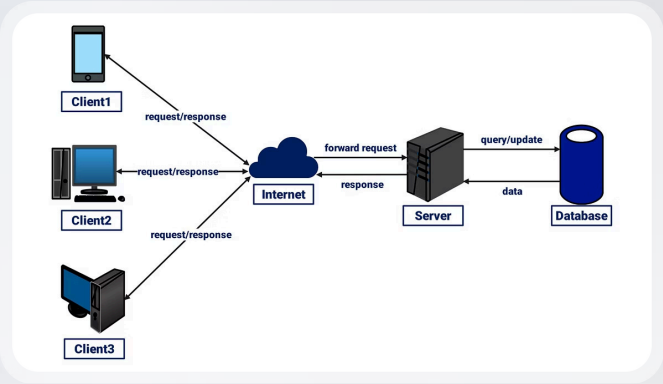
Networking Core Protocols: FTP, SMTP, POP3, and IMAP

This presentation explores four essential networking protocols that enable file transfers and email communications. We'll examine how these protocols work, their commands, and see real-world examples of their implementation.



File Transfer Protocol (FTP)

Purpose

Designed specifically for efficient file transfer between clients and servers

More efficient than HTTP for file transfers under equal conditions

Key Commands

- USER - Input username
- PASS - Enter password
- RETR - Download file from server
- STOR - Upload file to server

Technical Details

Listens on TCP port 21 by default

Data transfer conducted via separate connection

FTP in Action: Terminal Example

```
user@terminal$ ftp MACHINE_IP
Connected to MACHINE_IP (MACHINE_IP).
220 (vsFTPd 3.0.5)
Name (MACHINE_IP:strategos): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (10,10,41,192,134,10).
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 1480 Jun 27 08:03 coffee.txt
-rw-r--r-- 1 0 0 14 Jun 27 08:04 flag.txt
-rw-r--r-- 1 0 0 1595 Jun 27 08:05 tea.txt
226 Directory send OK.
ftp> type ascii
200 Switching to ASCII mode.
ftp> get coffee.txt
local: coffee.txt remote: coffee.txt
227 Entering Passive Mode (10,10,41,192,57,100).
ftp> quit
221 Goodbye.
```

Note: When using Wireshark, client messages appear in red, server responses in blue. Commands may differ between client and server (e.g., "ls" becomes "LIST").

Simple Mail Transfer Protocol (SMTP)

Purpose

Defines how mail clients communicate with mail servers and how mail servers communicate with each other

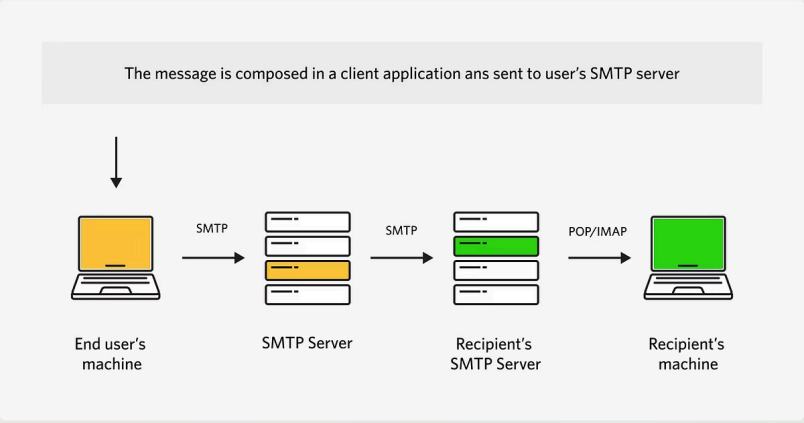
Similar to visiting a post office to send a package

Technical Details

Listens on TCP port 25 by default

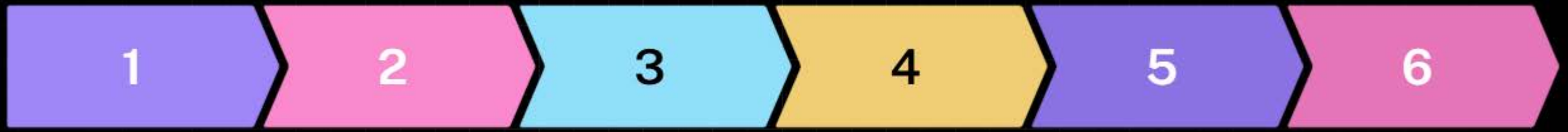
Key Commands

- HELO/EHLO - Initiates SMTP session
- MAIL FROM - Specifies sender's email
- RCPT TO - Specifies recipient's email
- DATA - Begins email content
- . (period) - Ends email message



Illustrative Example of an SMTP Session Using Telnet

Step-by-step SMTP commands demonstrating email transmission using Telnet protocol



Initiating an SMTP session via Telnet.

The session starts with the Telnet command directed at the SMTP server's IP address, establishing a connection for email transmission.

Server greeting message received.

Upon connection, the server responds with a greeting message indicating its name and capabilities, confirming a successful connection.

Sending HELO command to identify client.

The client sends the HELO command to introduce itself to the server, which is acknowledged with a positive response from the server.

Specifying the sender's email address.

The MAIL FROM command is issued to inform the server of the sender's email address, leading to an acknowledgment from the server.

Identifying the recipient's email address.

The RCPT TO command follows, specifying the intended recipient's email address, which is also accepted by the server.

Sending the email content.

The DATA command initiates the email content transmission, concluding with a period on a separate line to signal completion, leading to a successful delivery response.

SMTP in Action: Sending Email via Telnet

```
user@terminal$ telnet MACHINE_IP 25
Trying MACHINE_IP...
Connected to MACHINE_IP.
220 example.thm ESMTP Exim 4.95 Ubuntu Thu, 27 Jun 2024 16:18:09 +0000
HELO client.thm
250 example.thm Hello client.thm [10.11.81.126]
MAIL FROM: user@client.thm
250 OK
RCPT TO: strategos@server.thm
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
From: user@client.thm
To: strategos@server.thm
Subject: Telnet email

Hello. I am using telnet to send you an email!
.
250 OK id=1sMrpq-0001Ah-UT
QUIT
221 example.thm closing connection
Connection closed by foreign host.
```

While cumbersome, using telnet helps understand the commands your email client issues behind the scenes.

Post Office Protocol version 3 (POP3)

Purpose

Allows clients to retrieve email messages from mail servers

Similar to checking your mailbox for new letters

Workflow

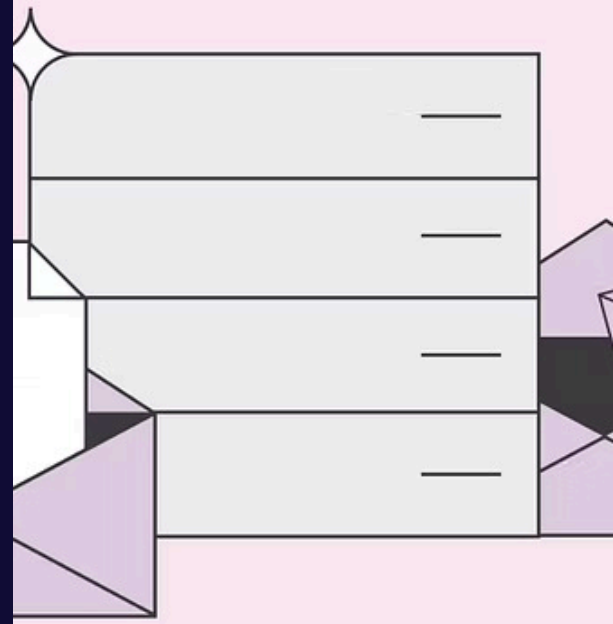
Email clients send messages via SMTP

Email clients retrieve messages via POP3

Technical Details

Listens on TCP port 110 by default

Typically downloads and deletes messages from server



POP3 Key Commands

Authentication

- USER - Identifies the user
- PASS - Provides user's password

Message Management

- STAT - Requests number of messages and total size
- LIST - Lists all messages and their sizes

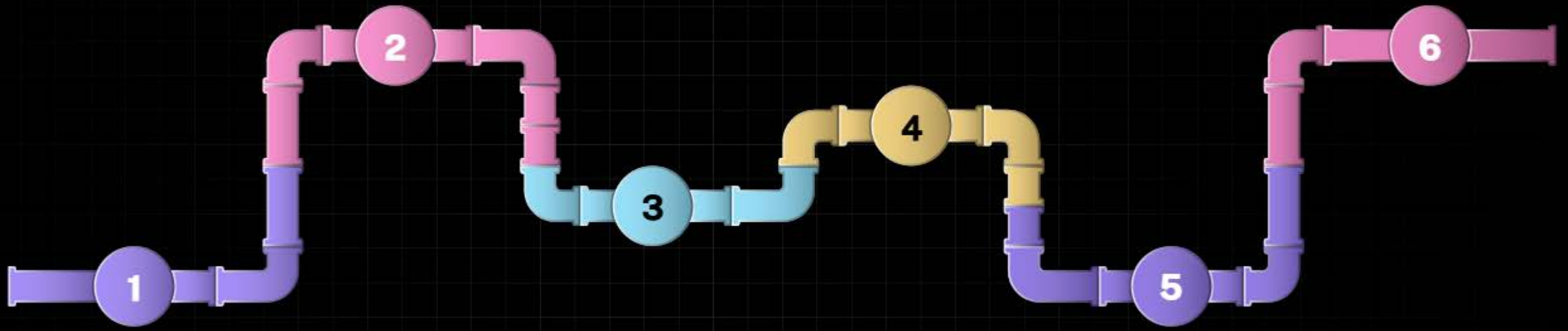
Message Actions

- RETR - Retrieves specified message
- DELE - Marks message for deletion
- QUIT - Ends session, applies changes

⊗ Security Note: POP3 traffic can be intercepted, including passwords, as shown in Wireshark captures.

Understanding POP3 Commands in Email Retrieval

Exploring the mechanics of a POP3 email session using Telnet



Initiating a connection

The session begins by connecting to the server via Telnet on port 110.

Authentication process

User authentication is performed using the USER and PASS commands.

Checking mailbox status

The STAT command retrieves the number of messages and total size in bytes.

Listing messages

The LIST command provides details on all messages in the mailbox.

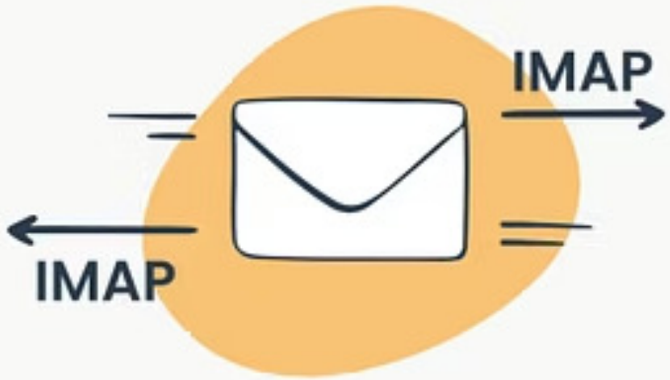
Retrieving a message

RETR command allows the user to download a specific email message.

Ending the session

The QUIT command logs out of the session and closes the connection.

Internet Message Access Protocol (IMAP)



Purpose

Allows synchronization of messages across multiple devices

Ideal when checking email from multiple clients (desktop, laptop, smartphone)

Compared to POP3

- Keeps email on server (vs. POP3 downloading and deleting)
- Synchronizes read, moved, and deleted messages
- Uses more server storage

Key Commands

- LOGIN - Authenticates the user
- SELECT - Selects mailbox folder
- FETCH - Retrieves messages (e.g., "fetch 3 body[]")
- MOVE - Moves messages to another mailbox
- COPY - Copies messages to another mailbox
- LOGOUT - Logs out

Technical Detail: Listens on TCP port 143 by default

Understanding IMAP: Synchronizing Email Across Devices

An Overview of Internet Message Access Protocol and Its Key Commands

IMAP enables message synchronization

Keeps emails accessible on multiple devices.

Essential IMAP commands

Key commands for email management.

LOGIN command for authentication

Authenticates user access to mail.

FETCH command retrieves messages

Fetches specific email content.

IMAP in Action: Terminal Example

```
user@terminal$ telnet 10.10.41.192 143
Trying 10.10.41.192...
Connected to 10.10.41.192.
* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+ STARTTLS AUTH=PLAIN] Dovecot (Ubuntu) ready.
A LOGIN strategos
A OK [CAPABILITY IMAP4rev1...] Logged in
B SELECT inbox
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* 4 EXISTS
* 0 RECENT
* OK [UNSEEN 2] First unseen.
B OK [READ-WRITE] Select completed (0.001 + 0.000 secs).
C FETCH 3 body[]
* 3 FETCH (BODY[] {445}
Return-path: user@client.thm
From: user@client.thm
To: strategos@server.thm
Subject: Telnet email

Hello. I am using telnet to send you an email!
)
C OK Fetch completed (0.001 + 0.000 secs).
D LOGOUT
* BYE Logging out
D OK Logout completed (0.001 + 0.000 secs).
Connection closed by foreign host.
```

Protocol Comparison: Key Takeaways

FTP

Optimized for file transfers

Uses separate connections for commands and data

TCP port 21

SMTP

Sends email messages

Used by clients to submit mail and servers to relay

TCP port 25

POP3

Downloads email from server

Typically deletes messages after retrieval

TCP port 110

IMAP

Synchronizes email across devices

Keeps messages on server

TCP port 143

Understanding these protocols is essential for network administrators and security professionals to properly configure and secure email and file transfer services.