HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN
****

GIAO THỨC AN TOÀN MẠNG

Bài 3.1. Vấn đề an toàn ở tầng ứng dụng

Giao thức tầng ứng dụng

- Host Configuration: DHCP
- Domain Name System: DNS
- Remote Login: TELNET, SSH
- File Transfer: FTP, TFTP
- World Wide Web: HTTP
- Electronic Mail: SMTP, POP, IMAP, MIME
- Network Management: SNMP
- ...

1. World Wide Web
2. Thư điện tử
3. Đăng nhập từ xa

Mục tiêu bài học

❑Kiến thức

- Nắm bắt được một số giao thức mạng điển hình ở tầng ứng dụng
- Hiểu được hiểm họa an toàn đối với các dịch vụ mạng và các giải pháp phòng chống

❑Kỹ năng

- Phân tích hiểm họa an toàn thông tin đối với từng dịch vụ mạng
- Phân tích hoạt động của giao thức qua việc chặn thu lưu lượng mạng

Tài liệu tham khảo

1. Giáo trình "Giao thức an toàn mạng máy tính"// Chương 4 "**Các giao thức bảo mật dịch vụ**"
2. Behrouz A. Forouzan, "TCP/IP Protocol Suite" (4e)// Part 4 "**Application Layer**", Mc Graw Hill, 2010
3. André Perez, "Network Security"//Chapter 6.2 "**SSH Protocol**", Wiley, 2014
4. William Stallings, "**Protocol Basics: Secure Shell Protocol**"//The Internet Protocol Journal, Volume 12, No.4
   https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-46/124-ssh.html
5. What is Network Security Application Layer?
   https://www.wisdomjobs.com/e-university/network-security-tutorial-449/network-security-application-layer-21963.html

1 World Wide Web

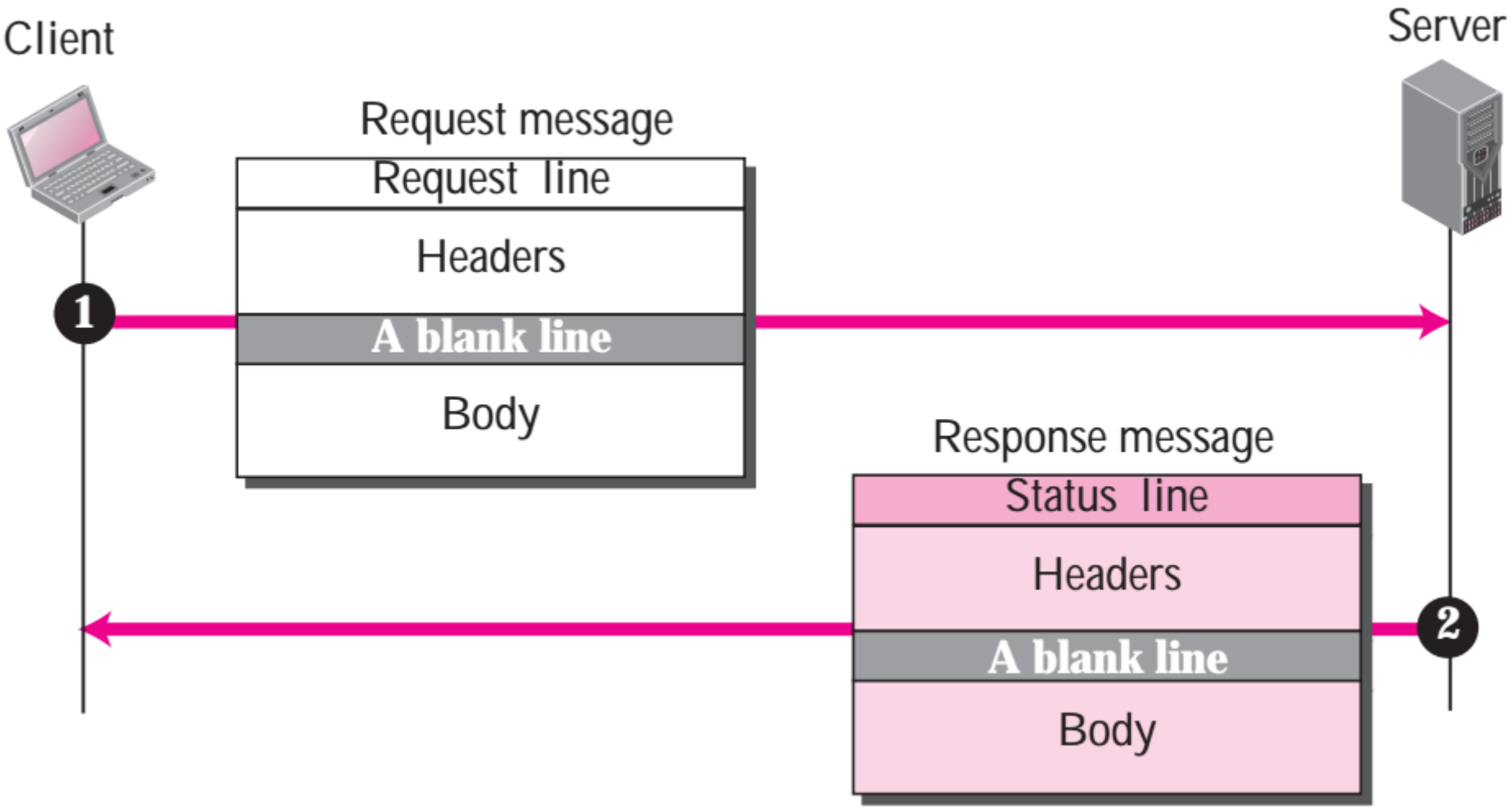
2 Thư điện tử

3 Đăng nhập từ xa

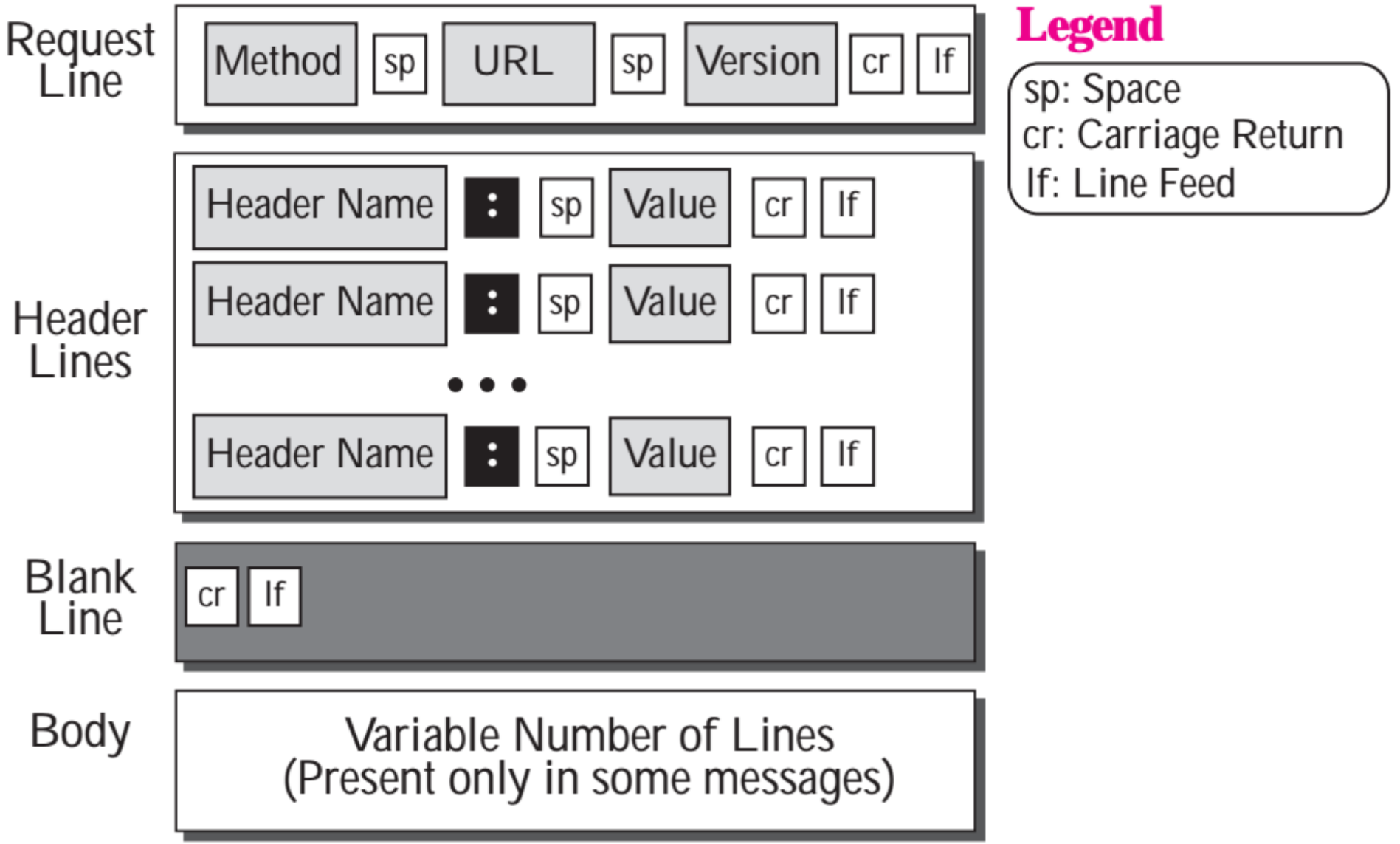
Giao thức HTTP

- HTTP = HyperText Transfer Protocol
- Cổng: 80 TCP
- Là giao thức chủ đạo cho web
- Phiên bản
  - Ver 0.9, 1.0: thuần túy văn bản
  - Ver 1.1: hỗ trợ "application/octet-stream"
  - Ver 2: chủ yếu là binary
- Request – Response (Yêu cầu – Đáp ứng)
- Không trạng thái

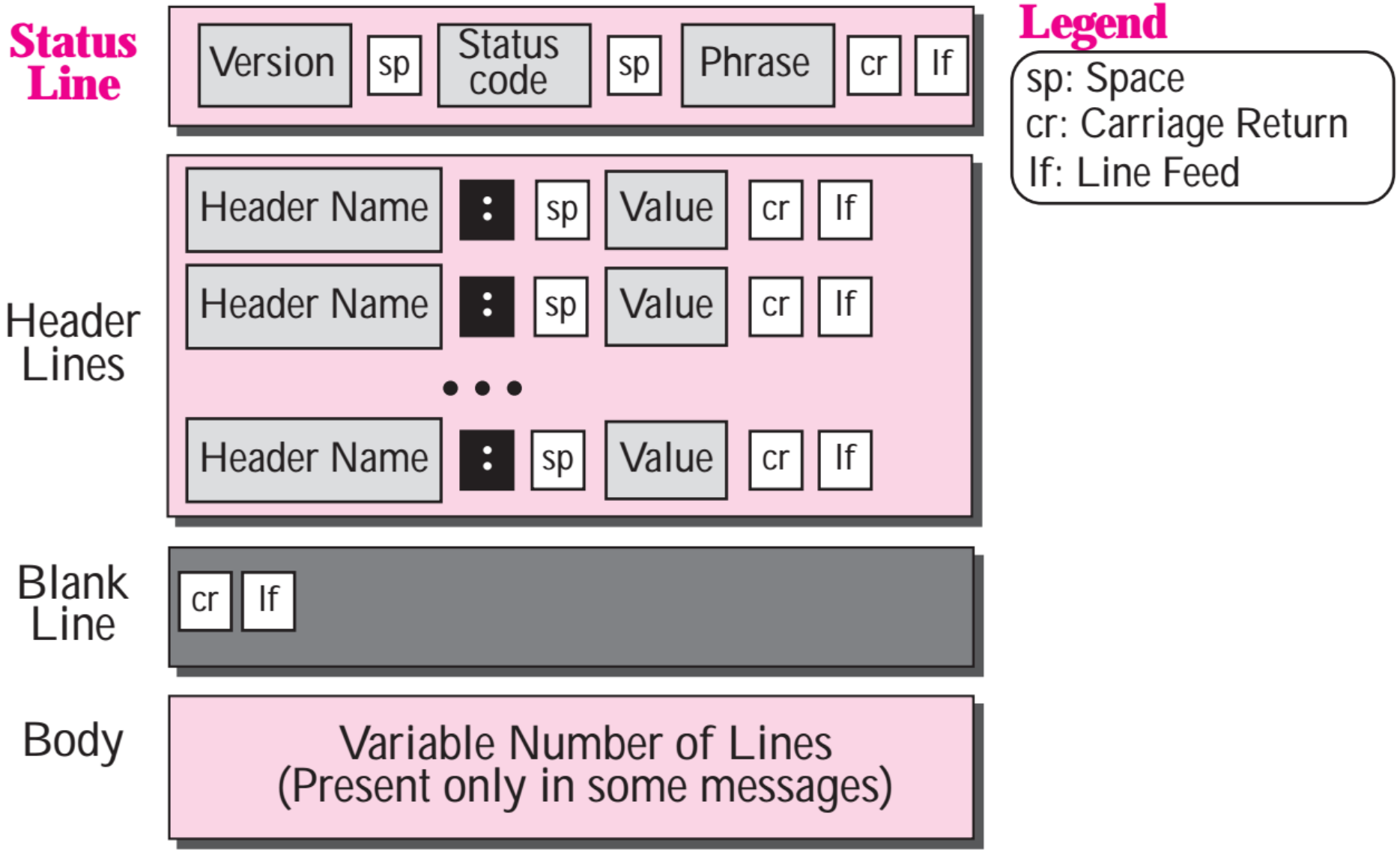
Giao thức HTTP



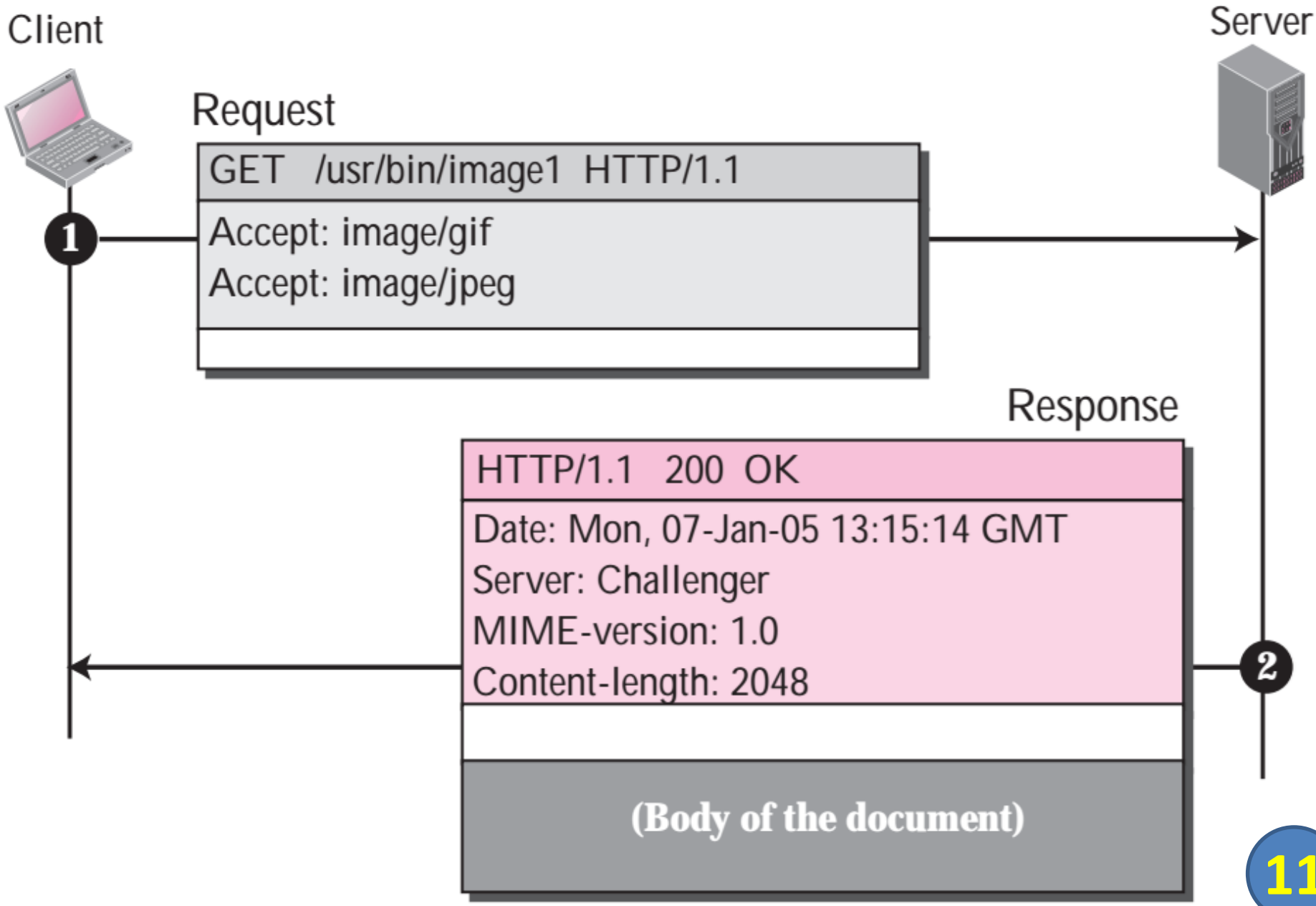
HTTP Request



HTTP Response



Ví dụ HTTP Request và Response



HTTP: Vấn đề an toàn

- Client không thể xác thực Server
- Client có thể được xác thực bởi
  - Web Server: Basic, Digest... nhưng hiếm khi được sử dụng
  - Web Application: username/password (KHÔNG thuộc phạm vi giao thức HTTP)
- Ngoài một vài cơ chế xác thực, HTTP không cung cấp dịch vụ an toàn nào khác (bí mật, toàn vẹn).

➔ Cần hỗ trợ của giao thức an toàn ở lớp dưới!

"Giao thức an toàn lớp dưới"

- TLS: Transport Layer Security
  (chi tiết ở bài kế tiếp)
- HTTPS = HTTP over TLS
- Sử dụng TLS
  - Kích hoạt TLS trước khi bắt đầu HTTP
  - Gọi TLS như là một dịch vụ tùy chọn (Alternative Services) của HTTP:
    - RFC 7838: HTTP Alternative Services
    - RFC 8164: Opportunistic Security for HTTP/2

1. World Wide Web
2. Thư điện tử
3. Đăng nhập từ xa

1. Tổng quan các giao thức thư điện tử
2. Vấn đề an toàn của thư điện tử
3. Giao thức S/MIME

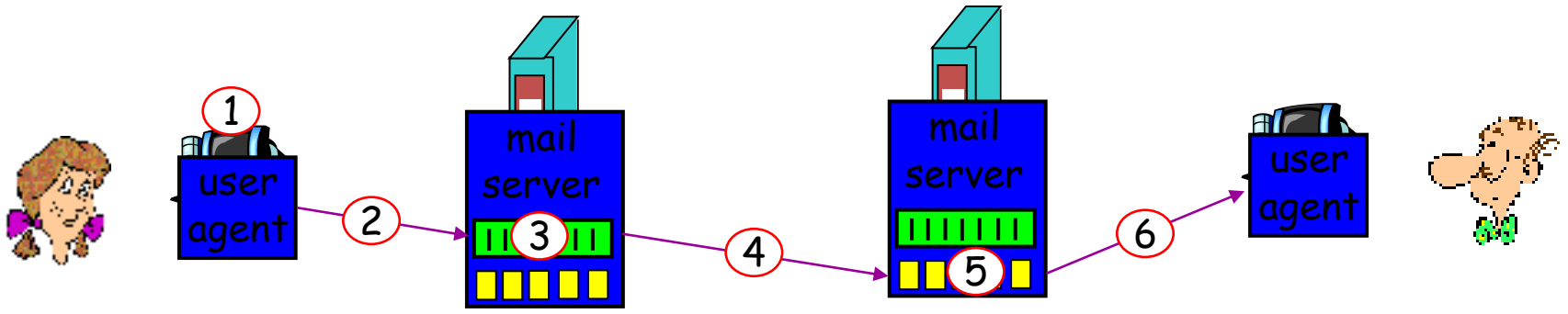
1 Tổng quan các giao thức thư điện tử

2 Vấn đề an toàn của thư điện tử

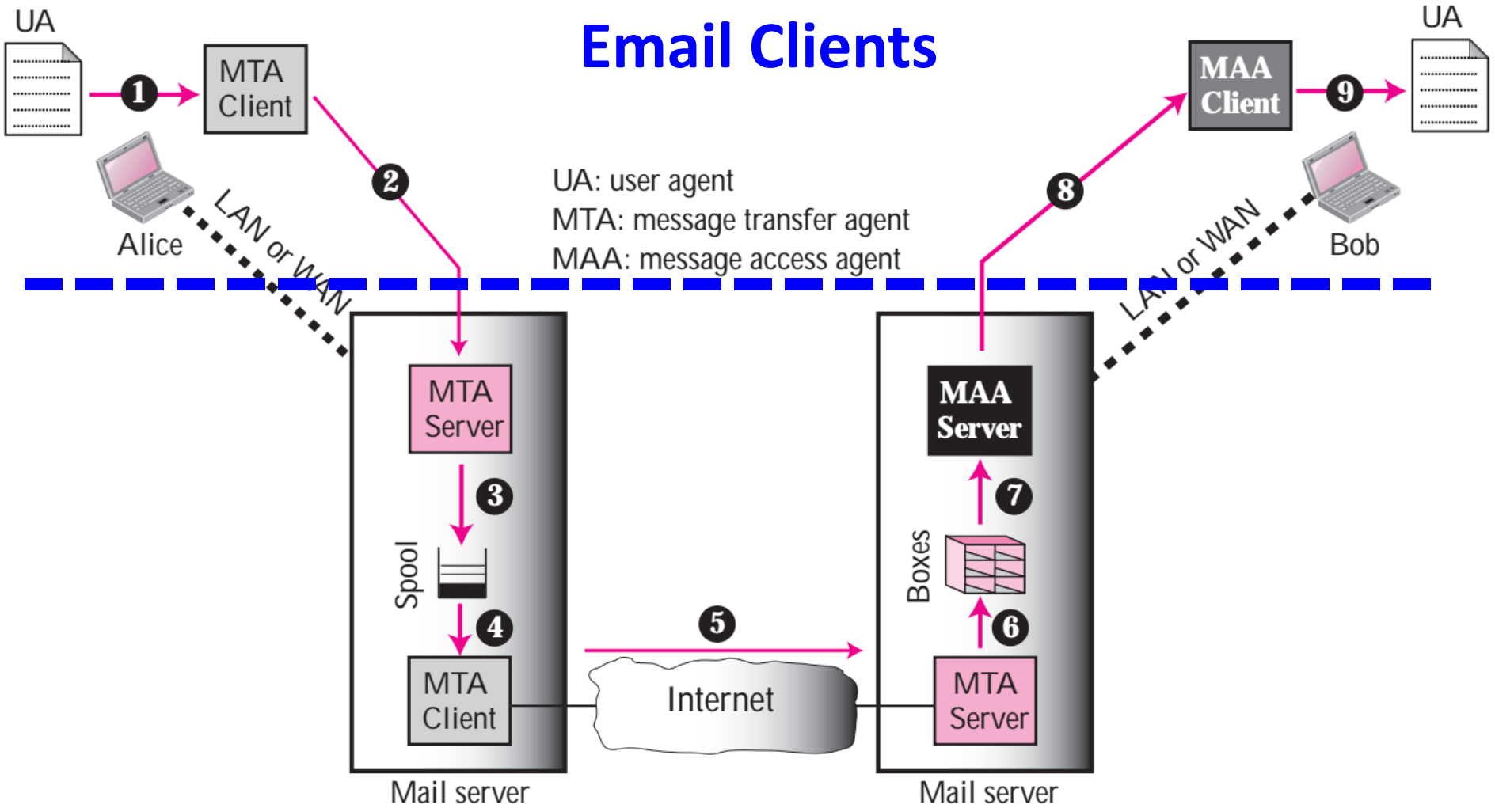
3 Giao thức S/MIME

Alice <alice@hau1.edu.vn> → Bob <bob@yahoo.com>

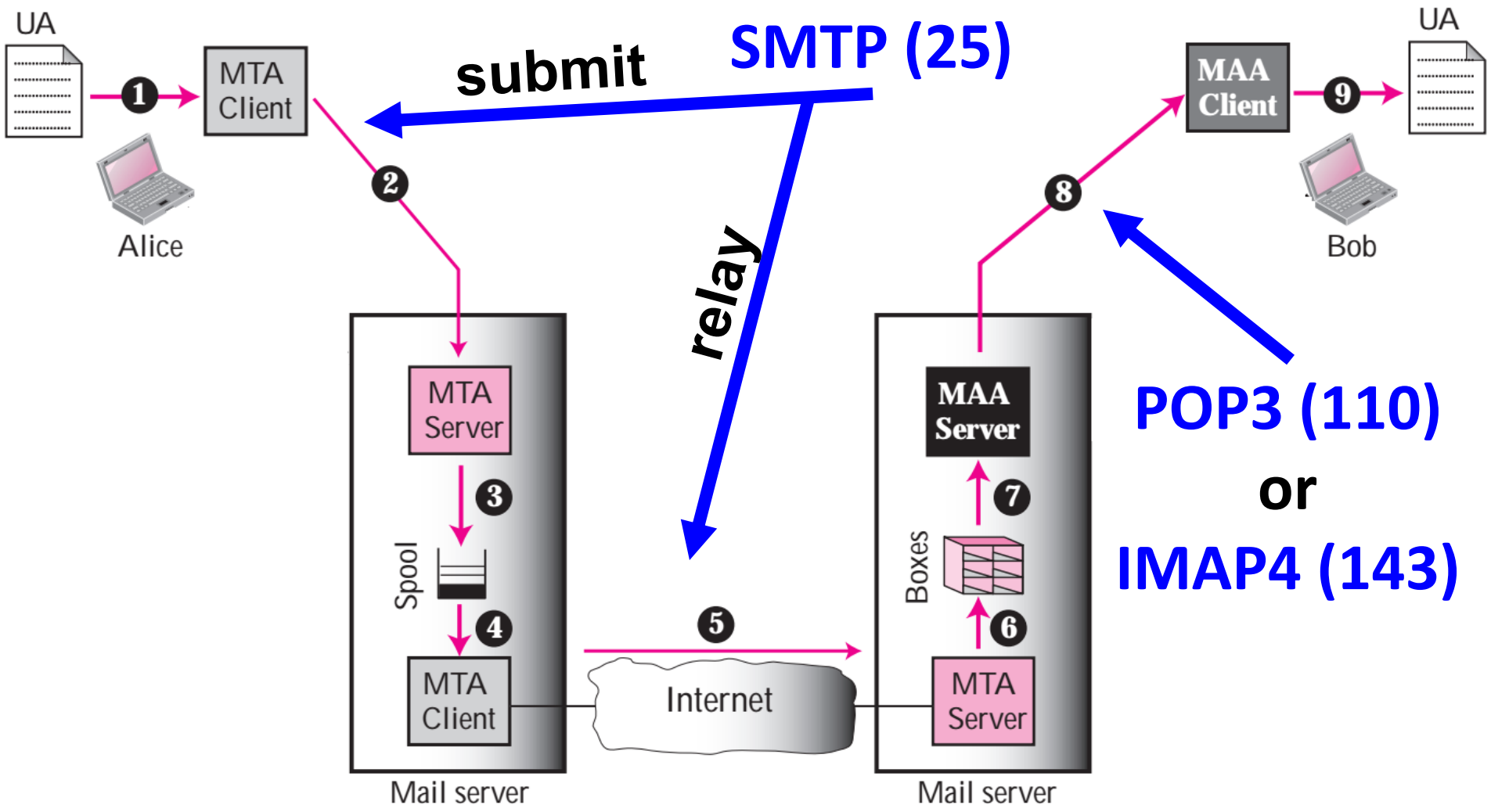
1) Alice sử dụng UA soạn thư, đ/c gửi tới "to": bob@yahoo.com.
2) Alice's UA gửi thư đến mail server của Alice,.
3) Mail server của Alice đưa bức thư xếp vào hàng đợi (message queue).
4) Mail server của Alice mở liên kết TCP tới mail server của Bob và gửi thư qua liên kết TCP.
5) Mail server của Bob cất thư nhận được vào hòm thư của Bob.
6) Bob dùng UA để lấy thư từ server về rồi đọc thư.



Mô hình thư điện tử



Giao thức thư điện tử



Giao thức thư điện tử

- Tất cả các giao thức thư điện tử đều sử dụng kiểu tương tác command – response
- Quá trình tương tác gồm 3 pha: khởi tạo, thực thi, kết thúc.

Giao thức thư điện tử

- Mỗi command hay response được kết thúc bằng cặp ký tự CR-LF
- Cấu trúc command:

  `VERB [arguments] <CR><LF>`
- Cấu trúc response

  `[CODE] information <CR><LF>`

Giao thức SMTP

- Ví dụ: các code trong SMTP

211 Trả lời trợ giúp, trạng thái hệ thống

214 Help message

220 Dịch vụ sẵn sàng (Service ready)

221 Đóng kết nối

250 Hành động yêu cầu được chấp nhận

251 Người sử dụng không ở mạng cục bộ, chuyển đến

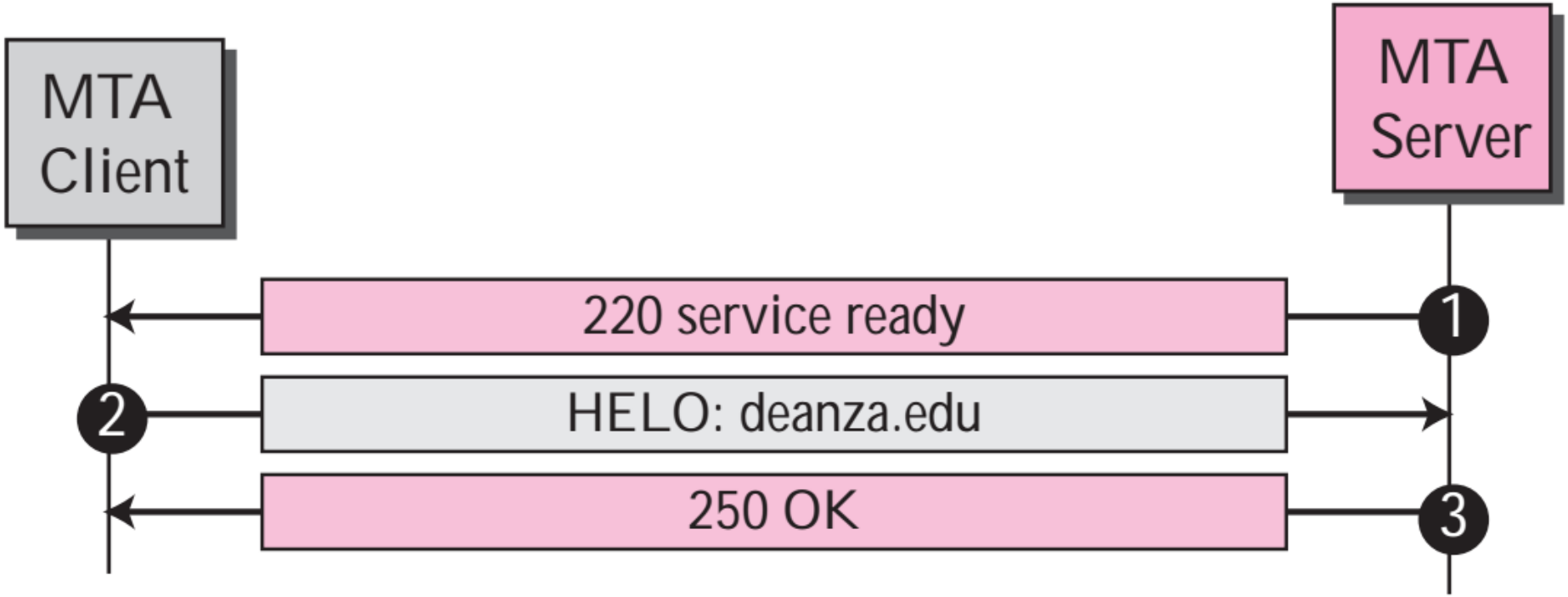
354 Bắt đầu nhập mail

421 Dịch vụ không sẵn sàng

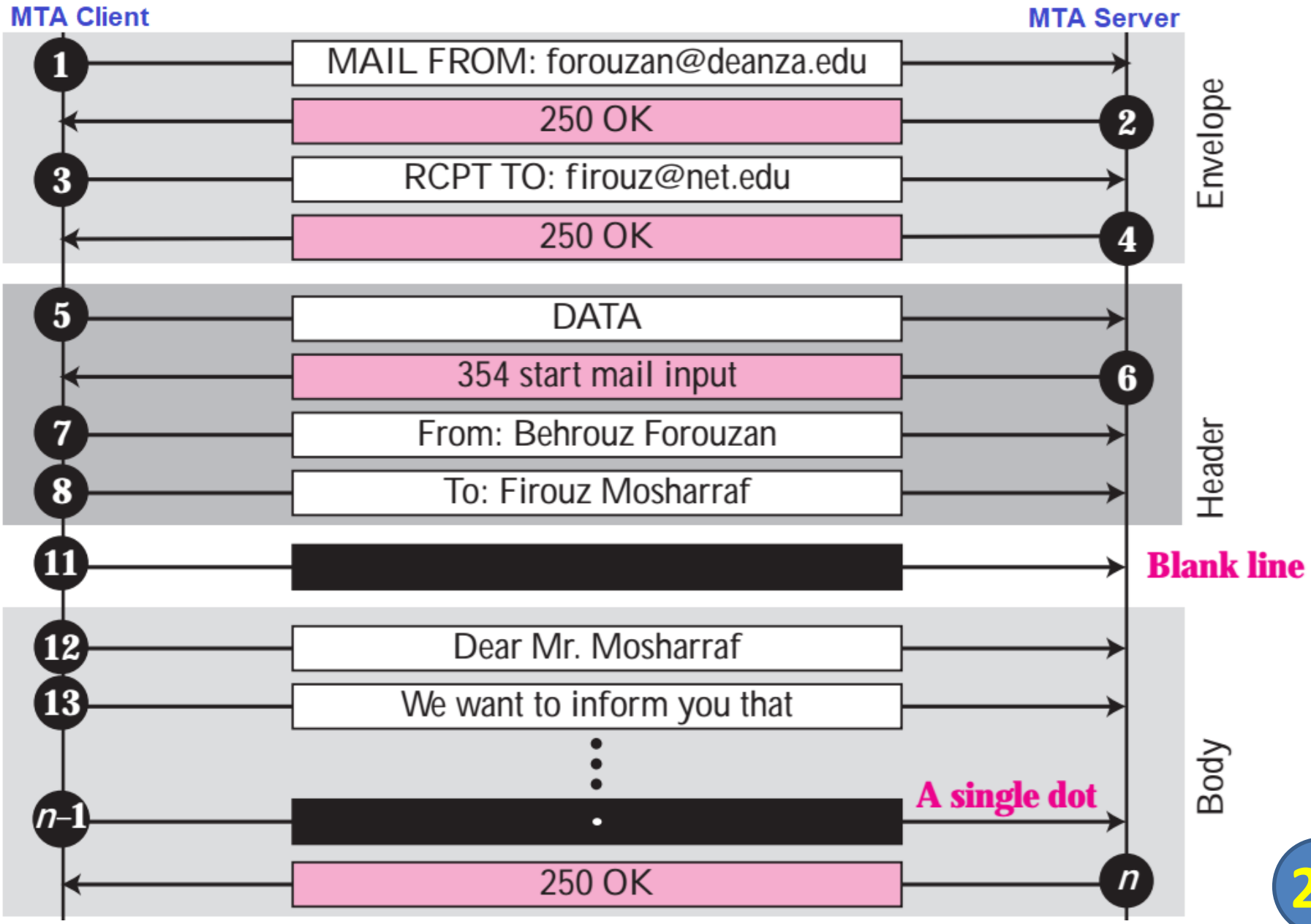
450 Hành động không chấp nhận, mailbox bận

451 Hành động bị hũy, lỗi cục bộ

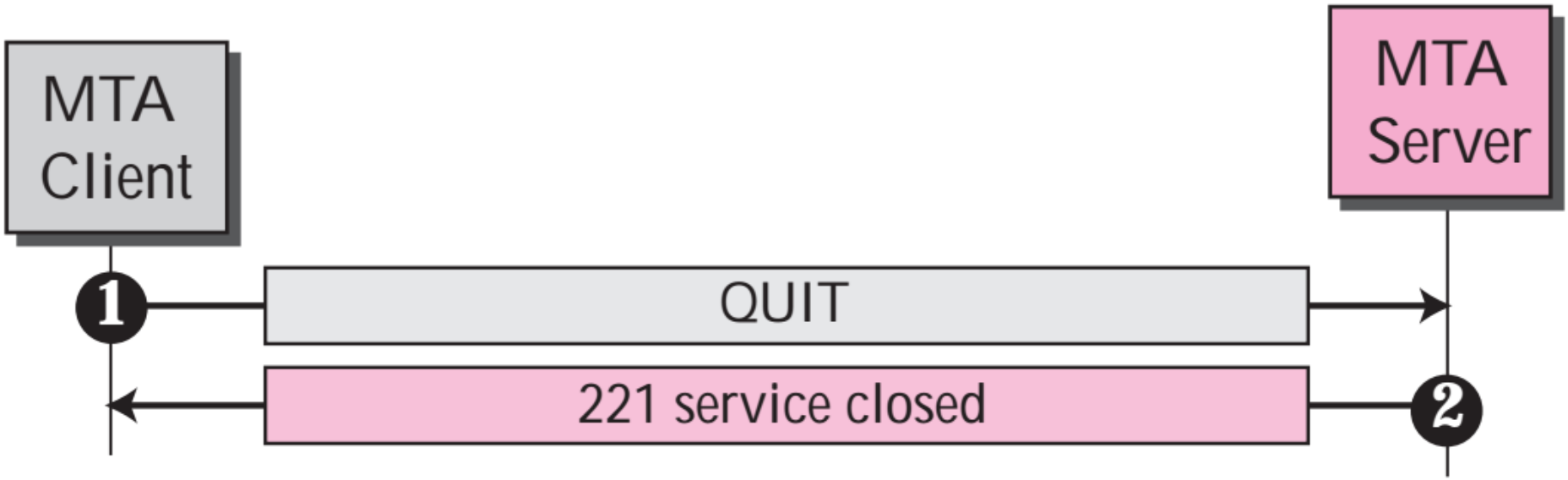
SMTP: Connection Establishment



SMTP: Transfer



SMTP: Connection Termination

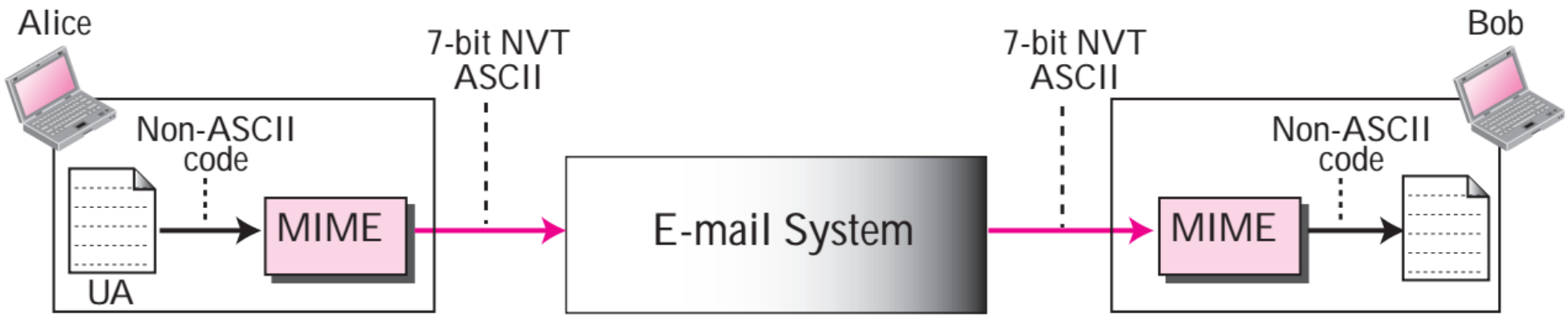


Giao thức SMTP

- **Hạn chế của SMTP:**
  - Chỉ sử dụng với dữ liệu dạng ASCII 7 bit.
  - Không có cơ chế xác thực
  - Thông điệp gửi đi không được mã hóa
  - Dễ bị tổn thương (bởi spam, mất định danh người gửi)

MIME: Multipurpose Internet Mail Extension

- Các giao thức SMTP, POP3, IMAP chỉ làm việc trên các ký tự ASCII chuẩn (7 bít)
- Khi cần gửi/nhận loại dữ liệu khác thì cần đóng gói về các ký tự ASCII chuẩn
- Giao thức được đề xuất: MIME



Phương pháp mã hóa base64

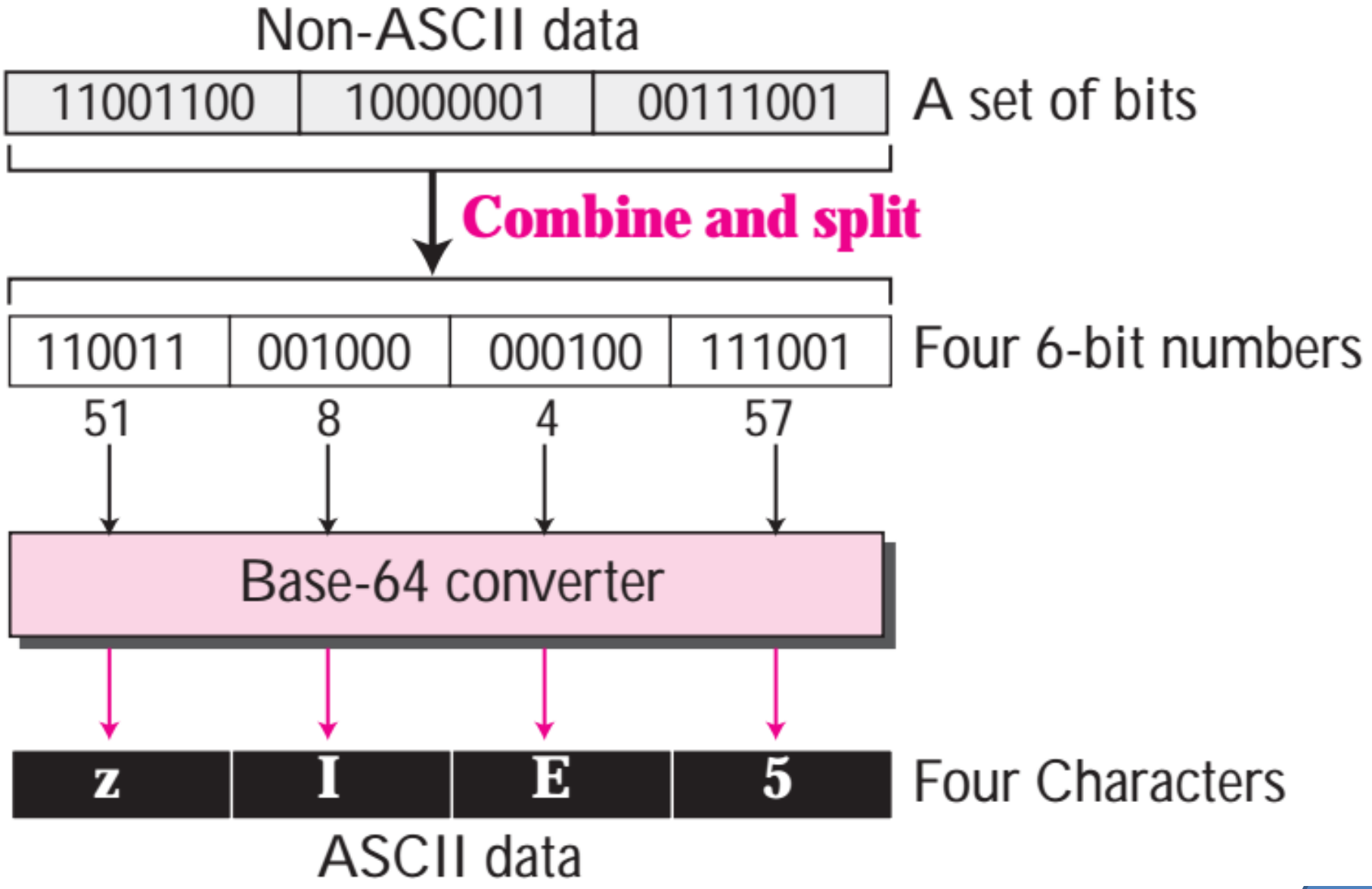
- Gồm các bước chính sau:
  - Chia file nhị phân thành nhiều nhóm nhỏ dài 3byte
  - Mã hóa từng nhóm 3byte thành 4 ký tự ASCII 7bit in ấn như sau:
    - Gộp 3 byte thành 24bit liên tiếp, chia thành 4 nhóm 6bit có giá trị từ 0-63.
    - Mỗi nhóm 6bit tương ứng với 1 ký tự in ấn như sau:

$$0 - 25 \longrightarrow A - Z$$
$$26 - 51 \longrightarrow a - z$$
$$52 - 61 \longrightarrow 0 - 9$$
$$62 \longrightarrow +$$
$$63 \longrightarrow /$$

Phương pháp mã hóa base64

6-Bit	Character Encoding
0	A
1	B
2	C
3	D
4	E
5	F
6	G
7	H
8	I
9	J
10	K
11	L
12	M
13	N
14	O
15	P
16	Q
17	R
18	S
19	T
20	U
21	V
22	W
23	X
24	Y
25	Z
26	a
27	b
28	c
29	d
30	e
31	f
32	g
33	h
34	i
35	j
36	k
37	l
38	m
39	n
40	o
41	p
42	q
43	r
44	s
45	t
46	u
47	v
48	w
49	x
50	y
51	z
52	0
53	1
54	2
55	3
56	4
57	5
58	6
59	7
60	8
61	9
62	+
63	/
(pad)	=

Base64 Encoding in MIME



Phương pháp mã hóa base64

- Ví dụ:

Thông báo M	77								97								110							
Bit pattern	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
Index	19								22				5				46							
Base64-encoded	T								W				F				u							

MIME Header

E-mail header
MIME-Version: 1.1 Content-Type: type/subtype Content-Transfer-Encoding: encoding type Content-Id: message id Content-Description: textual explanation of nontextual contents
E-mail body

MIME Content-Types

Type	Subtype	Description
Text	Plain	Unformatted
	HTML	HTML format
Image	JPEG	Image is in JPEG format
	GIF	Image is in GIF format
Application	PostScript	Adobe PostScript
	Octet-stream	General binary data

1 Tổng quan các giao thức thư điện tử

2 Vấn đề an toàn của thư điện tử

3 Giao thức S/MIME

Vấn đề an toàn của thư điện tử

❑Từ quan điểm của server

- Khả năng mạo danh người gửi
- Máy chủ thư bị lạm dụng để phát tán thư rác, mã độc

❑Từ quan điểm của người dùng

- Thư có thể bị đọc/sửa trên đường truyền
- Thư có thể bị đọc/sửa trên máy chủ

Giải pháp chống lạm dụng máy chủ

- SMTP không yêu cầu xác thực, mọi server đều mở
- POP3 luôn yêu cầu xác thực

➔ Giải pháp xác thực cho SMTP:

  - Kỹ thuật POP Before SMTP
  - Mở rộng SMTP thành ESMTP, thêm module xác thực "Authentication"

Extended (Enhanced) SMTP

- Mặc định sử dụng cổng 587 (thay cho 25)
- Sử dụng EHLO thay cho HELO
- Thêm lệnh xác thực: AUTH, STARTTLS
- Phương thức xác thực (AUTH):
  - Luôn dùng mã Base64 để truyền thông điệp
  - Truyền trực tiếp bí mật: PLAIN, LOGIN (thực hiện trên nền TLS)
  - Khác: CRAM-MD5, DIGEST-MD5, GSSAPI, OAUTH10A, OAUTHBEARER

StartTLS

- StartTLS: Opportunistic TLS
- StartTLS cho phép triển khai một cơ chế an toàn linh hoạt (cần thì dùng, không cần thì thôi) cho các giao thức vốn không có (có ít) các cơ chế an toàn.
- StartTLS sẽ thiết lập kênh TLS ngay trên cổng hiện thời, không cần cổng mới
- RFC 2595: Using TLS with IMAP, POP3 and ACAP
- RFC 3207: SMTP Service Extension for Secure SMTP over TLS

Ví dụ sử dụng ESMTP (1/2)

########## Example from RFC 2549 ######################

S: 220-smtp.example.com ESMTP Server

C: EHLO client.example.com

S: 250-smtp.example.com Hello client.example.com

S: 250-AUTH GSSAPI DIGEST-MD5

S: 250-ENHANCEDSTATUSCODES

S: 250 STARTTLS

C: STARTTLS

S: 220 Ready to start TLS

... TLS negotiation proceeds, further commands protected by TLS layer ...

.....

Ví dụ sử dụng ESMTP (2/2)

.....

C: EHLO client.example.com

S: 250-smtp.example.com Hello client.example.com

S: 250 AUTH GSSAPI DIGEST-MD5 PLAIN

C: AUTH PLAIN dGVzdAB0ZXN0ADEyMzQ=

S: 235 2.7.0 Authentication successful

##Base64: dGVzdAB0ZXN0ADEyMzQ=

##ASCII 7bit: testtest1234

##Hint: Online Base64 Decoder

Xác thực trong POP3

- POP3 nguyên bản: plaintext USER/PASS
- POP3 mới (RFC 1460): them lệnh APOP, cho phép xác thực như CRAM-MD5
- POP3 với module mở rộng AUTH: các phương thức SASL (Simple Authentication and Security Layer) như ESMTP
- Trong POP3 cũng có thể gọi STARTTLS

Xác thực trong POP3: APOP

S: +OK POP3 server ready
<1896.697170952@dbc.mtview.ca.us>
C: APOP mrose c4c9334bac560ecc979e58001b3e22fb
S: +OK maildrop has 1 message (369 octets)

##User: mrose
##Pass: tanstaaf
##MD5 in: <1896.697170952@dbc.mtview.ca.us>tanstaaf
##MD5 out: c4c9334bac560ecc979e58001b3e22fb

Giải pháp chống mạo danh người gửi

- SMTP cho phép điền bất kỳ địa chỉ nào vào trường "FROM"
- SPF = Sender Policy Framework
  - RFC 7208 (2014)
  - Áp dụng cho SMTP giữa các mail server
  - Chủ sở hữu domain quy định những máy (IP) nào được phép gửi thư với domain của mình (qua SPF Record trong cấu hình DNS)
  - Chỉ chống giả mạo domain, không chống được giả mạo định danh (nhưng giúp truy vết nhanh chóng)

Chống can thiệp nội dung

❑Chống can thiệp trên đường truyền

- Mã hóa, Ký số nội dung thư: S/MIME, PGP
- Mã hóa, xác thực kênh truyền: SSL/TLS
  - Như là một phần giao thức thư
  - Như là giao thức tầng giao vận

❑Chống can thiệp bởi server

- Mã hóa, Ký số nội dung thư

Tóm lược cổng dịch vụ thư điện tử

- Tất cả giao thức email đều sử dụng TCP
- Truyền thống:
  - SMTP: 25 (465 cho SMPTS)
  - POP3: 110 (995 cho POP3S)
  - IMAP: 143 (993 cho IMAPS)
- SMTP mở rộng
  - submit (user - server): 25 hoặc 587
  - relay (server - server): 25

1 Tổng quan các giao thức thư điện tử

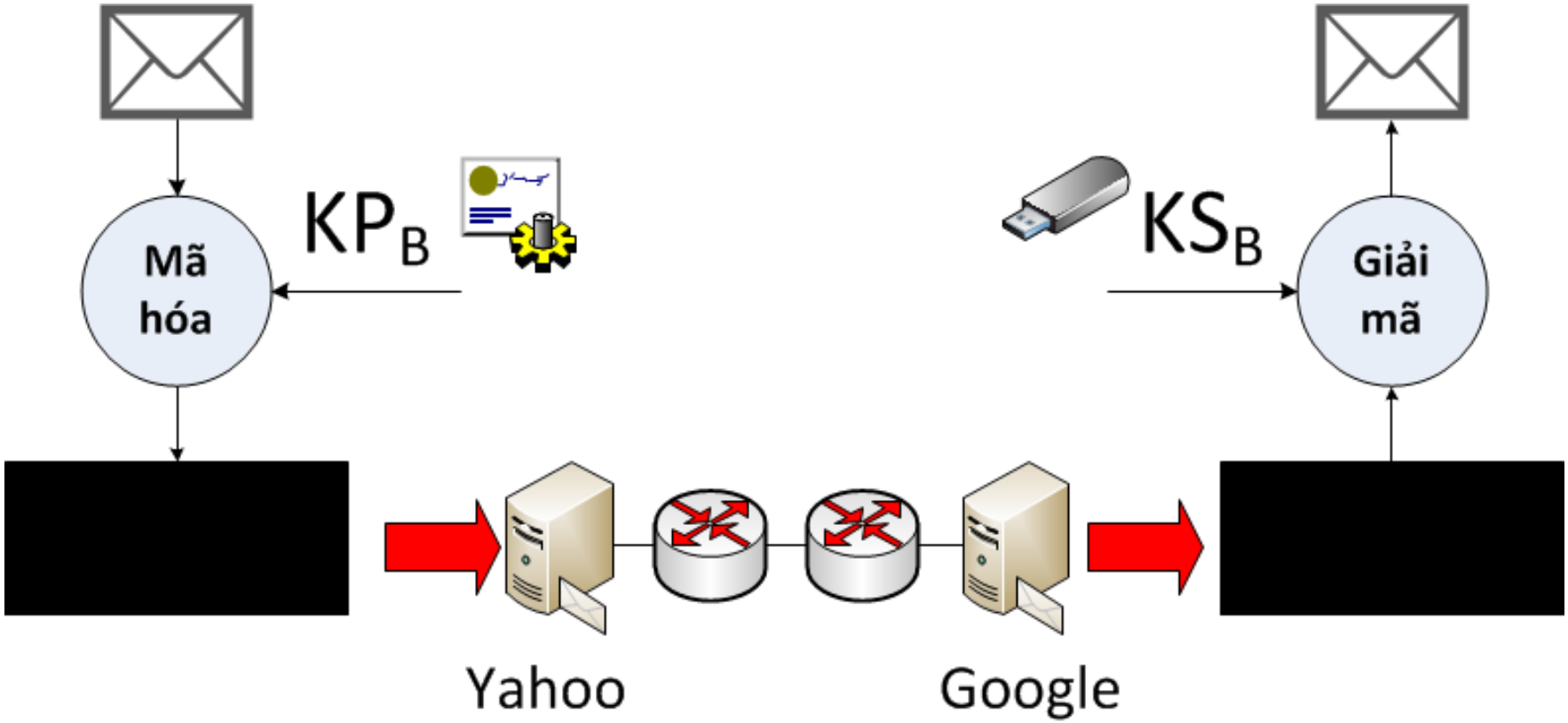
2 Vấn đề an toàn của thư điện tử

3 Giao thức S/MIME

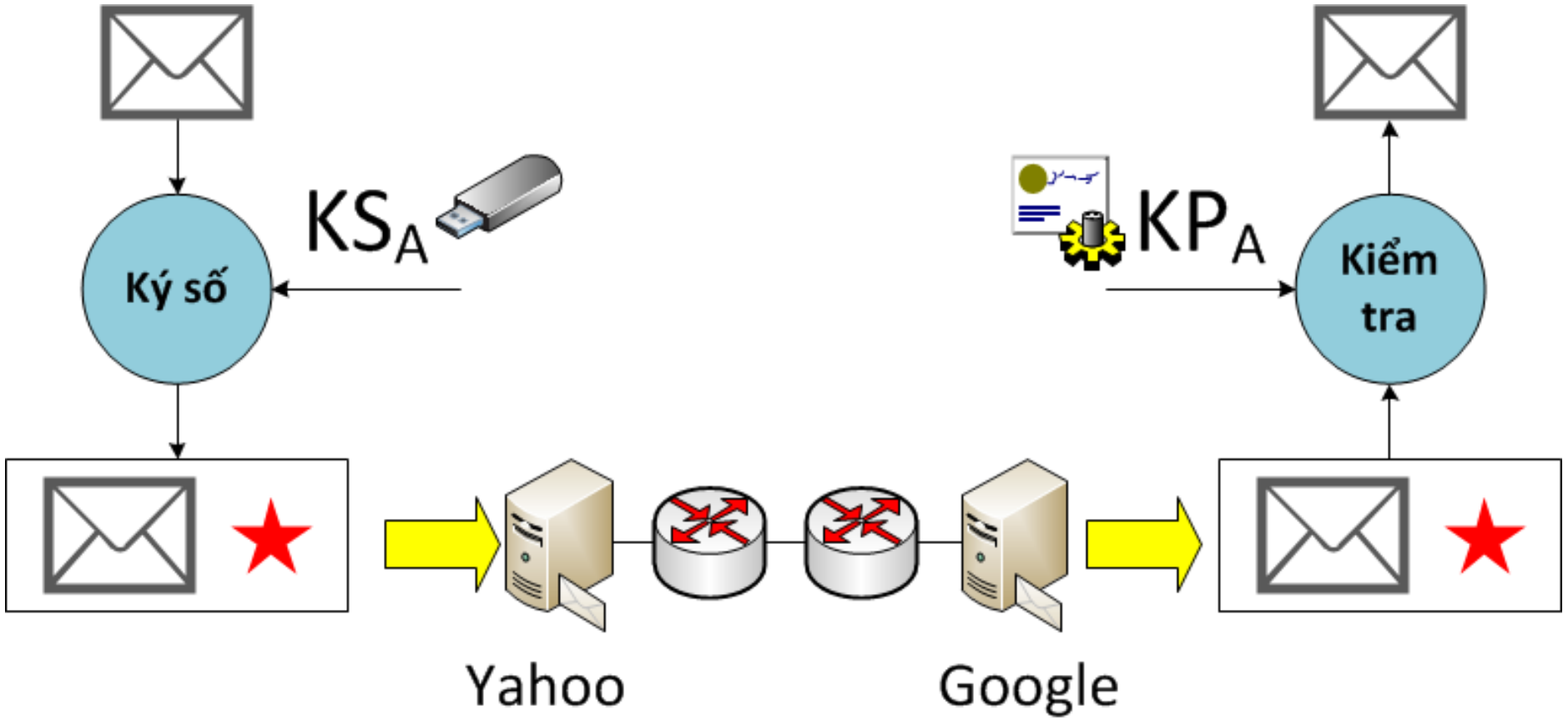
Bảo vệ thư ngay tại tầng ứng dụng

- **Nguyên tắc**
  - Mã hóa
  - Ký số
  - Kết hợp ký và mã
- **Thực thi**
  - S/MIME
  - PGP

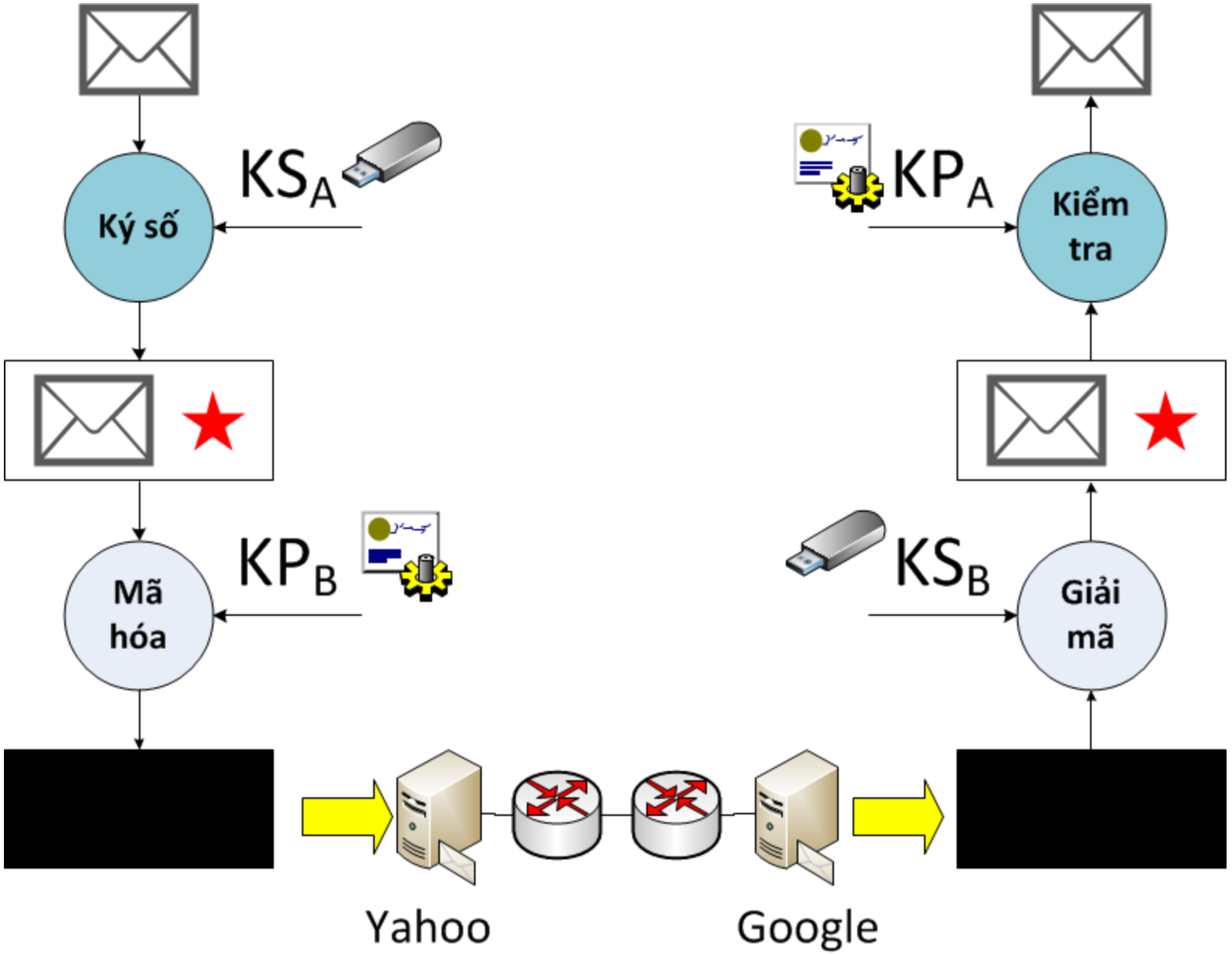
Mã hóa thư điện tử



Ký thư điện tử



Mã hóa kết hợp ký số



Cách thức làm việc của S/MIME

- Sử dụng PKI → khóa công khai (dù là của người nhận hay người gửi) được lưu ở dạng chứng thư số
- Nội dung thư được mã (base64) lại bằng MIME
- Thông điệp MIME sẽ được ký hoặc mã, hoặc kết hợp ký và mã
- Kết quả được mã lại bằng MIME

Ví dụ về mã hóa thư với S/MIME

Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

rfvbnj756tbBghyHhHUujhJhjH77n8HHGT9HG4VQpfyF467GhIGfHfYT6
7n8HHGghyHhHUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H
f8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
0GhIGfHfQbnj756YT64V

Ví dụ về ký số thư với S/MIME

Content-Type: multipart/signed; protocol="application/pkcs7-signature";
micalg=sha1; boundary=boundary42

--boundary42
Content-Type: text/plain

This is a clear-signed message.

--boundary42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
7GhIGfHfYT64VQbnj756

--boundary42--

1 World Wide Web

2 Thư điện tử

3 Đăng nhập từ xa

Remote Login

- Ở chế độ văn bản, người dùng tương tác với hệ điều hành thông qua "terminal"
- Network Virtual Terminal: cơ chế tạo cửa sổ terminal cho phép người dùng tương tác với hệ điều hành trên một máy ở xa
- Giải pháp (giao thức):
  - TELNET
  - SSH

1. Đăng nhập từ xa với TELNET
2. Đăng nhập từ xa với SSH

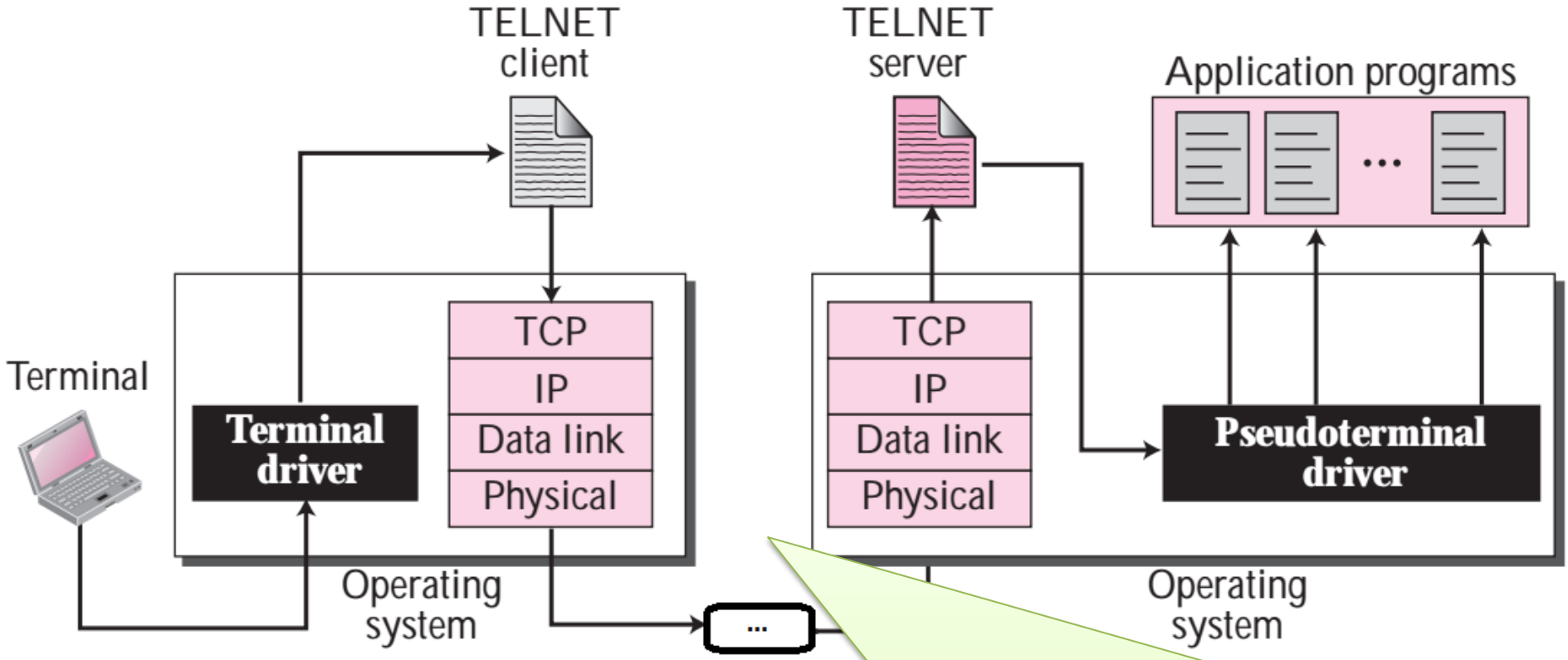
1 Đăng nhập từ xa với TELNET

2 Đăng nhập từ xa với SSH

TELNET

- Ra đời: 1960s
- TELNET = TErminaL NETwork
- TELNET là một giao thức TCP/IP chuẩn
- TELNET cho phép kết nối từ máy cục bộ tới máy ở xa, trong đó máy cục bộ đóng vai trò như một terminal của máy ở xa

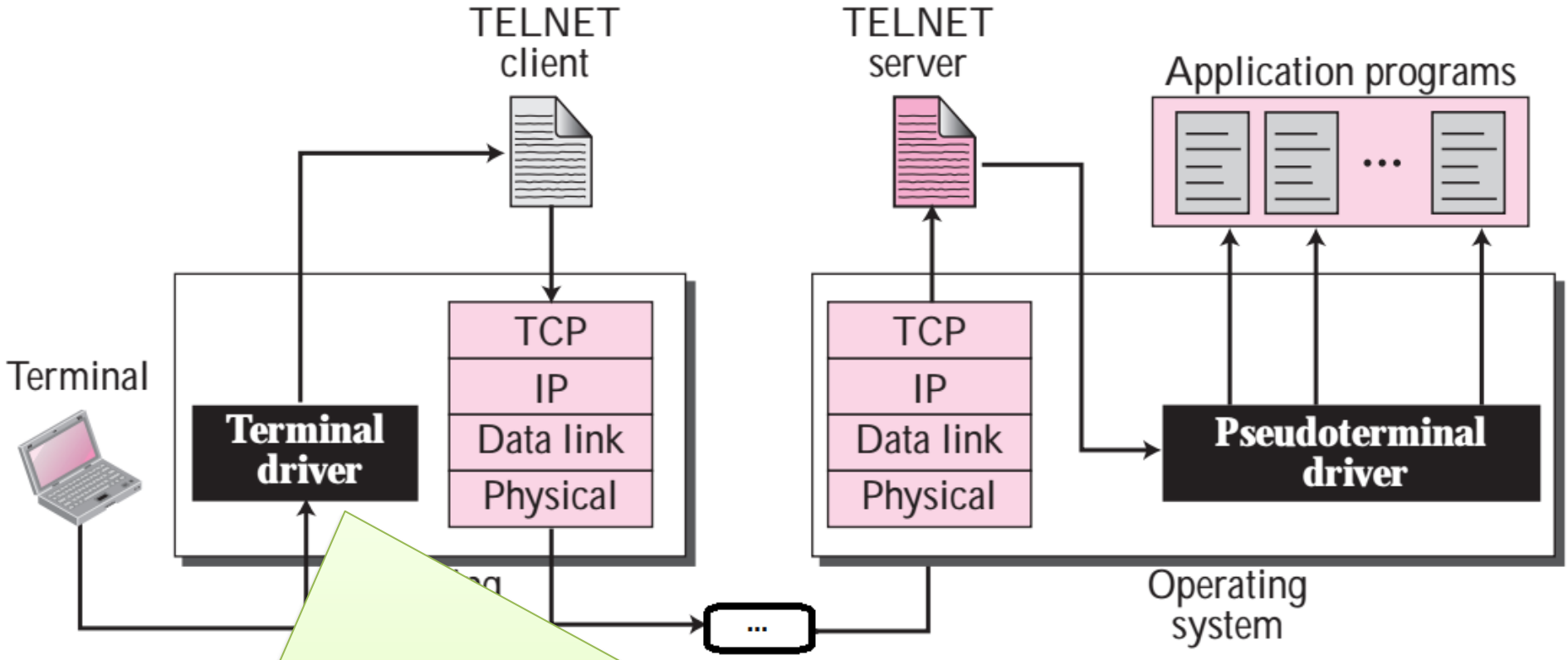
Remote Login với TELNET



Để sử dụng TELNET cần có 2 thành phần:

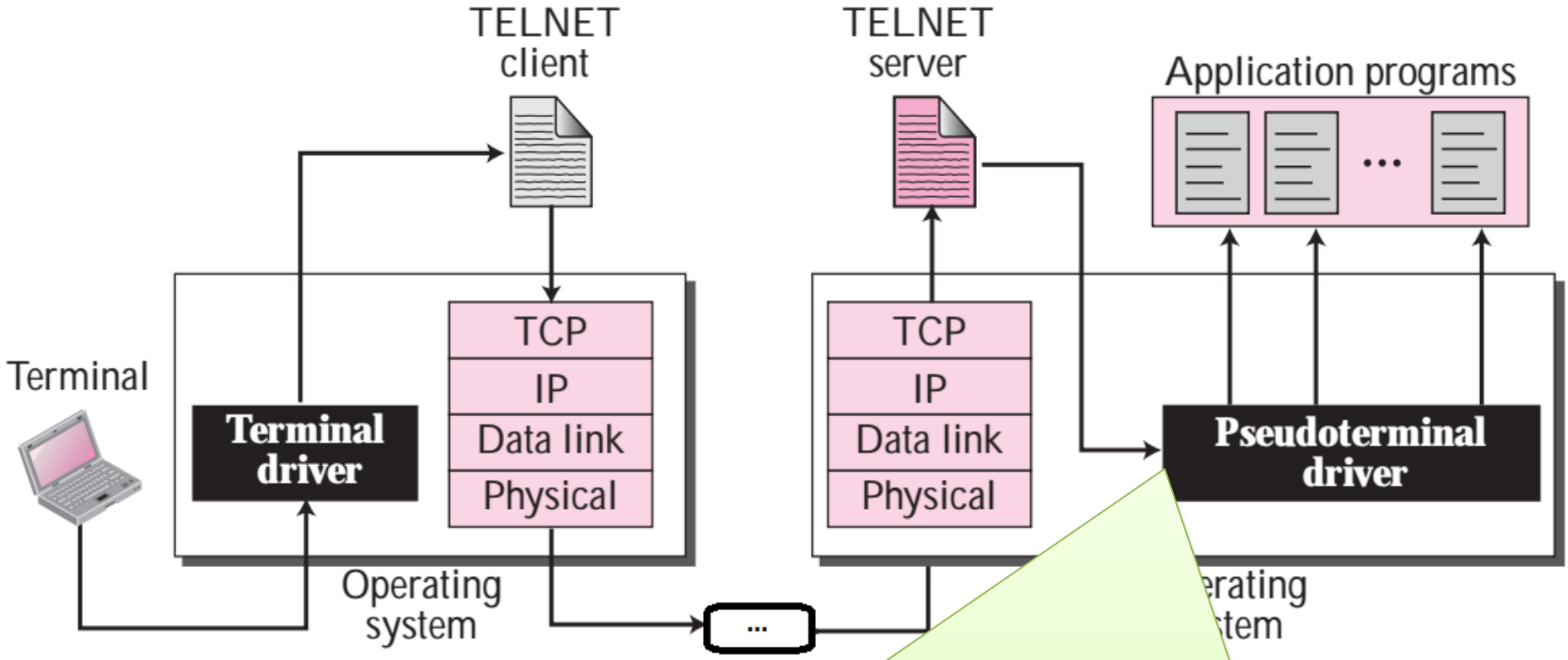
- TELNET Client (trên máy người dùng)
- TELNET Server (trên máy ở xa)

Remote Login với TELNET



1. Người dùng khởi chạy TELNET Client trên terminal của mình
2. TELNET Client chuyển câu lệnh của người dùng tới TELNET Server

Remote Login với TELNET



3. TELNET Server thực thi câu lệnh người dùng trên máy ở xa và gửi kết quả tới Client
4. TELNET Client hiển thị kết quả lên terminal

TELNET

- TELNET hoạt động trên TCP
- TELNET có thể được sử dụng cho những mục đích cụ thể khác nhau
  - Chức năng mặc định là để đăng nhập từ xa (remote login)
    - cổng mặc định là 23
    - xác thực bằng tài khoản trên hệ điều hành
  - Có thể dùng để làm việc với máy ở xa bằng các giao thức trao đổi văn bản (SMTP, POP3,...)
    - sử dụng cơ chế xác thực (nếu có) của giao thức tương ứng
- TELNET hoàn toàn không dùng mật mã

TELNET gmail-smtp-in.l.google.com 25

```
220 mx.google.com ESMTP l25si47138695pfi.9 - gsmtp
EHLO google.com
250-mx.google.com at your service, [2402:800:4364:21aa:c5a2:deca:d580:ea2f]
250-SIZE 157286400
250-8BITMIME
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250 SMTPUTF8
MAIL FROM: <user1@gmail.com>
250 2.1.0 OK l25si47138695pfi.9 - gsmtp
RCPT to: <user2@gmail.com>
550-5.1.1 The email account that you tried to reach does not exist. Please try
550-5.1.1 double-checking the recipient's email address for typos or
550-5.1.1 unnecessary spaces. Learn more at
550 5.1.1  https://support.google.com/mail/?p=NoSuchUser l25si47138695pfi.9 - gsmtp
RCPT TO: <tuananh1982act@gmail.com>
250 2.1.5 OK l25si47138695pfi.9 - gsmtp
DATA
354  Go ahead l25si47138695pfi.9 - gsmtp
FROM:user1
TO:anyuser
This is the body of the email message.
The body is ended with a single dot in a line.
.
```

1 Đăng nhập từ xa với TELNET

2 Đăng nhập từ xa với SSH

SSH

- SSH = Secure SHell
- SSH có vai trò chính là giao thức quản trị từ xa an toàn, thay thế cho TELNET
- SSH có 2 phiên bản hoàn toàn KHÔNG tương thích nhau: SSH-1 (1995), SSH-2 (1996)
- Hiện nay, SSH-2 (RFC 4251) là giao thức quản trị từ xa mặc định của mọi admin.

Dịch vụ của SSH

- Secure login connections
- Secure file transfer
- Secure data transfer (tunneling)

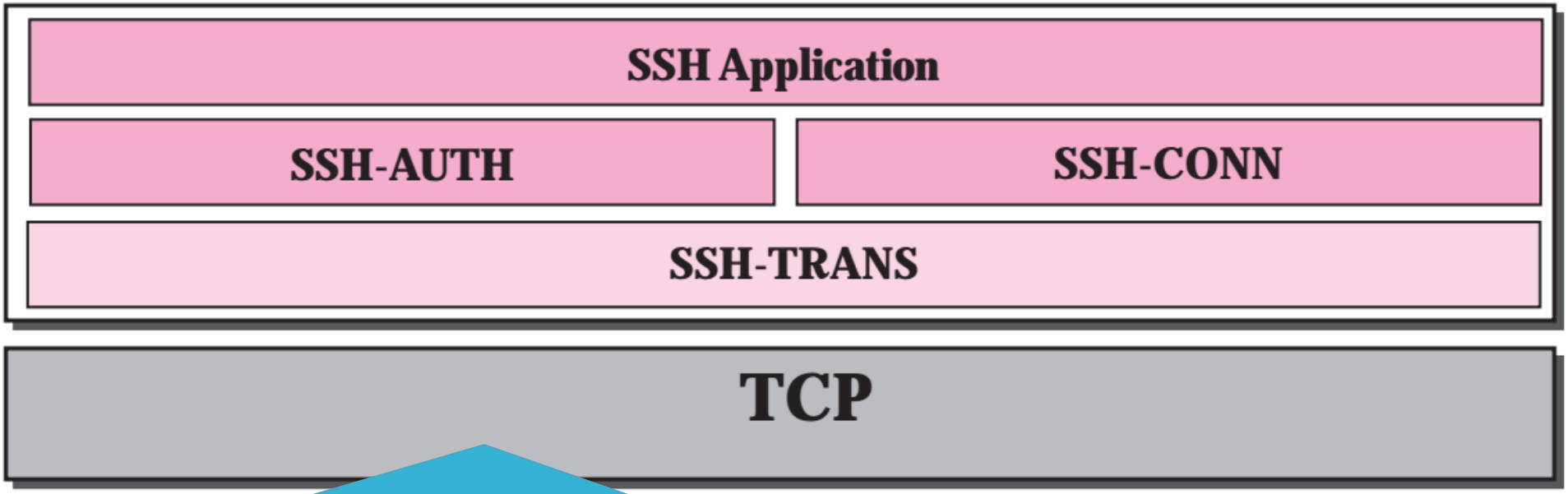
Chức năng an toàn của SSH

- Xác thực thực thể 2 chiều
  - Xác thực SSH server: public key (RSA)
  - Xác thực SSH user: password, public key
- Xác thực thông điệp: HMAC (MD5, SHA1)
- Mã hóa dữ liệu: symmetric ciphers
- Nén dữ liệu (tùy chọn): GZIP

SSH RFCs

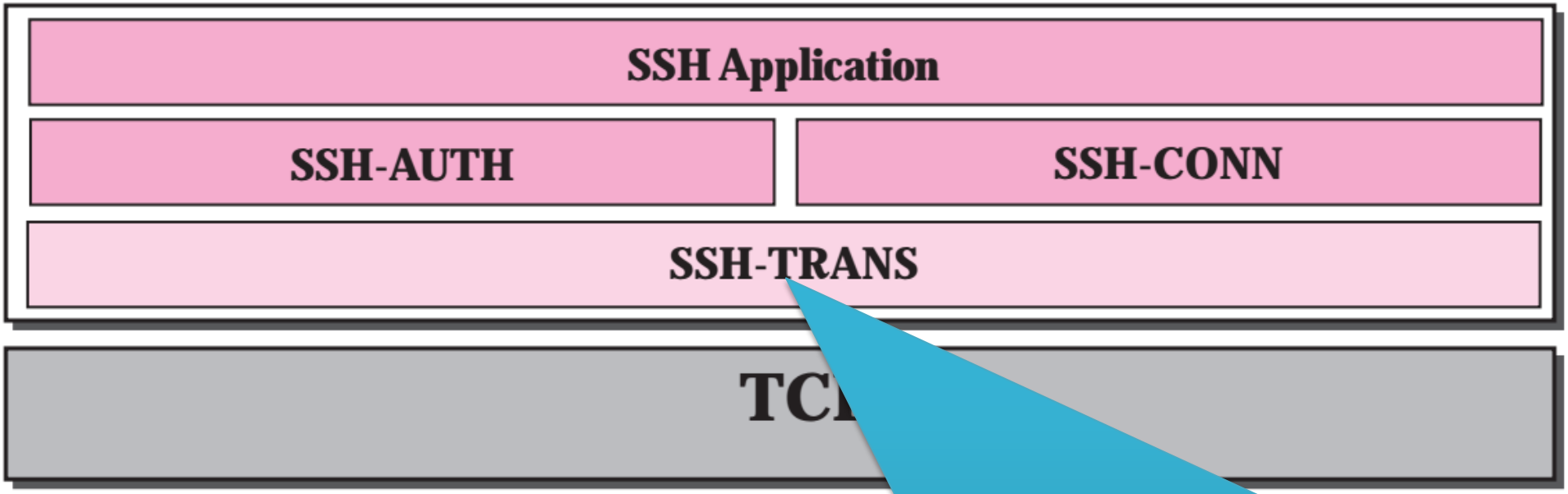
- RFC 4250: SSH Protocol Assigned Numbers
- RFC 4251: SSH Protocol Architecture
- RFC 4252: SSH Authentication Protocol
- RFC 4253: SSH Transport Layer Protocol
- RFC 4254: SSH Connection Protocol
- RFC 4344: SSH Transport Layer Encryption Modes
- …

Kiến trúc giao thức SSH



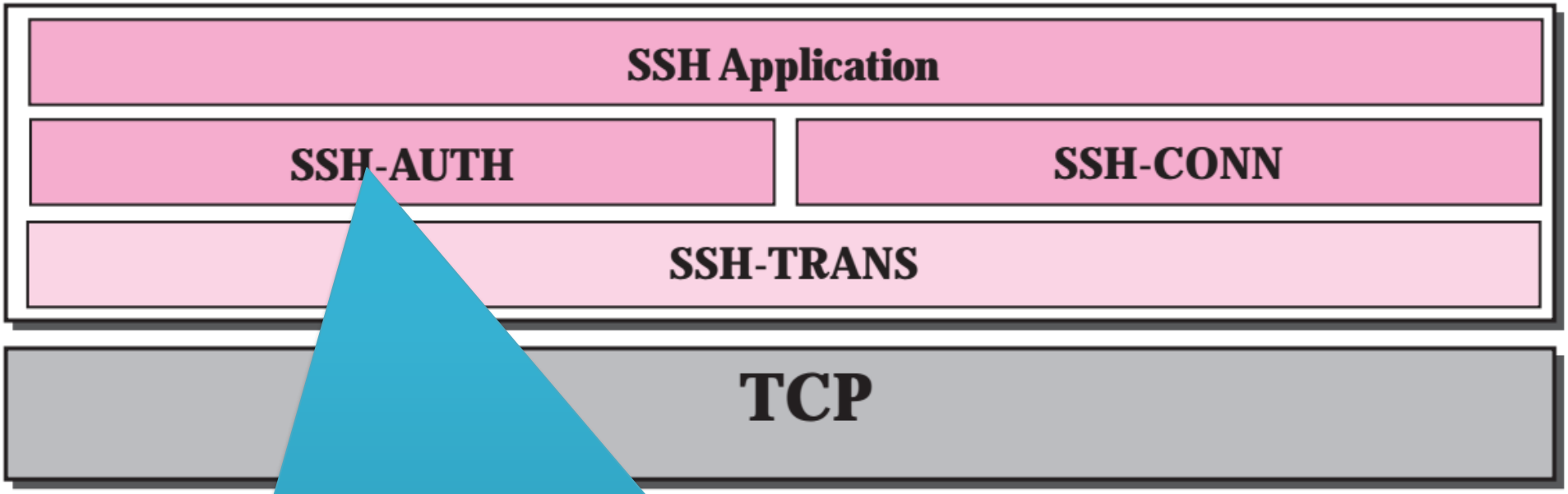
- SSH làm việc trên TCP (hoặc bất kỳ giao thức giao vận tin cậy nào)
- Cổng mặc định: 22 (TCP)
- Kiến trúc SSH-2: RFC 4251

Kiến trúc giao thức SSH



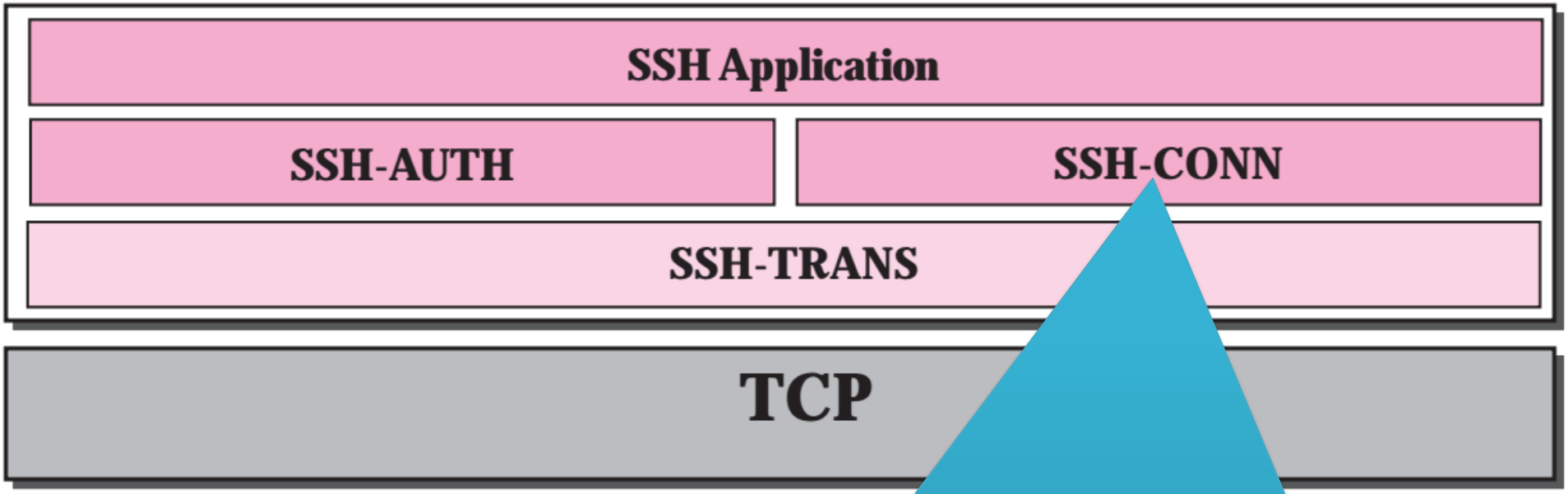
- SSH Transport Layer Protocol (RFC 4253)
- Server Authentication and Key Exchange, Data Confidentiality, Data Integrity (with forward secrecy), Compression

Kiến trúc giao thức SSH



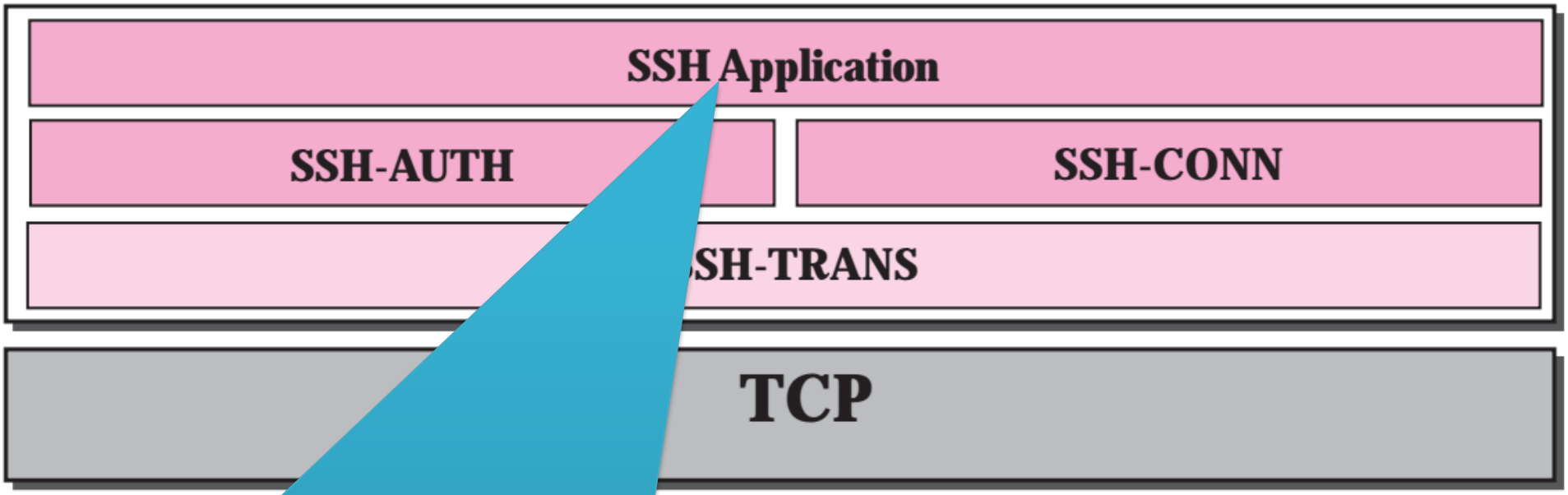
- SSH User Authentication Protocol (RFC 4252)
- Xác thực client
- Thực thi trên SSH-TRANS

Kiến trúc giao thức SSH



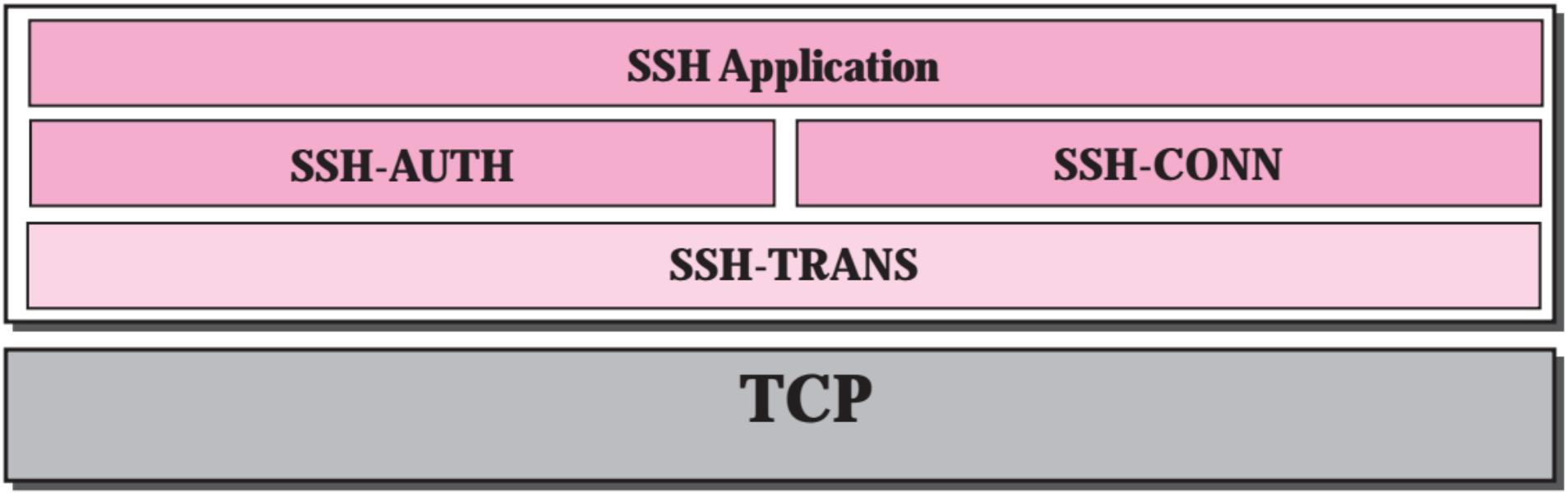
- SSH Connection Protocol (RFC 4254)
- Ghép (multiplex) nhiều kết nối logic vào một kết nối SSH.
- Thực thi trên SSH-TRANS sau khi hoàn tất SSH-AUTH

Kiến trúc giao thức SSH



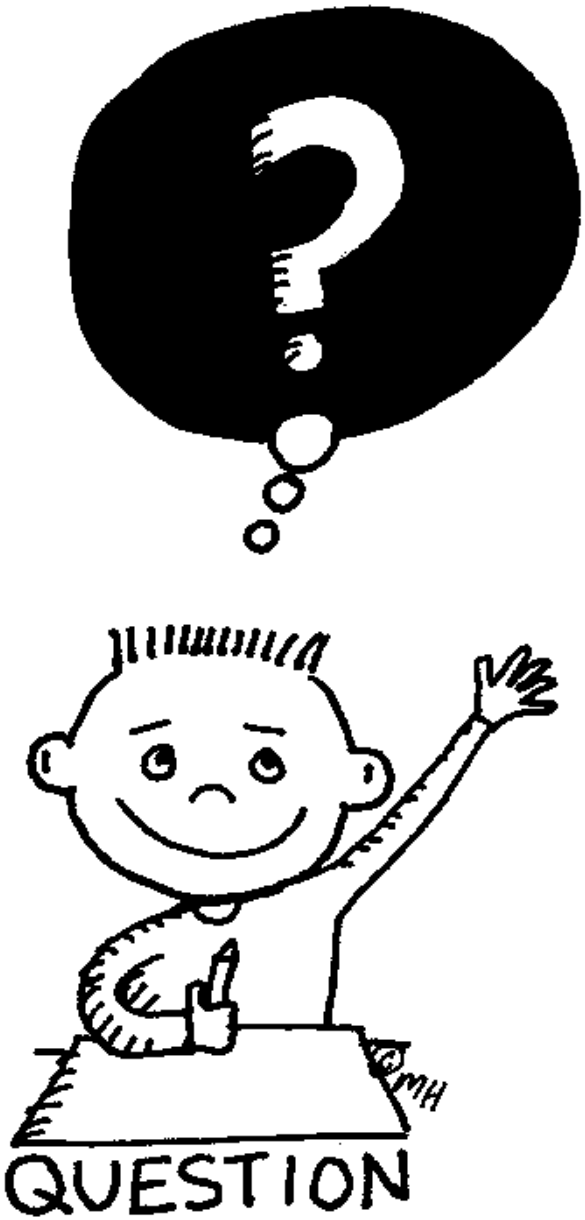
- Triển khai các ứng dụng an toàn trên SSH
- Sử dụng giao thức SSH-CONN
- Ví dụ: remote login, file transfer...

Kiến trúc giao thức SSH



Như vậy, Remote Login bằng SSH được đảm bảo an toàn với các dịch vụ:

- Xác thực thực thể (2 chiều)
- Thỏa thuận thuật toán, tham số mật mã
- Mã hóa, xác thực thông điệp


QUESTION

Tự tìm hiểu

- Chi tiết các câu lệnh trong SMTP và POP3 ([2: Chapter 23.3-23.4])
- Tìm hiểu chi tiết về TELNET ([2: Ch. 22])
- Tìm hiểu chi tiết về SSH ([3],[4])
- Tìm hiểu Pretty Good Privacy

Thực hành

- Bài tập đã giao
- OpenSSH cho Windows 10 (Version 1709)

  https://winaero.com/blog/enable-openssh-server-windows-10/
- Cấp chứng thư số cho SSH Server

  https://social.technet.microsoft.com/Forums/en-US/1ad28f33-a4f0-4cd8-aa9b-e03553f97f50/enterprise-ca-could-generate-host-linux-sshd-host-keys?forum=winserversecurity