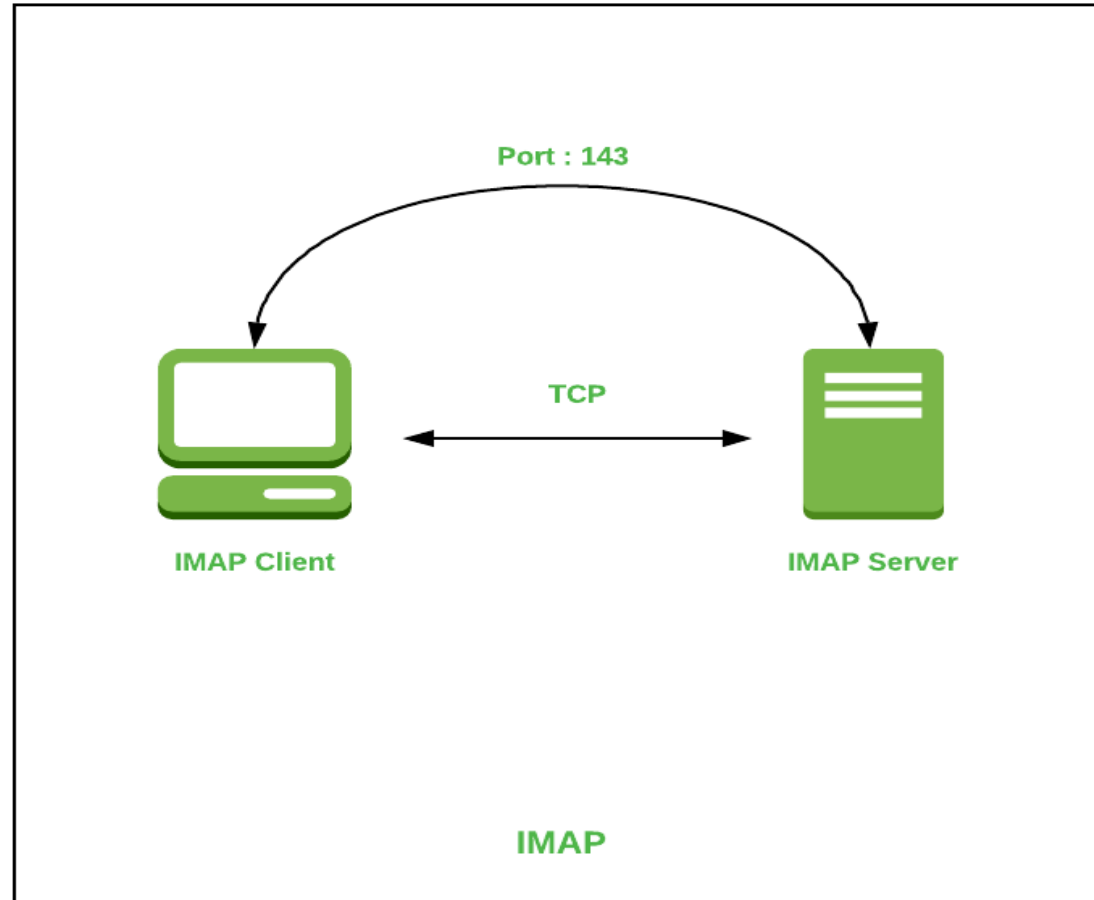
Internet Message Access Protocol(IMAP)

- 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.

Internet Message Access Protocol(IMAP)

- 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.

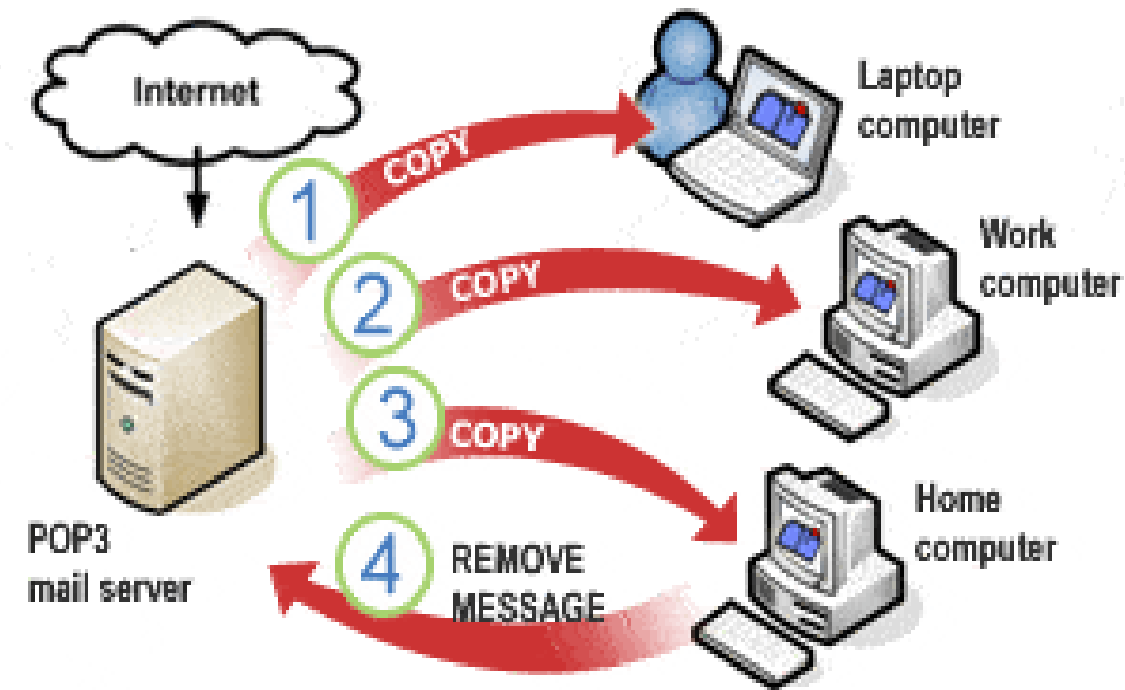
Internet Message Access Protocol(IMAP)



Post Office Protocol(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.
- 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.

Post Office Protocol(POP)

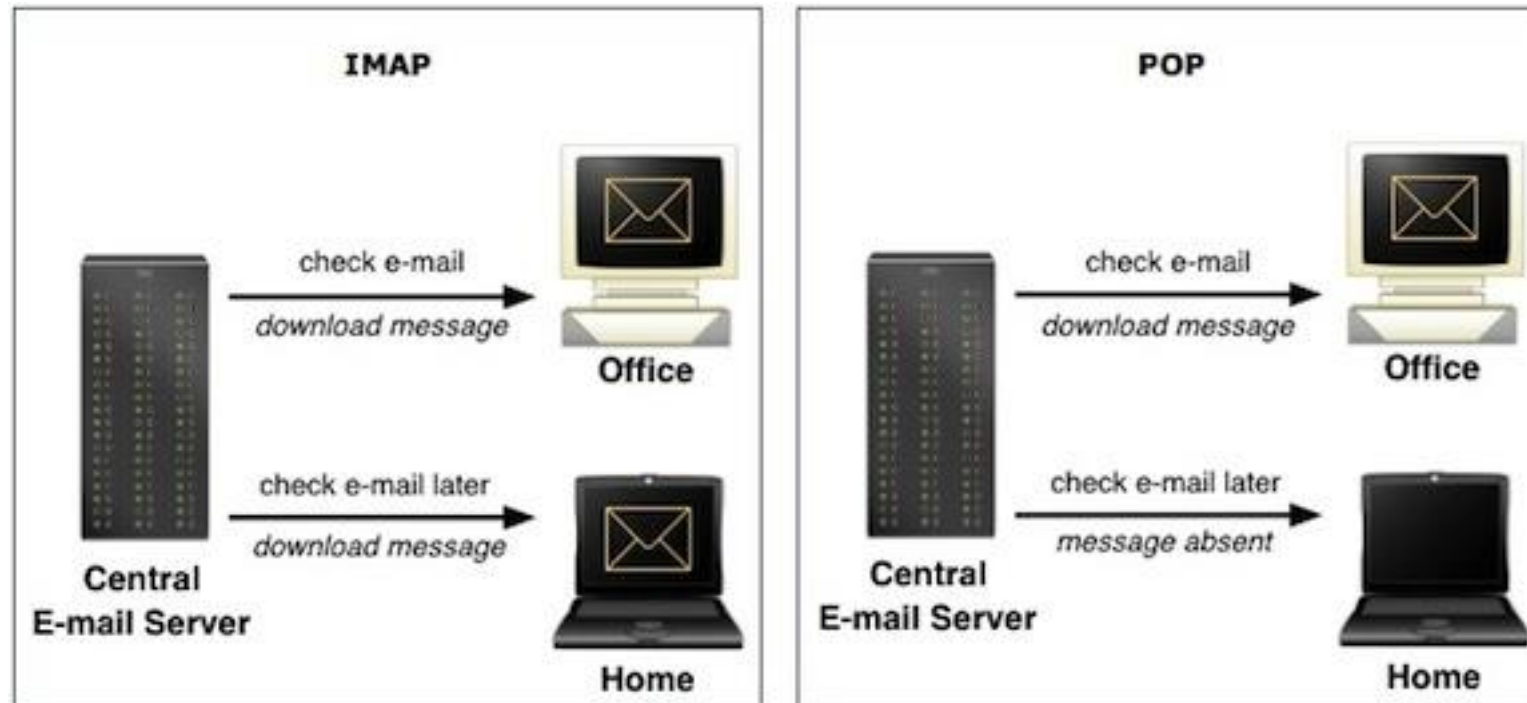


IMAP vs POP

IMAP VERSUS POP3

IMAP	POP3
IMAP is an acronym for Internet Message Access Protocol.	POP3 is short for Post Office Protocol Version 3.
The first IMAP was developed by Mark Crispin in 1986 as a potential alternative to POP.	The original POP was introduced in 1984 as a simple means to access emails on a remote server.
IMAP is an application layer internet standard protocol used when you need to access your emails from multiple devices.	POP3 is the latest version of the original email protocol used as a standardized method of delivering emails.
Any changes made on one device will be reflected on others.	Any changes made on one device won't be replicated on others.
Ideal for users who use multiple devices to access their emails.	Ideal for those who access their emails from one device and back up their drive regularly.
	

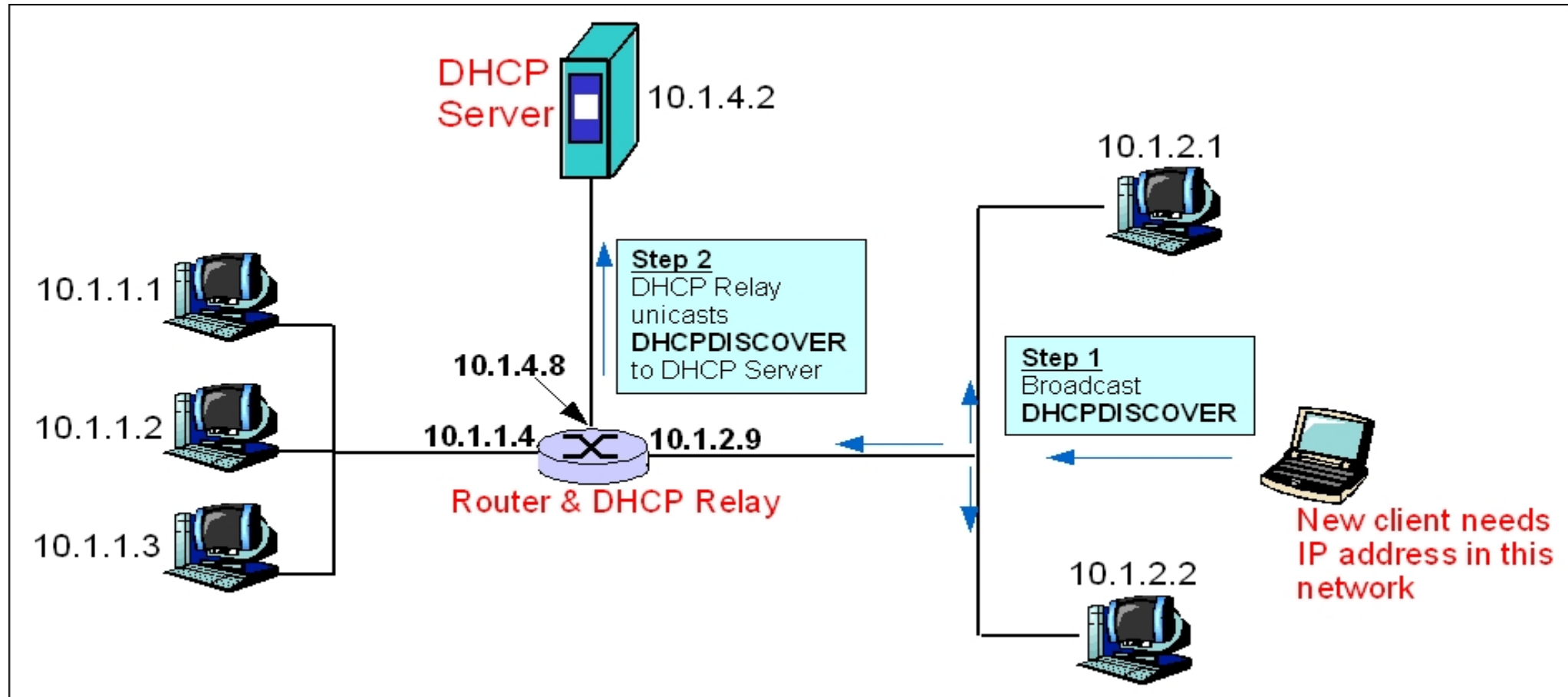
IMAP vs POP



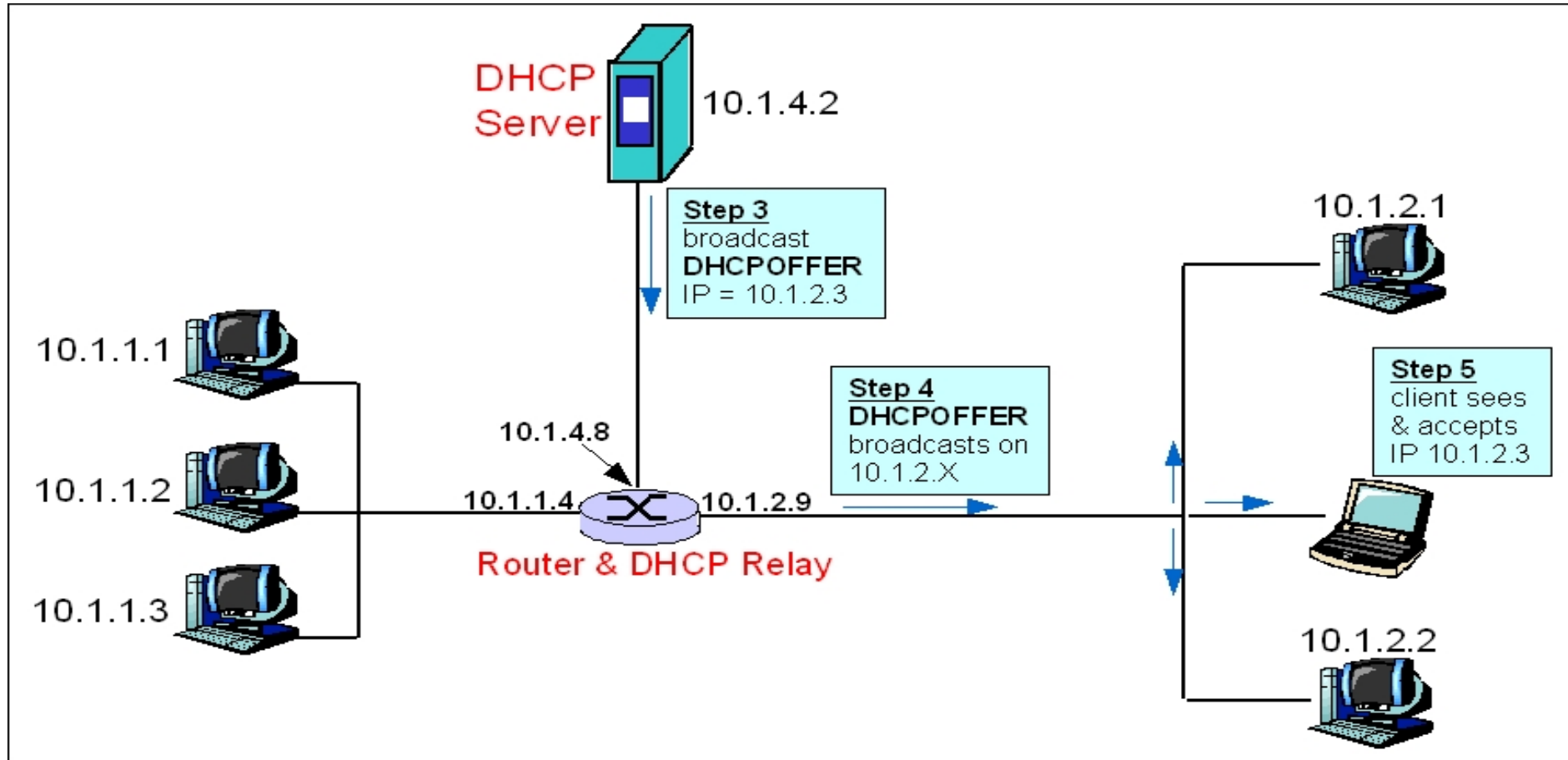
Dynamic Host Configuration Protocol (DHCP)

- The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on TCP/IP networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.
- A DHCP server enables computers to request IP addresses and networking parameters automatically from the Internet service provider (ISP), reducing the need for a network administrator or a user to manually assign IP addresses to all network devices.
- In the absence of a DHCP server, a computer or other device on the network needs to be manually assigned an IP address.

Dynamic Host Configuration Protocol (DHCP)



Dynamic Host Configuration Protocol (DHCP)



Web Services

- 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.
- **WWW(World wide web)**
- 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.

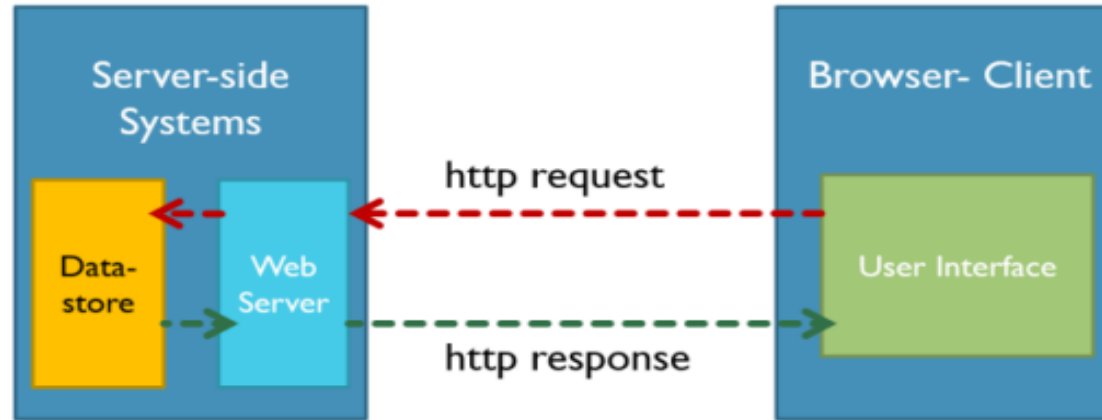
Web Services

- 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(Hypertext Transfer Protocol)**
- 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.

Web Services

- 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 information is only valid until the session exists.

Web Services



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

Web Services

- **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.

Web Services

- 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.

Web Services

- **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.

Web Services

- 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.
- 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.

Web Services

What is FTP Server?



Web Services

- **TELNET**
- is an abbreviation for Terminal Network.
- It is a standard TCP/IP protocol for virtual terminal service for remote logging.
- TELNET enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system.
- TELNET operates in the timesharing environment in which the users are part of the system with some right to access resources.
- Each authorized user has an ID and probably a password.
- The user identification defines the user as part of the system.
- To access the system, the user logs into the system with a user ID and password to prevent an unauthorized user from accessing the resources.

Web Services

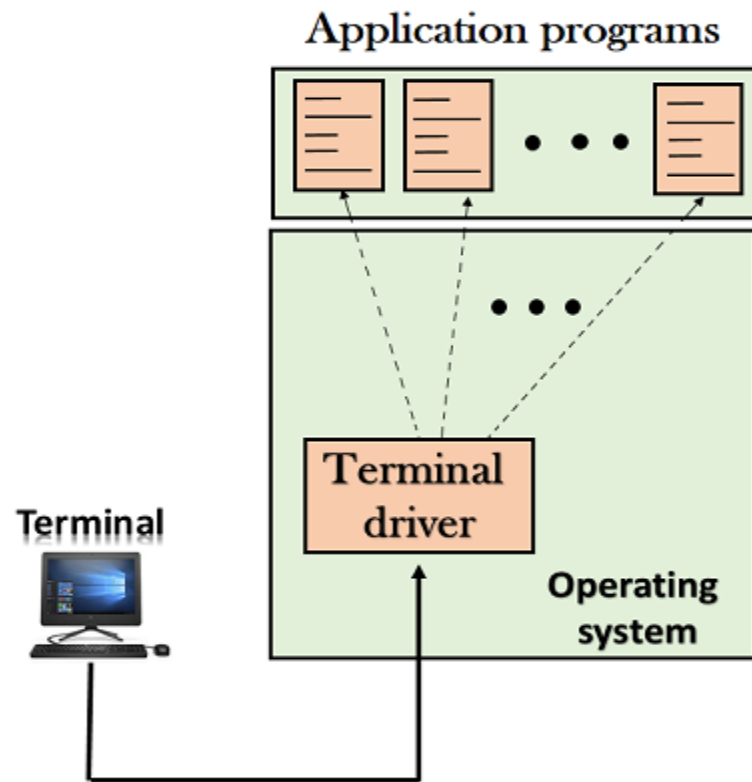


Fig: Local Login

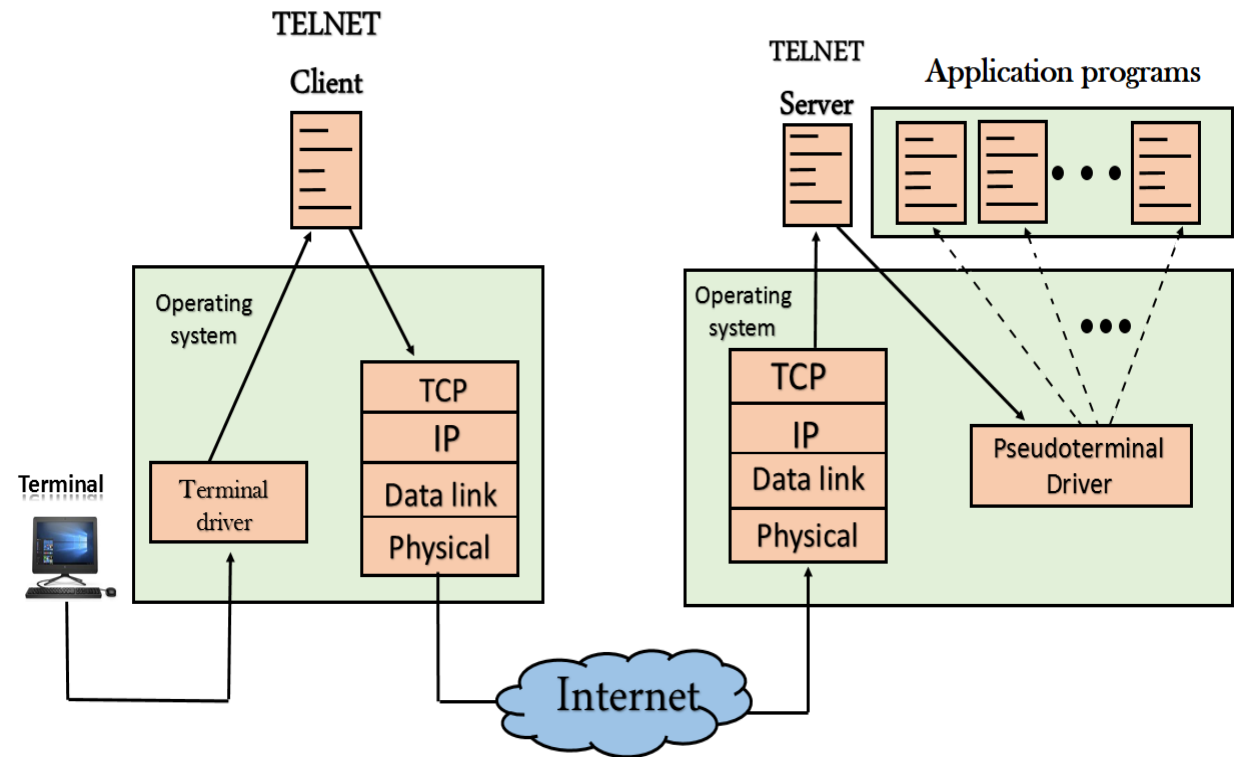


Fig : Remote Login

Web Services

- **Working of Telnet**
- When a user wants to access an application program or utility located on a remote machine, he/she should perform remote log-in.
- Here the TELNET client and server programs come into use.
- The user sends the request to the terminal driver and delivered to TCP/IP protocol stack through TELNET client.
- It then travels through the internet and arrive at the TCP/IP stack at the remote machine.
- The request is delivered to the TELNET server, which forwards it to the pseudo terminal driver and finally to the application program.

Web Services

- The operating system cannot accept the request from the TELNET server, which is designed to receive request from the terminal driver.
- Thus, a piece of software called a pseudo terminal driver is added since it pretends that the requests are coming from the terminal.
- **Client Server Architecture**
- In a client-server architecture, there is an always-on host, called the server, which services requests from many other hosts, called clients.
- A classic example is the Web application for which an always-on Web server services requests from browsers running on client hosts.
- When a Web server receives a request for an object from a client host, it responds by sending the requested object to the client host.
- Note that with the client-server architecture, clients do not directly communicate with each other; for example, in the Web application, two browsers do not directly communicate.

Web Services

- Another characteristic of the client-server architecture is that the server has a fixed, well-known IP address.
- Because the server has a fixed, well known address, and because the server is always on, a client can always contact the server by sending a packet to the server's IP address.
- Some of the better-known applications with a client-server architecture include the Web, FTP, Telnet, and e-mail.
- Often in a client-server application, a single-server host is incapable of keeping up with all the requests from clients.
- For example, a popular social-networking site can quickly become overwhelmed if it has only one server handling all of its requests.
- For this reason, a data center, housing a large number of hosts, is often used to create a powerful virtual server.

Web Services

- The most popular Internet services—such as search engines (e.g., Google and Bing), Internet commerce (e.g., Amazon and e-Bay), Web-based email (e.g., Gmail and Yahoo Mail), social networking (e.g., Facebook and Twitter)—employ one or more data centers.
- Google has 30 to 50 data centers distributed around the world, which collectively handle search, YouTube, Gmail, and other services.
- A data center can have hundreds of thousands of servers, which must be powered and maintained.
- Additionally, the service providers must pay recurring interconnection and bandwidth costs for sending data from their data centers.

Web Services

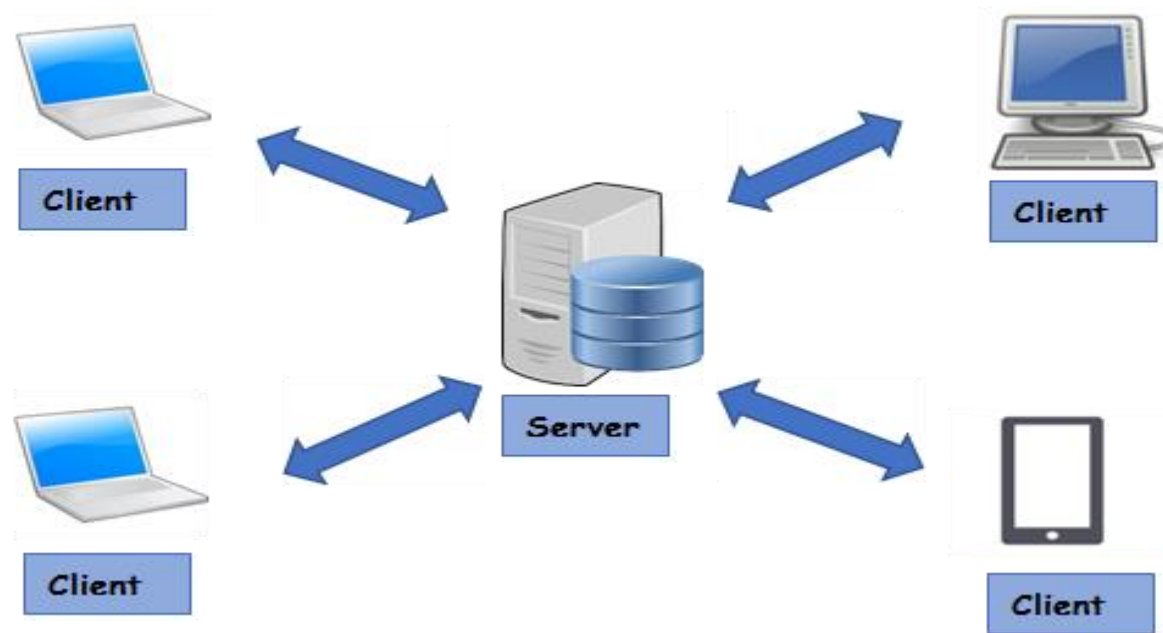


Fig : Client Server Architecture

Web Services

- **Peer-to-Peer Architecture**

- In a P2P architecture, there is minimal (or no) reliance on dedicated servers in data centers.
- Instead the application exploits direct communication between pairs of intermittently connected hosts, called peers.
- The peers are not owned by the service provider, but are instead desktops and laptops controlled by users, with most of the peers residing in homes, universities, and offices.
- Because the peers communicate without passing through a dedicated server, the architecture is called peer-to-peer.
- Many of today's most popular and traffic-intensive applications are based on P2P architectures.
- These applications include file sharing too. (e.g., BitTorrent)

Web Services

- One of the most compelling features of P2P architectures is their self-scalability.
- For example, in a P2P file-sharing application, although each peer generates workload by requesting files, each peer also adds service capacity to the system by distributing files to other peers.
- P2P architectures are also cost effective, since they normally don't require significant server infrastructure and server bandwidth.

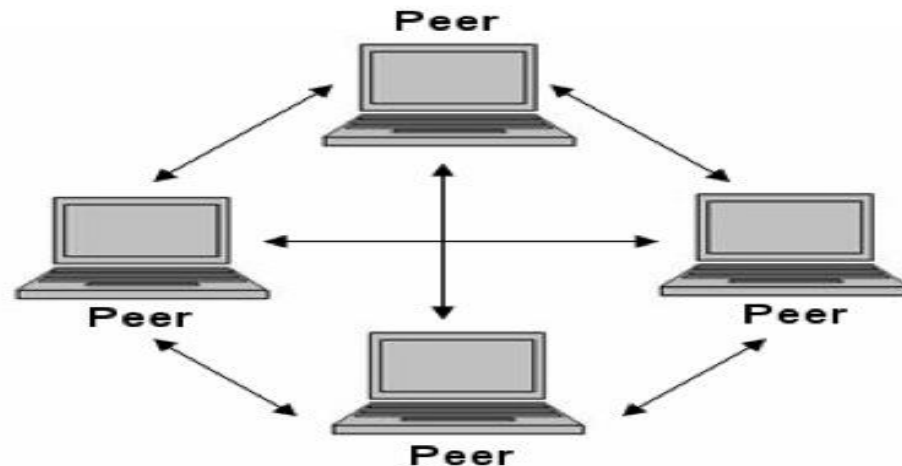


Fig : Peer to Peer Architecture

Relationship between Transport Layer and Application Layer

- Transport Layer is responsible for transmitting data between two processes.
- It takes care of retransmission of data if the data fails in the first attempt to reach the destination properly, flow control, error control etc.
- Application layer is near to user-end which facilitates the users to interact to the network.
- Application layer defines set of rules for data transmission, identify the end partner and provide the data to lower layers.
- So, transport layer takes care of sending this data to another end process in the network.
- The application layer data goes to the transport layer and gets segmented into multiple segments.
- Application layer is responsible for all the services provided by the internet.
- Every application protocol running in the application layer is supported by the transport layer for end-to-end communication and process-to-process connection establishment and delivery of data.

THANK YOU