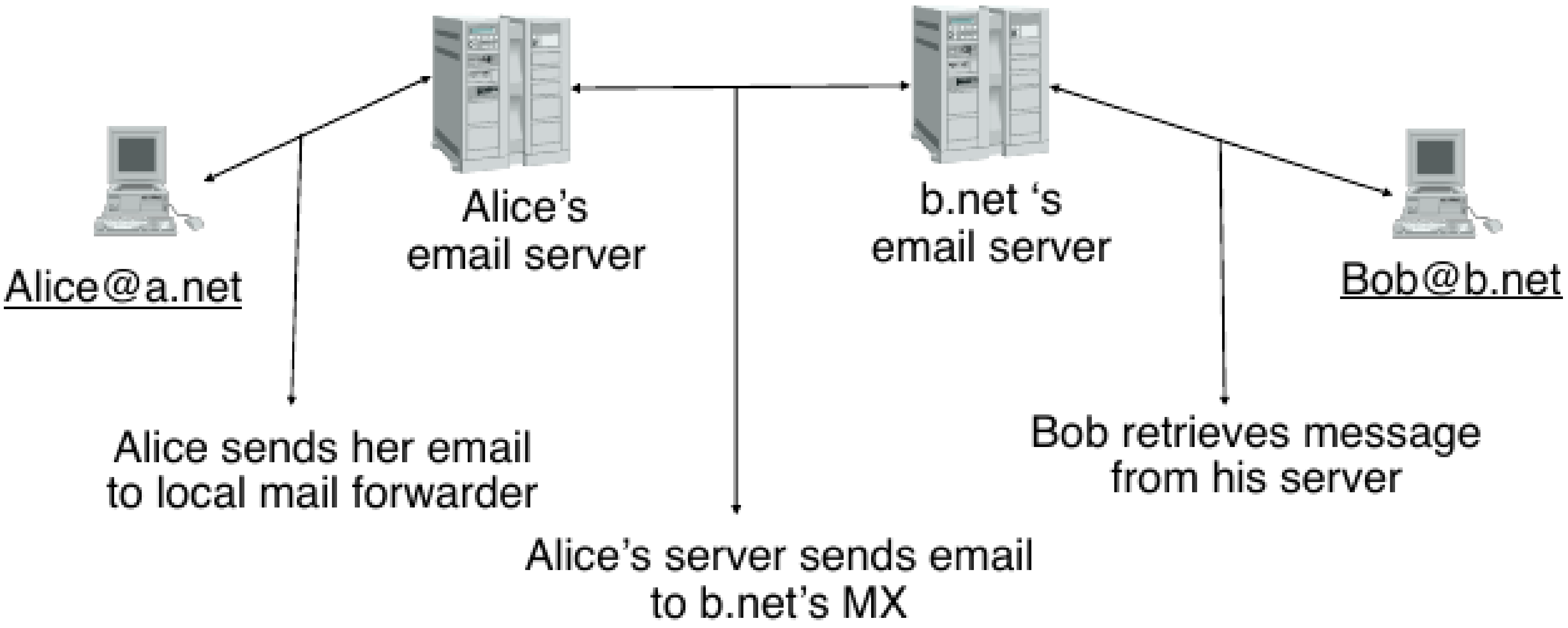
Internet, Principes et Protocoles (IPP)

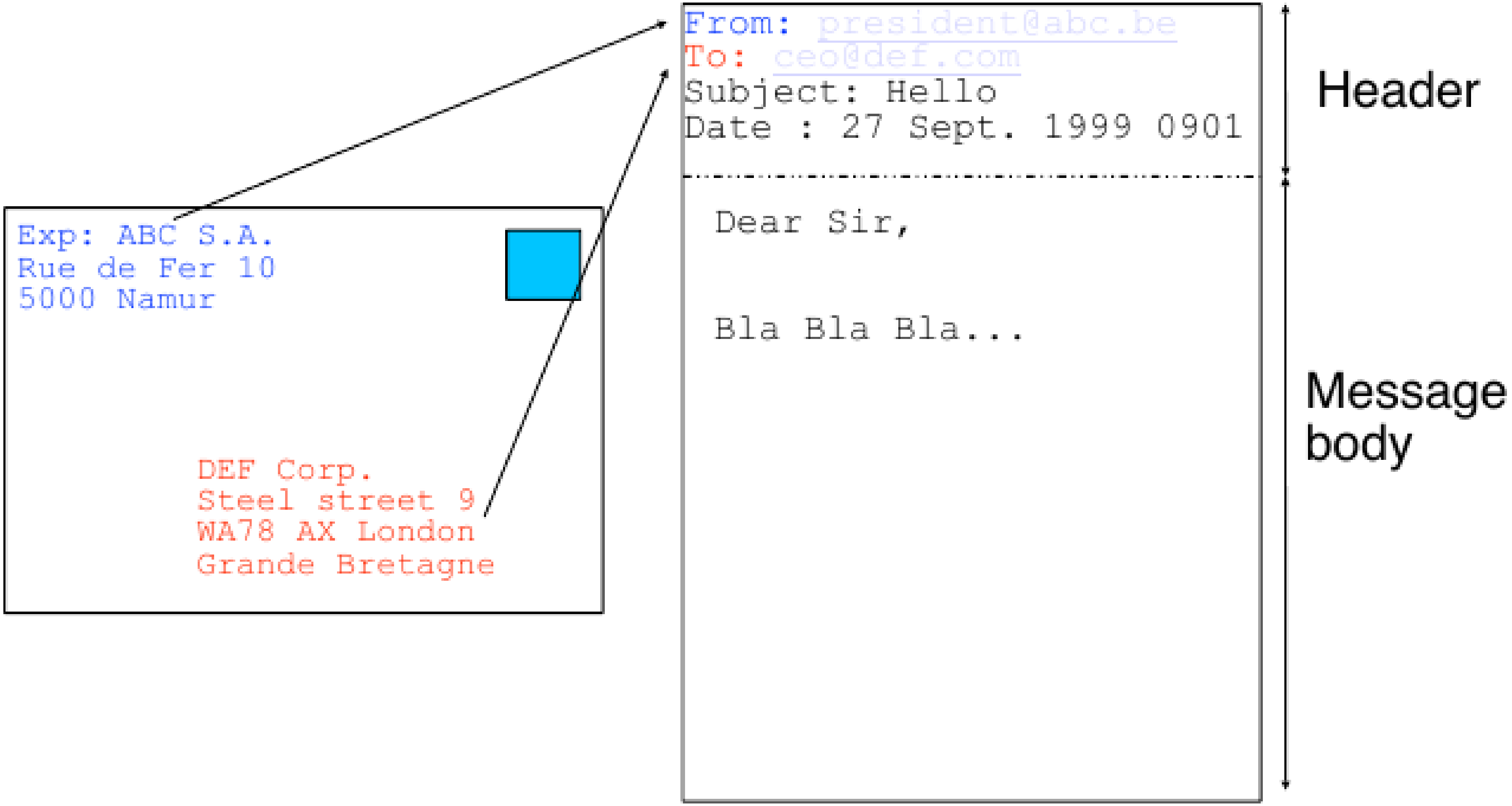
Recap

- Telnet
- SSH – SCP
- NTP
- RDP
- FTP
- WHOIS

Email


Alice@a.net
Alice's
email server
b.net 's
email server
Bob@b.net
Alice sends her email
to local mail forwarder
Alice's server sends email
to b.net's MX
Bob retrieves message
from his server

Email message format



Exp: ABC S.A.
Rue de Fer 10
5000 Namur

DEF Corp.
Steel street 9
WA78 AX London
Grande Bretagne

From: president@abc.be
To: ceo@def.com
Subject: Hello
Date : 27 Sept. 1999 0901

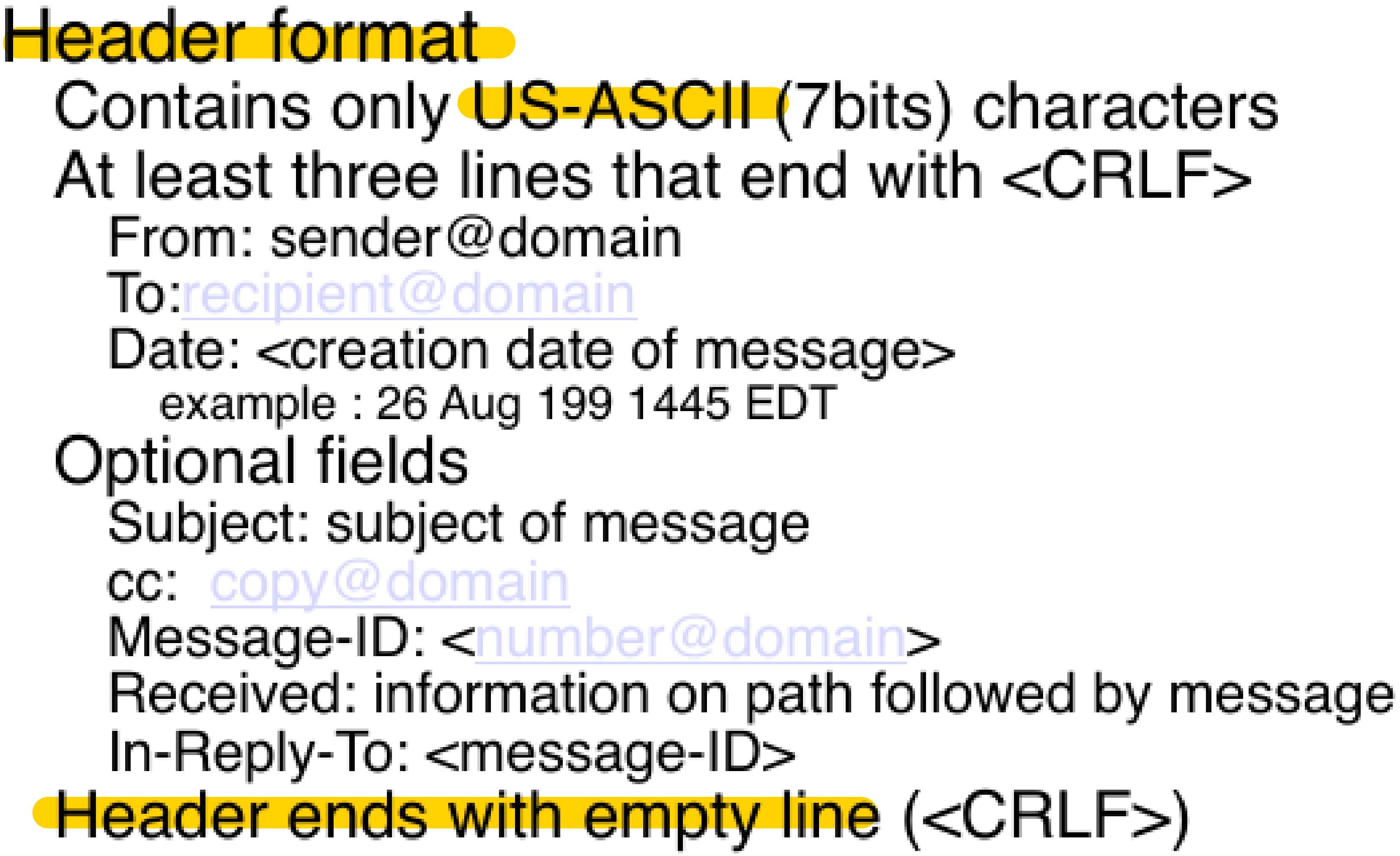
Dear Sir,

Bla Bla Bla...

Header

Message body

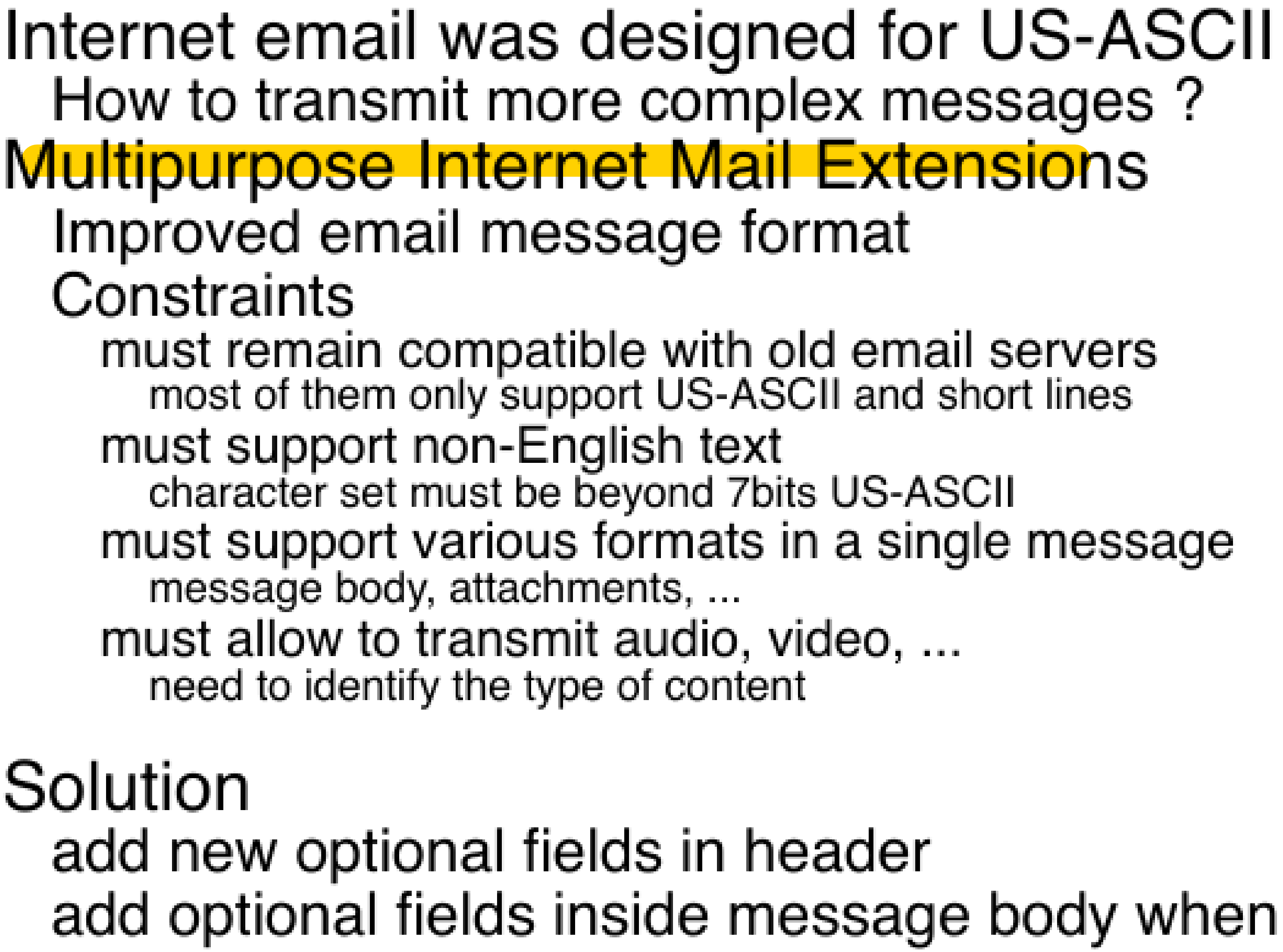
Email message format



Header format

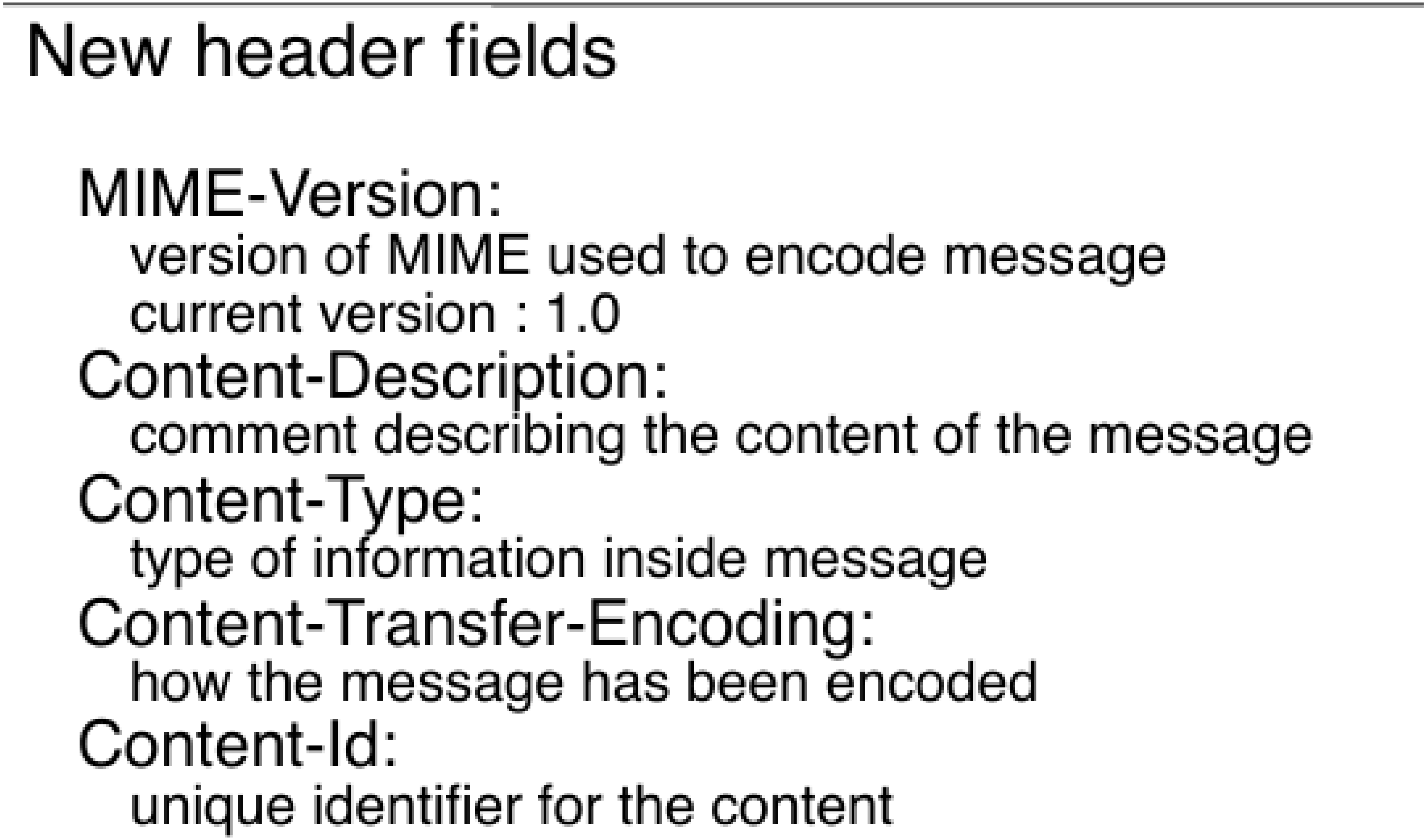
- Contains only US-ASCII (7bits) characters
- At least three lines that end with <CRLF>
  - From: sender@domain
  - To:recipient@domain
  - Date: <creation date of message>
    - example : 26 Aug 199 1445 EDT
- Optional fields
  - Subject: subject of message
  - cc: copy@domain
  - Message-ID: <number@domain>
  - Received: information on path followed by message
  - In-Reply-To: <message-ID>
- Header ends with empty line (<CRLF>)

MIME



- Internet email was designed for US-ASCII
  - How to transmit more complex messages ?
- Multipurpose Internet Mail Extensions
  - Improved email message format
  - Constraints
    - must remain compatible with old email servers
      - most of them only support US-ASCII and short lines
    - must support non-English text
      - character set must be beyond 7bits US-ASCII
    - must support various formats in a single message
      - message body, attachments, ...
    - must allow to transmit audio, video, ...
      - need to identify the type of content
- Solution
  - add new optional fields in header
  - add optional fields inside message body when

MIME



New header fields

MIME-Version:
- version of MIME used to encode message
- current version : 1.0

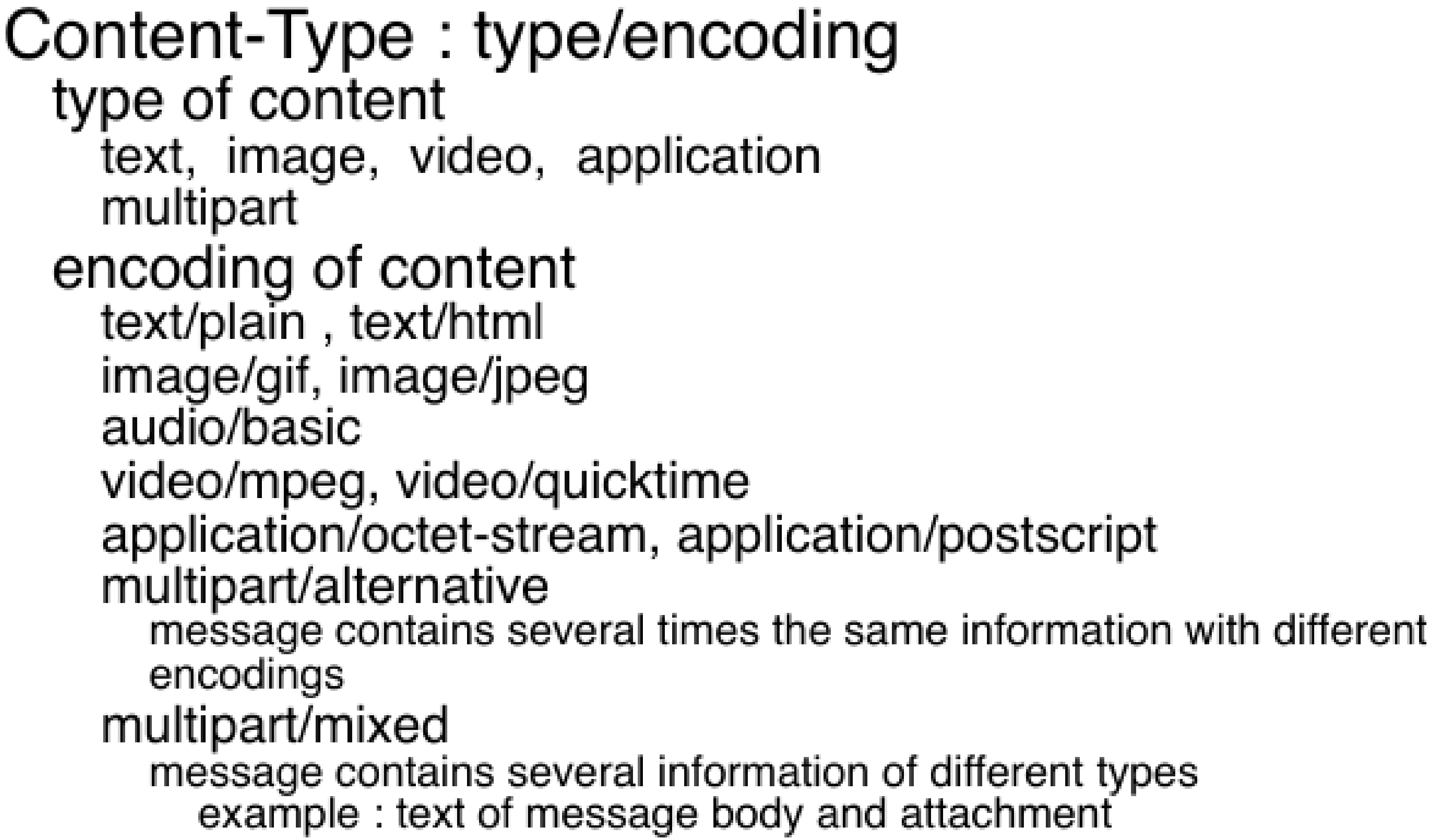
Content-Description:
- comment describing the content of the message

Content-Type:
- type of information inside message

Content-Transfer-Encoding:
- how the message has been encoded

Content-Id:
- unique identifier for the content

MIME



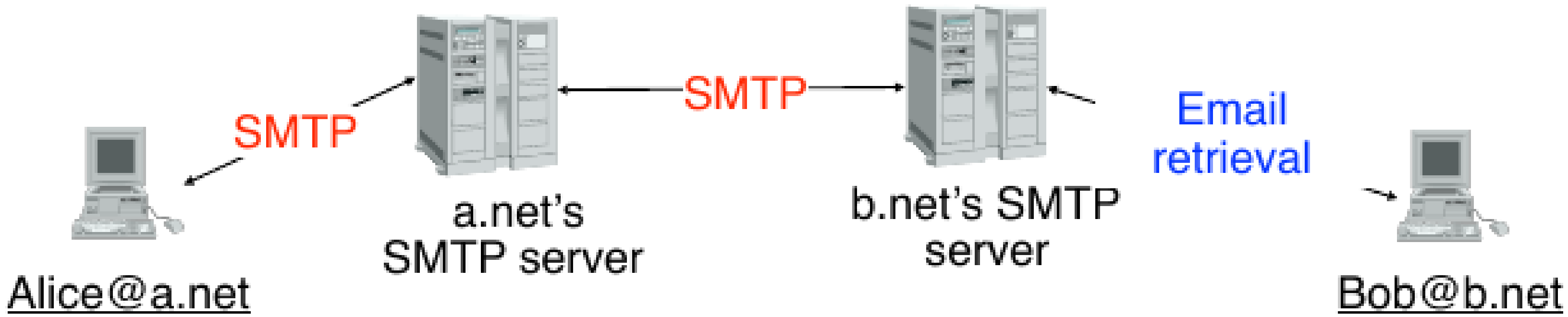
Content-Type : type/encoding

- type of content
  - text, image, video, application
  - multipart
- encoding of content
  - text/plain , text/html
  - image/gif, image/jpeg
  - audio/basic
  - video/mpeg, video/quicktime
  - application/octet-stream, application/postscript
  - multipart/alternative
    - message contains several times the same information with different encodings
  - multipart/mixed
    - message contains several information of different types
      - example : text of message body and attachment

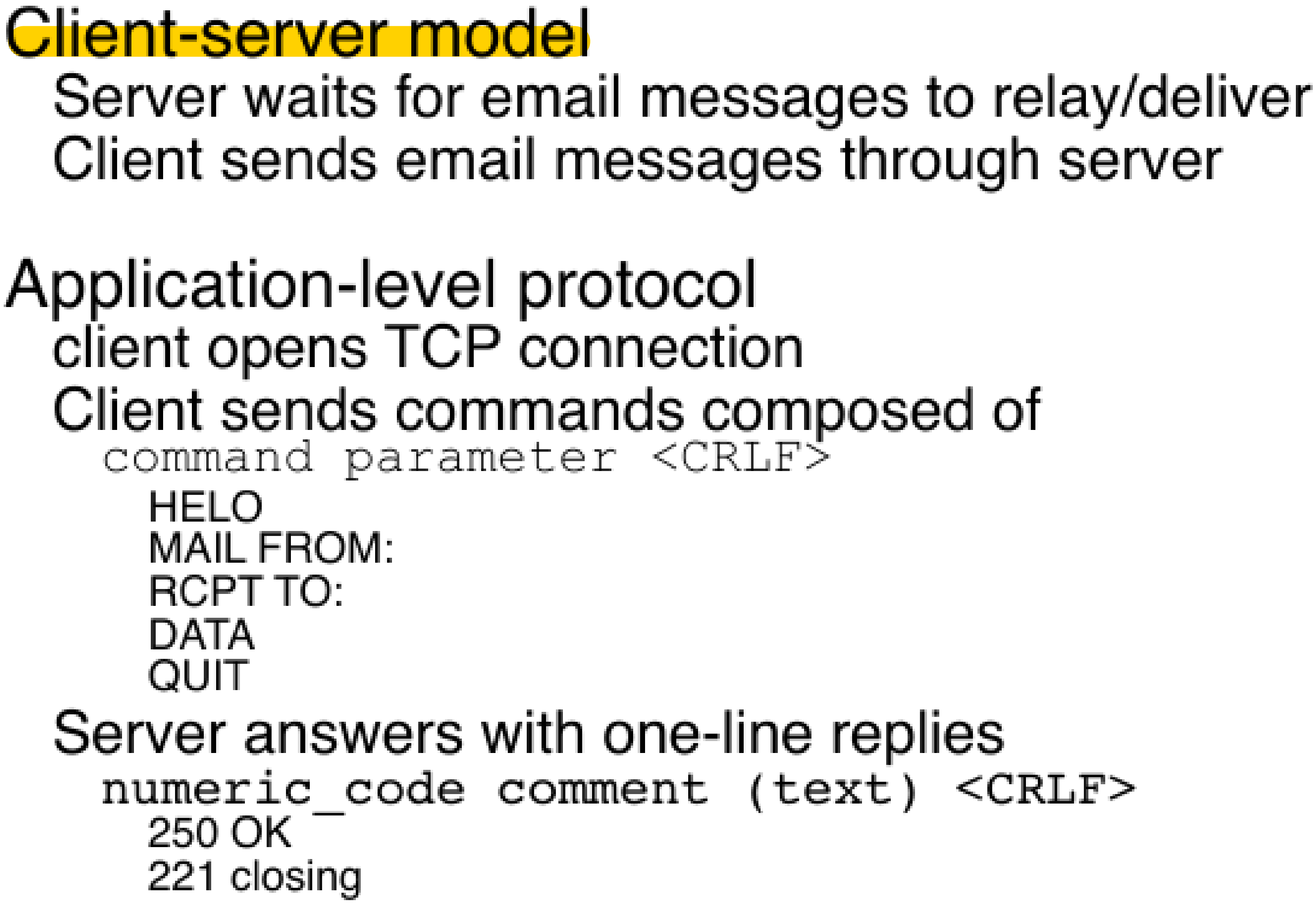
Protocols

SMTP : Simple Mail Transfer protocol

- uses TCP service
- Address of SMTP server
  - IP address of server + TCP + port number: 25
    - RR of type MX can be used to find the SMTP server responsible for a given domain



SMTP



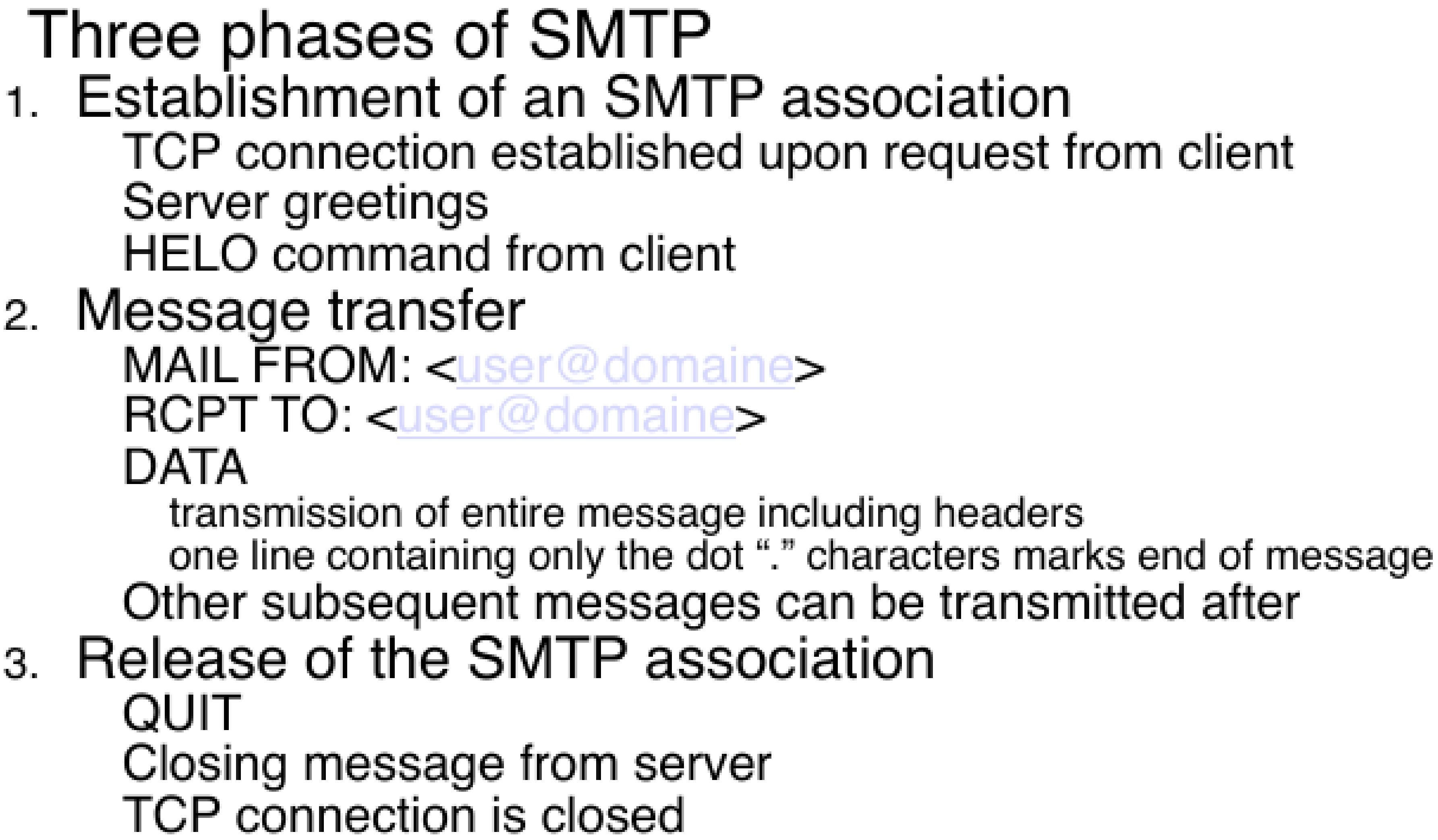
Client-server model

- Server waits for email messages to relay/deliver
- Client sends email messages through server

Application-level protocol

- client opens TCP connection
- Client sends commands composed of
  - `command parameter <CRLF>`
    - HELO
    - MAIL FROM:
    - RCPT TO:
    - DATA
    - QUIT
- Server answers with one-line replies
  - `numeric_code comment (text) <CRLF>`
    - 250 OK
    - 221 closing

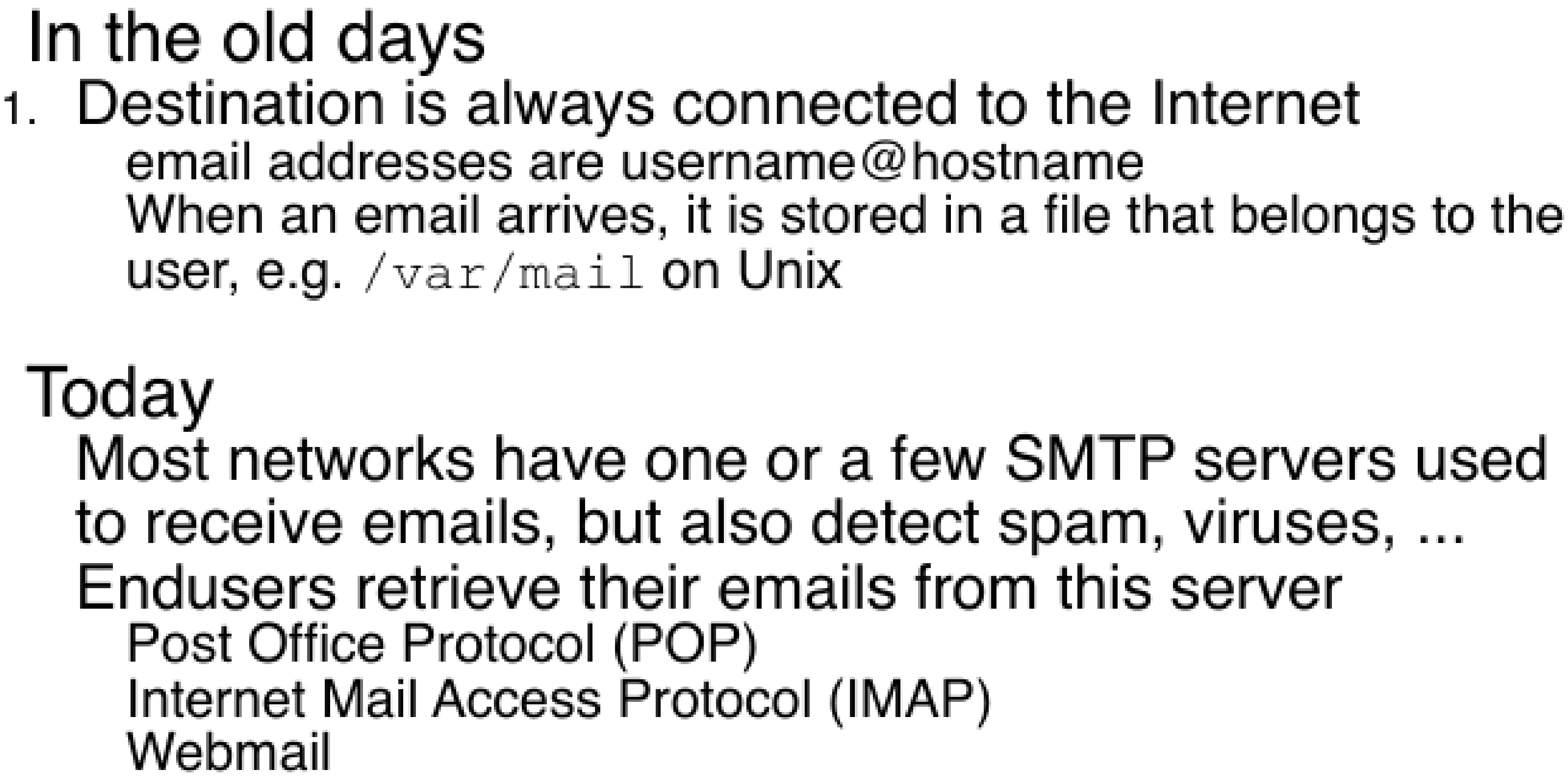
STMP



Three phases of SMTP

1. Establishment of an SMTP association
   - TCP connection established upon request from client
   - Server greetings
   - HELO command from client
2. Message transfer
   - MAIL FROM: <user@domaine>
   - RCPT TO: <user@domaine>
   - DATA
     - transmission of entire message including headers
     - one line containing only the dot "." characters marks end of message
   - Other subsequent messages can be transmitted after
3. Release of the SMTP association
   - QUIT
   - Closing message from server
   - TCP connection is closed

Retreival of Email Messages



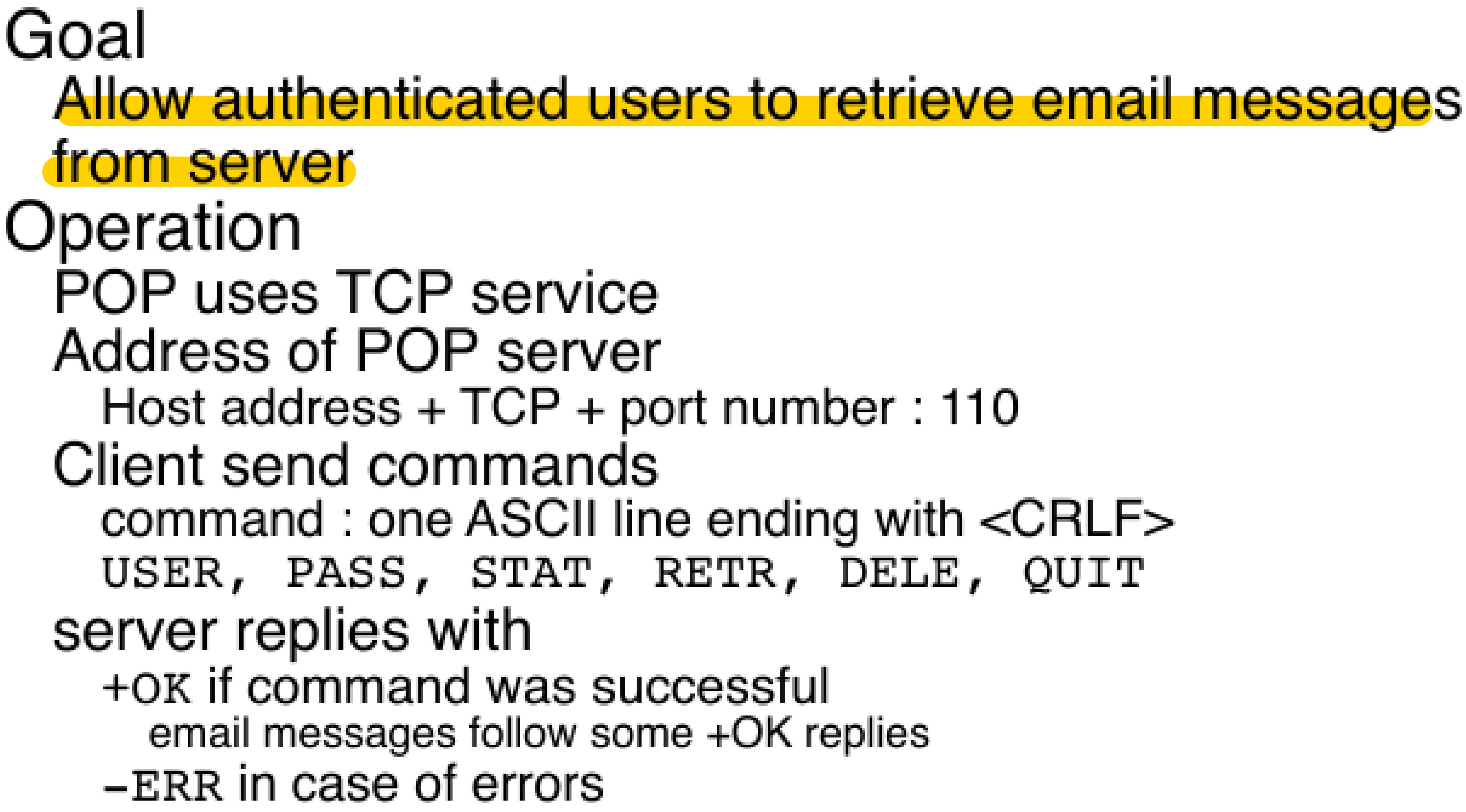
In the old days

1. Destination is always connected to the Internet
   - email addresses are username@hostname
   - When an email arrives, it is stored in a file that belongs to the user, e.g. `/var/mail` on Unix

Today

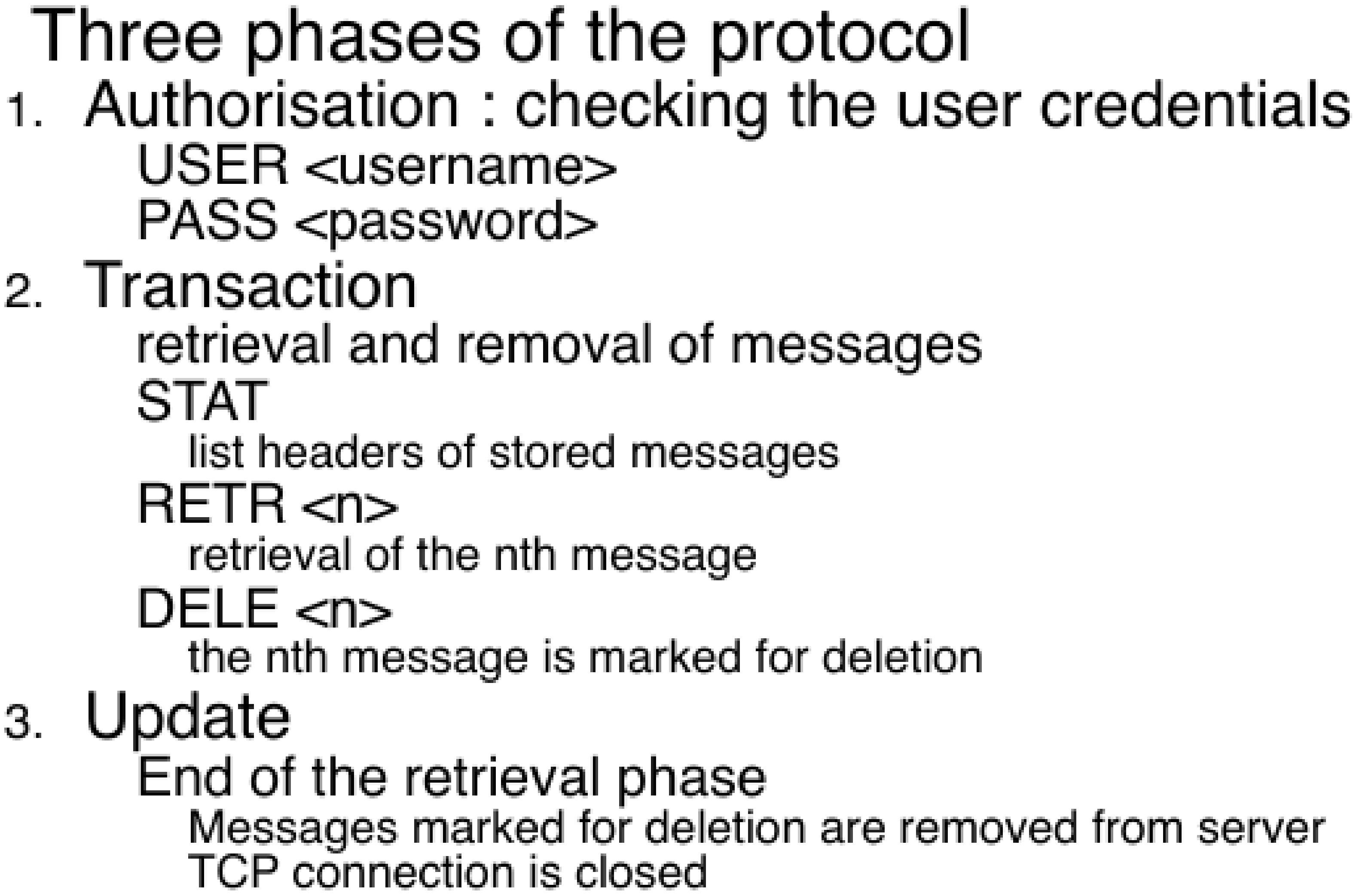
- Most networks have one or a few SMTP servers used to receive emails, but also detect spam, viruses, ...
- Endusers retrieve their emails from this server
  - Post Office Protocol (POP)
  - Internet Mail Access Protocol (IMAP)
  - Webmail

POP3



- Goal
  - Allow authenticated users to retrieve email messages from server
- Operation
  - POP uses TCP service
  - Address of POP server
    - Host address + TCP + port number : 110
  - Client send commands
    - command : one ASCII line ending with <CRLF>
    - `USER, PASS, STAT, RETR, DELE, QUIT`
  - server replies with
    - `+OK` if command was successful
      - email messages follow some +OK replies
    - `-ERR` in case of errors

POP3



Three phases of the protocol

1. Authorisation : checking the user credentials
   - USER <username>
   - PASS <password>
2. Transaction
   - retrieval and removal of messages
   - STAT
     - list headers of stored messages
   - RETR <n>
     - retrieval of the nth message
   - DELE <n>
     - the nth message is marked for deletion
3. Update
   - End of the retrieval phase
     - Messages marked for deletion are removed from server
     - TCP connection is closed

IMAP

- Used to consult the messages on the server.
- Allows the synchronization of email actions among devices.
- Port 143, can run over SSL (port 993)
- Server side searches

POP vs IMAP

- POP if you want to download the emails and do operations locally
- IMAP to do email operations online
- IMAP was designed as an improvement over POP3

Phishing and Spam

- Spoofing emails
- Domain Typosquating
- Links with a different text
- How to filter Spam?

- Example + Video

- https://www.safeonweb.be/fr/quiz/test-du-phishing

SPF – DKIM - DMARC

- SPF - the receiving mail server runs an TXT DNS query against the claimed domain SPF entry. In case the check fails a rejection message is given to the sender server.
- DKIM - when sending an outgoing message, the last server within the domain infrastructure checks if the domain used in the “From:” header is included in its “signing table”. If not the process stops here. Else, a new header, called “DKIM-Signature”, is added to the mail message. From here on the message main content cannot be modified otherwise the DKIM header won’t match anymore.
- DMARC – General Policy advertised by a sender mail server. The receiver checks if the email received matches the policy.

This Semester

- Introduction
  - OSI Model, topologies, networks
- Network Layer
  - Routing (LSP, routing tables), ARP, IP, MAC addresses, ...
- Transport Layer
  - TCP, UDP, ICMP
- Application Layer
  - Email, HTTP, SSL/TLS, DNS, SSH, FTP, ...

Next Semester

- VPN, Proxys, TOR
- Bitcoin and blockchain
- Peer to Peer networks
- General tips and tricks
- ...port knoking

- Quick Question? When connecting to WiFi, how do you exchange password with the modem if you are not connected?

Filtrer le spam, ides

- Vpn proxy tor