CASE STUDY REPORT ON
LAYER 7 (APPLICATION LAYER) PROTOCOLS

Selected Protocols: HTTP / HTTPS, FTP, SMTP, DNS, DHCP, POP3

SUBMISSION DETAILS

Course: *Computer Networks*
Assignment Type: *Case Study (Group of 2)*
Submitted To*: Dr. Vasundhara Rathod*
Academic Year: *2025–2026*

SUBMITTED BY

Shreya Thakur (BT23CSE221)
Ananya Singh (BT23CSE220)

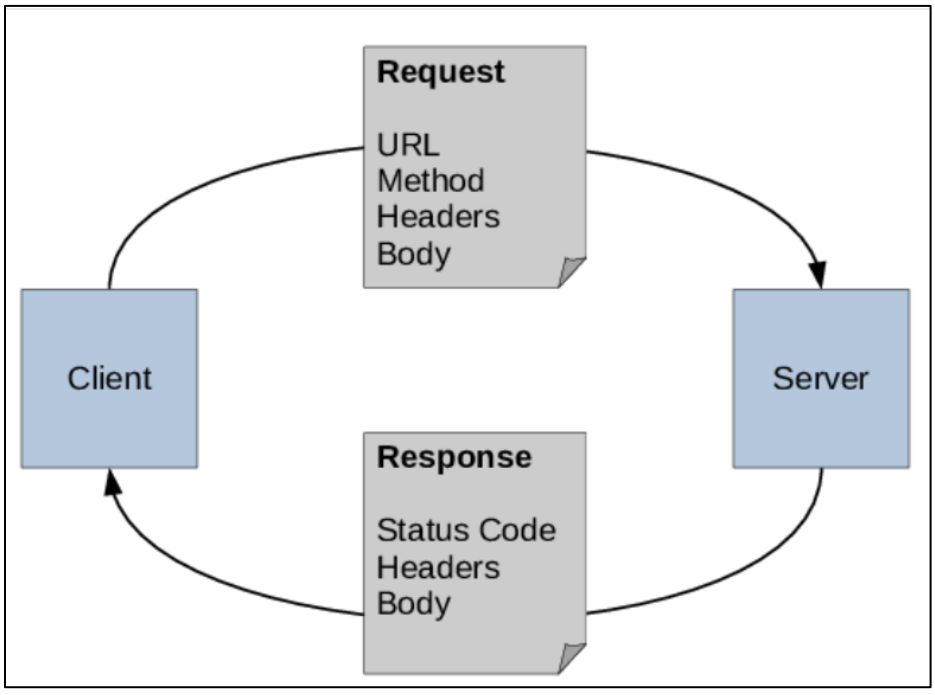
HTTP / HTTPS

Introduction & Working Principle

- **HTTP (Hypertext Transfer Protocol):**
  HTTP is an application-layer protocol used for transmitting hypertext (web pages) between a web client (browser) and a web server. It defines how messages are formatted and transmitted, and how servers and browsers should respond to various commands.
  Example: When you type a URL like `http://example.com`, your browser uses HTTP to request and receive the web page.

- **HTTPS (Hypertext Transfer Protocol Secure):**
  HTTPS is the secure version of HTTP, which uses SSL/TLS (Secure Sockets Layer / Transport Layer Security) to encrypt data transmitted between the client and server. It ensures confidentiality, integrity, and authentication of the communication.

Flowchart



Real-World Case Study

- **HTTP Case Study:**
  Earlier versions of websites like Wikipedia and small news blogs operated using HTTP. When users visited pages such as `http://example.com`, their browsers communicated with servers in plain text. This made it easy to access public information quickly, but also left data like login credentials and cookies vulnerable to interception. HTTP worked efficiently for non-sensitive data but lacked encryption, making it insecure for modern applications.
- **HTTPS Case Study:**
  Modern platforms like Amazon and HDFC Bank use HTTPS to ensure secure communication. When a user connects to `https://www.amazon.in`, the browser and server perform an SSL/TLS handshake, verifying the site's authenticity and encrypting all transmitted data. This protects sensitive information such as passwords and payment details from hackers. HTTPS has become essential for online transactions, providing confidentiality, data integrity, and trust, which are crucial for e-commerce, banking, and secure user interactions.

Advantages & Limitations

HTTP

ADVANTAGE:

- Faster performance – No encryption overhead, so data transfer is quick.
- Easy implementation – Simple protocol supported by all browsers and servers.

DISADVANTAGE:

- Insecure – Data is sent in plain text, making it vulnerable to interception.
- No authentication – Cannot verify if the server is genuine, enabling phishing attacks.

HTTPS

ADVANTAGE:

- Secure communication – Encrypts data, protecting user information from attackers.
- Trust and SEO benefits – Displays a lock icon and improves website ranking.

DISADVANTAGE:

- Slightly slower – Encryption and decryption add processing overhead.
- Certificate cost and management – Requires purchasing and renewing SSL/TLS certificates.

COMPARISION

FEATURE	HTTP	HTTPS
Port Number	80	443
Security	Unsecured	Encrypted using SSL/TSL
Certificate Requirement	Not Required	Requires certificate
Speed	Slightly faster	Slightly slower

FTP(FILE TRANSFER PROTOCOL)

Introduction & Working Principle

Purpose:

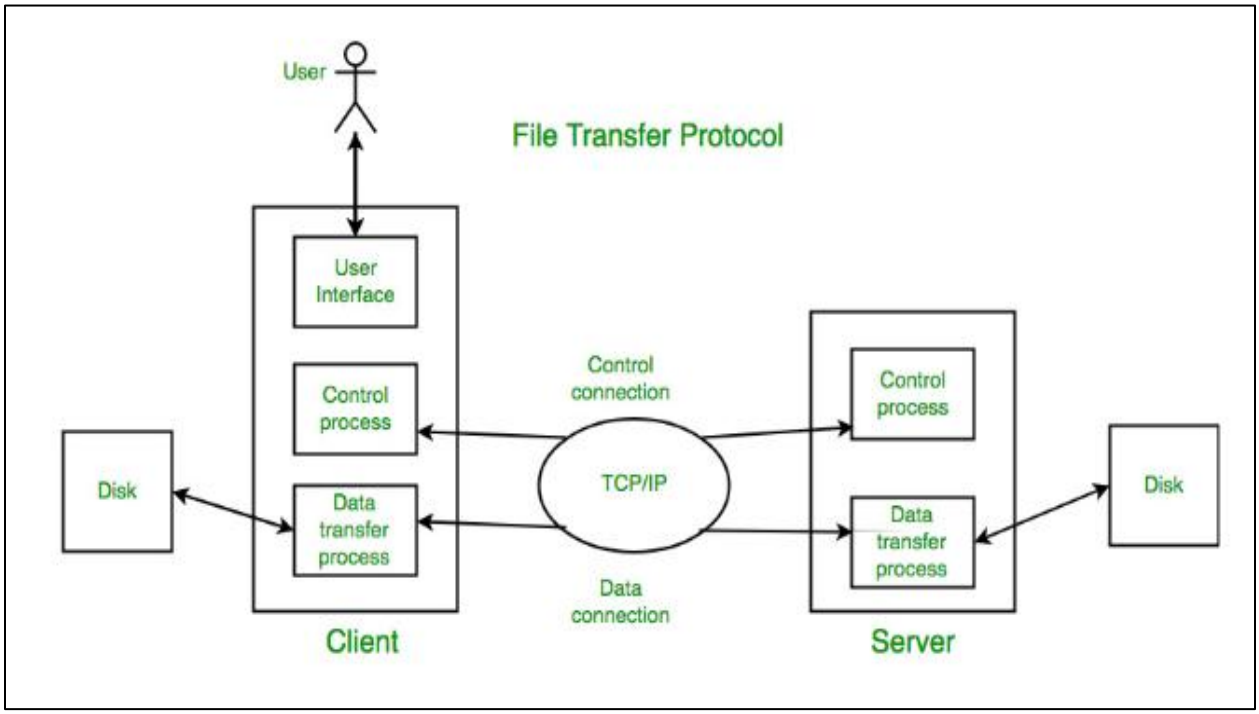
FTP (File Transfer Protocol) is an **application-layer protocol** used to **transfer files** between a **client** and a **server** over a network. It enables users to upload, download, rename, or delete files on remote servers.

Working Principle:

FTP operates on a client–server model using two channels:

1. Command Channel (Port 21): For sending commands and responses.
2. Data Channel (Port 20): For transferring actual file data.

Flowchart



Real-World Case Study

Case Study:

Web Hosting Services (e.g., FileZilla with GoDaddy or Hostinger)

Web developers commonly use **FTP** to upload website files (HTML, CSS, images) from their local system to a **web server**. Using FTP clients like **FileZilla**, they connect to hosting servers with FTP credentials (host, username, password).

Role of FTP:

- Allows quick and direct file management on remote servers.
- Supports uploading website updates without logging into the hosting control panel.

ADVANTAGE:

1. Efficient file transfer – Handles large files faster than HTTP.
2. Supports resume and batch transfer – Interrupted downloads can be resumed.

LIMITATIONS :

1. Lack of security – Data and credentials are transmitted in plain text.
2. Requires manual setup – Needs configuration and client software for access.

COMPARISON

FEATURE	FTP	SFTP
Port Number	20 and 21	22
Security	No Security	Security via ssh
Use case	Simple file transfer	Secured file tranfer
Speed	Faster	Slightly Slower

SMTP (SIMPLE MAIL TRANSFER PROTOCOL)

Introduction & Working Principle

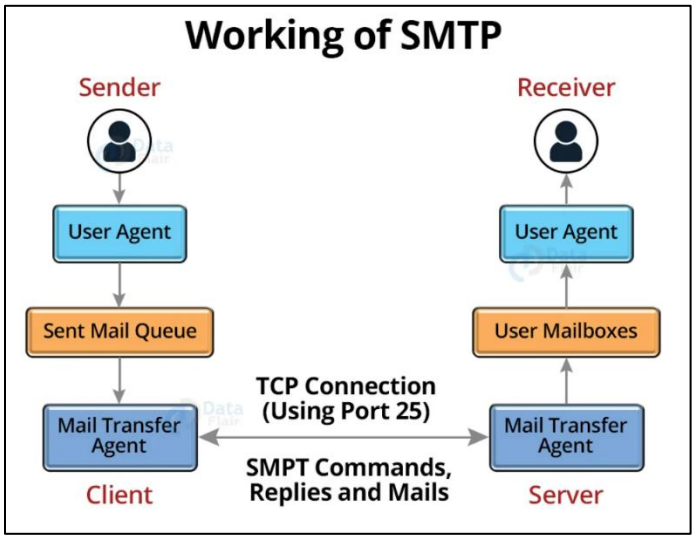
Purpose:

SMTP (Simple Mail Transfer Protocol) is an **application-layer protocol** used for **sending and routing emails** between mail servers. It defines how email messages are formatted, transmitted, and relayed across networks.

Working Principle:

- SMTP works on a client–server model using port 25 (or 587 for secure transmission).
- When a user sends an email, the SMTP client (like Gmail or Outlook) connects to the SMTP server and transmits the message.
- The server forwards the message to the recipient's mail server using the DNS MX (Mail Exchange) record.
- The recipient retrieves the email later using POP3 or IMAP.

Flowchart



Real-World Case Study

Case Study:

Gmail Email Transmission System

When a user sends an email via Gmail, SMTP is responsible for delivering that message to the recipient's mail server. For example, when sending a message from Gmail to Yahoo, Gmail's SMTP server (`smtp.gmail.com`) connects to Yahoo's mail server using DNS lookup and transfers the email securely.

Role of SMTP:

- Handles the outgoing mail delivery process.
- Ensures messages reach the correct mail server.
- Works with TLS encryption in modern systems for secure transmission.

Advantages & Limitations

Advantages:

1. Reliable delivery – Ensures email messages are sent to the correct server.
2. Widely supported – Works with all major email clients and servers.

Disadvantages:

1. No built-in encryption – Standard SMTP transmits data in plain text.
2. Spam vulnerability – Can be misused for sending unsolicited emails.

COMPARISON

FEATURE	SMTP	POP3
FULL FORM	Simple Mail Transfer Protocol	Post Office Protocol v3

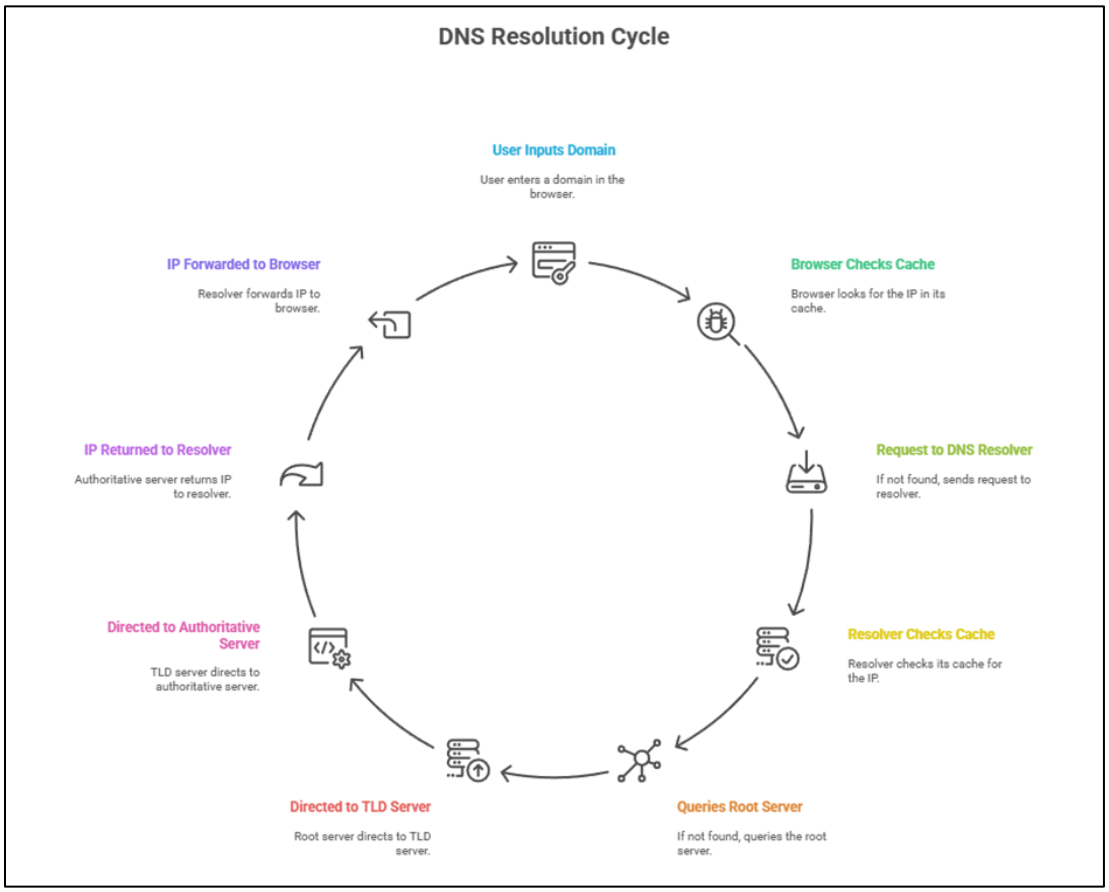
PORT	25/587	110
PURPOSE	Sending/Forwarding emails	Recieving emails
DIRECTION	Outgoing Emails	Incoming Emails

DNS (DOMAIN NAME SYSTEM)

Introduction & Working Principle

The Domain Name System (DNS) protocol serves as the internet's directory service, converting human-readable domain names (like www.example.com) into machine-readable IP addresses (e.g., 192.0.2.1). When a user enters a domain in their browser, DNS enables connecting to the appropriate web server without needing to remember numeric addresses. It operates at the application layer, using a hierarchical, distributed architecture of DNS servers (root, TLD, authoritative). DNS queries first check a local cache, then are resolved recursively through several tiers—root, TLD, authoritative—until the correct IP address is returned to the client.

DNS Resolution Flow



Real-World Case Study

Enterprise Network Performance:

A large enterprise's virtualization infrastructure suffered lag due to DNS issues. DNS monitoring revealed excessive failed lookups (NXDOMAIN errors) and abnormal reverse lookup activity. Analysis pinpointed excessive DNS and local multicast queries as the root cause. Utilizing DNS analytics tools improved troubleshooting, performance, and security posture for thousands of users.

Advantages & Limitations

Advantages:

- Eliminates need to remember IP addresses; human-friendly.
- Streamlines browsing and updates records dynamically.
- Essential for web, email, Active Directory, etc.
- Caching speeds up responses and reduces query load.

Limitations:

- Vulnerable to DNS spoofing, DDoS, cache poisoning, and privacy leaks; queries can be intercepted if not encrypted.
- Performance may degrade under heavy traffic or misconfiguration.
- Complexity in large-scale deployments; mismanagement can cause resolution failures.
- Partial reliance on centralized/global authorities (ICANN).

Comparative Analysis: DNS vs. Hosts File

Feature	**DNS**	**Hosts File**

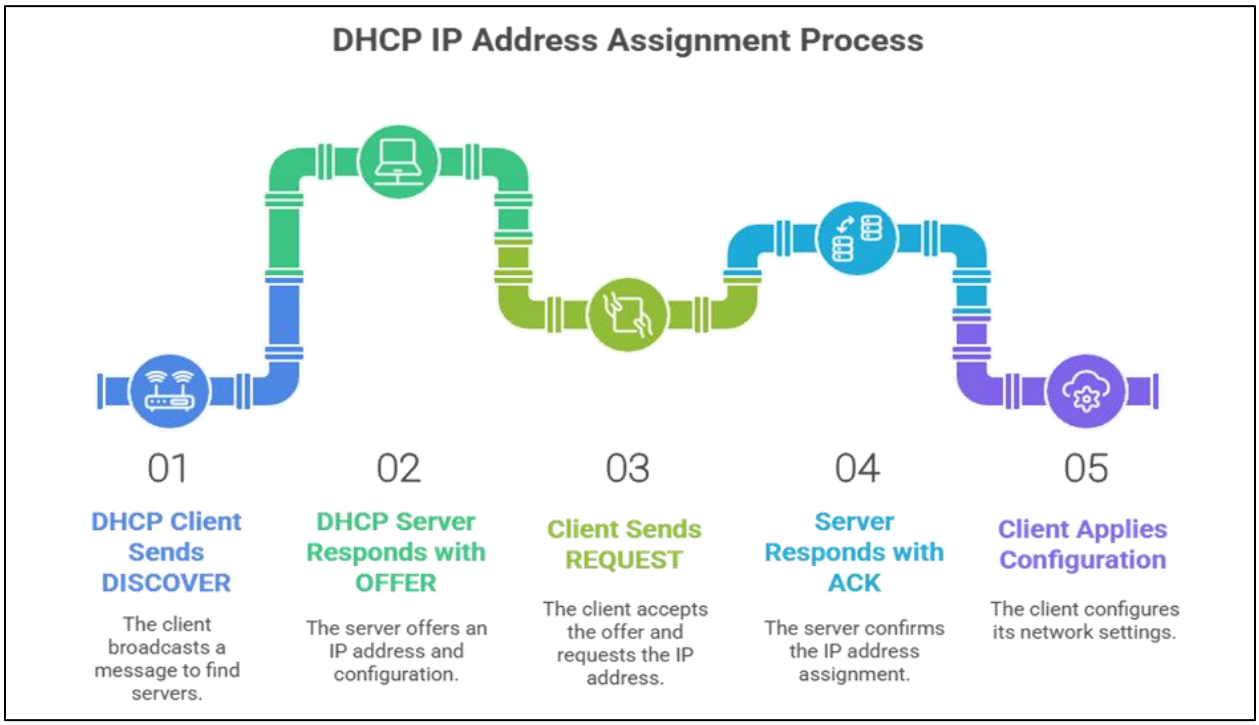
Scope	Global, hierarchical, scalable	Local, device-specific
Management	Centralized, dynamic	Manual, static
Use Case	Internet/App-wide name resolution	Testing, overrides, small networks
Updates	Propagated over network automatically	Manual edits required
Speed	Fast (w/ caching), but multi-step lookup	Fast at device level
Security	Vulnerable to poisoning/interceptions	No remote attacks; local risks

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

Introduction & Working Principle

DHCP is a client-server protocol at the application layer, automating IP address assignment and network configuration for devices on a network. It removes manual configuration hassles, especially in large, dynamic environments. When a device joins a network, the DHCP process (DORA) is initiated: Discover (client broadcast), Offer (server response), Request (client asks for offered address), Acknowledge (server finalizes assignment). Configuration may include subnet mask, gateway, and DNS addresses.

DHCP IP Assignment Flowchart



Real-World Case Study

Corporate Networks & Data Centers:

DHCP is critical in environments with many clients, such as enterprises and ISPs. For example, Wi-Fi networks serving tens of thousands of users automate handle address

leases and configuration. In large universities or virtual data centers, DHCP manages addressing for massive fleets of devices and virtual machines, significantly reducing manual errors and overhead.

Advantages & Limitations

Advantages:

- Minimizes manual configuration errors and administrative effort.
- Centralized and scalable management of network settings.
- Efficiently handles mobile or transient clients (e.g., guests, IoT, BYOD).
- Supports dynamic network changes, facilitating device mobility.

Limitations:

- Single-point-of-failure (if only one server); network outage risks if server fails.
- Security vulnerabilities: unauthorized clients/servers, address spoofing.
- DHCP traffic doesn't cross routers unless relay is configured.
- Static IP is preferable for servers, printers, and infrastructure needing fixed addresses.

Comparative Analysis: DHCP vs Static IP Assignment

Feature	**DHCP**	**Static IP**
Configuration	Automatic	Manual
Scalability	High (suits large environments)	Low (practical for small setups)

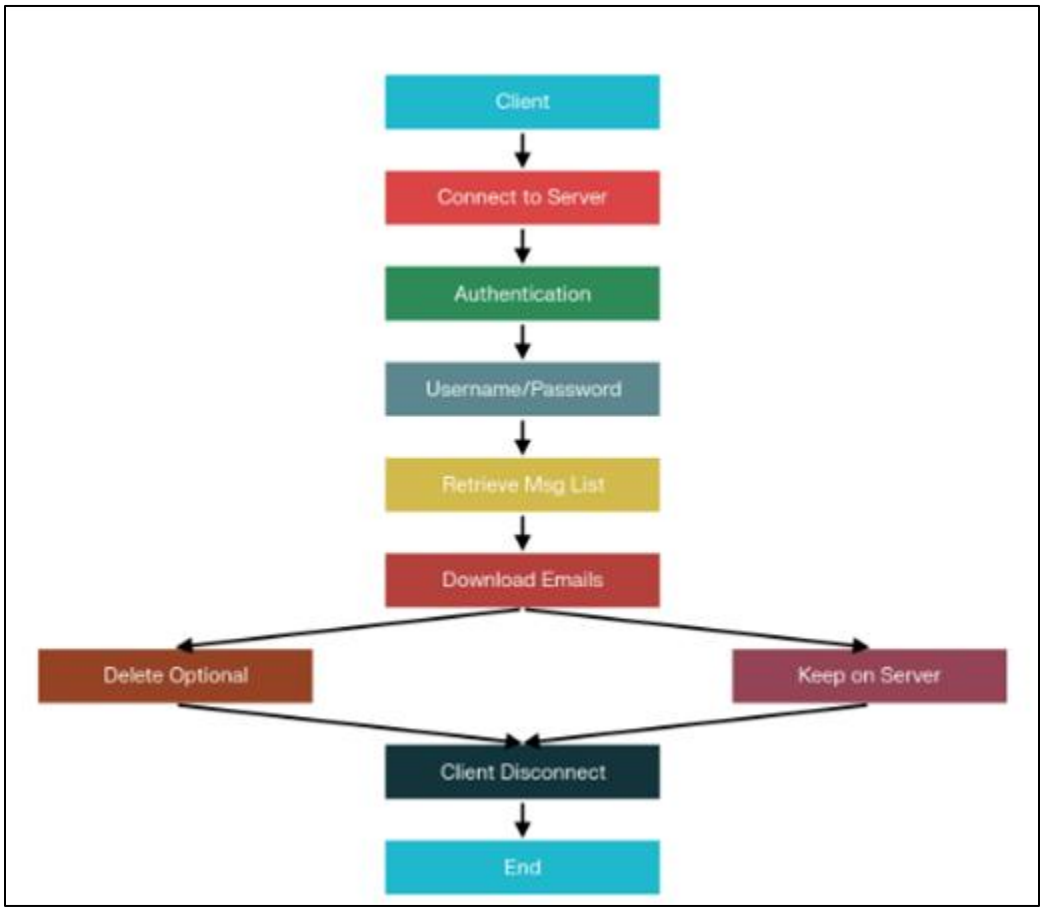
Management	Centralized, less error-prone	Per-device; risk of duplicates
Flexibility	Supports mobile devices	Devices remain at fixed IP
Use Case	LANs/WLANs, corporate, cloud	Servers, printers, access points
Security	Relies on server/authentication	More predictable, requires upkeep

POP3 (POST OFFICE PROTOCOL V3)

Introduction & Working Principle

POP3 is an email retrieval protocol at the application layer. It enables an email client to connect to a mail server, download emails, and manage (delete/read) them locally. Typically, emails are downloaded to the client device and deleted from the server, making them available offline but not synchronized across multiple devices. Sessions consist of connection, authentication, transaction (retrieval), optional deletion, and disconnection sequences.

POP3 Workflow Diagram



Real-World Case Study

Remote/Intermittent Access:

POP3 is often used in rural, remote, or bandwidth-constrained environments, enabling users to download emails for offline reading. For instance, users configuring Gmail for POP3 can read and manage mail offline, which is useful for business travelers or areas with unstable internet.

Advantages & Limitations

Advantages:

- Offline access: Emails are available after download—no live internet required.
- Simplicity: Easy to set up, less resource-intensive on servers.
- Server storage is freed post-download; good for users with storage limits.

Limitations:

- No multi-device synchronization: Actions on one device do not reflect elsewhere.
- Security concerns: Limited encryption in standard POP3; credentials can be intercepted if not using SSL/TLS.
- Risk of data loss if client device is damaged and messages were deleted from server.
- Does not support server-side folder management or advanced features (unlike IMAP).

Comparative Analysis: POP3 vs. IMAP

Feature	**POP3**	**IMAP**
Storage	Downloads; removes from server	Emails remain on server, sync devices

Synchronization	No	Yes, all devices remain in sync
Offline Access	Yes (after download)	Partial (headers, not full emails)
Multi-device Support	Poor	Excellent
Folder Management	Local only	Server and local
Security	SSL/TLS only where configured	SSL/TLS, better encryption options
Best Use-case	Single device, intermittent internet	Multi-device, constant connectivity

REFERENCES

1. Bhushan, "File transfer protocol," Introduction, Apr. 16, 1971.
2. J. C. R. Licklider, "Licklider networking ideas," Early research and development, 1960–1962.
3. R. J. Droms, "Dynamic host configuration protocol," 1997.
4. K. W. Ross, J. F. Kurose, and M. W. Ross, *Computer Networking: A Top-Down Approach*, 8th ed. New York, NY, USA: Pearson, 2021.
5. S. Sunder, “HTTP vs HTTPS: Understanding the Difference and Importance of Secure Communication,” Apr. 04, 2024.
6. V. V. Riabov, “SMTP (Simple Mail Transfer Protocol),” Handbook of Computer Networks, pp. 388–406, Nov. 2007, doi:
7. M. Dooley and T. Rooney, “Introduction to the Domain Name System (DNS),” IEEE Xplore, 2017.
8. Mayank Kumar Tiwari et al., “The Comprehensive Review: Internet Protocol (IP) Address a Primer for Digital Connectivity,” Asian Journal of Research in Computer Science, vol. 17, no. 8, pp. 34–45, Jul.