***What is HTTP (Hypertext Transfer Protocol)?***

*HTTP stands for Hypertext Transfer Protocol and is the foundation for data communication on the World Wide Web (WWW). It enables web browsers and servers to communicate, allowing users to access information over the internet. HTTP is closely tied with HTML (Hypertext Markup Language), which formats and displays web content. The protocol has evolved, with HTTP/2 improving performance, and HTTP/3, introduced in 2022, further enhancing speed and security.*

***Key Points of HTTP:***

***Basic Structure:*** *HTTP forms the core of web communication, enabling data transfer and file sharing.*

***Web Browsing:*** *Most websites operate over HTTP, facilitating activities like clicking links or downloading files.*

***Client Server Model:*** *HTTP follows a request response system, where the client (browser) sends a request, and the server provides the requested data.*

***Application Layer Protocol:*** *HTTP functions within the Internet Protocol Suite, managing data transmission and reception.*

***Working of HTTP***

*1. When accessing a website, a user types the website URL into a browser.*

*2. The Domain Name Server (DNS) processes this URL and returns the corresponding IP address to the browser.*

*3. The browser then uses this IP address to send a request to the server hosting the website.*

*4. Once the server responds, the connection closes. To make further requests, a new connection must be established.*

***HTTP Requests and Responses***

***HTTP Request:*** *Data needed by a browser to load a webpage. Key elements of an HTTP request include:*

*HTTP Version*

*URL*

*HTTP Method (e.g., GET, POST)*

*{GET Method: Retrieves data from the server without modifying it, with data sent in the URL.*

*POST Method: Sends data to the server to create or update a resource, with data sent in the request body.}*

*HTTP Headers (provides client information)*

*HTTP Body (contains the data to be transferred)*

***HTTP Response:*** *The server's answer to a client request.* ***Components of an HTTP response include:***

*HTTP Status Code*

*HTTP Headers (provides data to the response body)*

*HTTP Body (usually HTML content for display on a webpage)*

*HTTP works on “port 80” by default.*

***Advantages of HTTP***

*1. Simplicity and Accessibility*

*2. Stateless Communication*

*3. Compatibility with Proxies and Caching*

*4. Evolvability*

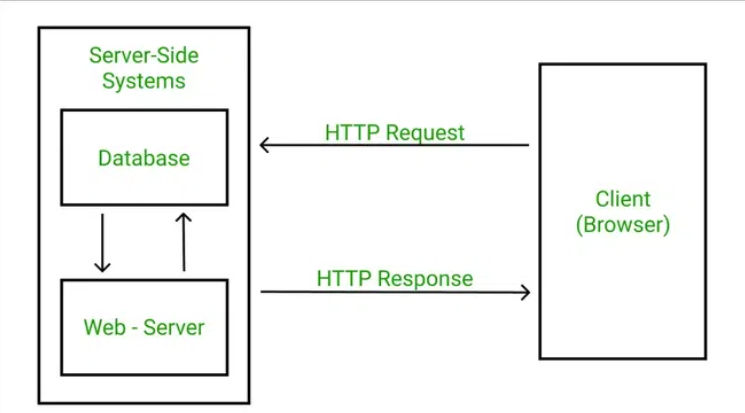
***Disadvantages of HTTP***

*1. Lack of Built in Security*

*2. Stateless Nature Can Limit Functionality*

*3. Higher Latency for Each Request*

*4. Limited Error Handling*

**

***What is SMTP (Simple Mail Transfer Protocol)?***

*SMTP stands for Simple Mail Transfer Protocol and is a standard protocol used to send emails over a TCP/IP network. It operates at the application layer, where the client opens a TCP connection with the SMTP server, typically over port 25. Once connected, the client can immediately send emails. The SMTP server remains on standby to initiate a connection whenever a TCP connection request is detected.*

***Types of SMTP Models:***

***Endtoend Method:*** *Used for sending emails across different organizations.*

***Store and Forward Method****: Used within an organization to relay messages.*

***In the SMTP process:***

*1. Client SMTP initiates the session.*

*2. Receiver SMTP responds to the request and receives the email data for delivery.*

***Components of SMTP:***

***Mail User Agent (MUA):*** *An application used by users to send and retrieve emails.*

***Mail Submission Agent (MSA):*** *Receives mail from the MUA and passes it to the MTA.*

***Mail Transfer Agent (MTA):*** *Transfers mail from one system to another using SMTP.*

***Mail Delivery Agent (MDA):*** *Delivers mail to the recipient's local system.*

***Advantages of SMTP:***

*Dedicated servers are possible if needed.*

*Enables bulk email sending.*

*Offers low cost and broad coverage.*

*Provides options for email tracking.*

*Ensures reliable and timely email delivery.*

***Disadvantages of SMTP:***

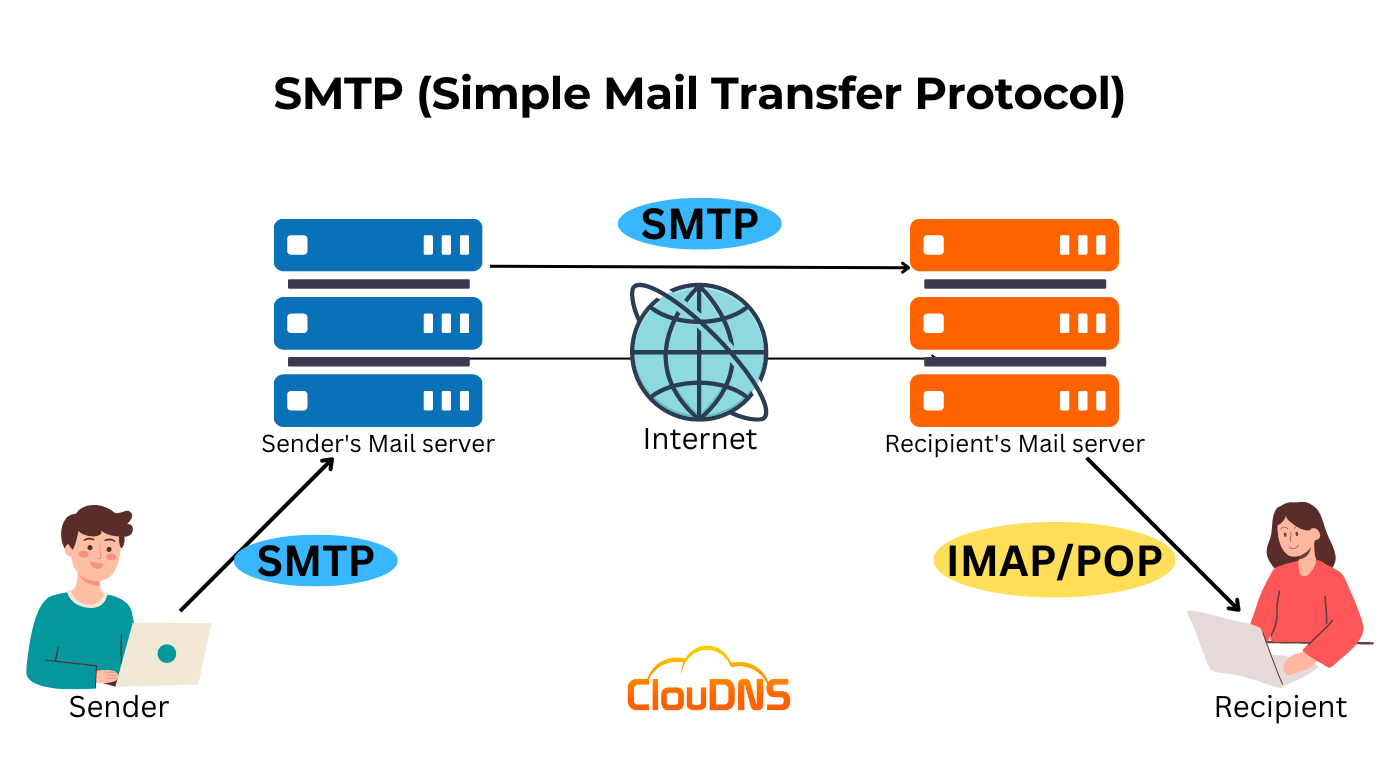
*Common SMTP port is vulnerable to firewall blocking.*

*Security remains a concern due to limited encryption capabilities.*

*SMTP is limited to 7bit ASCII characters.*

*Messages longer than a specific length may be rejected.*

*SMTP involves additional server to server exchanges, which may delay message delivery or increase the chances of non delivery.*



***ICMP (Internet Control Message Protocol)***

***Definition:***

*ICMP is used for reporting errors and management queries. It is a supporting protocol and is used by network devices like routers for sending error messages and operations information.*

***Uses of ICMP:***

*An important use of ICMP protocol is to perform network diagnosis by making use of Traceroute and Ping utilities.*

***Traceroute:*** *Traceroute utility is used to know the route between two devices connected over the internet. It routes the journey from one router to another, and a traceroute is performed to check network issues before data transfer.*

***Ping:*** *Ping is a simple kind of traceroute known as the echo request message. It is used to measure the time taken by data to reach the destination and return to the source. These replies are known as echo replies to messages.*

***How Does ICMP Work?***

*ICMP is connectionless, unlike TCP (which is connection oriented). It transmits packets in the form of datagrams that contain an IP header with ICMP data.*

***ICMP in DDoS Attacks:***

***Ping of Death Attack:*** *Attacker sends a ping, whose size is greater than the maximum allowable size. Oversized packets cause a buffer overflow, freezing the machine.*

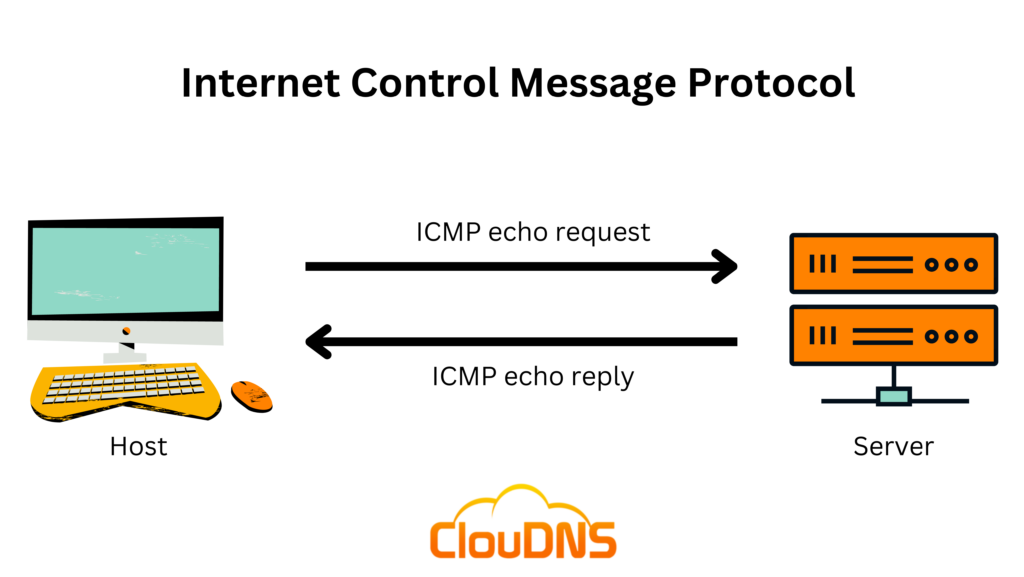
***ICMP Flood Attack:*** *The attacker sends too many pings, overwhelming the target machine's resources, leading to a Denial of Service (DoS).*

***Smurf Attack:*** *The attacker sends an ICMP packet with a spoofed source IP address, affecting older devices like the Ping of Death.*

***Types of ICMP Messages:***

*A screenshot of a computer

Description automatically generated*



***FTP (File Transfer Protocol)***

***Definition:***

*FTP is a standard communication protocol used for transferring files between computers. It ensures efficient and reliable file transfer, especially between heterogeneous systems.*

***Types of FTP:***

***Anonymous FTP:*** *Enabled on some sites where files are available for public access, and no username or password is required.*

***Password Protected FTP:*** *Requires a username and password for access.*

***FTPS (FTP Secure):*** *A more secure version of FTP using Transport Layer Security (TLS) for secure data transfer.*

***Uses of FTP:***

***Transferring Large Files:*** *FTP is used for large file transfers, such as hosting websites, backing up servers, or sharing large quantities of files.*

***Remote File Management:*** *Users can upload, download, delete, rename, and copy files on remote servers.*

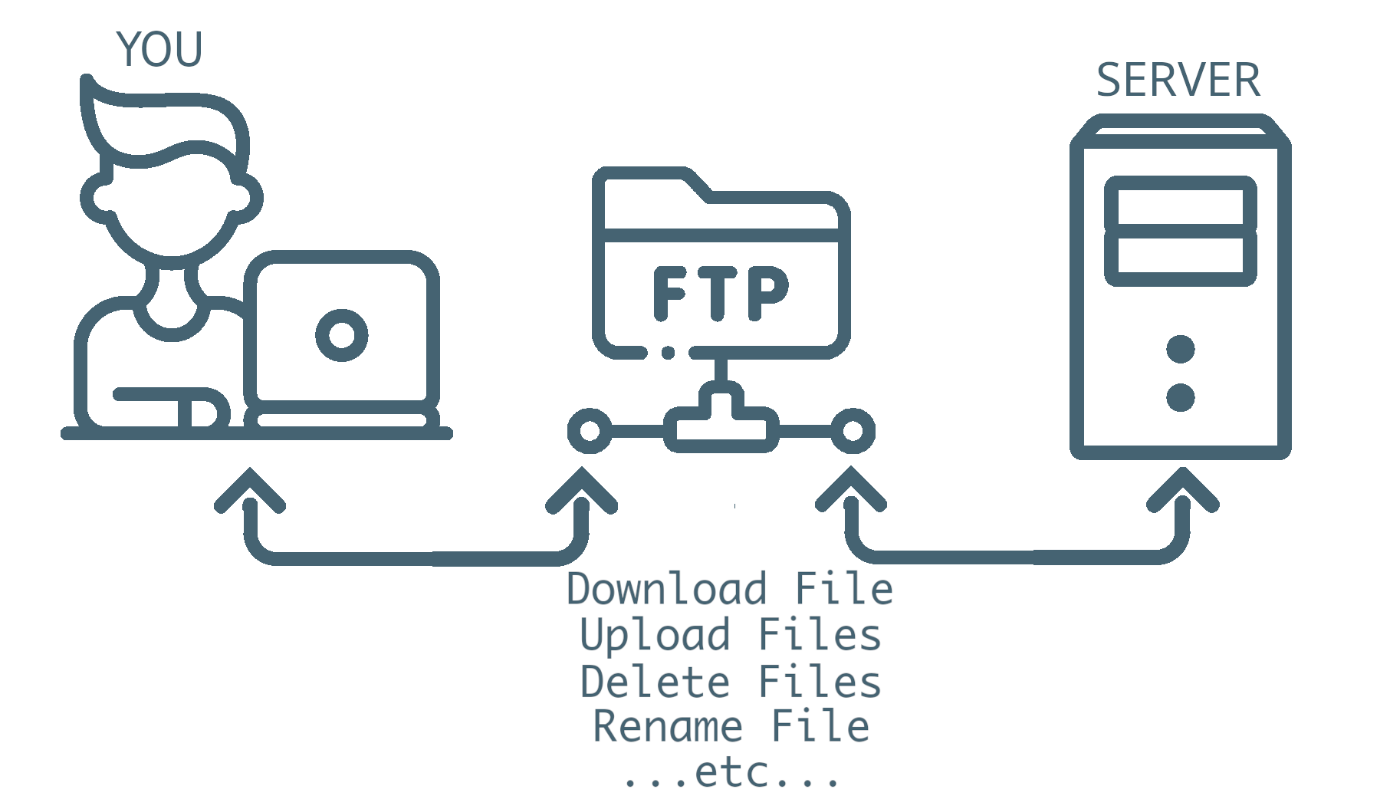
***Automating File Transfers:*** *FTP can execute predefined file transfers using scheduled scripts.*

***Accessing Public Files:*** *Anonymous FTP allows public access to download files without permissions.*

***Types of FTP Connections:***

***Control Connection:*** *Initiated on Port 21 for sending control information (e.g., authentication, commands).*

***Data Connection:*** *Initiated on Port 20 for transferring the actual file data.*



***POP (Post Office Protocol)***

***Definition:***

*POP is a protocol used to retrieve messages from a mail server. It allows users to download their emails from the server and store them locally, removing the message from the server after download.*

***Working of POP:***

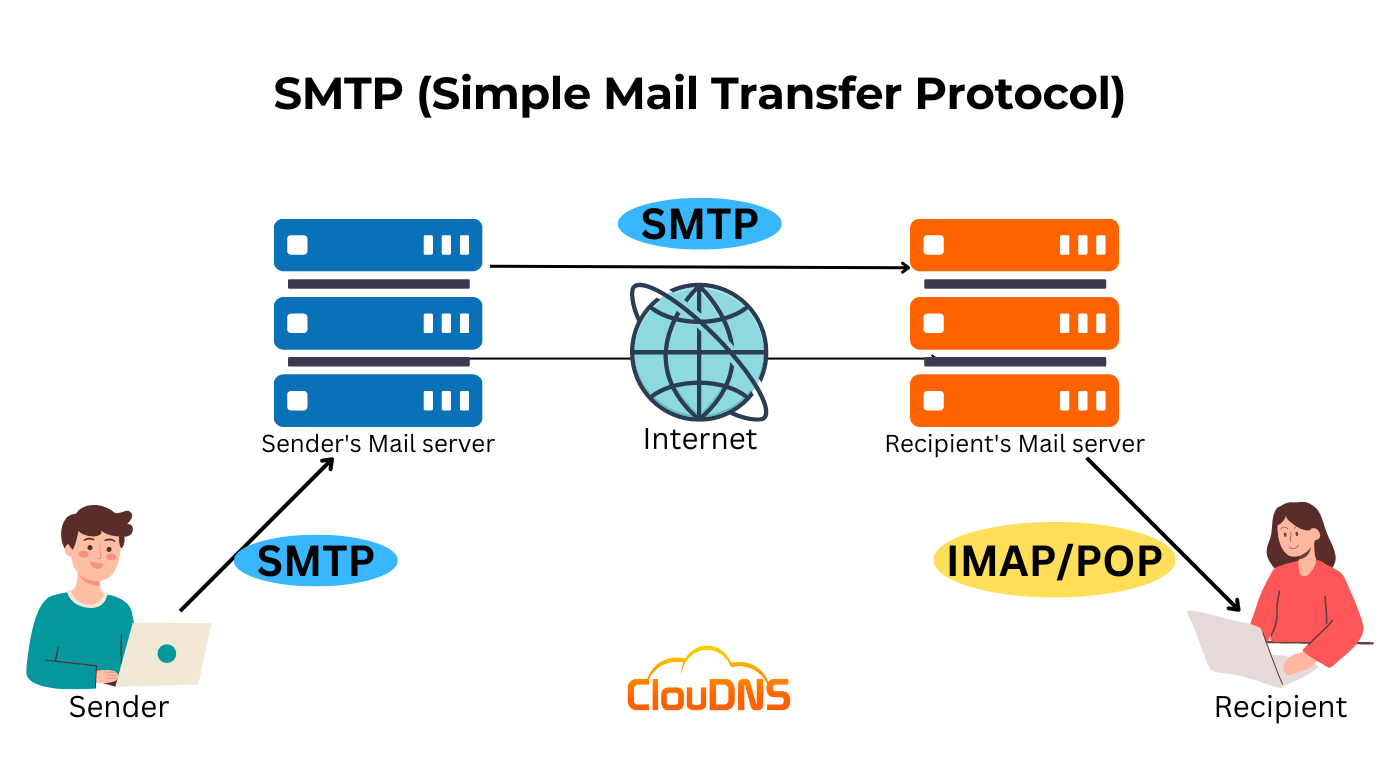
*Until the user logs in and downloads the message, all incoming messages are kept on the POP server. Once downloaded, the message is removed from the server.*

***Characteristics of POP:***

*POP is an open protocol, defined by Internet RFCs.*

*It is compatible with various client platforms and allows access to new mail.*

*POP only handles the retrieval of emails and does not allow for sending messages.*



***MIME (Multipurpose Internet Mail Extensions)***

***Definition:***

*MIME is an addon protocol that allows the transmission of nonASCII data through SMTP, enabling users to exchange various data types (audio, video, images, etc.).*

***Purpose and Functionality of MIME:***

*MIME is used to overcome the limitations of SMTP, which is restricted to 7bit ASCII characters. MIME transforms nonASCII data into 7bit ASCII format for transmission.*

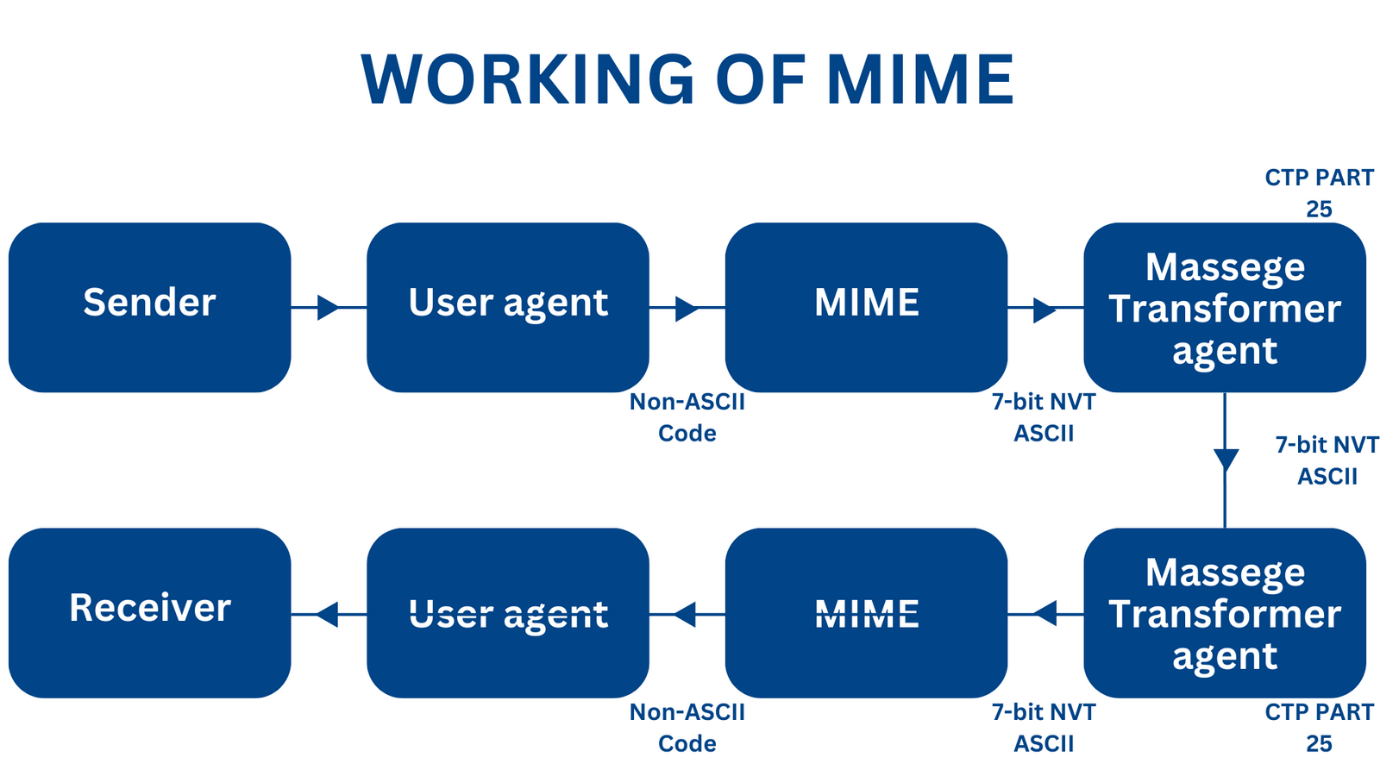
***Features of MIME:***

*Unlimited message length.*

*Supports multiple attachments within a single message.*

*Binary attachments (e.g., executable, images, videos) may be divided into smaller parts.*

*Supports varying content types and multi part messages.*



***DNS (Domain Name System)***

***Definition:***

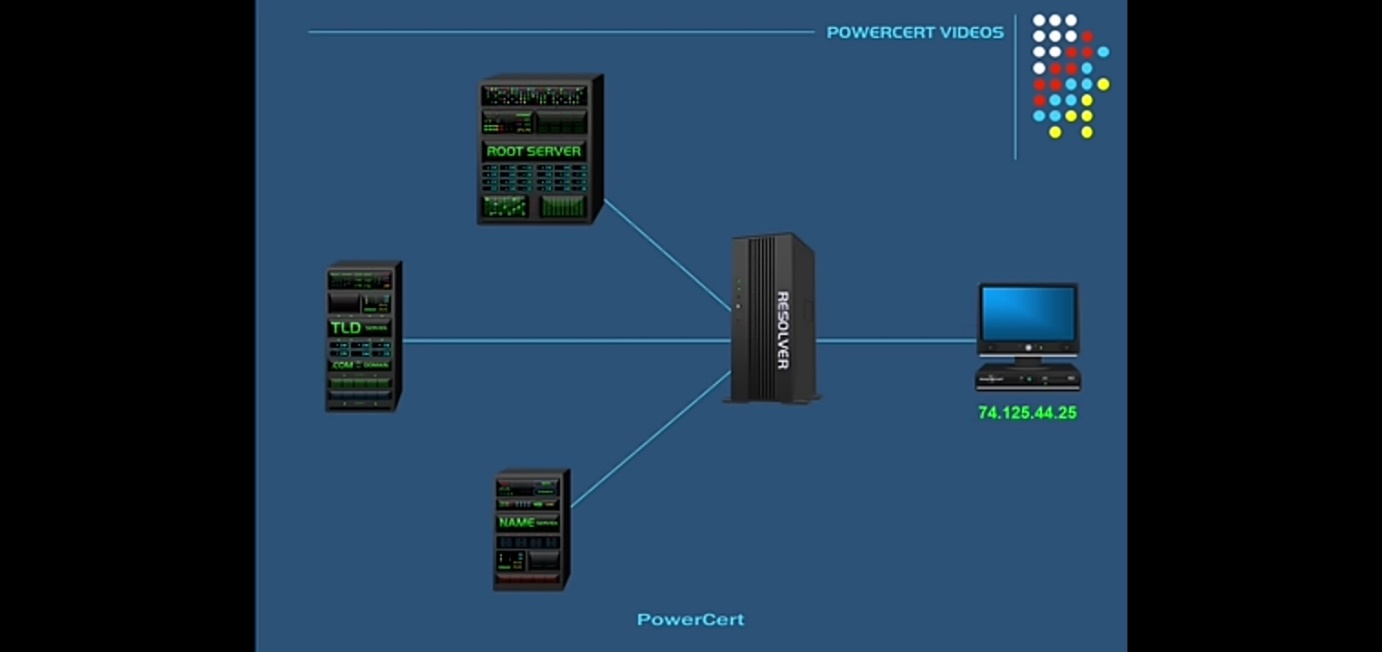
*DNS is the Internet's phone book, translating easy to remember domain names (e.g., www.example.com) into IP addresses (e.g., 192.0.2.1) that computers use to locate each other.*

***Types of Domains:***

***Generic Domains:*** *(.com, .edu, .org, .net)*

***Country Domains:*** *(.in for India, .us for the USA, .uk for the UK)*

***Inverse Domain:*** *Maps an IP address back to its corresponding domain name.*



***DHCP (Dynamic Host Configuration Protocol)***

***Definition:***

*DHCP is a protocol used to automatically assign IP addresses and network configuration parameters to devices on a network, eliminating the need for manual configuration.*

***Components of DHCP:***

***DHCP Server:*** *Manages and allocates IP addresses to clients.*

***DHCP Client:*** *The device (e.g., laptop, smartphone) that receives configuration information from the DHCP server.*

***DHCP Relay:*** *Acts as an intermediary between the client and server.*

***IP Address Pool:*** *A range of available IP addresses maintained by the DHCP server.*

***Subnets:*** *Divisions of a larger network to maintain efficient resource allocation.*

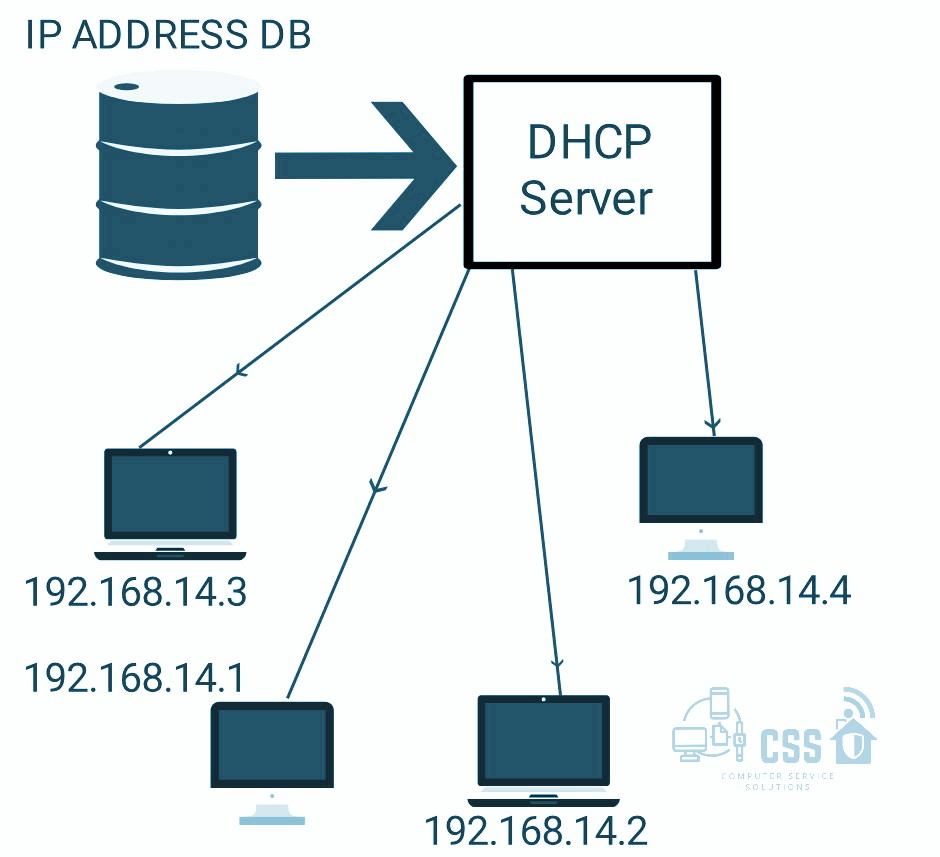
***DHCP Ports:***

*Server Port: 67*

*Client Port: 68*

***Working of DHCP:***

*DHCP operates using the UDP protocol at the application layer, and it dynamically assigns IP addresses from a pool, providing network configuration details to clients.*



***RIP (Routing Information Protocol)***

***Definition:***

*Routing Information Protocol (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance vector routing protocol with an AD (Administrator Distance) value of 120 and operates at the Network layer of the OSI model. RIP uses port number 520.*

***Features of RIP:***

*1. Updates of the network are exchanged periodically.*

*2. Updates (routing information) are always broadcast.*

*3. Full routing tables are sent in updates.*

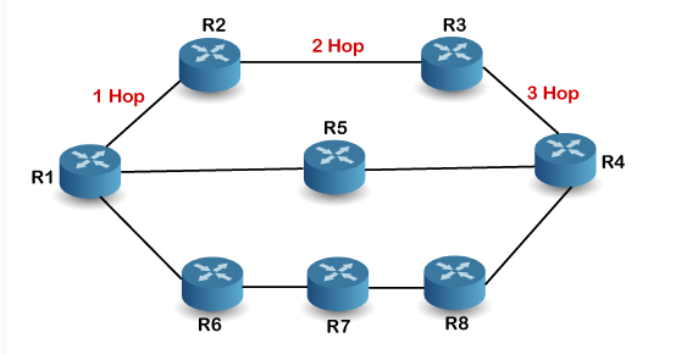
*4. Routers always trust routing information received from neighbor routers. This is also known as Routing on rumors.*

***RIP Versions:***

***RIP v1:*** *Sends update as broadcast; broadcast at 255.255.255.255.*

***RIP v2:*** *Sends update as multicast; multicast at 224.0.0.9; supports authentication of RIPv2 update messages.*

***RIPng:*** *Sends update as multicast; multicast at FF02::9 (only for IPv6 networks).*

**

***IGMP (Internet Group Management Protocol)***

***Definition:***

*IGMP is a protocol used for multicasting communication within IP networks, used by hosts and routers to transmit data packets efficiently. IGMP is mainly used for applications like streaming videos, gaming, and web conferencing.*

***Applications of IGMP:***

***Streaming:*** *Used for audio and video streaming over the network.*

***Gaming:*** *Often used in simulation games with multiple network users, like online games.*

***Web Conferencing:*** *Connects users for video conferencing, efficiently transmitting message/data packets.*

***Working of IGMP:***

*Operates on devices that handle multicast groups, allowing hosts to join/leave the group.*

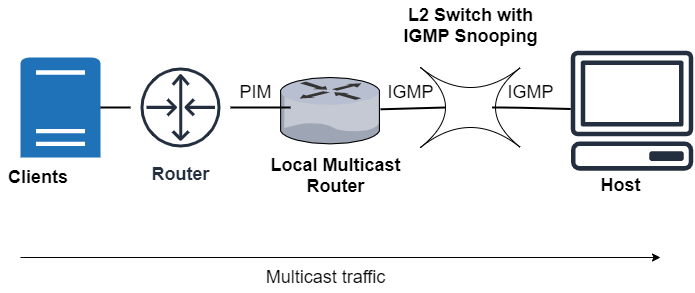
*Uses L2 devices (switches) for IGMP snooping, which monitors IGMP network traffic in a controlled way.*

***IGMP Versions:***

***1. IGMPv1:*** *Basic features allow joining multicast groups; group members leave after a timeout.*

***2. IGMPv2:*** *Allows leaving a multicast group using group membership.*

***3. IGMPv3:*** *Supports source specific multicast and membership report aggregation.*



***IGRP (Interior Gateway Routing Protocol)***

***Definition:***

*IGRP is a proprietary distance vector routing protocol used to exchange routing information among routers within an autonomous system (AS). It updates itself as network changes occur and includes error management to minimize routing loops.*

***Characteristics of IGRP:***

*Created by Cisco; measures bandwidth, delay, reliability, load, and MTU.*

*Send updates every 90 seconds with a hold down time of 280 seconds.*

*Uses an AS number for router communication and a max hop count of 255 (default is 100).*

*IGRP AD value: 100.*

***Goals of IGRP:***

*1. Provide routing information to all routers within its autonomous system.*

*2. Automatically updates when the network topology changes.*

***Advantages:***

*Simple and accurate in route selection.*

*Supports composite metrics and straightforward configuration.*

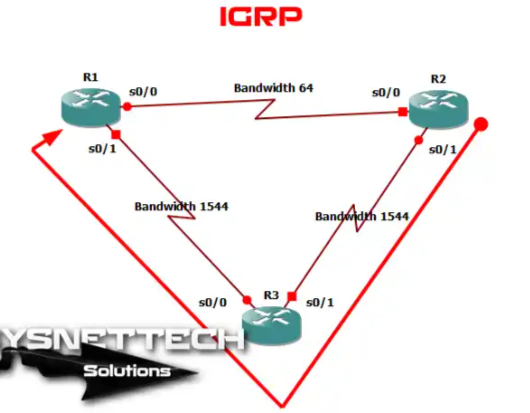
*Offers better scalability than RIP.*

***Disadvantages:***

*Slow convergence on large networks.*

*Cannot measure bandwidth on connections.*

*Doesn’t support multiple pathways for the same route.*

**

***IMAP (Internet Message Access Protocol)***

***Definition:***

*IMAP is an application layer protocol for retrieving emails from a mail server. It allows email synchronization across devices, keeping emails on the server until explicitly deleted.*

***Features of IMAP:***

*Manages multiple mailboxes and organizes them into categories.*

*Adds message flags for tracking.*

*Allow previewing emails before downloading.*

*Supports media download when multiple files are attached.*

***Steps in IMAP Operation:***

*1. An email client (e.g., Outlook) connects to the server via IMAP.*

*2. IMAP shows headers of email; messages are downloaded only when tapped.*

*3. Emails remain on the server until deleted by the user.*

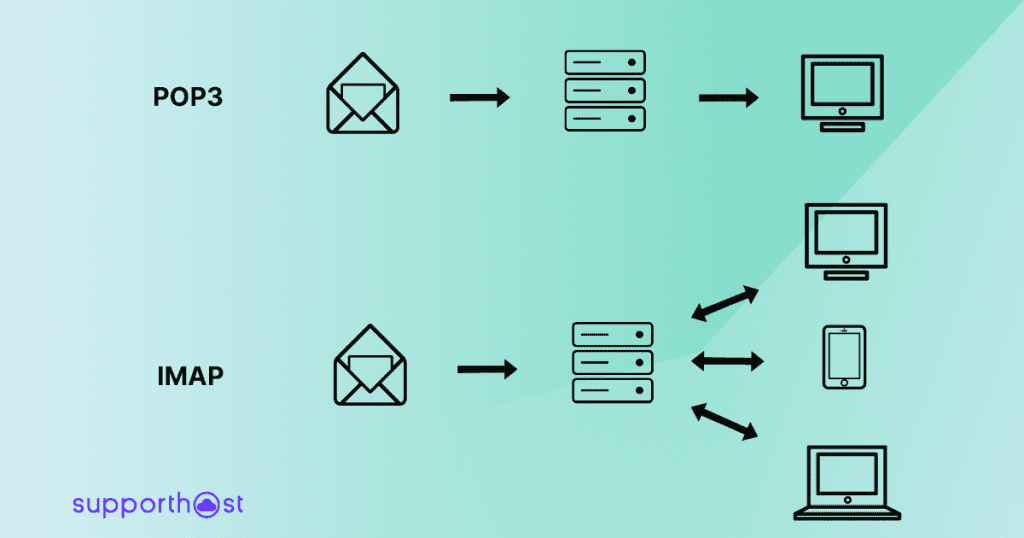
***IMAP and SSL/TLS Ports:***

*IMAP server: Port 143*

*IMAP with SSL: Port 993*

*A screenshot of a computer

Description automatically generated*



***SNMP (Simple Network Management Protocol)***

***Definition:***

*Simple Network Management Protocol (SNMP) is an Internet Standard protocol used for managing and monitoring network connected devices within IP networks. It operates at the application layer and uses UDP ports 161/162. SNMP helps monitor networks, detect faults, and sometimes configure remote devices.*

***Components of SNMP:***

***1. SNMP Manager:*** *A centralized system that monitors the network. The router running the SNMP server is an agent, while the host running the SNMP client is the manager.*

***2. SNMP Agent:*** *A management software module on managed devices, storing network variables (e.g., packet quantities) in a database accessible by the manager.*

***3. Management Information Base (MIB):*** *Consists of resource information, including objects or variables, organized into categories like system, IP, UDP, ICMP, and TCP.*

***Characteristics of SNMP:***

*Monitors networks*

*Detects network faults*

*Configures remote devices*

*Standardized collection of information about all device types*

***Advantages of SNMP:***

*Simple implementation*

*Minimal overhead at agent level*

*Effective manager agent interface*

***Limitations of SNMP:***

*Limited scalability*

*Lacks object oriented data view*

*No standard control definition*

*High communication overhead due to polling*

***BGP (Border Gateway Protocol)***

***Definition:***

*BGP’s main function is to exchange network reachability information between BGP systems, constructing an autonomous systems graph through BGP router exchanges.*

***Characteristics of BGP:***

***Inter Autonomous System Communication:*** *BGP provides communication between two autonomous systems (AS).*

***NextHop Paradigm Support***

***Coordination among BGP Speakers:*** *Allows multiple BGP speakers within an AS to coordinate.*

***Path Information:*** *Contains reachable destinations and next hop information.*

***Policy Support:*** *Administrators can configure policies (e.g., distinguishing routes within vs. outside AS).*

***TCP Based:*** *Operates over TCP.*

***Bandwidth Conservation***

***CIDR Support***

***Security Features***

***Functionality of BGP:***

***1. Peer Acquisition & Authentication:*** *Establishes a TCP connection and authenticates both peers.*

***2. Reachability Information Exchange:*** *Sends positive or negative reachability information.*

***3. Connection Verification:*** *Ensures peers and connections are functioning correctly.*

***Importance of BGP:***

***Security:*** *Authenticates messages between routers.*

***Scalability:*** *Manages numerous routes and networks on the internet.*

***Supports Multihoming:*** *Allows connections to multiple networks simultaneously.*

***Best Path Calculation:*** *Determines the next step for data packets en route from source to destination.*

***TCP/IP Model Integration:*** *Operates at the network layer, controlled by transport layer protocol.*

*A screen shot of a black screen

Description automatically generated*

***Routing***

***Definition:***

*Routing is the process of finding paths within a network for sending data packets from source to destination, optimizing resource use and maintaining communication consistency. Routers, operating at the network layer (OSI model) or internet layer (TCP/IP model), forward packets based on header and forwarding table information.*

***Types of Routing:***

***1. Static Routing:*** *Administrator manually sets routes at the routing table.*

***Advantages:*** *No CPU overhead, minimal bandwidth usage, higher security.*

***Disadvantages:*** *Difficult for large networks; requires knowledge of network topology.*

***2. Default Routing:*** *Configures a router to send packets to a designated nexthop device regardless of the destination network.*

*Used for networks with a single exit point.*

***3. Dynamic Routing:*** *Routes are automatically added to the routing table in response to network condition changes.*

*Examples: RIP, OSPF protocols.*

***Advantages:*** *Easier configuration, adaptive to network changes.*

***Disadvantages:*** *Higher CPU and bandwidth usage, less secure than static routing.*

***Routing Algorithms:***

***Distance Vector Routing:*** *Uses Bellman Ford algorithm, where routers share routing tables with immediate neighbors. Challenges include count to infinity and routing loops.*

***Link State Routing:*** *Routers maintain global network knowledge and broadcast link state information across the network. Dijkstra’s Algorithm calculates the shortest paths.*

***Flooding***

***Definition:***

*Flooding is a network communication method where data packets are sent to all devices on the network, even if they aren’t the target recipients.*

***Flooding Steps:***

***1. Sending Data:*** *Device creates a packet when unsure of the recipient’s address.*

***2. Broadcasting:*** *Packet is sent to all devices in the network.*

***3. Packet Inspection:*** *Each device checks the destination address in the header.*

***4. Filtering:*** *Devices discard packets if the destination doesn’t match; the correct device accepts it.*

***5. Loop Prevention:*** *TTL (Time to Live) counters prevent packets from looping indefinitely by decrementing with each hop, discarding packets when TTL reaches zero.*

***Advantages:***

*Simple setup, robustness, and ensures all network nodes are reached.*

*Always select the shortest path.*

***Limitations:***

*Generates duplicate packets and clogs network with excess traffic.*

*Wasteful for single destination packet transmissions.*

***OSPF (Open Shortest Path First)***

***Definition:***

*OSPF is an IP routing protocol that calculates efficient paths for IP traffic within a single autonomous system (AS) using a link state routing algorithm. Each router holds a full network topology and uses Dijkstra's algorithm to determine the shortest paths.*

***Process:***

***1. LSA (Link State Advertisement) Exchanges:*** *Routers exchange LSAs containing information about routers, subnets, and links.*

***2. LSDB (Link State Database):*** *Routers store received LSA information in the LSDB.*

***3. Shortest Path Calculation:*** *OSPF computes the shortest path for all routers in the AS area.*

***Types of LSAs:***

***1. Type 1 – Router LSA:*** *Generated by each router for its area.*

***2. Type 2 – Network LSA:*** *Generated by the Designated Router (DR).*

***3. Type 3 – Summary LSA:*** *Created by Area Border Routers (ABRs) and shared across areas.*

***4. Type 4 – Summary ASBR LSA:*** *Used to advertise the location of the AS Boundary Router (ASBR).*

***5. Type 5 – External LSA:*** *Generated by the ASBR to advertise external network routes.*

***6. Type 6 – Multicast LSA:*** *Not supported in OSPF.*

***7. Type 7 – NSSA LSA:*** *Used in NSSA areas that don’t accept external LSAs (Type 5); substitutes with Type 7 LSAs.*