SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ARTIFICIAL INTELIGENCE & MACHINE LEARNING

23AMT302- COMPUTER NETWORK AND SECURITY

UNIT 1 – Introduction and Application layer

Prepared by
A.catherine
AP/AIML

Simple Mail Transfer Protocol (SMTP): The Backbone of Email

What is SMTP?

Application Layer Protocol

SMTP is an application layer protocol. It is specifically designed for email transmission.

Standardised Transmission

It provides a standardised way for mail servers to send and receive email.

Internet Protocol Suite

SMTP forms a key part of the Internet Protocol Suite (TCP/IP).

Establishes Communication

The protocol establishes communication channels between mail servers.

How SMTP Works

1

Client-Server Model

SMTP operates on a client-server model for mail exchange.

2

MUA to MSA Connection

A Mail User Agent (MUA) connects to a Mail Submission Agent (MSA).

3

MSA to MTA Transfer

The MSA then forwards the email to a Mail Transfer Agent (MTA).

4

MTA Relay to Recipient

The sender's MTA relays the email to the recipient's MTA.

5

Port Usage

It uses TCP ports 25 (legacy), 587 (submission), or 465 (SMTPS).

Core SMTP Commands and Responses

Initiation

HELO/EHLO: Initiates communication and identifies the sender.

MAIL FROM: Specifies the sender's email address.

RCPT TO: Specifies the recipient's email address.

Content & End

DATA: This command starts the transmission of email content.

QUIT: Ends the current SMTP session cleanly.

Success Codes

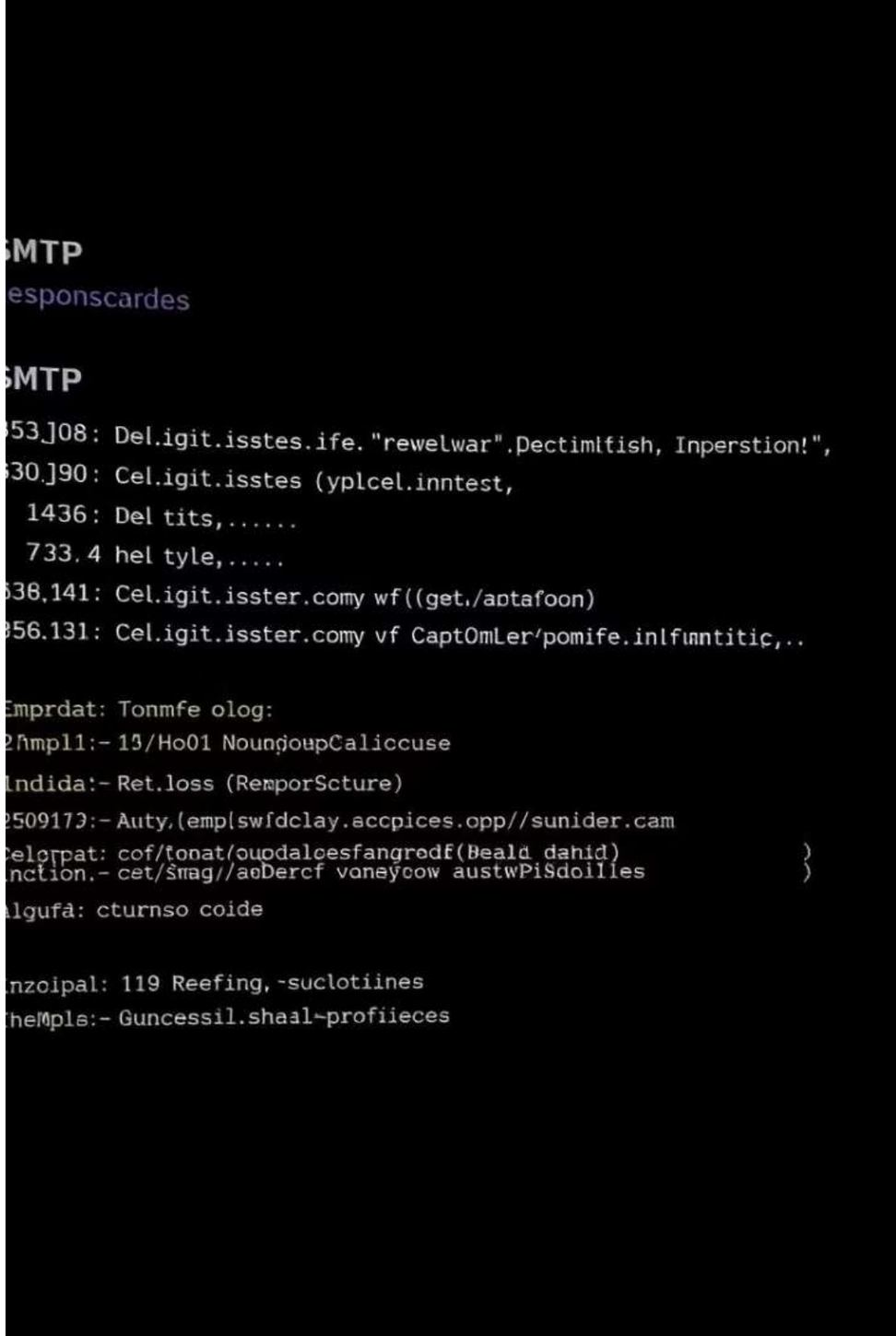
2xx Codes: Indicate successful operations (e.g., 250 OK).

3xx Codes: Signify intermediate success, requiring more input (e.g., 354 Start mail input).

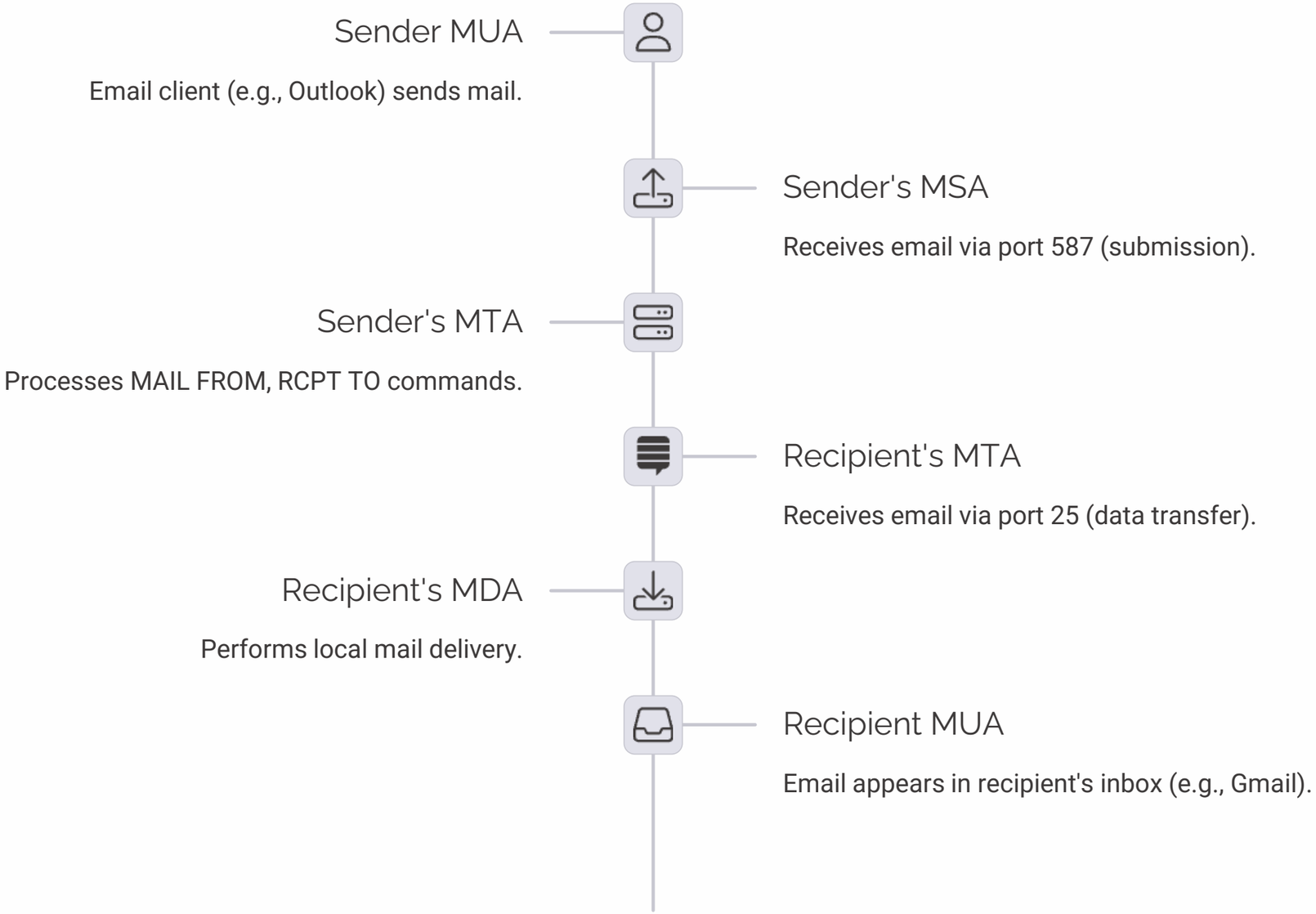
Failure Codes

4xx Codes: Represent transient failures; try again later (e.g., 451 Action aborted).

5xx Codes: Indicate permanent failures; action cannot be completed (e.g., 550 Mailbox unavailable).

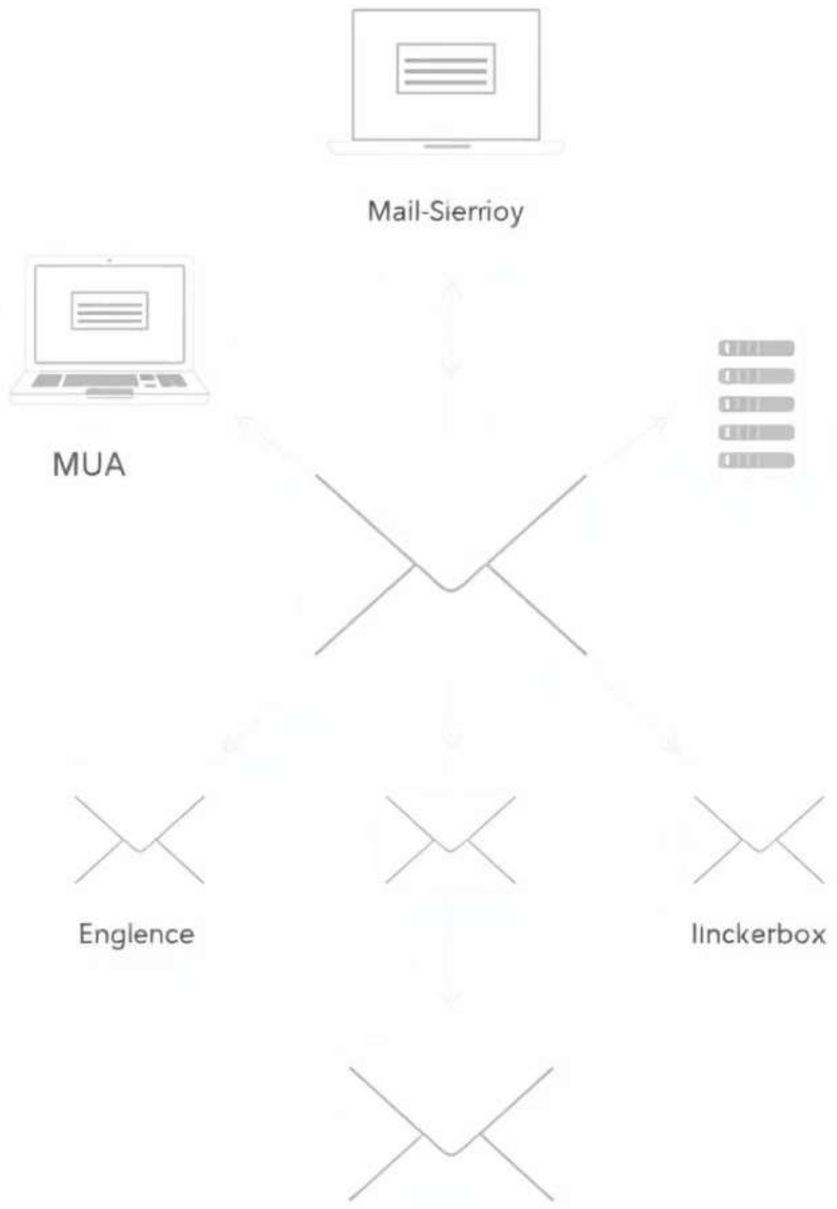


SMTP Session Flow



Key Components in Email Delivery

- **MUA (Mail User Agent):** Your email client, like Outlook or Gmail's web interface.
- **MSA (Mail Submission Agent):** The server that receives your email from your MUA.
- **MTA (Mail Transfer Agent):** Responsible for routing mail between different mail servers.
- **MDA (Mail Delivery Agent):** Puts the email into the recipient's specific mailbox.



The Journey of an Email

Compose Email

User writes an email in their MUA.

Submission

MUA connects to MSA using SMTP (port 587).

Sender Routing

MSA forwards email to sender's MTA for routing.

Server Transfer

Sender's MTA connects to recipient's MTA via SMTP (port 25).

Local Delivery

Recipient's MTA passes email to MDA.

Inbox Arrival

MDA places email in mailbox, accessible via POP3/IMAP.

SMTP Enhancements and Security

ESMTP

Adds authentication and STARTTLS capabilities to SMTP.

STARTTLS

Upgrades insecure connections to encrypted TLS/SSL.

SPF

Authenticates sender's domain, preventing email spoofing.

DKIM

Uses digital signatures to verify sender and content integrity.

DMARC combines SPF and DKIM, defining policies for failed authentication. These enhancements greatly improve email security and reliability.

Common SMTP Ports and Issues

Port 25 (Legacy)

Original, unencrypted, often blocked due to spam.

Port 465 (SMTPS)

SMTP over SSL/TLS, deprecated but still in use.

Port 587 (Submission)

Preferred, authenticated, with STARTTLS encryption.

Common errors include "550 Relay Denied" (server not configured for your domain), "550 Mailbox not found" (recipient address does not exist), and "421 Service not available" (temporary server issue). Authentication failures often result from incorrect credentials.

Conclusion: SMTP's Enduring Importance

SMTP is the fundamental protocol for internet email. It continues to evolve with vital security enhancements. This ensures reliable and efficient communication across global networks. Despite new communication methods, SMTP remains critical infrastructure.