NHẬP MÔN MẠNG MÁY TÍNH

Chương 1

GIỚI THIỆU

MẠNG MÁY TÍNH

Nội dung chương 1

I. Định nghĩa mạng máy tính

II. Các mô hình mạng máy tính

III. Kiến trúc mạng máy tính

IV. Môi trường truyền vật lý mạng cục bộ

I. Định nghĩa mạng máy tính

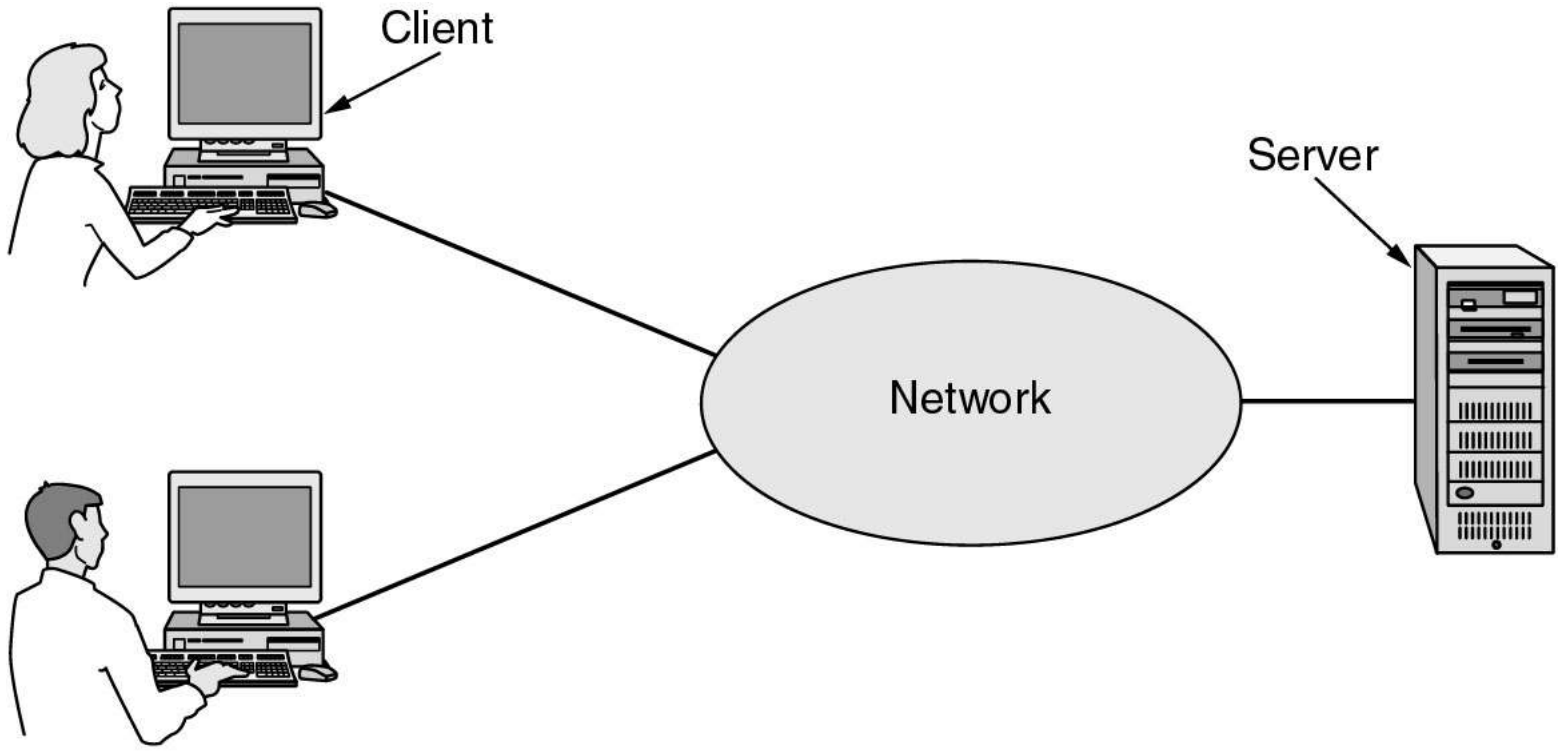
Mạng máy tính:

- bao gồm các máy tính độc lập,
- được kết nối với nhau trên mạng
- nhằm chia sẻ tài nguyên

  và trao đổi dữ liệu

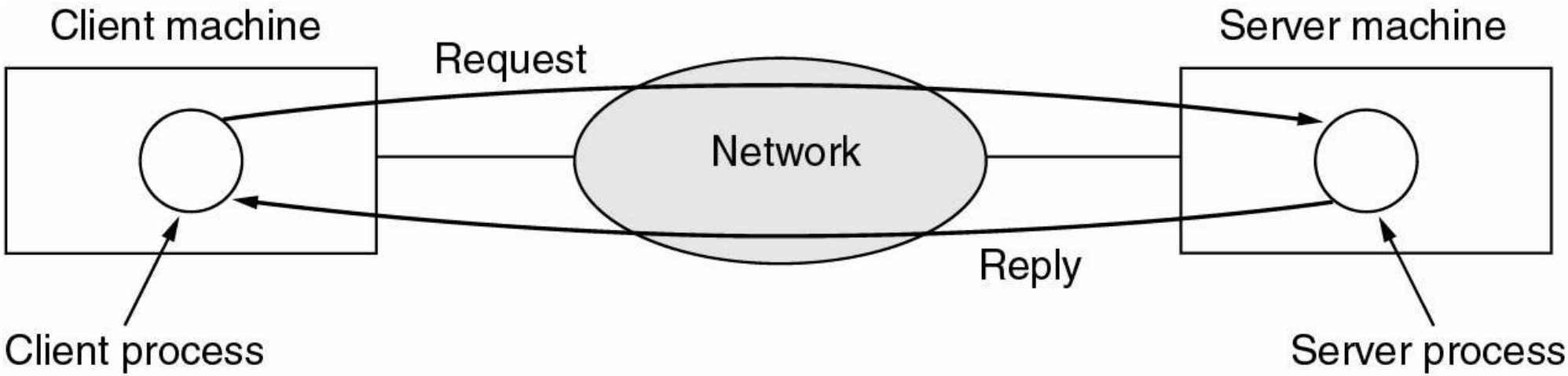
Host: máy tính trên mạng

Ví dụ 1: mô hình client-server

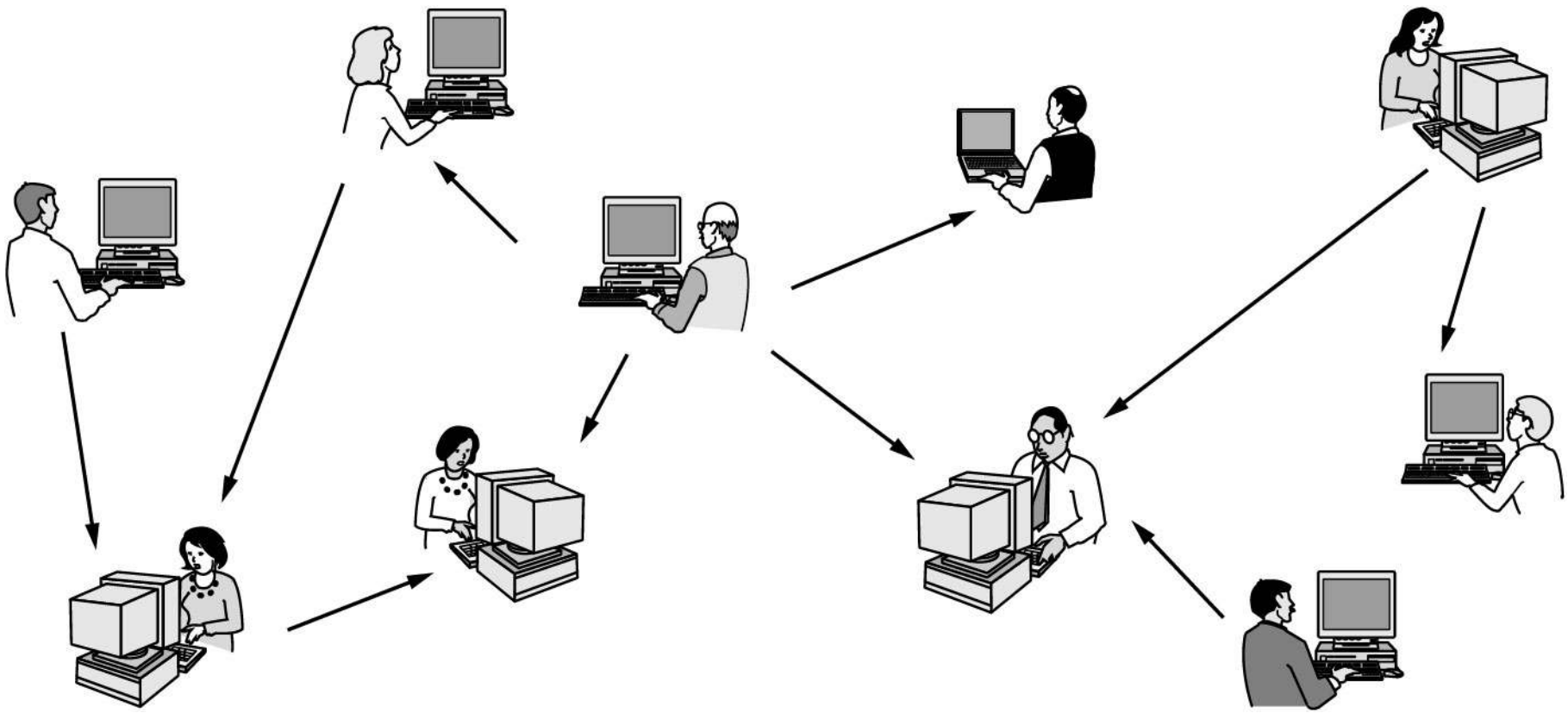


Mạng máy tính với 2 Client và 1 Server

Mô hình ứng dụng mạng Client-Server



Ví dụ 2: mô hình peer-to-peer



Mạng ngang hàng (peer-to-peer network)

Các ứng dụng của mạng máy tính

- Ứng dụng trong cơ quan, doanh nghiệp
- Ứng dụng trong gia đình, cá nhân
- Ứng dụng trên thiết bị di động

Ví dụ: e-commerce – thương mại điện tử

	Dạng đầy đủ	Ví dụ
B2C	Business-to-consumer	Đặt mua hàng trên mạng
B2B	Business-to-business	Nhà sản xuất đặt hàng
G2C	Government-to-consumer	Chính phủ phát hành biểu mẫu
C2C	Consumer-to-consumer	Đấu giá trên mạng
P2P	Peer-to-peer	Chia sẻ file

Một số dạng thương mại điện tử

II. Các mô hình mạng máy tính

II.1 Các kỹ thuật truyền dữ liệu

II.2 Phân loại mạng máy tính

II.3 Phần cứng mạng máy tính

II.4 Phần mềm mạng máy tính

II.1 Các kỹ thuật truyền dữ liệu

Hai dạng truyền dữ liệu cơ bản:

- Broadcast (quảng bá)
- Point-to-point (giữa hai điểm)

Truyền dữ liệu dạng broadcast

- Dùng 1 kênh truyền chung cho tất cả các máy trên mạng
- Dữ liệu (packet) gởi từ 1 máy sẽ đến tất cả các máy khác
- Có địa chỉ máy nhận cùng với dữ liệu

Multicast: 1 máy gởi dữ liệu và một nhóm máy nhận

Truyền dữ liệu dạng point-to-point

- Tồn tại một kênh truyền riêng giữa hai máy
- Kênh truyền này có thể qua các máy trung gian khác trên mạng
- Còn được gọi là dạng unicast

II.2 Phân loại mạng máy tính

Khoảng cách	Loại mạng
10m – 1km	Local Area Network (LAN)
10km-100km	Metropolitan Area Network (MAN)
100km-1.000km	Wide Area Network (WAN)
10.000km	Internet

Phân loại mạng máy tính theo khoảng cách

Các dạng mạng cục bộ (LAN)

- Mạng ngang hàng (workgroup)
  - Các máy tương đương nối mạng để chia sẻ tài nguyên
- Mạng client/server
  - Có một hoặc nhiều máy dùng làm server để quản lý user, cài đặt các ứng dụng, lưu trữ dữ liệu …
  - Các máy khác kết nối đến server để truy xuất có kiểm soát các tài nguyên

II.3 Phần cứng mạng máy tính

- Local Area Network

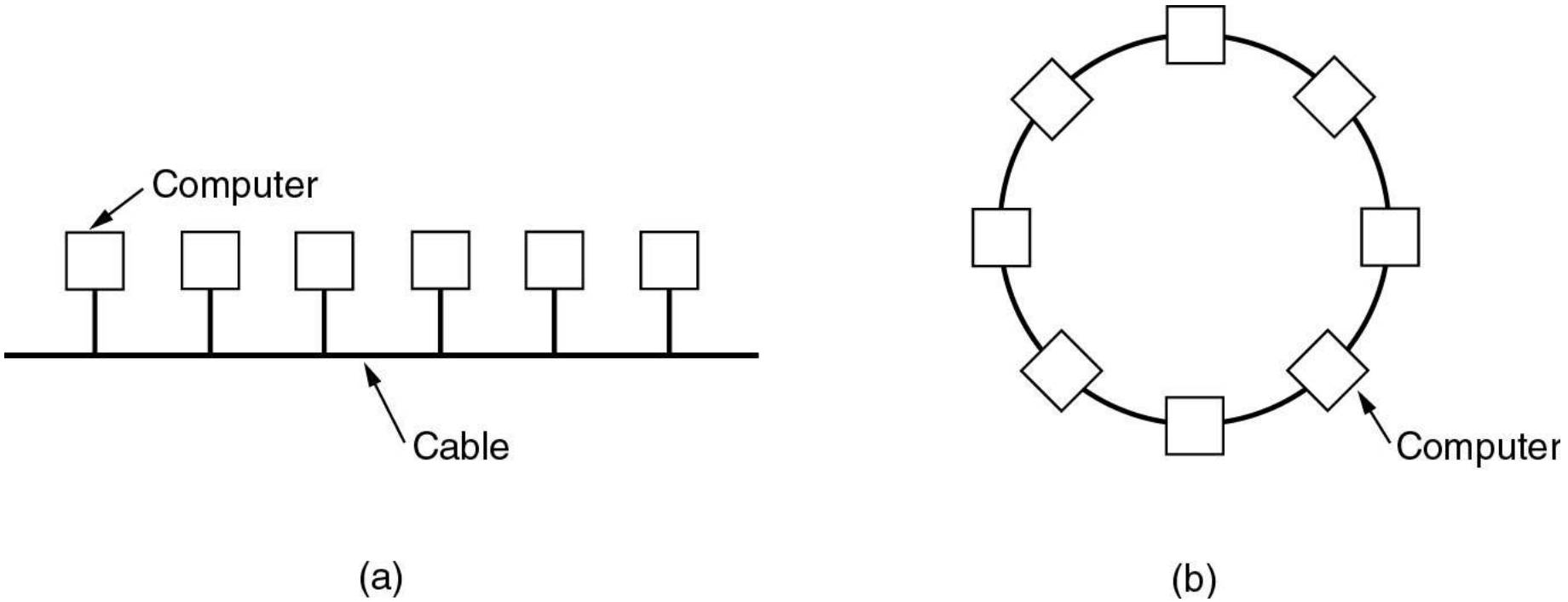
  Mạng cục bộ
- Wide Area Network

  Mạng miền rộng/Mạng diện rộng
- Wireless Network

  Mạng cục bộ không dây (ví dụ Wi-Fi)

  Mạng miền rộng không dây (ví dụ WiMax)

Mạng cục bộ - LAN



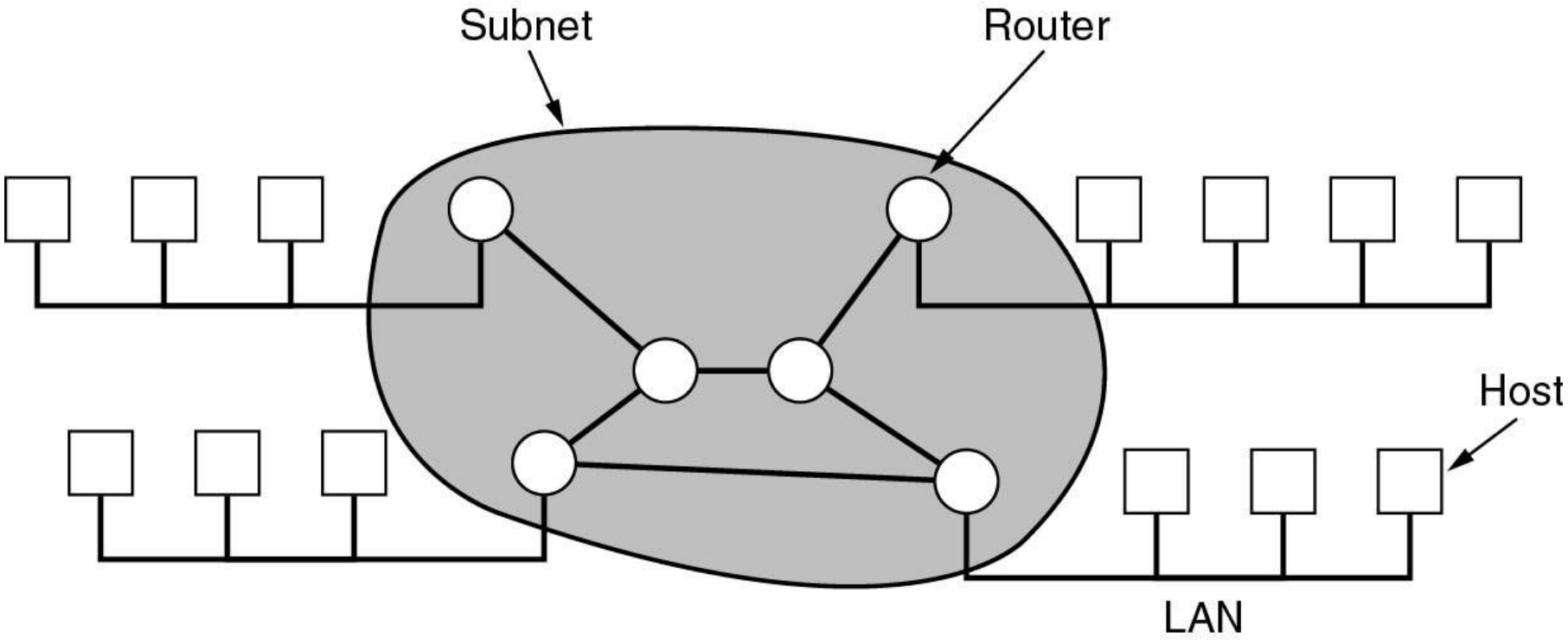
Hai dạng mạng cục bộ

a. Bus b. Ring

Các thành phần kết nối LAN

- Card mạng – Network Interface Card (NIC)
- Dây mạng – Cable
- Các thiết bị kết nối: Hub, Switch, …

Mạng miền rộng - WAN



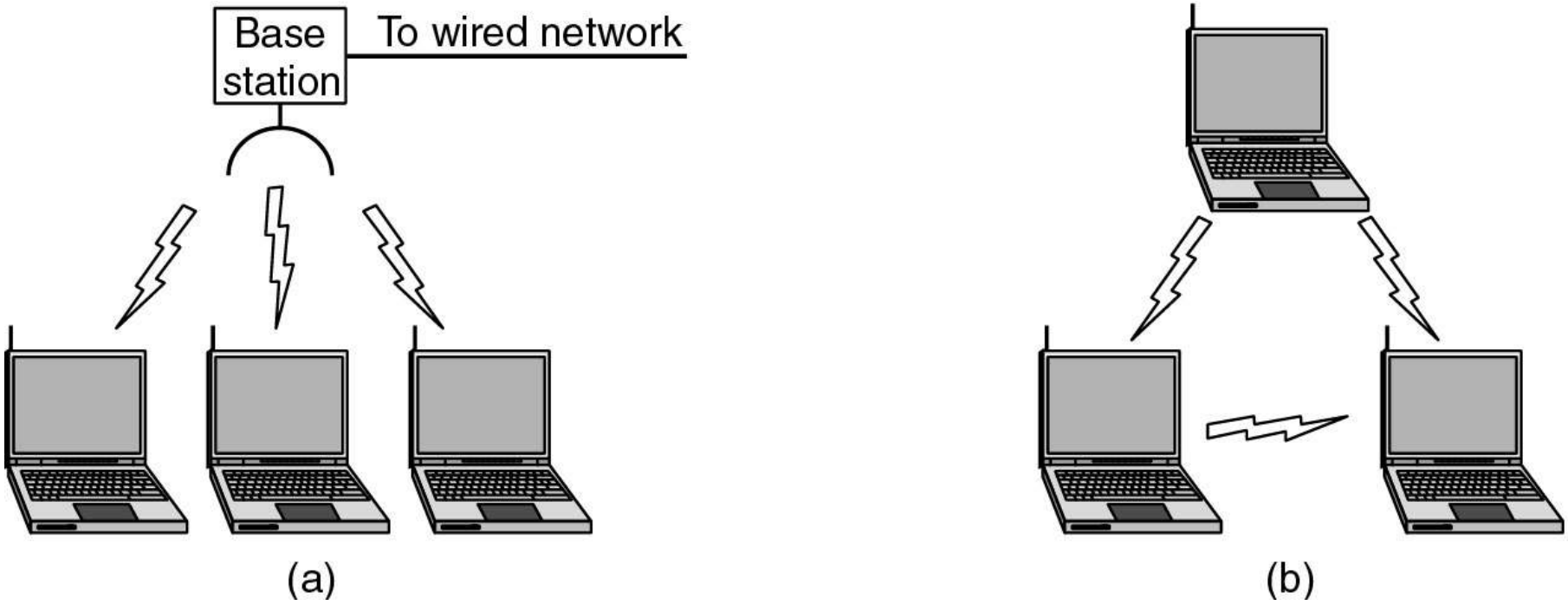
WAN gồm các LANs và phần kết nối (subnet)

Subnet

Phần kết nối mạng miền rộng gồm 2 phần:

- Các đường truyền (transmission lines) dây đồng, cáp quang, sóng điện từ, …
- Các phần tử chuyển mạch (switching elements), thường được gọi là router
  - Kết nối với nhiều đường truyền
  - Nhận dữ liệu và chọn đường truyền để chuyển sang mạng khác

Mạng không dây –Wireless LAN

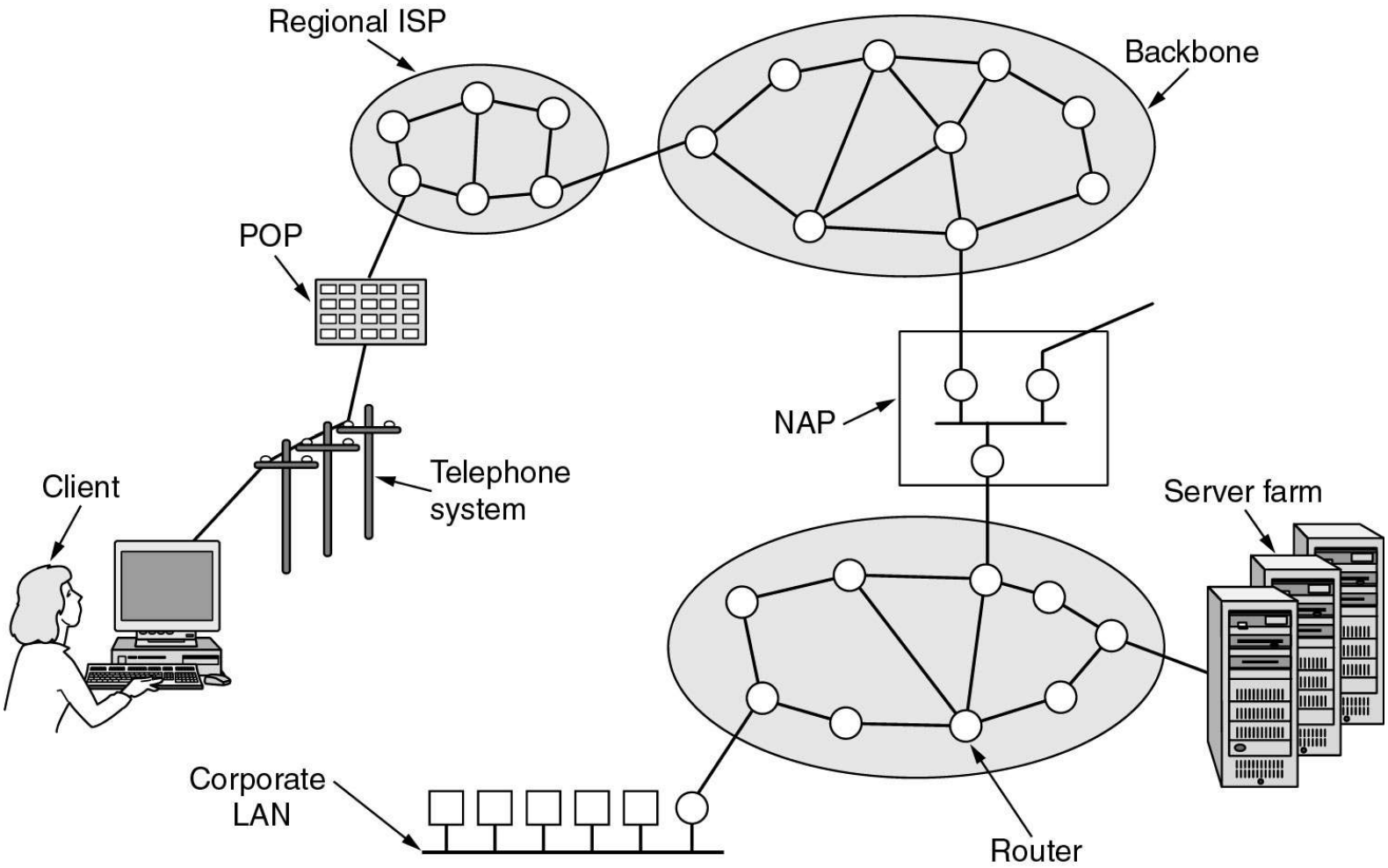


Hai dạng kết nối mạng không dây

a. Có dùng base station, còn gọi là access point

b. Các máy gởi nhận trực tiếp, ad hoc networking

Mạng Internet



Tổng quan mạng Internet

Các thành phần chính trên mạng Internet

- Trục chính – Backbone
- Các nhà cung cấp dịch vụ - ISPs (Internet Service Provider)
  - POP (Point of Presence):nơi nhận tín hiệu từ mạng điện thoại và đưa vào mạng của ISP
- NAP (Network Access Point)
- Các server
- Client từ máy lẻ, các LANs

II.4 Phần mềm mạng máy tính

- Hệ điều hành mạng
- Phần mềm phía server
- Phần mềm phía client

III. Kiến trúc mạng máy tính

III.1 Tổ chức thứ bậc của các giao thức

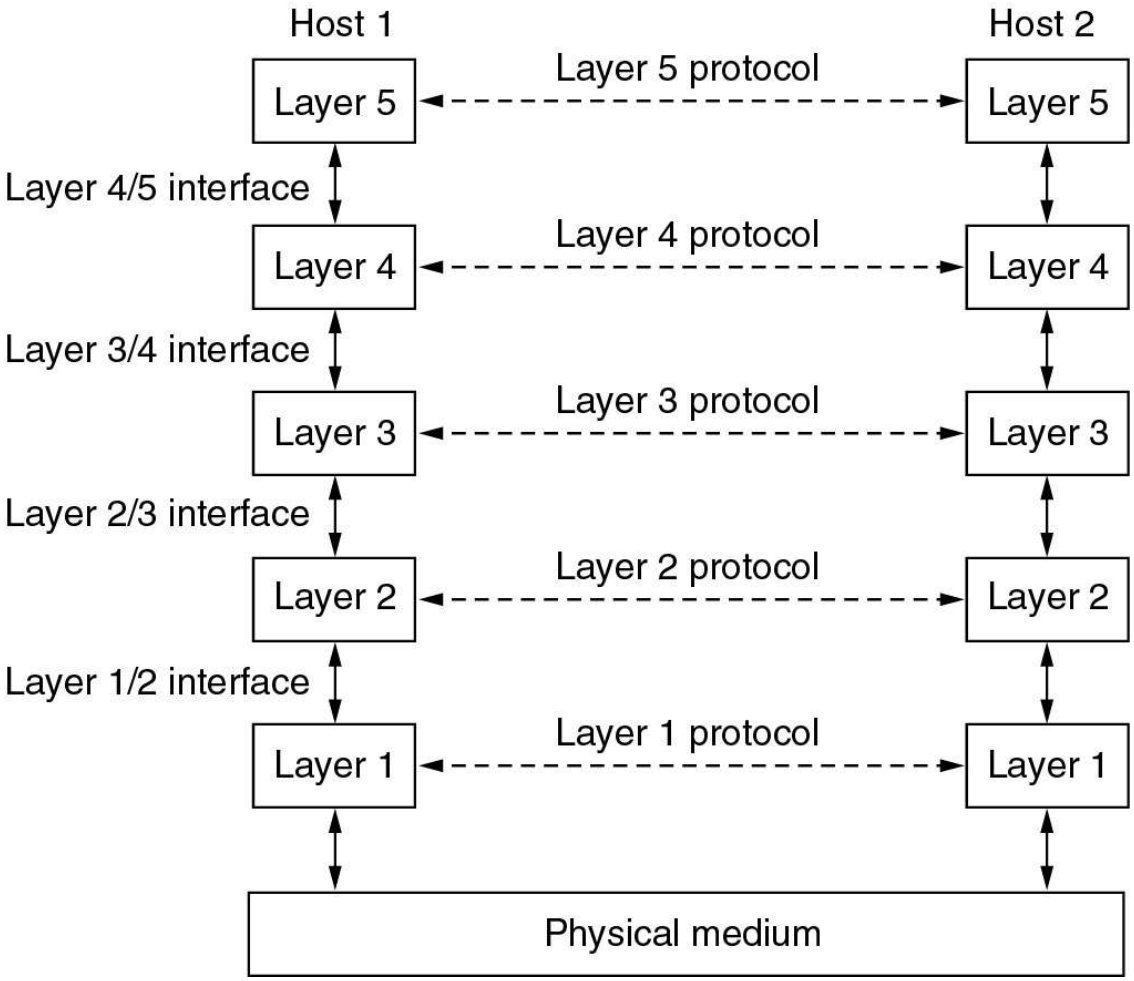
III.2 Các tiêu chuẩn mạng

- ISO OSI
- TCP/IP

III.1 Tổ chức thứ bậc của các giao thức

- Tổ chức luận lý mạng máy tính: gồm các lớp (layers/levels)
  - Số lớp, chức năng mỗi lớp phụ thuộc loại mạng.
- Giao thức (protocol): tập hợp các luật và thủ tục thực hiện việc truyền thông giữa hai bên truyền thông.
- Giao diện (Interface): định nghĩa các thao tác cơ sở của lớp dưới cung cấp cho lớp trên

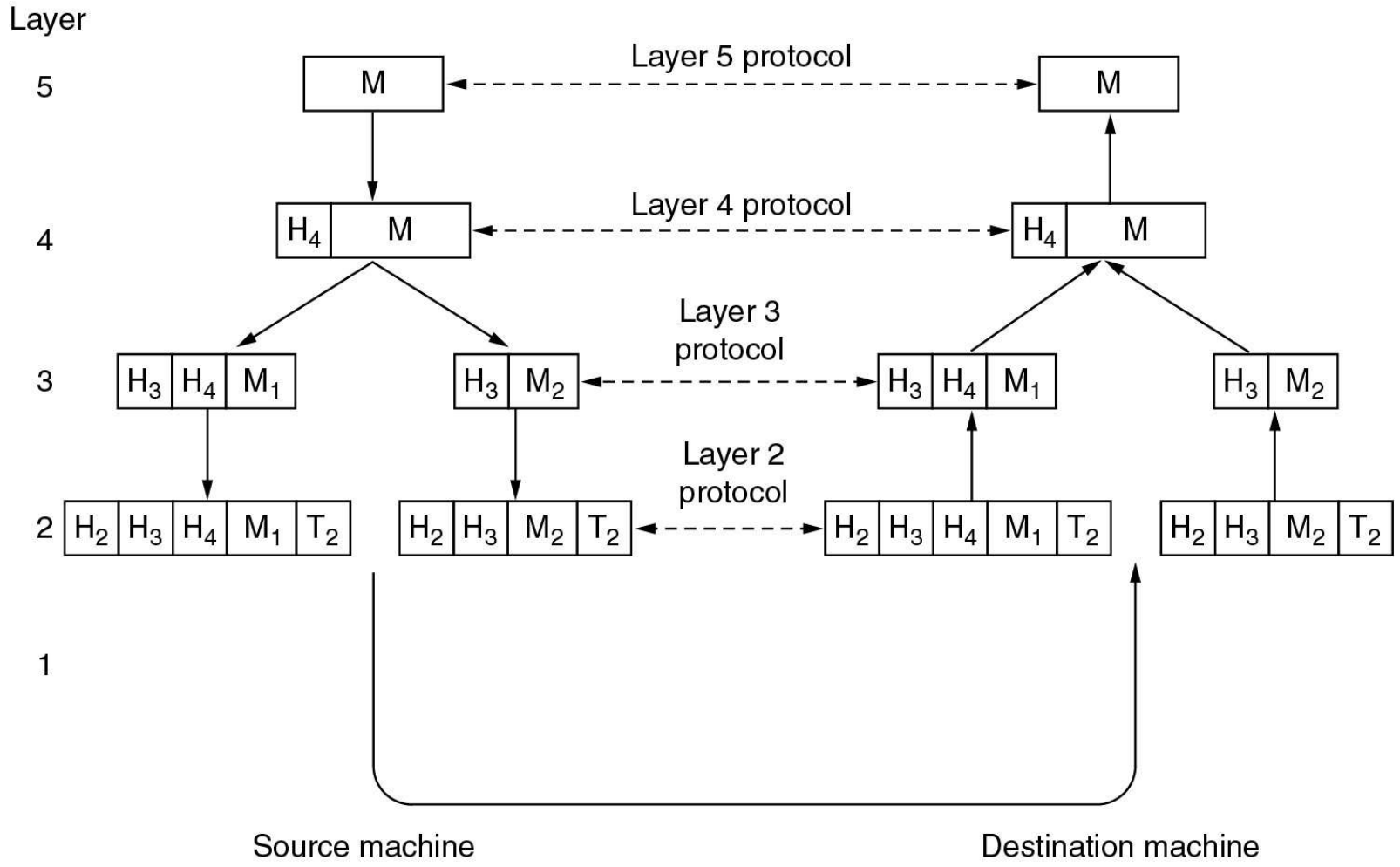
Ví dụ: tổ chức mạng có 5 lớp



Mục đích của tổ chức mạng theo lớp

- Giảm sự phức tạp khi thiết kế
- Mô tả chi tiết quá trình truyền dữ liệu từ một máy đến một máy khác

Ví dụ: truyền dữ liệu M giữa 2 máy



H: Header, T: Trailer

Kiến trúc mạng máy tính

- Kiến trúc mạng máy tính:

  Tập hợp các lớp và giao thức.

- Bộ giao thức (protocol stack / protocol suite): Danh sách các giao thức được sử dụng cho từng lớp trên một hệ thống xác định.

III.2 Các tiêu chuẩn mạng

- Hai mô hình kiến trúc mạng quan trọng:

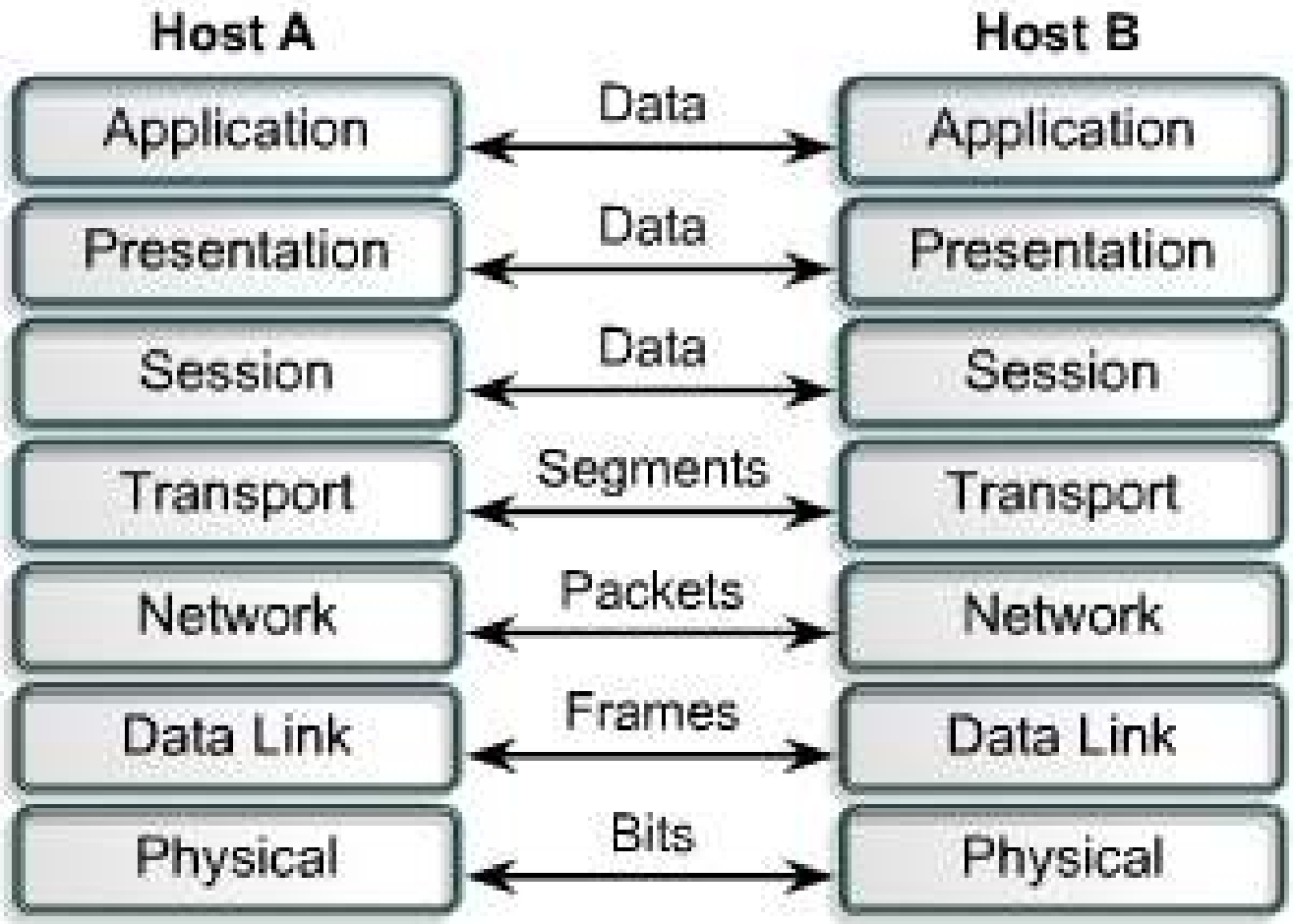
  OSI (Open Systems Interconnection)

  TCP/IP (Transmission Control Protocol/ Internet Protocol)

- Các bộ giao thức khác:
  - IPX/SPX (Internetwork Packet Exchange/ Sequenced Packet Exchange)
  - NetBEUI (NetBIOS Extended User Interface)
  - AppleTalk

OSI

a. Mô hình OSI



b. Truyền thông giữa 2 máy

Sơ lược chức năng các lớp mô hình OSI

Lớp vật lý - Physical

- Truyền chuỗi bít trên kênh truyền
- Quy định về môi trường truyền vật lý, tín hiệu điện, cơ khí.

Lớp liên kết dữ liệu – Data Link

- Truyền dữ liệu có cấu trúc (frame) tin cậy giữa hai máy trên môi trường vật lý.
- Quy định về địa chỉ thiết bị, kiểm soát lỗi

Sơ lược chức năng các lớp mô hình OSI (tt)

Lớp mạng – Network

- Xác định con đường (route) từ máy gởi đến máy nhận, quản lý các vấn đề lưu thông trên mạng
- Quy định về địa chỉ mạng

Lớp giao vận - Transport

- Chia dữ liệu thành các đơn vị nhỏ hơn nếu cần và ghép lại tại nơi nhận.
- Thực hiện kiểm soát lỗi

Sơ lược chức năng các lớp mô hình OSI (tt)

Lớp phiên – Session

- Thiết lập, quản lý, kết thúc các phiên làm việc giữa các ứng dụng

Lớp trình diễn – Presentation

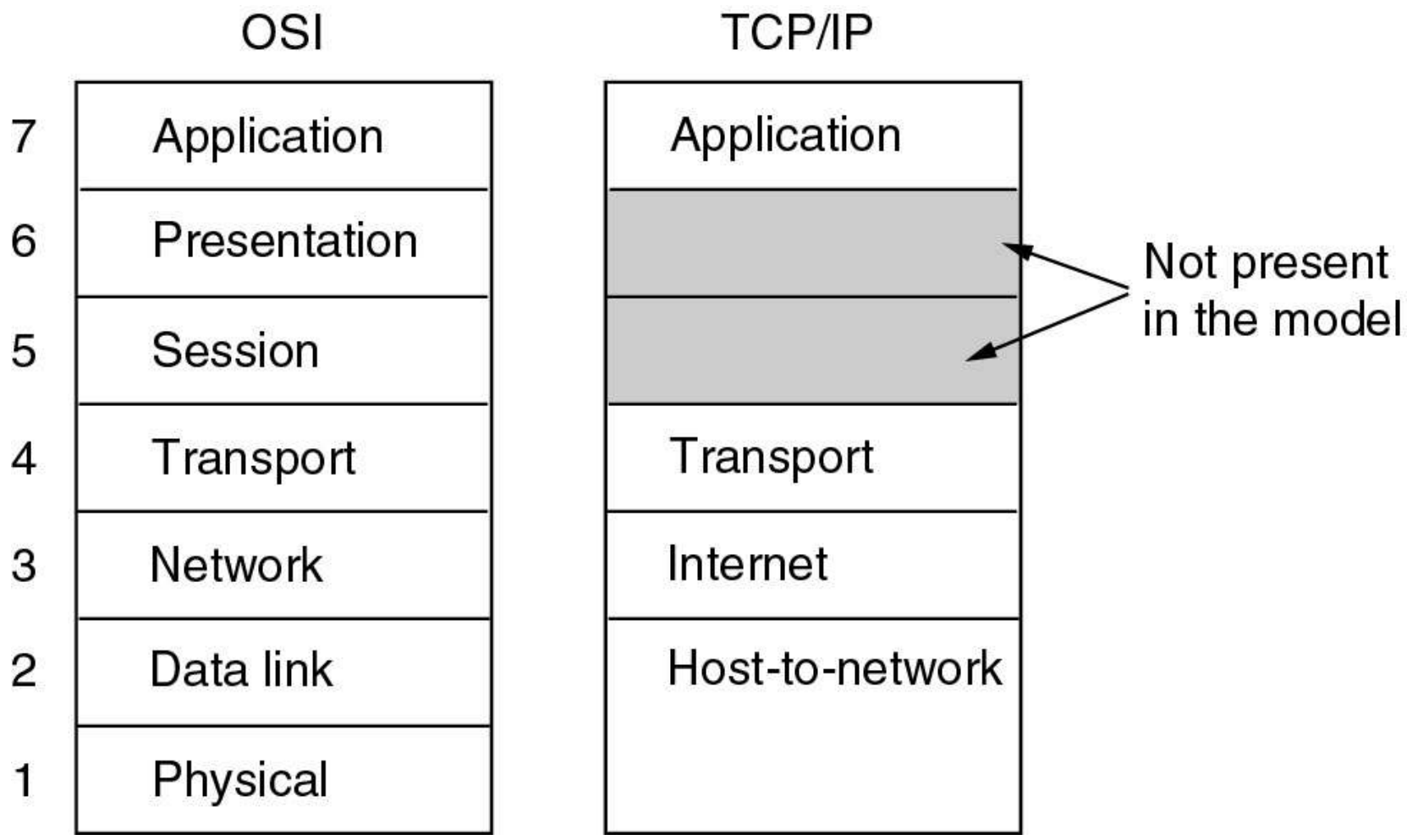
- Quy định về khuôn dạng, cú pháp, ngữ nghĩa của dữ liệu khi truyền thông

  → data representation

Lớp ứng dụng – Application

- Bao gồm các giao thức của các dịch vụ mạng

OSI và TCP/IP

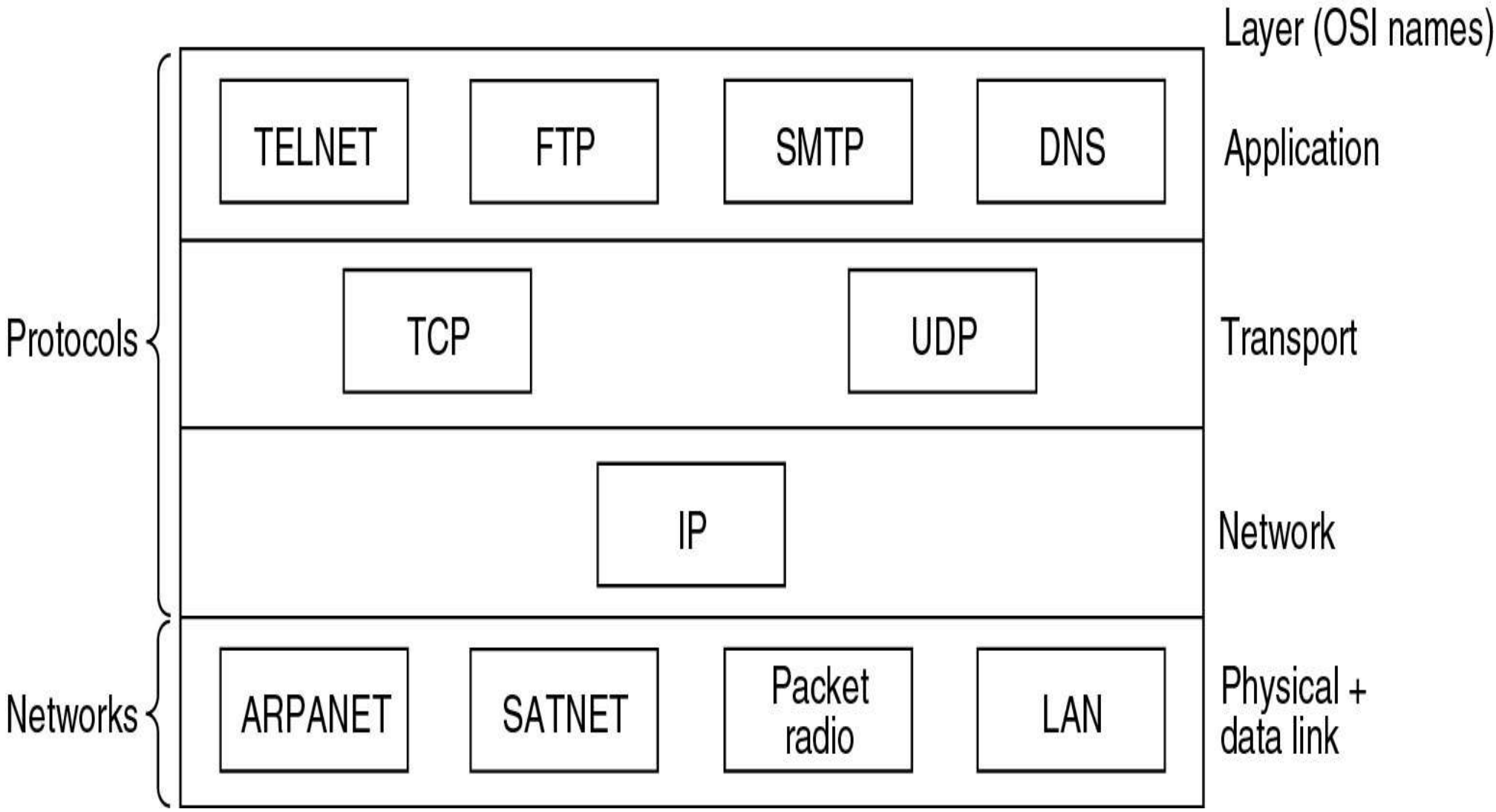

OSI
TCP/IP
7
Application
6
Presentation
5
Session
4
Transport
3
Network
2
Data link
1
Physical
Application
Transport
Internet
Host-to-network
Not present
in the model

TCP/IP

Có 4 lớp, so với mô hình OSI:

- Lớp ứng dụng (application) bao gồm lớp presentation và lớp session của mô hình OSI
- Lớp giao vận giải quyết vấn đề chất lượng dịch vụ (quality of service) như độ tin cậy, kiểm soát lỗi, kiểm soát lưu lượng
- Lớp internet chia dữ liệu từ lớp transport thành các gói (packet)
- Lớp host-to-network thực hiện tạo kết nối vật lý, bao gồm các lớp Physical và Data Link của mô hình OSI

Một phần của bộ giao thức TCP/IP



IV. Môi trường truyền vật lý mạng cục bộ

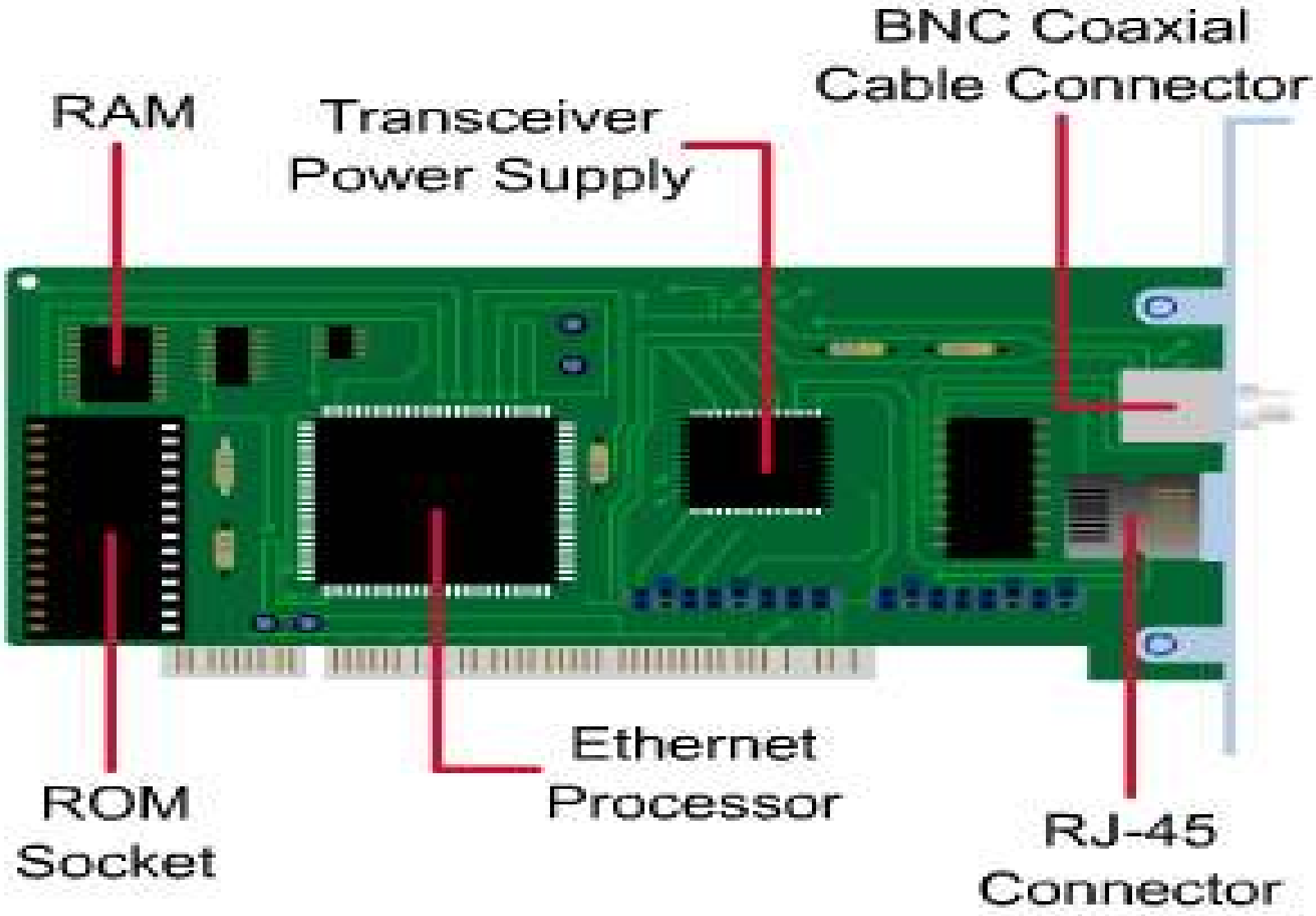
IV.1 Card mạng

IV.2 Dây mạng

IV.3 Một số thiết bị kết nối

IV.1 Card mạng

Các thành phần trên card mạng

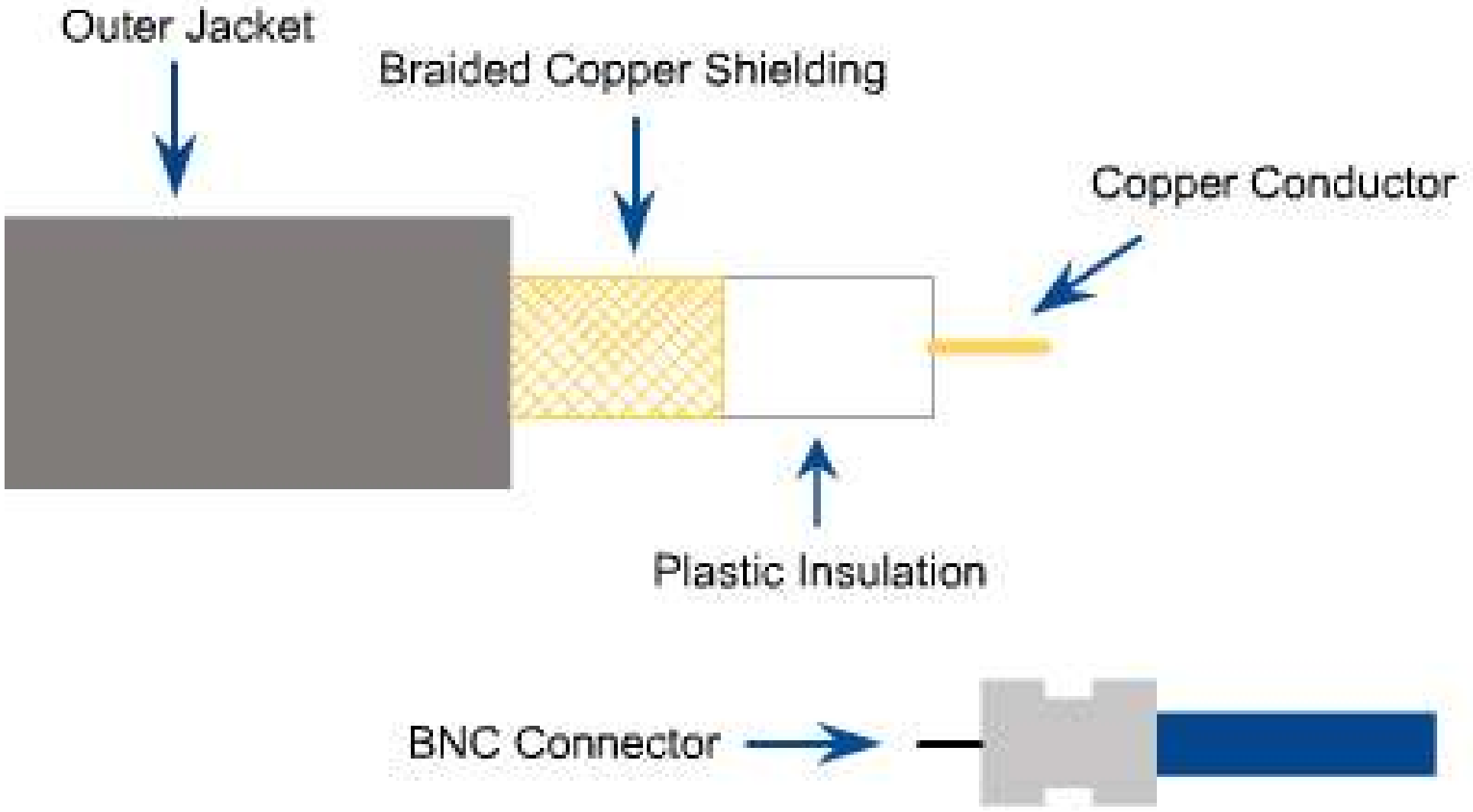


Card mạng không dây

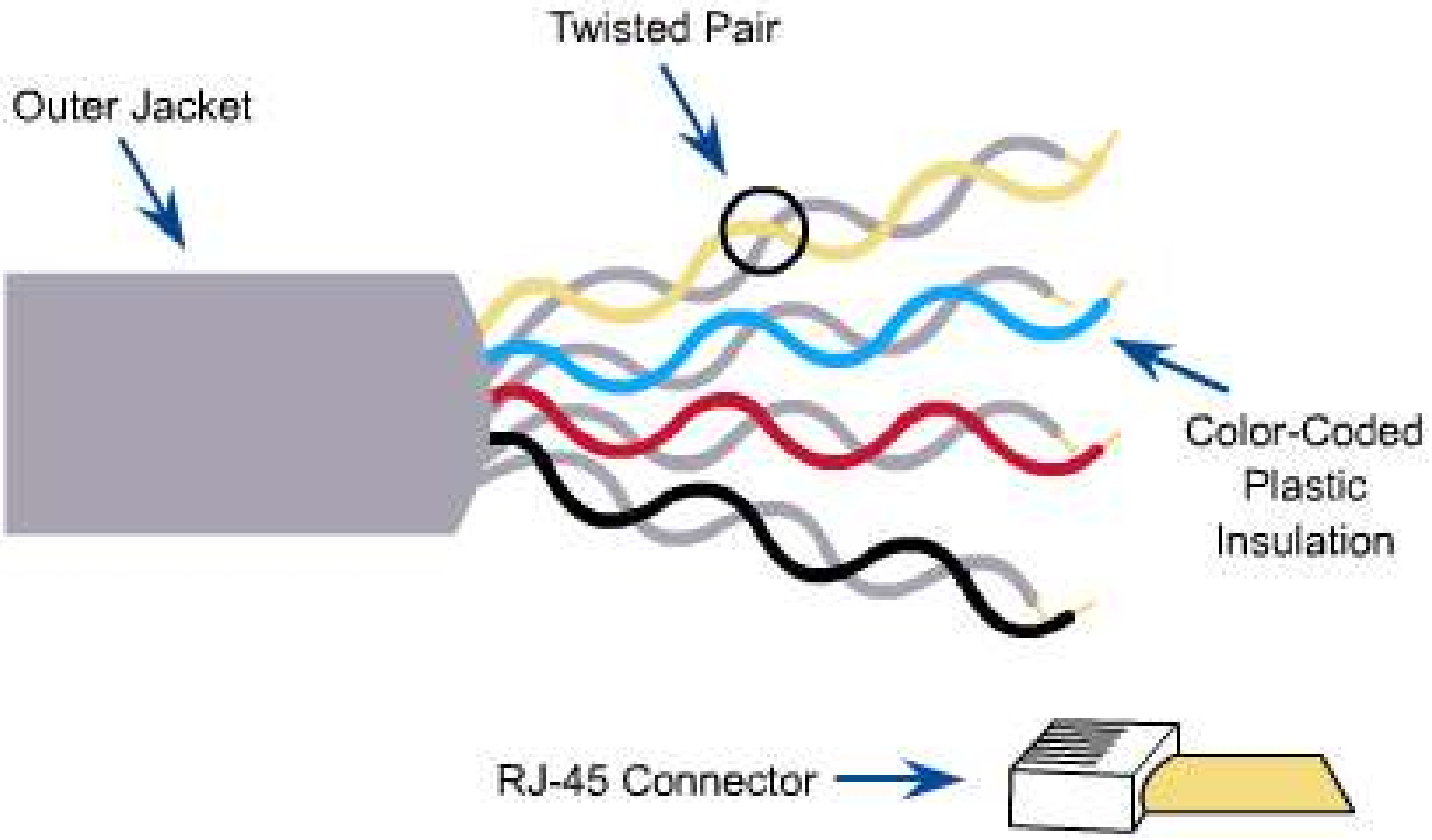
IV.2 Dây mạng

- Cáp đồng trục – Coaxial cable
- Các đôi dây xoắn – Twisted pairs
  - UTP – Unshielded Twisted - Pair
  - STP – Shielded Twisted - Pair
- Cáp quang – Fiber optic

Cáp đồng trục

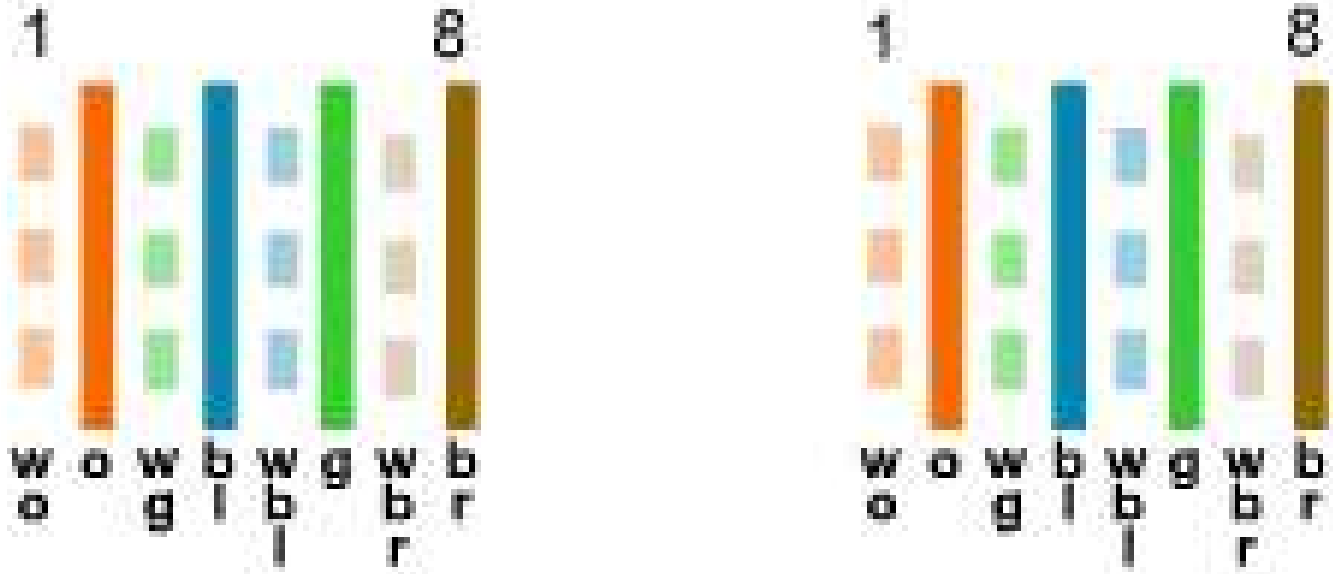


UTP – Unshielded Twisted-Pair



Dạng nối thẳng – Straight-Through

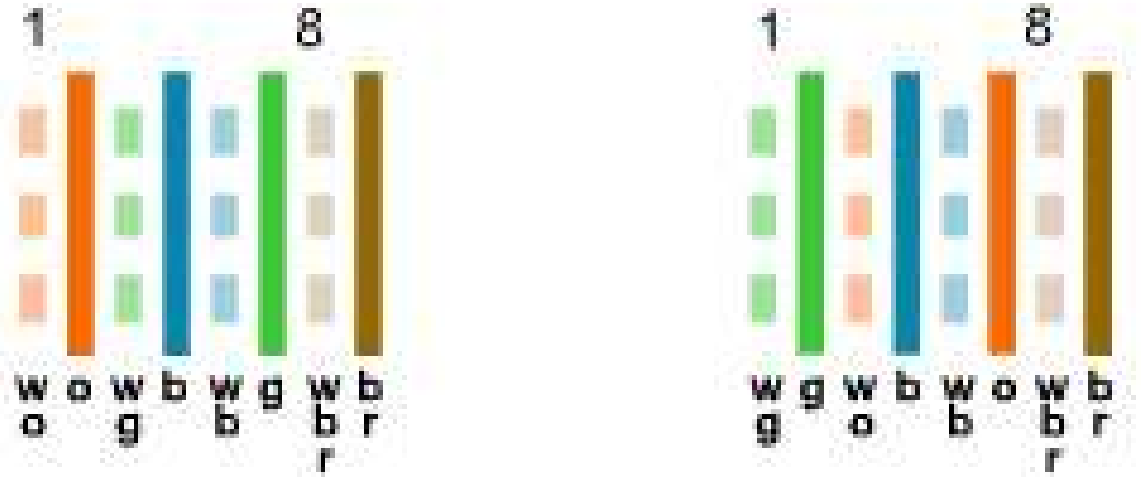
Pin	Label
1	TD+
2	TD-
3	RD+
4	NC
5	NC
6	RD-
7	NC
8	NC



Wires on cable ends are in same order.

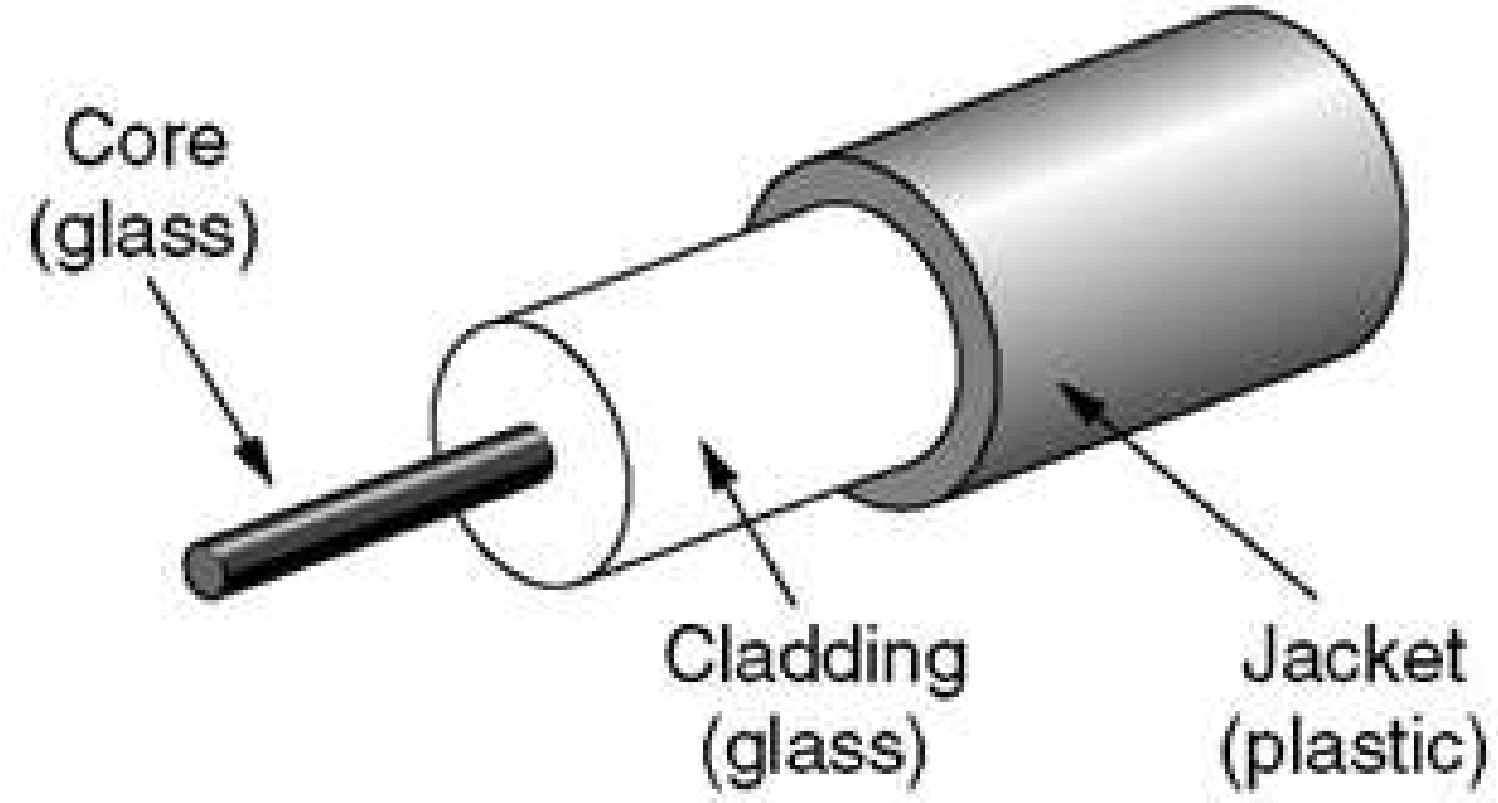
Dạng nối chéo – Crossover

Pin	Label	Pin	Label
1	TD+	1	TD+
2	RD-	2	RD-
3	RD+	3	RD+
4	NC	4	NC
5	NC	5	NC
6	TD+	6	TD-
7	NC	7	NC
8	NC	8	NC

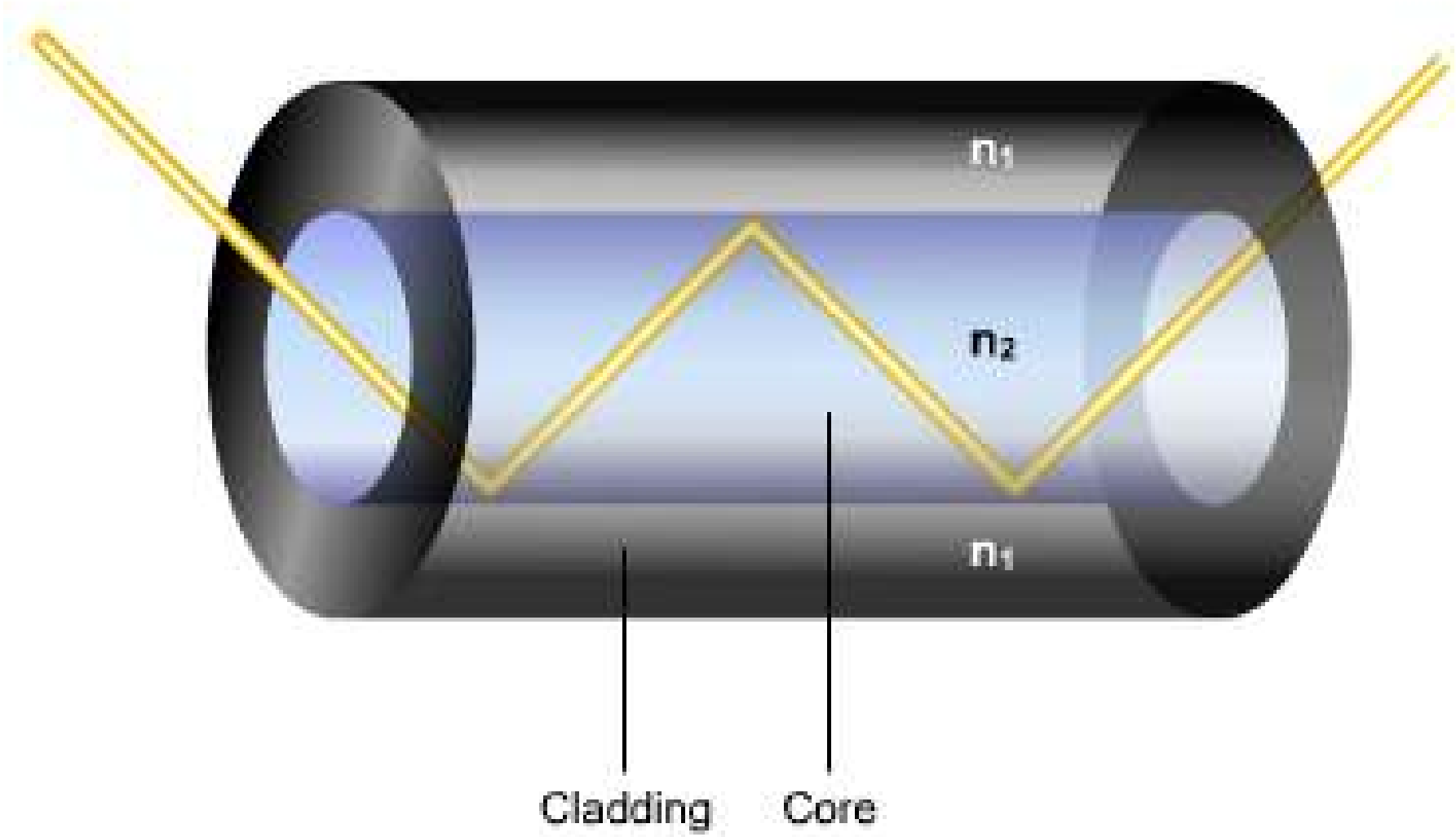


The orange wire pair and the green wire pair switch places on one end of the cable.

Cáp quang



Nguyên tắc phản xạ toàn phần trong cáp quang



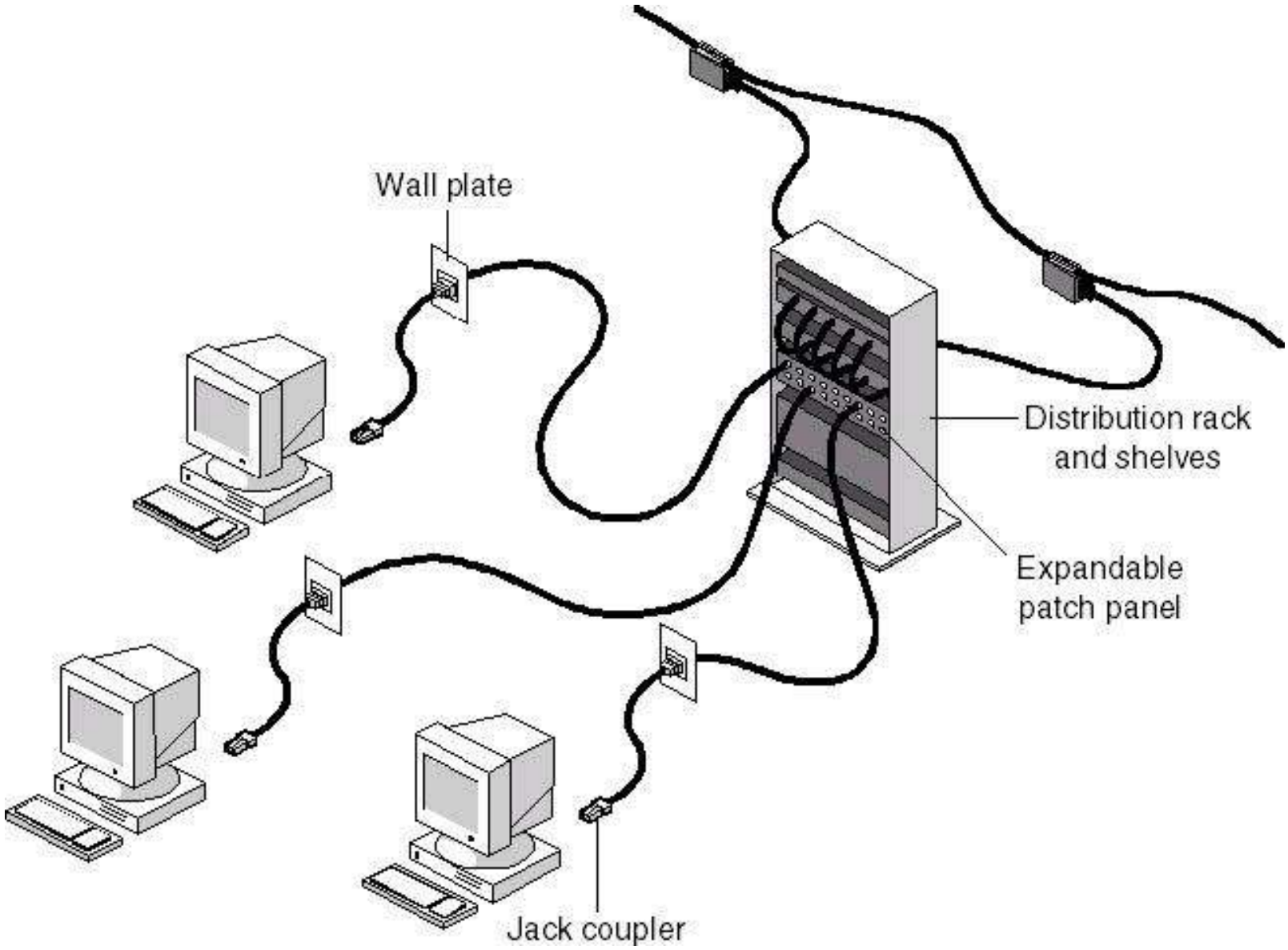
Đầu nối cáp quang

IV.3 Các thiết bị kết nối

- Phụ thuộc loại mạng, sơ đồ kết nối
- Ví dụ:
  - Hub: điểm nối dây trên mạng cục bộ dạng Ethernet
  - Access Point trên mạng không dây

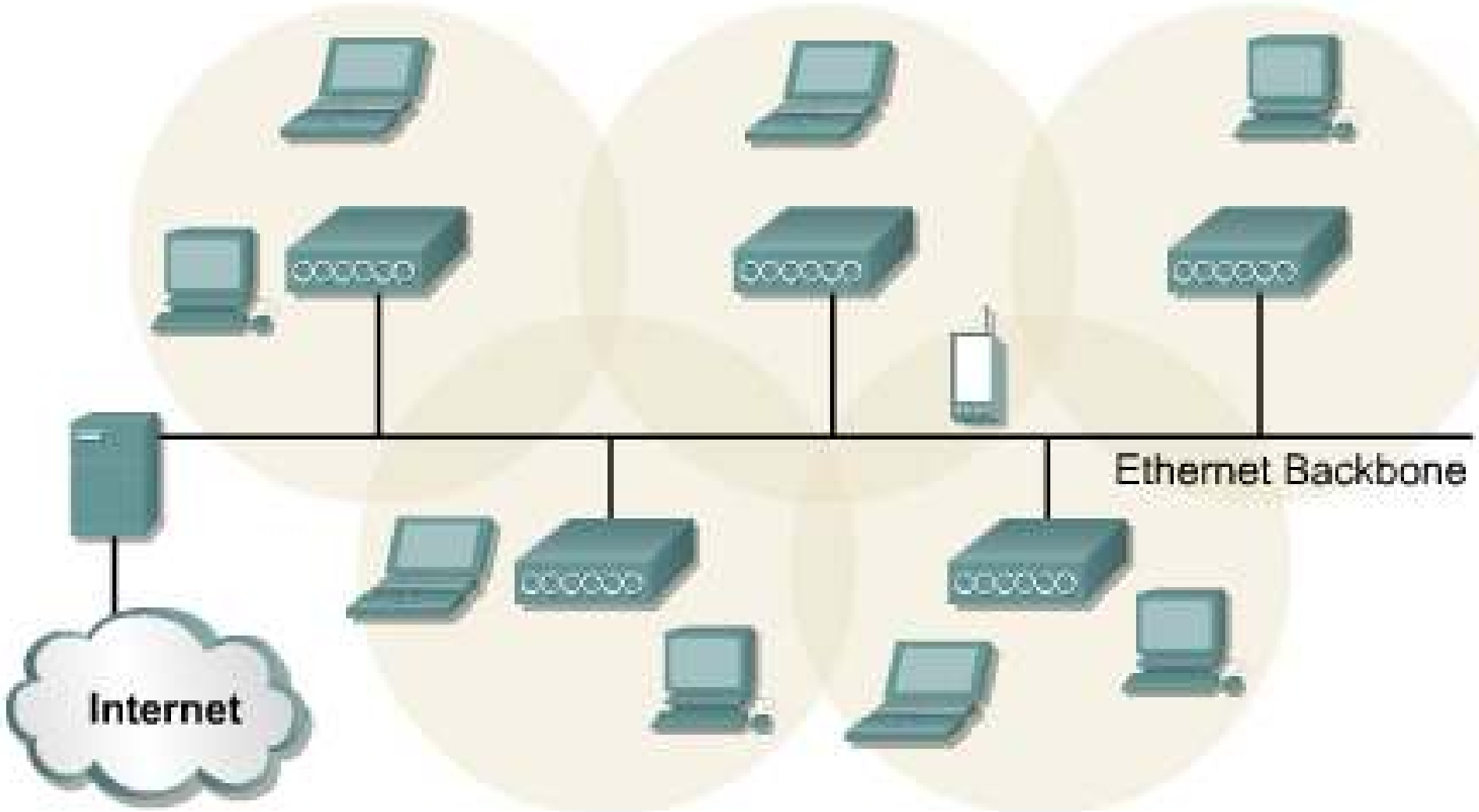
Hub

Kết nối mạng dùng dây UTP



Access point

Kết nối mạng không dây



NHẬP MÔN MẠNG MÁY TÍNH

Chương 2

LỚP DATA LINK

(LỚP LIÊN KẾT DỮ LIỆU)

Nội dung chương 2

I. Các vấn đề thiết kế lớp data link

II. Các giao thức gởi nhận frame cơ bản

III. Các kỹ thuật kết nối mạng miền rộng

IV. Ví dụ giao thức lớp data link

Giao thức PPP

I. Các vấn đề thiết kế lớp data link

I.1 Nhiệm vụ lớp data link

I.2 Các dịch vụ cung cấp cho lớp network

I.3 Các phương pháp tạo frame

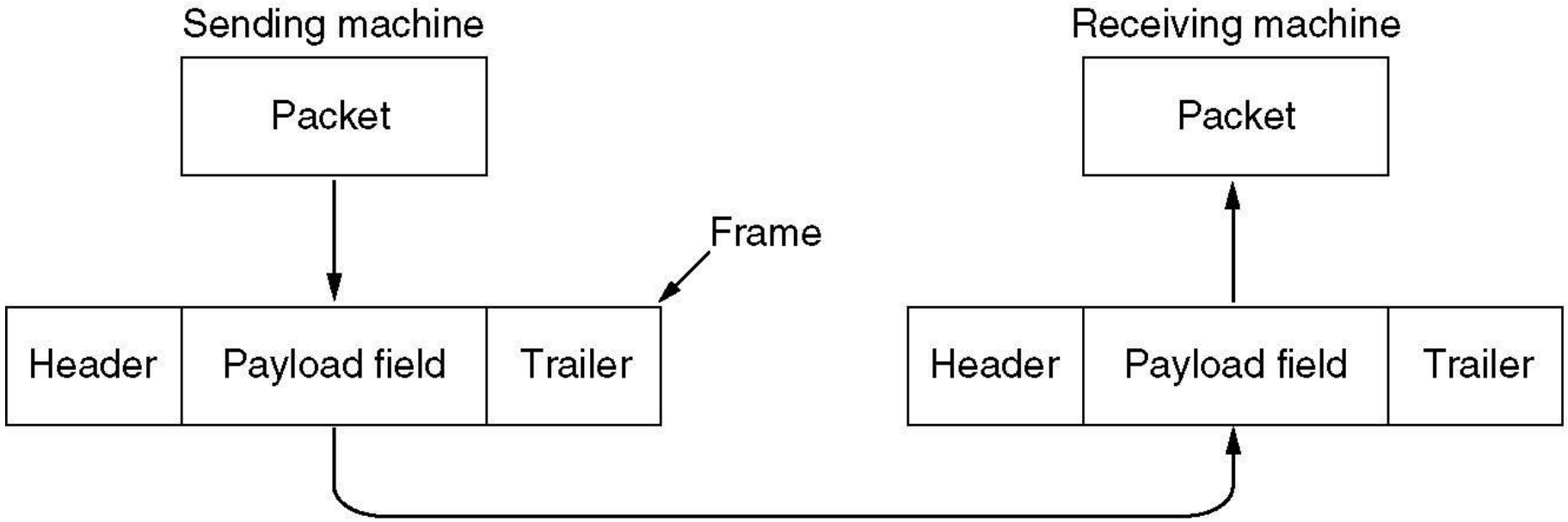
I.4 Các kỹ thuật kiểm soát lỗi

I.5 Kiểm soát lưu lượng

I.1 Nhiệm vụ lớp data link

- Cung cấp dịch vụ gởi nhận dữ liệu (frame) tin cậy giữa hai máy láng giềng

  hai máy láng giềng: hai máy có kết nối vật lý
- Kiểm soát lỗi và kiểm soát lưu lượng



I.2 Các dịch vụ cung cấp cho lớp network

- Gởi nhận không kiểm soát

  Unacknowledged connectionless service
- Gởi nhận có xác nhận của máy nhận

  Acknowledged connectionless service
- Gởi nhận có kết nối

  Acknowledged connection-oriented service

Gởi nhận không kiểm soát

Máy gởi tạo frame và gởi cho máy nhận

Gởi nhận có xác nhận của máy nhận

- Máy gởi tạo frame (data frame) và gởi cho máy nhận
- Máy nhận gởi trả frame khác (acknowledge frame, ACK) để xác nhận đã nhận được data frame.

Gởi nhận có kết nối

- Máy gởi và máy nhận thiết lập kết nối (connection) trước khi trao đổi dữ liệu
- Mỗi frame được gởi trên kết nối có số thứ tự → không sai, không mất, không đảo lộn thứ tự.

Có ba giai đoạn trong gởi nhận frame:

- Thiết lập kết nối → khởi động biến, …
- Gởi nhận frame
- Hủy kết nối → giải phóng bộ nhớ, …

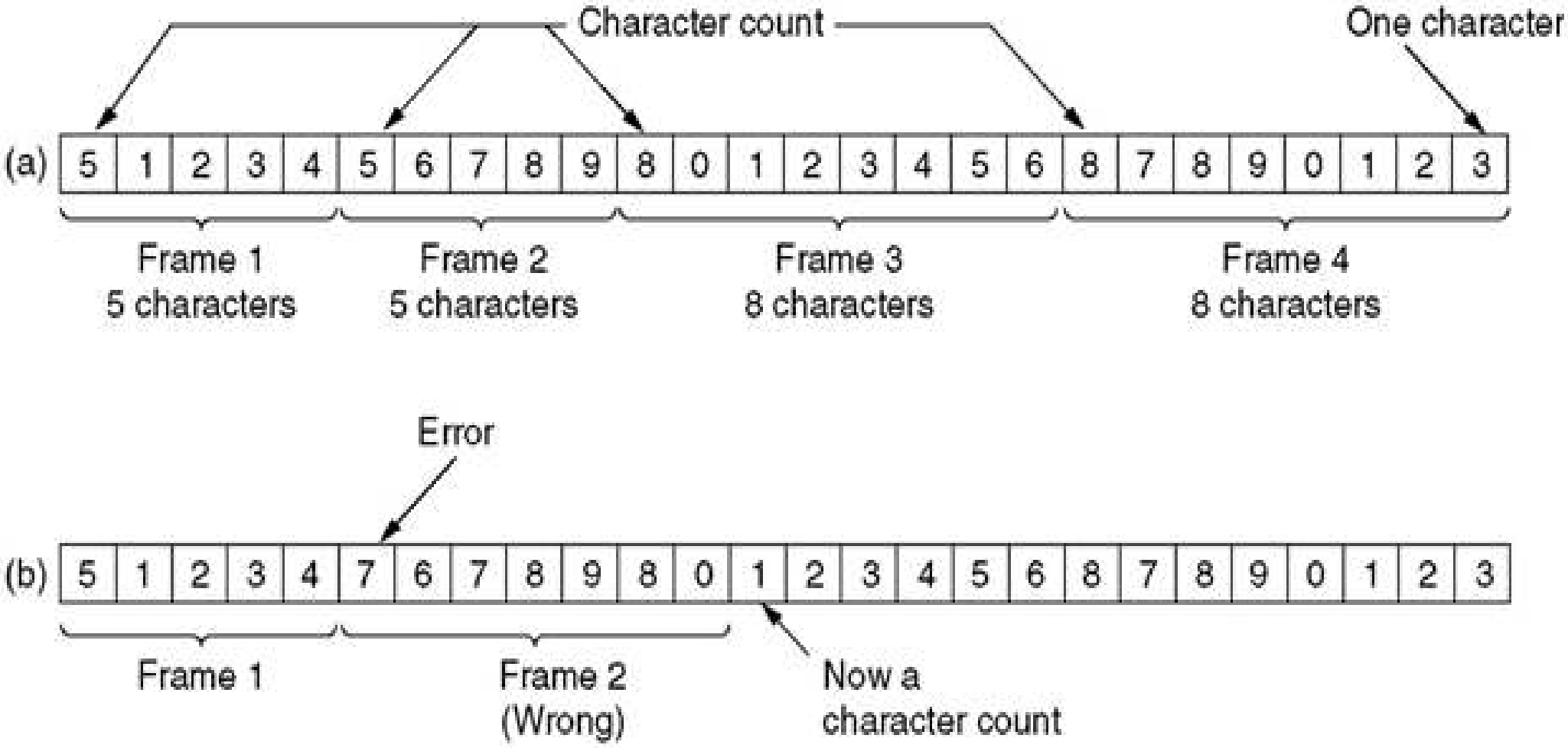
I.3 Các phương pháp tạo frame

Có hai kỹ thuật cơ bản:

- Đếm ký tự trong frame
- Dùng các ký tự đặc biệt đánh dấu frame

Thực tế: dùng kết hợp hai kỹ thuật

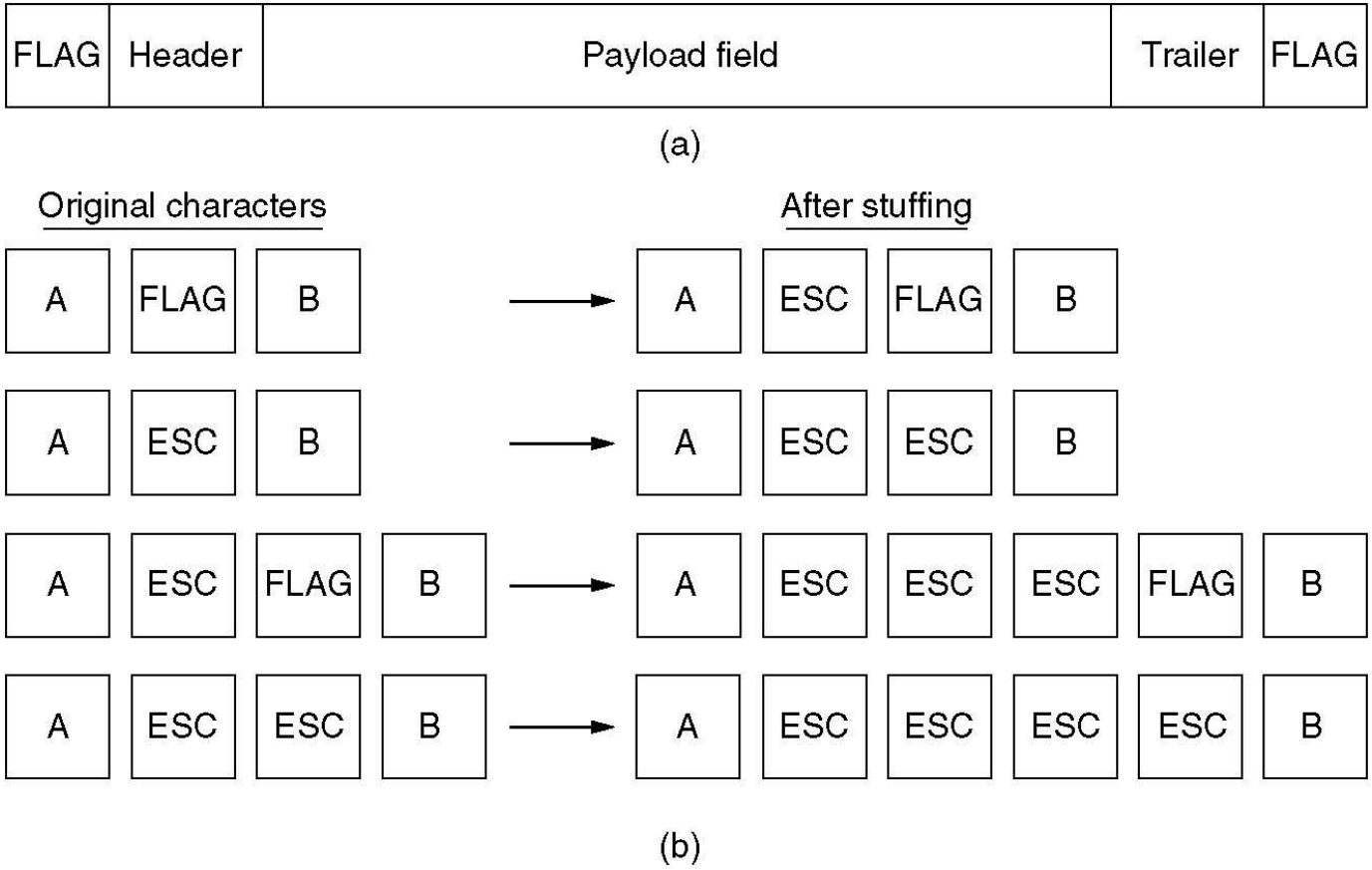
Tạo frame bằng cách đếm ký tự



a. Không có lỗi

b. Có lỗi tại counter frame 2

Tạo frame dùng ký tự đánh dấu (FLAG)



a. Frame được đánh dấu bằng flag

b. Ví dụ kỹ thuật chèn ký tự (character stuffing)

I.4 Các kỹ thuật kiểm soát lỗi

- Dùng checksum
- Có xác nhận của máy nhận (ACK)
- Định thời (timer)
- Số thứ tự trình tự (sequence number)

Kiểm soát lỗi bảo đảm việc gởi nhận frame:

- không sai
- không mất
- không đảo lộn thứ tự.

Checksum

- Máy gởi tạo frame và tính checksum
- Máy gởi sẽ gởi frame có checksum
- Nhờ vùng checksum máy nhận xác định frame không có lỗi

Với checksum → không sai

ACK

- Khi nhận một frame không có lỗi thì máy nhận sẽ gởi một frame điều khiển (ACK) cho máy gởi để xác nhận
- Nếu không có ACK thì máy gởi sẽ gởi lại frame

Với ACK → không mất

Timer

- Sau khi gởi frame, máy gởi khởi động một bộ định thời (timer)
- Nếu hết thời gian (timeout) mà không có ACK từ máy nhận thì máy gởi sẽ gởi lại frame

Sequence number

- ACK từ máy nhận có thể không đến máy gởi, và máy gởi sẽ gởi lại frame
- Máy nhận có thể nhận cùng một frame nhiều lần
- Để tránh nhận trùng frame, mỗi frame có một số thứ tự
- Số thứ tự frame thuộc về một khoảng giá trị xác định → số thứ tự trình tự

  Ví dụ: dùng số thứ tự 3 bit → có số thứ tự từ 0 đến 7

I.5 Kiểm soát lưu lượng

- Mục đích: máy gởi không nhanh hơn máy nhận
- Hai kỹ thuật cơ bản:
  - Máy gởi chờ ACK từ máy nhận
  - Máy gởi hoạt động theo tốc độ giới hạn

II. Các giao thức gởi nhận frame cơ bản

- Giao thức đơn giản trên đường truyền 1 chiều lý tưởng
- Giao thức stop-and-wait
- Giao thức trên đường truyền 1 chiều thực tế
- Các giao thức dạng sliding window

Giao thức đơn giản
trên đường truyền 1 chiều lý tưởng

Đường truyền lý tưởng:

- Không có lỗi → không cần kiểm soát lỗi
- Máy nhận tốc độ vô hạn → không cần kiểm soát lưu lượng

Đường truyền 1 chiều:

- dữ liệu 1 chiều từ máy gởi đến máy nhận
- simplex

Máy gởi tạo frame và gởi cho máy nhận

Giao thức stop-and-wait

Đường truyền: không có lỗi và máy nhận tốc độ hữu hạn

- *Máy gởi tạo frame gởi đến máy nhận*
- *Máy gởi chờ ACK từ máy nhận*
- *Máy gởi gởi frame tiếp theo*

Đường truyền 1 chiều dữ liệu nhưng có chiều truyền ACK

→ 2 chiều không đồng thời: half-duplex

Giao thức đơn giản
trên đường truyền 1 chiều thực tế

Đường truyền thực tế:

- Có thể có lỗi
- Máy nhận tốc độ hữu hạn

- *Máy gởi tạo frame, tính checksum, ghi số thứ tự frame, khởi động timer, gởi đến máy nhận*
- *Nếu có ACK thì gởi frame tiếp theo*
- *Nếu không có ACK thì gởi lại frame*

Các giao thức dạng sliding window

Mục tiêu:

- Sử dụng đường truyền với 2 chiều dữ liệu → full-duplex
- Gởi nhận theo nhóm frame

Khái niệm cơ bản:

- Piggybacking: chờ gởi kèm ACK với frame dữ liệu tiếp theo
- Sliding Window

Sliding window – cửa sổ trượt

Một máy sẽ gởi một nhóm frame trước khi chờ ACK.

Danh sách số thứ tự các frame đã gởi chưa có ACK thuộc *sending window*

Tương tự, danh sách số thứ tự các frame chờ nhận thuộc về *receiving window*

Ví dụ: sequence number 3 bit

Gởi các frame 1 đến 4	0 [1 2 3 4] 5 6 7
Nhận ACK frame 1	0 1 [2 3 4] 5 6 7
Gởi tiếp frame 5	0 1 [2 3 4 5] 6 7

Sliding window (tt)

Kỹ thuật sliding window còn được dùng trên giao thức TCP (chương 5)

Máy gởi truyền mỗi chuỗi dữ liệu không cần chờ ACK của từng dữ liệu

Máy nhận có thể nhận dữ liệu chưa đúng thứ tự và sắp xếp lại trong khi chờ dữ liệu khác

Nếu không có ACK sau 1 khoảng thời gian thì dữ liệu sẽ được gởi lại

Các giao thức dạng sliding window cơ bản

Có hai dạng cơ bản với cách xử lý frame có lỗi (mất, checksum error) khác nhau

- Go back n
  - Máy gởi sẽ gởi lại tất cả các frame từ frame có lỗi
- Selective Repeat
  - Máy gởi chỉ gởi lại frame có lỗi
  - Máy nhận phải lưu lại các frame tốt sau frame có lỗi

III. Các kỹ thuật kết nối mạng miền rộng

- Dùng đường dây điện thoại
- Kết nối trực tiếp dùng cable
- ISDN

  (Integrated Services Digital Network)
- Kết nối không dây
- Kết nối qua vệ tinh

Kết nối dùng đường dây điện thoại

- Dạng quay số (Dial-up)
- DSL (Digital Subcriber Line)

Dạng quay số

Thiết bị:

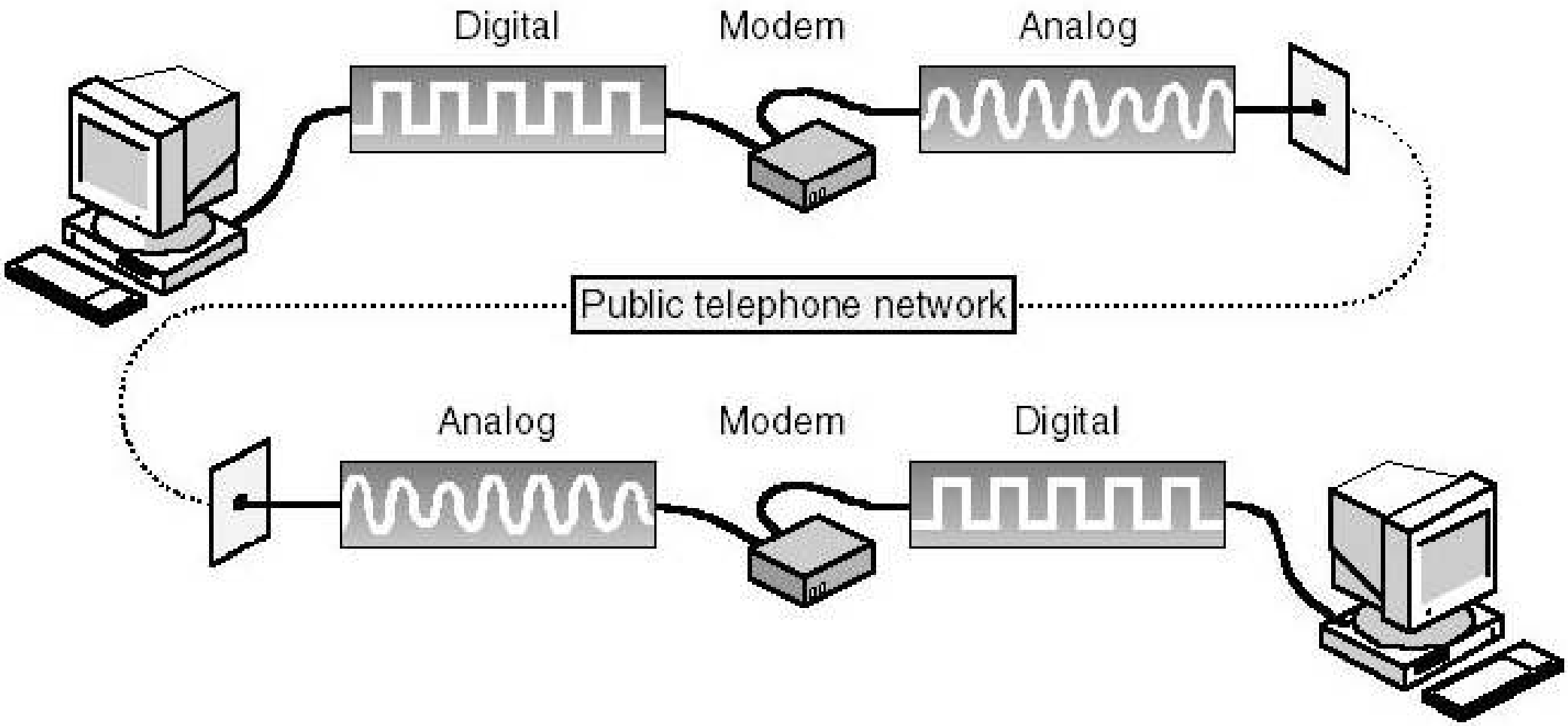
- Người sử dụng: modem
- Nhà cung cấp dịch vụ: modem

Giao thức thông dụng: PPP

(Point-to-Point Protocol)

Phần mềm: tích hợp trên các hệ điều hành

Modem



Modem thực hiện điều chế (MOdulation) khi gởi và giải điều chế (DEModulation) khi nhận

Modem (tt)

Các dạng modem:

- Internal – mạch điều khiển gắn trong máy
  - Kết nối với I/O bus, ví dụ PCI
  - Tích hợp trên mainboard
- External – Thiết bị đặt ngoài kết nối qua cổng COM hay USB

Một số tiêu chuẩn modem theo ITU:

V34 – tốc độ 28.800 bps (bits per second)

V90 – tốc độ 56.600 bps

Digital Subcriber Line - DSL

- Dùng chung kết nối mạng trên đường dây điện thoại
- Không có quay số → kết nối thường trực
- Tốc độ cao hơn so với dùng modem

DSL (tt)

Có các dạng:

- ADSL-Asymmetric DSL: thông dụng

  Tốc độ download: 384Kbps → 8Mbps

  Tốc độ upload: 64Kbps → 1 Mbps

  Có giới hạn về khoảng cách ~ 5.500 mét

- SDSL-Symmetric DSL

  Tốc độ download và upload đến 3Mbps

- VDSL-Very High Data Rate DSL

  Tốc độ download và upload đến 52Mbps

ADSL

Thiết bị

- Người sử dụng:

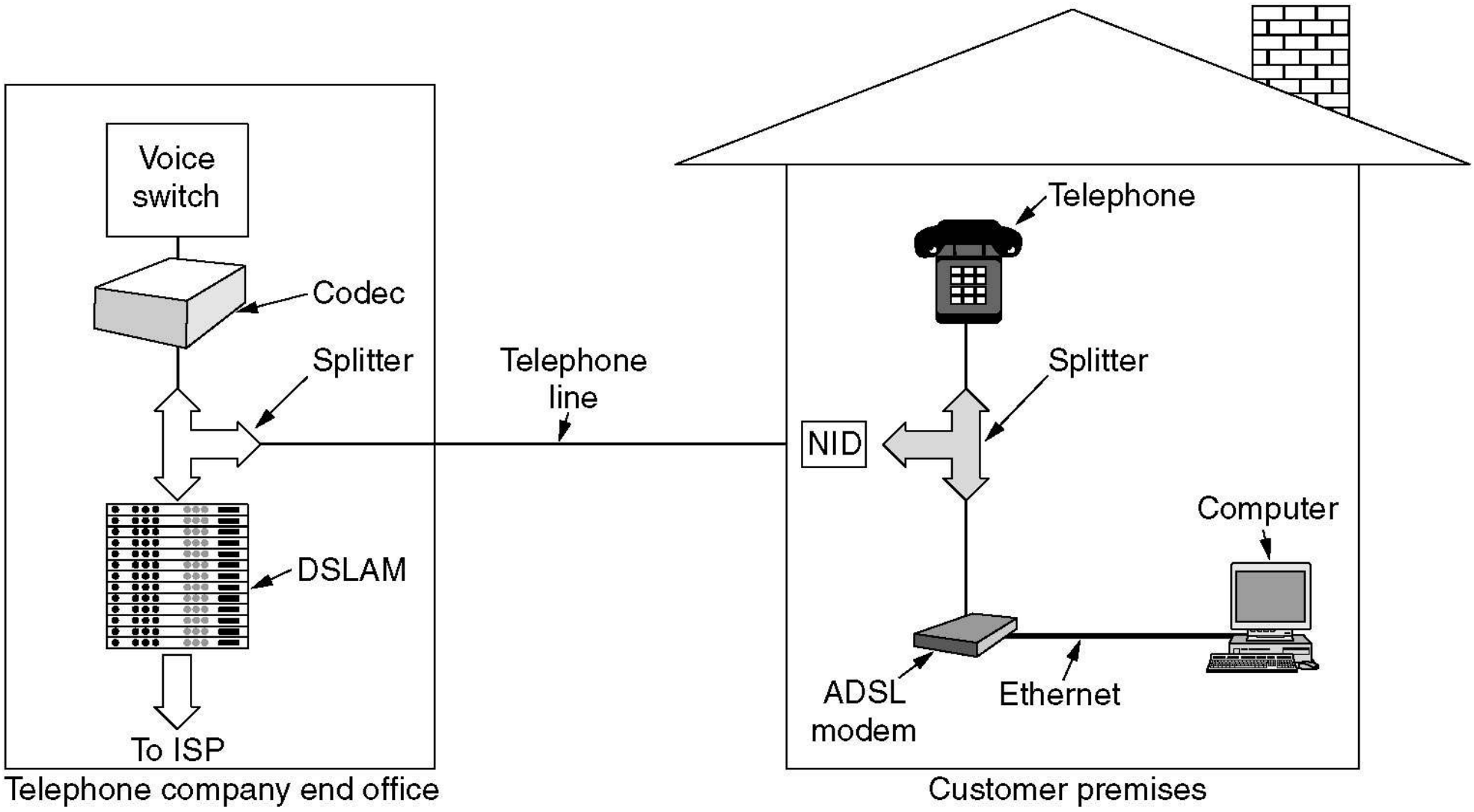
  ADSL modem/ ADSL router
- Nhà cung cấp dịch vụ: Access Multiplexer

Phần mềm:

- Người sử dụng dùng phần mềm do nhà sản xuất thiết bị cung cấp
- Nhà cung cấp dịch vụ thường dùng kỹ thuật ATM (Asynchronous Transfer Mode)

ADSL là tiêu chuẩn của lớp vật lý

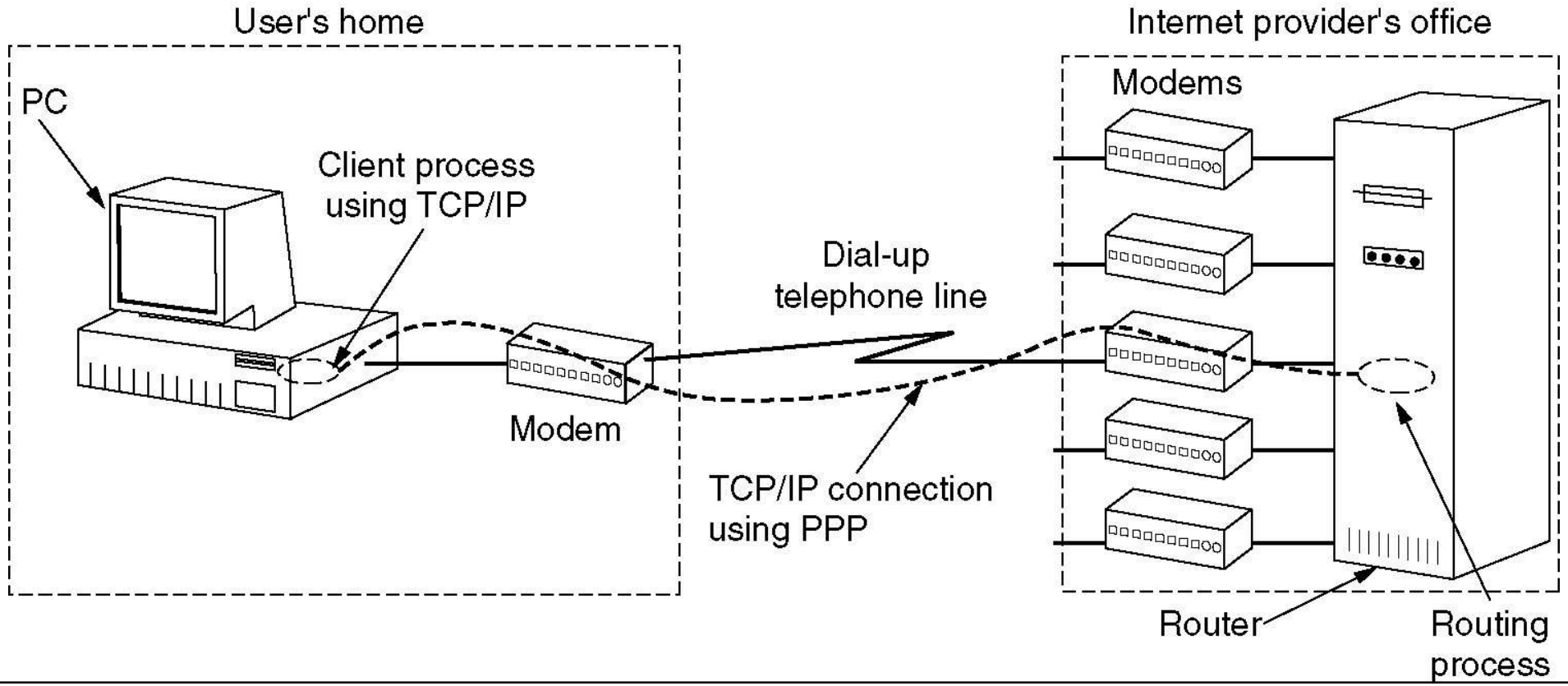
ADSL (tt)



Cấu hình cơ bản dùng ADSL

IV.Giao thức PPP (Point-to-Point Protocol)

Giao thức PPP dùng trong kết nối giữa máy tính cá nhân (PC) với nhà cung cấp dịch vụ Internet (ISP) qua đường điện thoại quay số.



Các đặc điểm của giao thức PPP

- Tạo frame theo giao thức HDLC (High-level Data Link Control), dùng kỹ thuật chèn ký tự, có kiểm soát lỗi
- Dùng giao thức LCP (Link Control Protocol) để kiểm soát kết nối, thoả thuận tham số…
- Dùng giao thức NCP (Network Control Protocol) để thiết lập tham số cho lớp Network, dùng được với nhiều loại mạng như TCP/IP, IPX/SPX, NetBEUI, Apple Talk

Các bước máy PC kết nối Internet

- Máy PC thiết lập kết nối vật lý với ISP bằng cách quay số qua modem
- Máy PC gởi một chuỗi LCP packet trên các PPP frame để thoả thuận tham số
- Máy PC gởi một chuỗi NCP packet trên các PPP frame để thiết lập cấu hình hoạt động lớp network

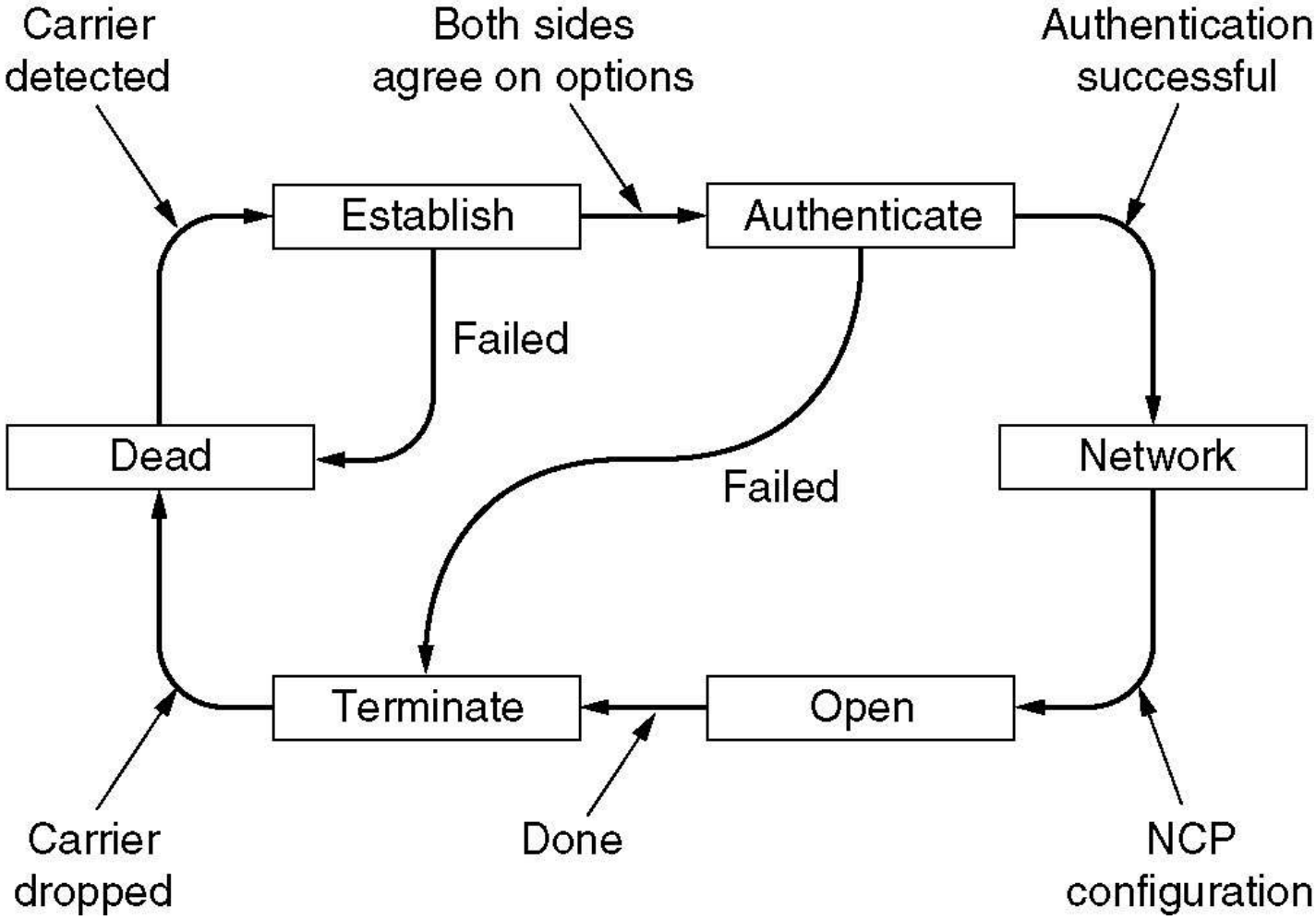
  → máy PC được cấp một địa chỉ IP động và trở thành Internet host, có thể gởi nhận dữ liệu theo các IP packet.

Các bước máy PC kết nối Internet (tt)

Khi kết thúc phiên làm việc:

- Dùng các NCP packet để hủy kết nối lớp network và trả lại địa chỉ IP
- Dùng các LCP packet hủy kết nối lớp data link
- Hủy kết nối vật lý bằng lệnh ngắt modem ra khỏi đường dây điện thoại

Các bước máy PC kết nối Internet(tt)



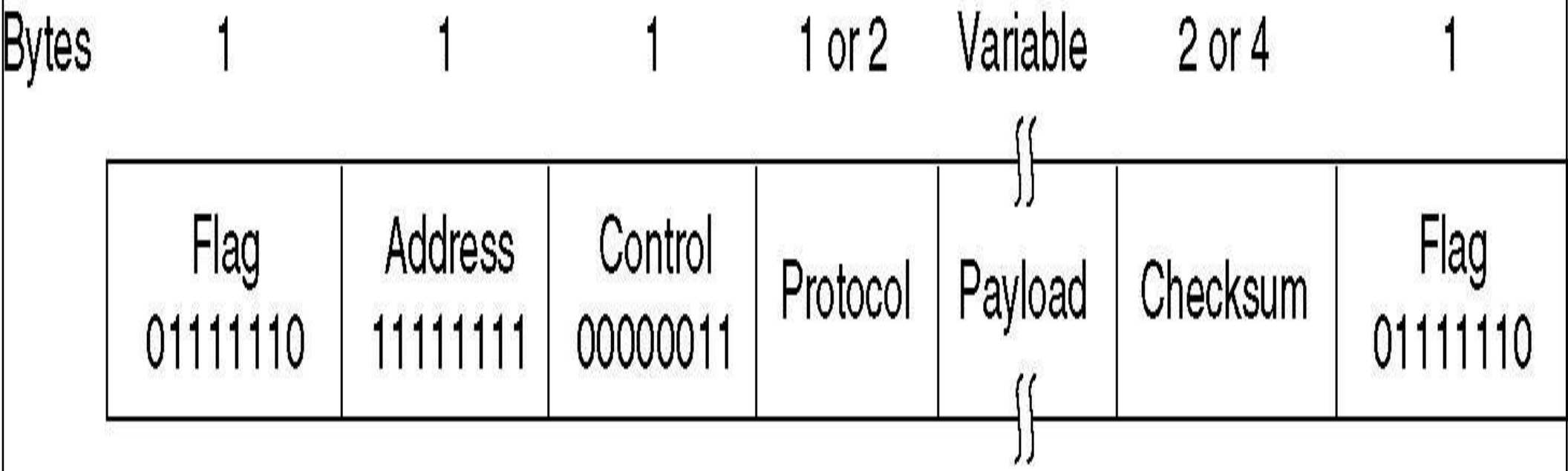
Các giai đoạn hoạt động theo giao thức PPP

Ví dụ PPP frame

Dạng frame điều khiển không có số thứ tự

- Flag: đánh dấu đầu và cuối frame
- Address và Control: hằng số đối với control frame
- Protocol: xác định loại dữ liệu trong vùng payload
- Payload: dữ liệu, kích thước do thoả thuận, mặc định là 1500 bytes
- Checksum: dùng kiểm soát lỗi

PPP Frame (tt)


Bytes
1
1
1
1 or 2
Variable
2 or 4
1
Flag
01111110
Address
11111111
Control
00000011
Protocol
Payload
Checksum
Flag
01111110

NHẬP MÔN MẠNG MÁY TÍNH

Chương 3

LỚP MAC

(LỚP CON ĐIỀU KHIỂN TRUY CẬP MÔI TRƯỜNG)

Nội dung chương 3

I. Khái niệm lớp MAC
II. Vấn đề cấp phát kênh truyền
III. Giao thức CSMA/CD
IV. Giới thiệu các tiêu chuẩn IEEE 802.x
V. Giới thiệu về Bridge, Switch

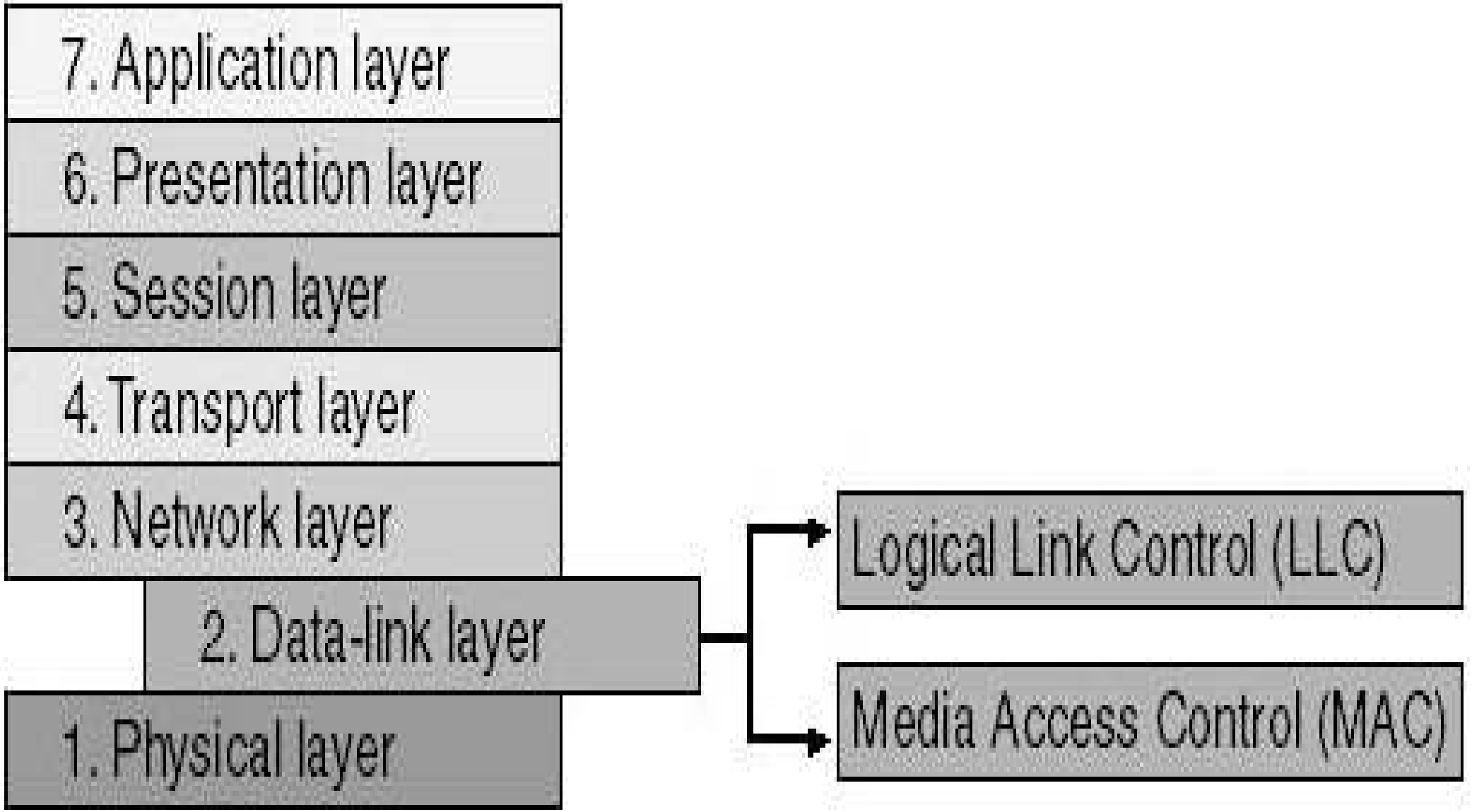
I. Khái niệm lớp MAC

Lớp Physical và Data link (mô hình OSI): giải quyết vấn đề các máy đồng thời truy cập đường truyền dạng broadcast (quảng bá)

Dự án IEEE 802: các đặc tả của 2 lớp này trên mạng cục bộ

→ tiêu chuẩn mạng cục bộ

Lớp Data Link trong IEEE 802

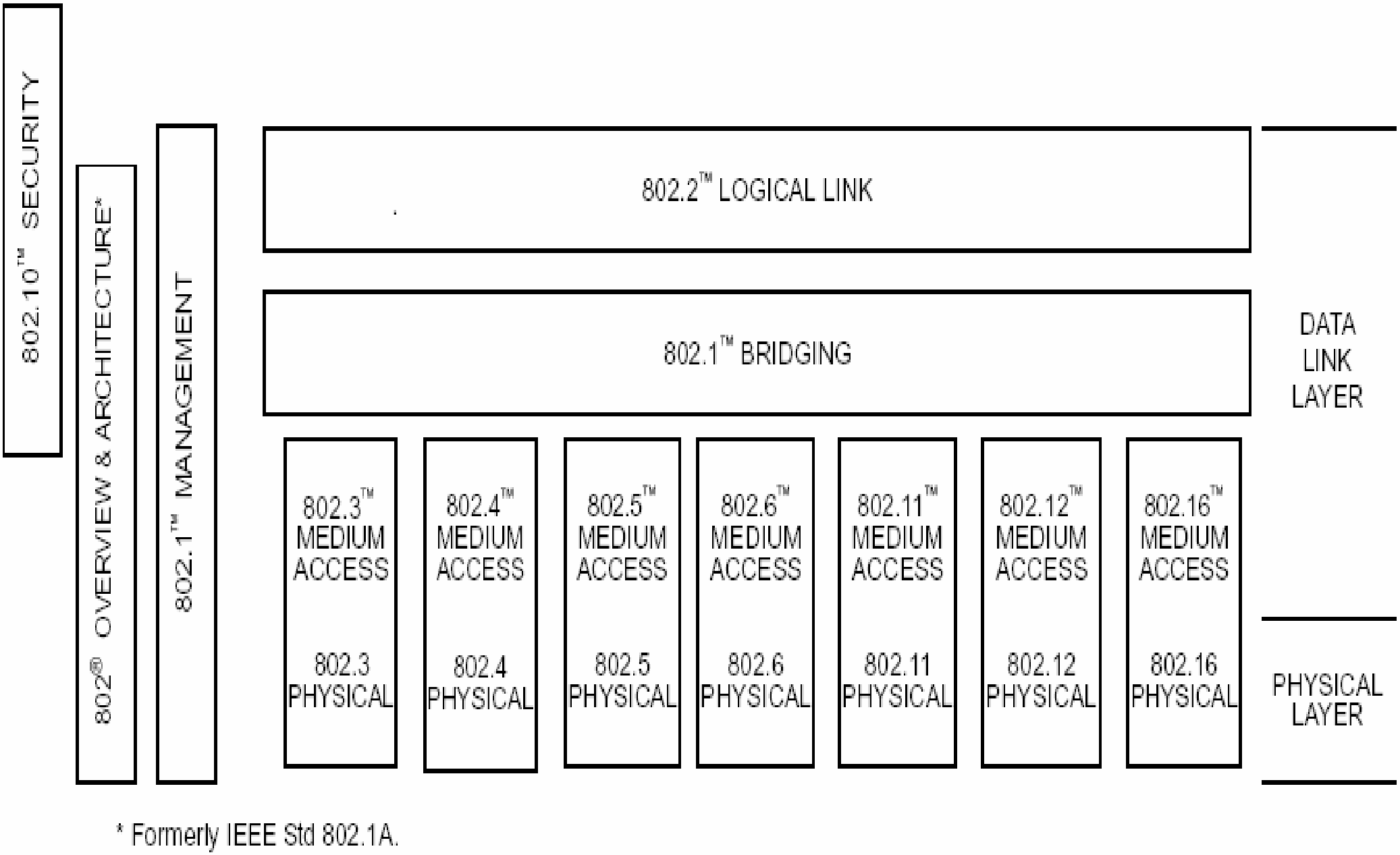


Lớp Data Link trong IEEE 802 (tt)

Gồm 2 lớp con (sublayer):

- Logical Link Control (LLC): thiết lập và kết thúc liên kết, quản lý truyền frame
- Medium Access Control (MAC): quản lý truy cập đường truyền, tạo frame, kiểm soát lỗi, xác định địa chỉ

Các tiêu chuẩn IEEE 802.x



* Formerly IEEE Std 802.1A.

Các tiêu chuẩn IEEE 802.x chính

- 802.2 - *Logical Link Control*
- 802.3 - *CSMA/CD Access Method and Physical Layer Specifications*
- 802.5 - *Token Ring Access Method and Physical Layer Specifications*
- 802.11 - *Wireless LAN Medium Access Control (MAC) Sublayer and Specifications*
- 802.16 - *Standard Air Interface for Fixed Broadband Wireless Access Systems*

II. Vấn đề cấp phát kênh truyền

Mục đích: cấp phát một kênh truyền dạng quảng bá cho nhiều máy cùng sử dụng

Một số thuật ngữ

- Đường truyền (Transmission line): vật lý
- Kênh truyền (Communication channel): luận lý
- Baseband: một kênh truyền trên đường truyền
- Broadband: nhiều kênh truyền trên đường truyền
- Multiplexing: ghép kênh tại nơi gởi
- Demultiplexing: tách kênh tại nơi nhận

Các kỹ thuật cấp phát kênh truyền

- Cấp phát tĩnh: số kênh truyền cố định
- Cấp phát động: số kênh truyền thay đổi

  → một máy truy cập đường truyền không làm ảnh hưởng các máy khác

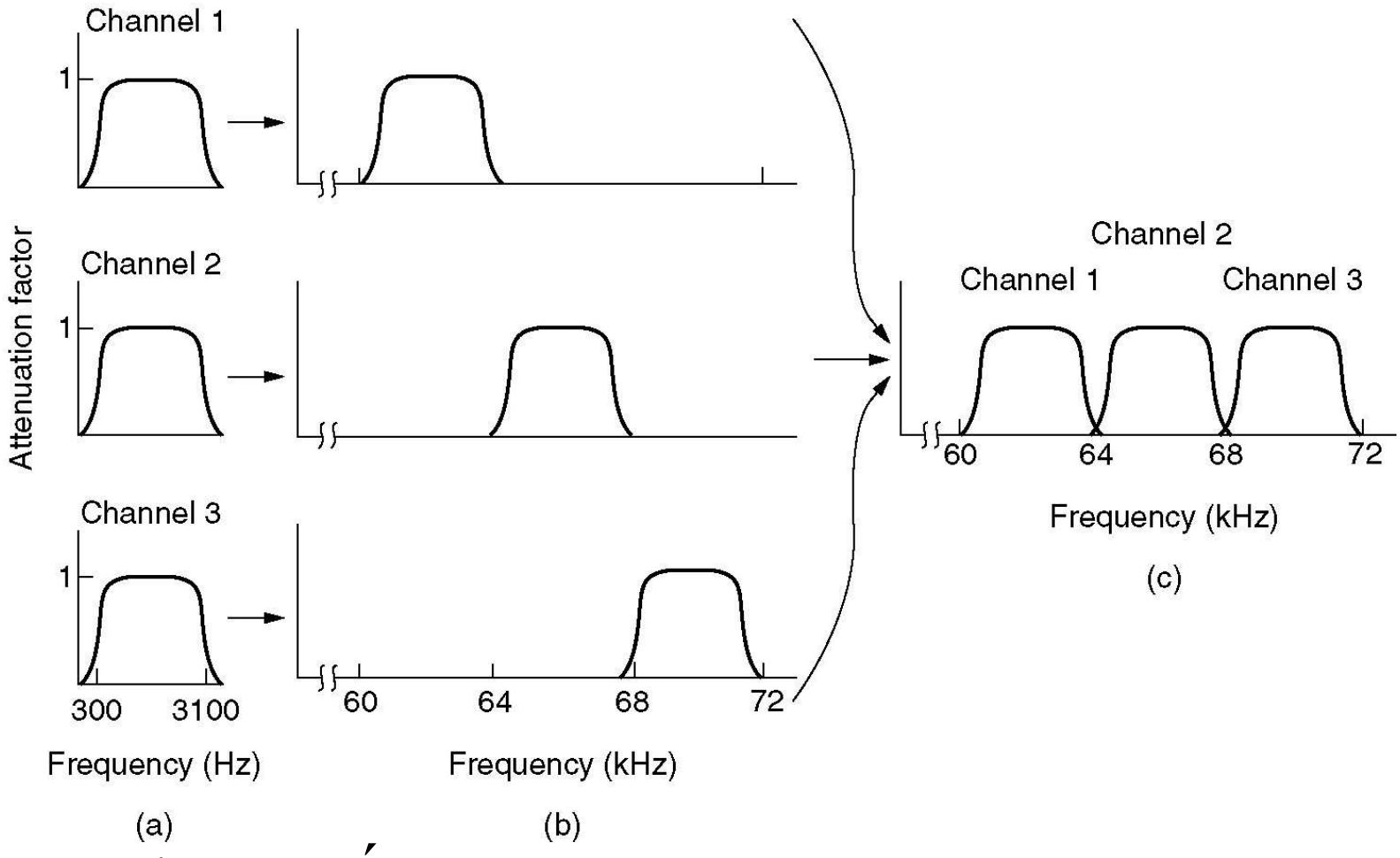
Cấp phát tĩnh kênh truyền

Hai kỹ thuật thông dụng:

- FDM – Frequency Division Multiplexing
  (Ghép kênh phân chia theo tần số)
- TDM – Time Division Multiplexing
  (Ghép kênh phân chia theo thời gian)

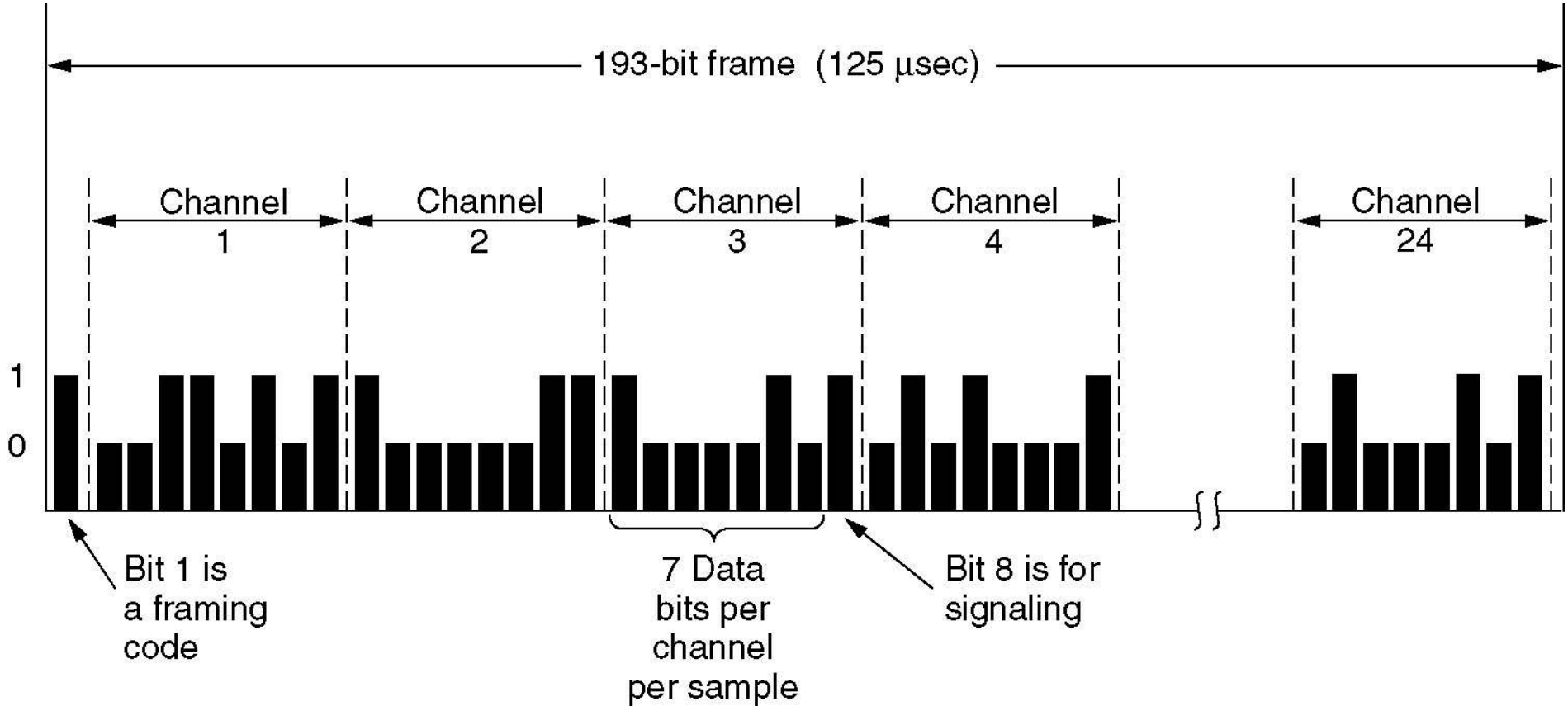
Ứng dụng: mạng điện thoại cổ điển

Ví dụ FDM



a. Băng thông gốc
b. Băng thông được nâng tần số
c. Kênh sau khi ghép

Ví dụ TDM



Ghép 24 kênh thoại trong 1 kênh T1

Cấp phát động kênh truyền

- Ứng dụng trong mạng máy tính, mạng điện thoại
- Có nhiều giao thức: ALOHA, CSMA, WDMA, …

Môi trường cấp phát động kênh truyền

- Mô hình trạm (station model)
  - Có N trạm (máy tính, điện thoại) có thể tạo và truyền frame
- Kênh truyền đơn (single channel)
  - Các trạm dùng chung 1 đường truyền
- Xung đột (collision)
  - Nếu 2 trạm truyền frame đồng thời
  - Tất cả trạm có thể phát hiện xung đột
  - Không có kết quả

Môi trường cấp phát động kênh truyền (tt)

- Thời gian liên tục – Continuous time
  - Truyền frame tại thời điểm bất kỳ
- Thời gian được phân khe – Slotted time
  - Thời gian được chia thành các khe (slot)
  - Truyền frame tại thời điểm bắt đầu một khe thời gian
- Cảm nhận truyền tải – Carrier sense
  - Các trạm có thể xác định kênh truyền đang được sử dụng

Môi trường cấp phát động kênh truyền (tt)

- Không cảm nhận truyền tải – No carrier sense
  - Các trạm không thể xác định kênh truyền đang được sử dụng

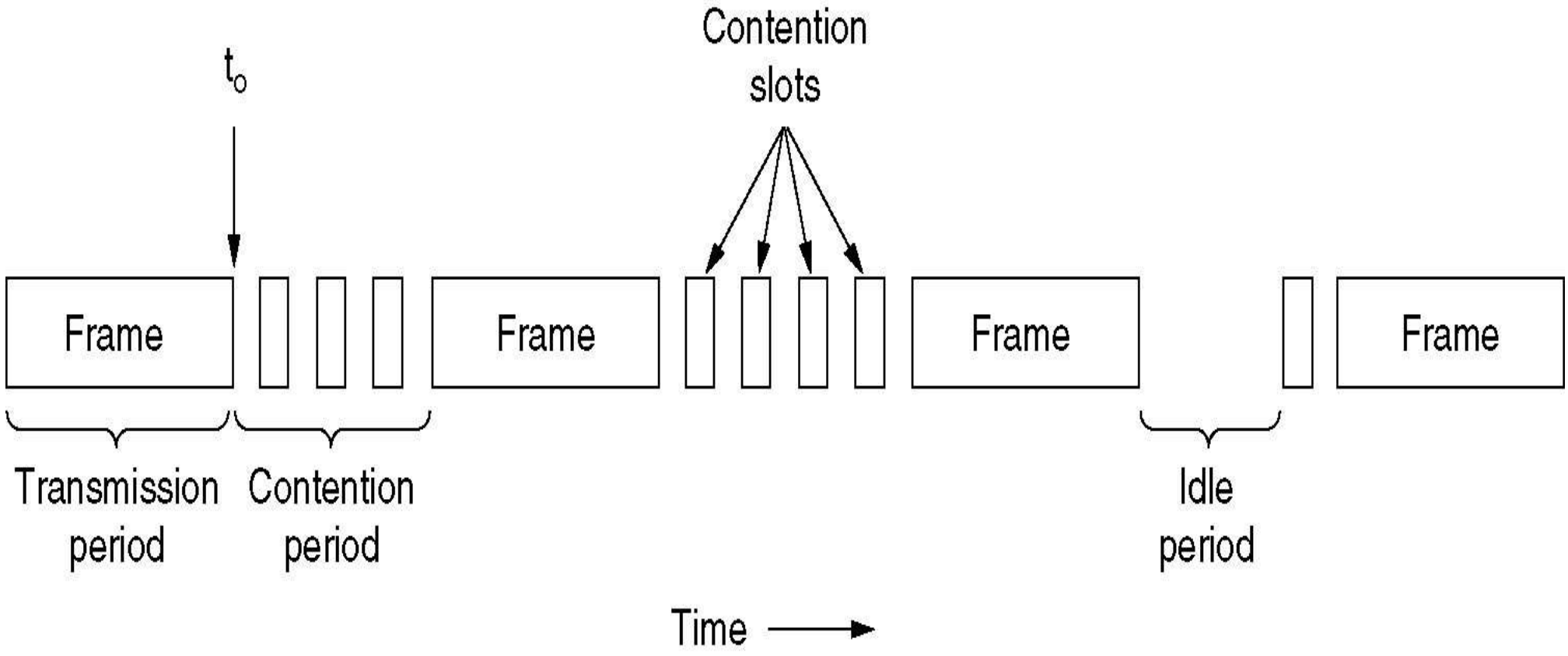
III. Giao thức CSMA/CD

Carrier Sense Multiple Access with Collision Detection

(Đa truy cập cảm nhận truyền tải có phát hiện xung đột)

Dùng trong tiêu chuẩn mạng IEEE 802.3

CSMA/CD (tt)



Ba trạng thái của đường truyền: Transmission (truyền), Contention (tranh chấp), Idle (nghỉ)

Hoạt động khi cần truyền frame

- Kiểm tra trạng thái đường truyền (cảm nhận truyền tải)
- Nếu đường truyền rảnh thì truyền frame

Xung đột và xử lý xung đột

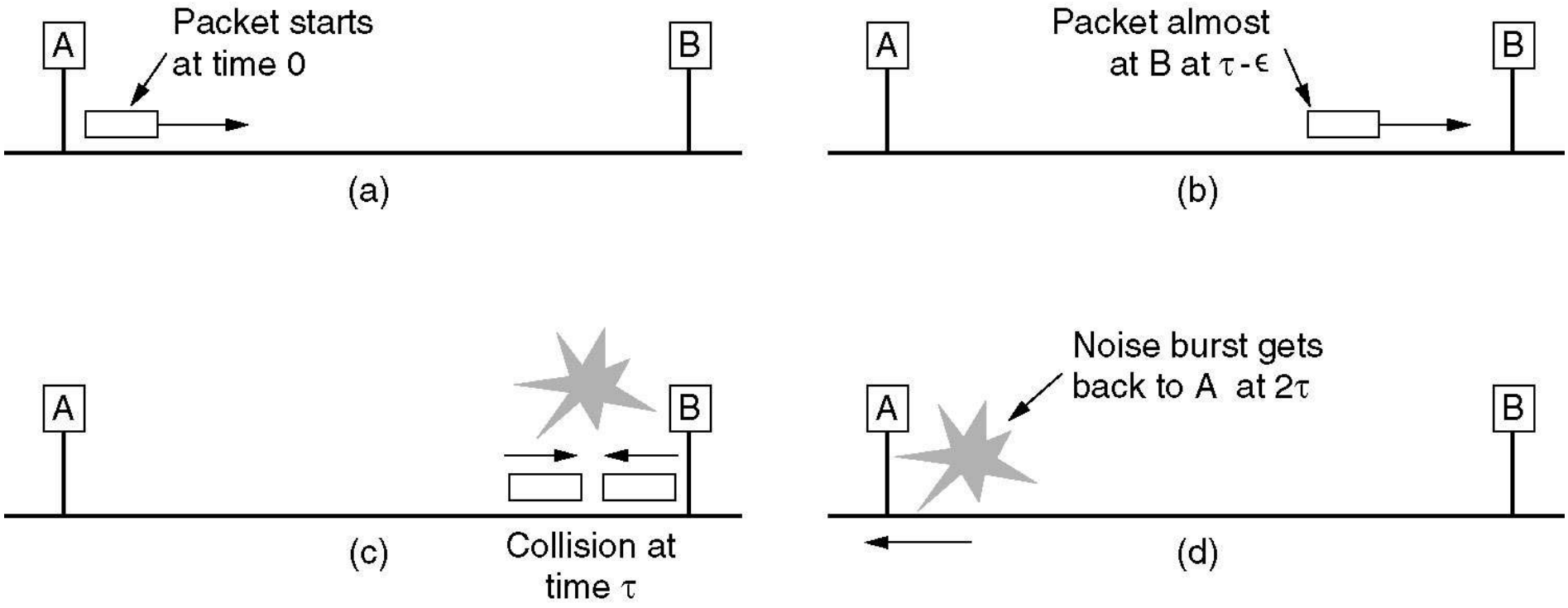
Xung đột:

- Nếu có 2 máy truyền đồng thời thì tạo xung đột
- Xung đột được phát hiện bởi phần cứng

Xử lý xung đột:

- Hủy frame đã truyền
- Chờ một khoảng thời gian ngẫu nhiên
- Kiểm tra đường truyền, nếu rảnh thì truyền lại

Thời gian để phát hiện xung đột



A, B: 2 máy xa nhau nhất trên mạng

Tau (τ): thời gian truyền giữa A, B

→ A phải truyền frame trong thời gian $\geq 2\,\tau$

IV. Giới thiệu các tiêu chuẩn IEEE 802

1. Mạng Ethernet – 802.3
2. Mạng Fast Ethernet
3. Mạng Gigabit Ethernet
4. Mạng Token Ring – 802.5
5. Mạng Wireless Lan – 802.11
6. IEEE 802.2 – Logical Link Control (LLC, Điều khiển liên kết luận lý)

1. Mạng Ethernet – 802.3

a. Giới thiệu mạng Ethernet
b. Nối cáp
c. Mã hoá bit
d. Giao thức lớp MAC
e. Giải quyết xung đột

a. Giới thiệu mạng Ethernet

- Xuất phát từ mạng LAN dạng CSMA/CD 2.94 Mbps của Xerox, mạng Ethernet
- 1978, DEC, Intel, Xerox thiết lập tiêu chuẩn mạng Ethernet 10 Mbps, chuẩn DIX
- 1983, chuẩn DIX trở thành IEEE 802.3
- Mạng Ethernet tiếp tục phát triển với các tốc độ cao hơn 100 Mbps, 1000 Mbps, …

b. Nối cáp

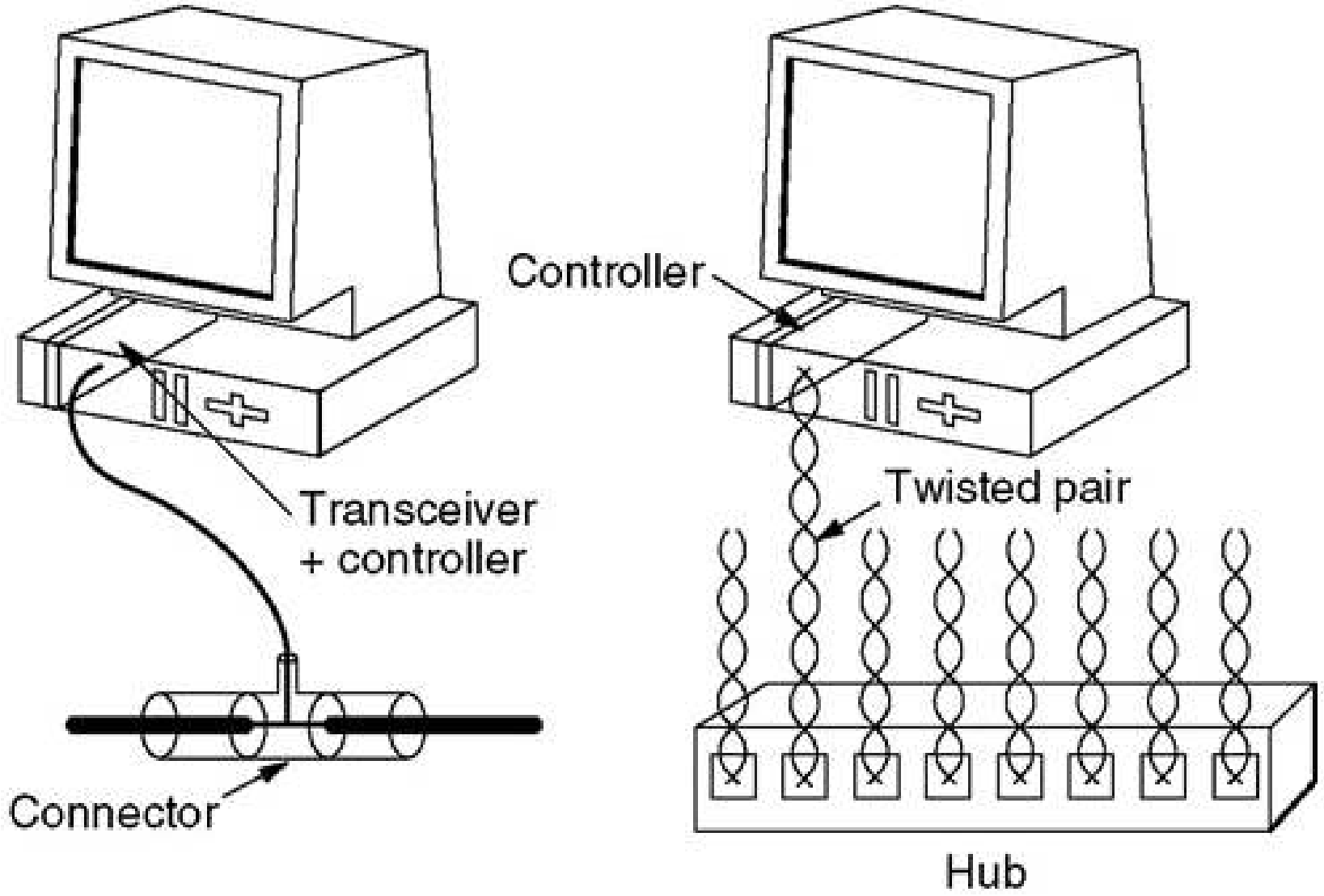
Name	Cable	Max. seg.	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Original cable; now obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheapest system
10Base-F	Fiber optics	2000 m	1024	Best between buildings

Các loại dây cáp thông dụng của Ethernet

(Cáp đồng trục dày, cáp đồng trục mỏng,

đôi dây xoắn, cáp quang)

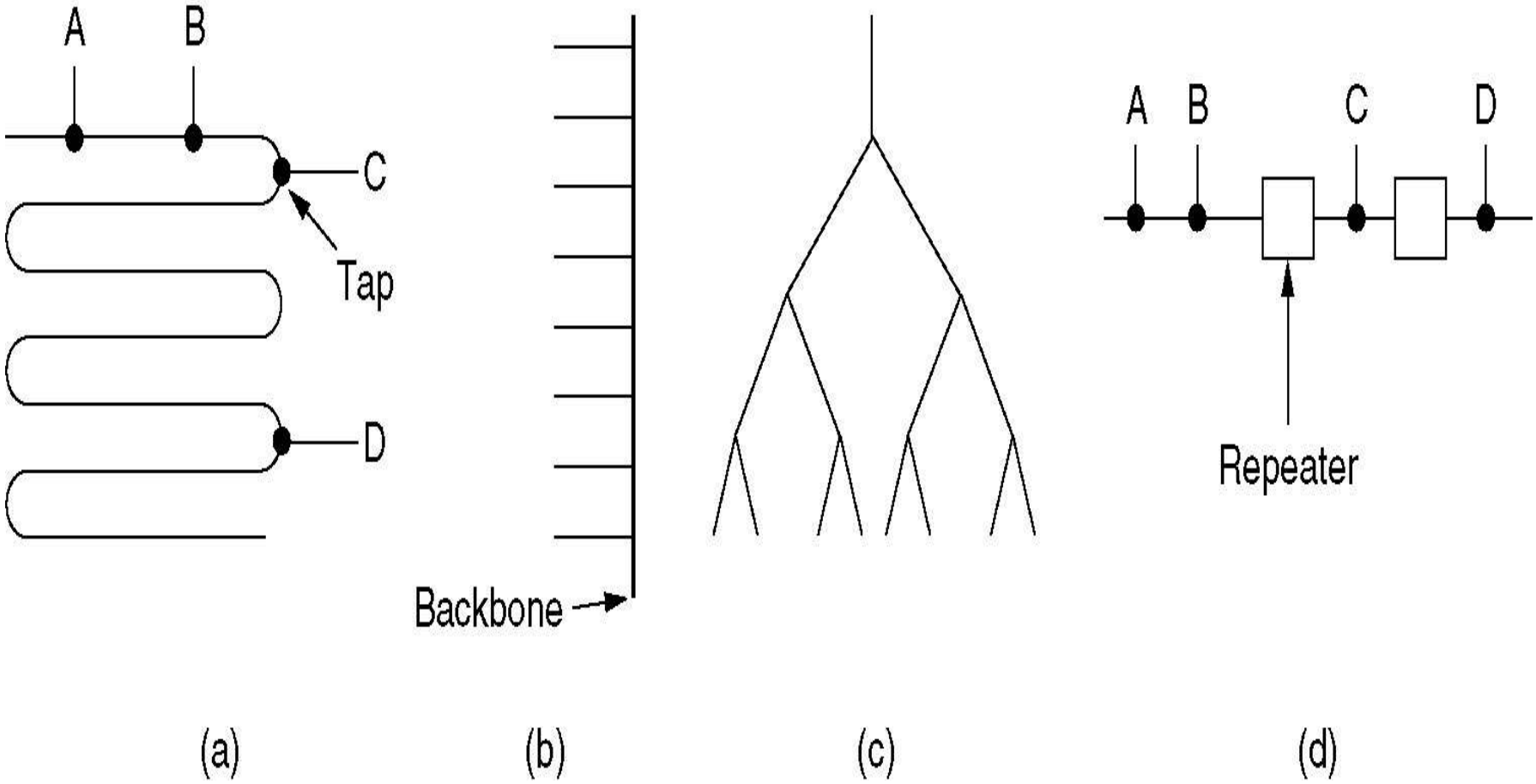
Một số dạng nối cáp



a. 10BASE2

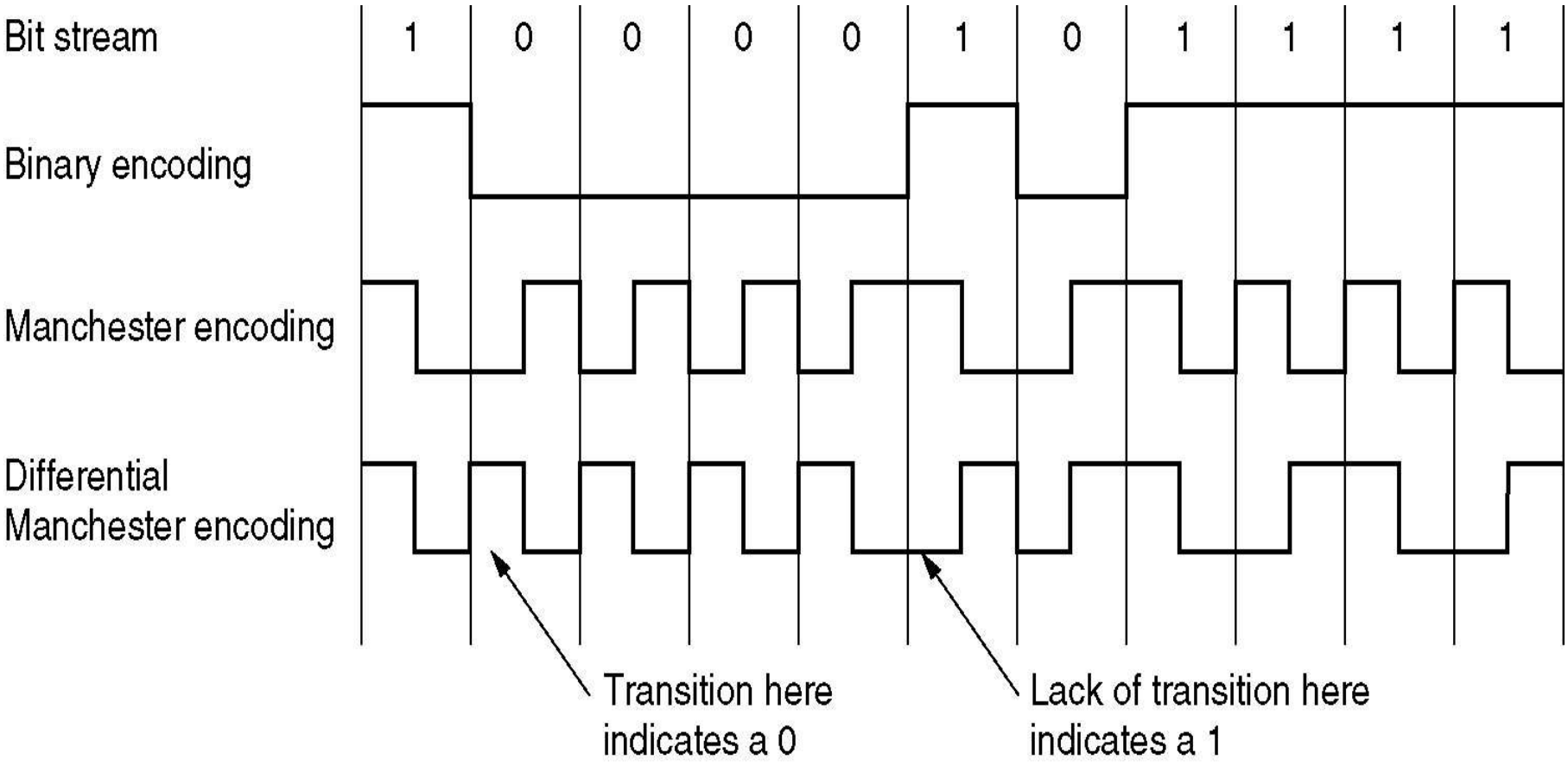
b. 10BASE-T

Các dạng hình học của cáp



a. Tuyến tính b. Đường trục c. Cây d. Phân đoạn

c. Mã hoá bit



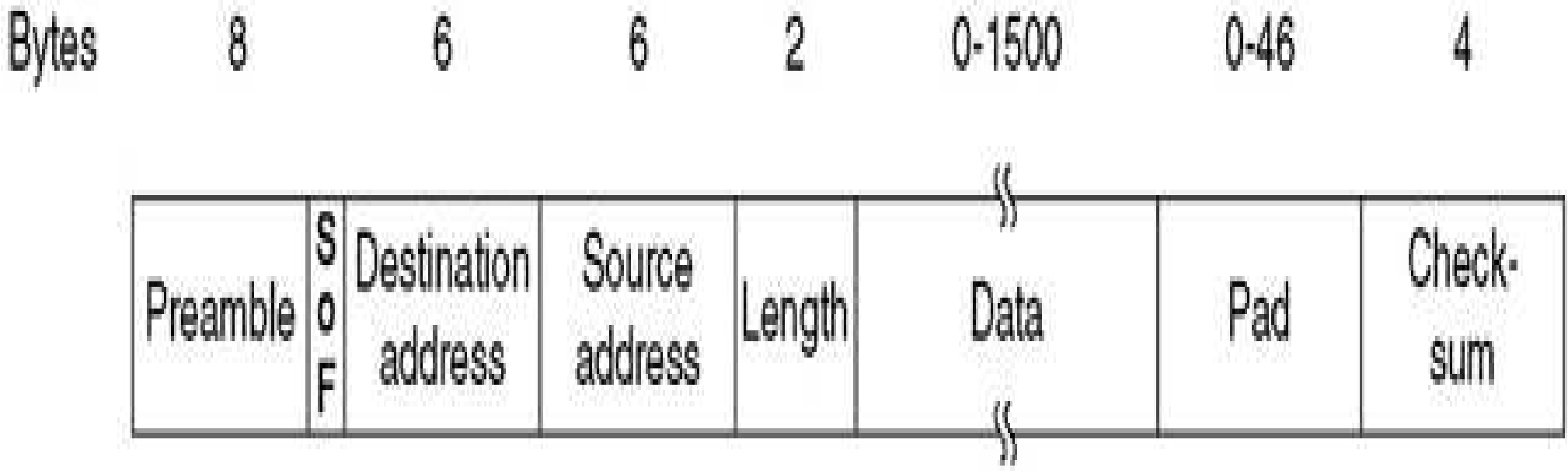
Mã hoá nhị phân (binary encoding)

Mã hoá Manchester (Manchester encoding)

Mã hoá Manchester vi phân (Differential Manchester encoding)

d. Giao thức lớp MAC

- CSMA/CD
- Cấu trúc frame theo IEEE 802.3



Các trường trong Ethernet frame

- Preamble – Mở đầu: 7 bytes 10101010

  SOF – Start Of Frame: 10101011

  đánh dấu bắt đầu frame
- Destination address – Địa chỉ MAC máy nhận (6 bytes địa chỉ card mạng)
- Source address – Địa chỉ MAC máy gởi (6 bytes địa chỉ card mạng)
- Length/Type: kích thước/loại frame

Các trường trong Ethernet frame (tt)

- Data: dữ liệu
- Pad: cần thêm vào để frame ≥ 64 bytes, từ yêu cầu phần cứng phát hiện xung đột
- Checksum: dùng trong phát hiện lỗi

e. Giải quyết xung đột

- Theo giao thức CSMA/CD
- Thời gian chờ ngẫu nhiên theo giải thuật dạng hàm mũ nhị phân (binary exponent backoff)

  đơn vị tính là slotTime = 512 bit times

  mạng 10 Mbps, 1 bit time = 100 nanosec

Giải quyết xung đột (tt)

- Nếu có xung đột, mỗi máy chờ ngẫu nhiên trong thời gian 0 → 1 slotTime
- Nếu có xung đột lần 2, mỗi máy chờ ngẫu nhiên trong thời gian 0 → 3 slotTime
- Nếu có xung đột lần i, mỗi máy chờ ngẫu nhiên trong thời gian 0 → 2^i - 1 slotTime
- Từ xung đột lần 10, mỗi máy chờ ngẫu nhiên trong thời gian 0 → 1023 slotTime
- Nếu xung đột đến lần 16 thì báo lỗi

2. Mạng Fast Ethernet

- Còn gọi là chuẩn IEEE 802.3u
- Giữ nguyên cấu trúc frame mạng Ethernet, giao thức CSMA/CD, tăng tốc độ 100 Mbps.

  1 bit time = 10 nanosec
- Không dùng cáp đồng trục

Một số loại cáp mạng Fast Ethernet

Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

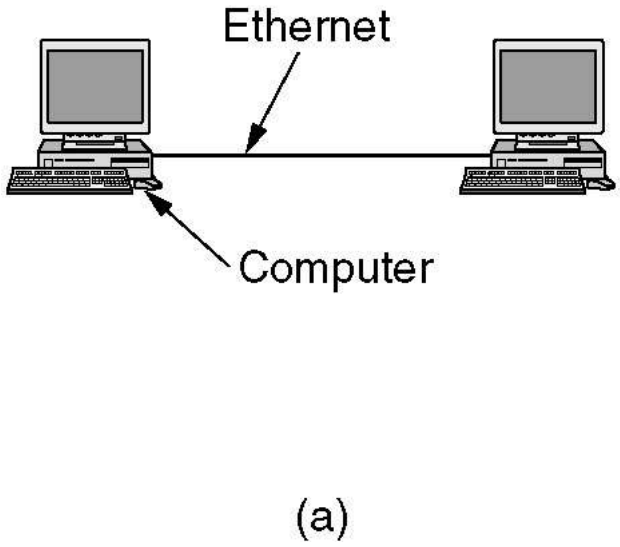
3. Mạng Gigabit Ethernet

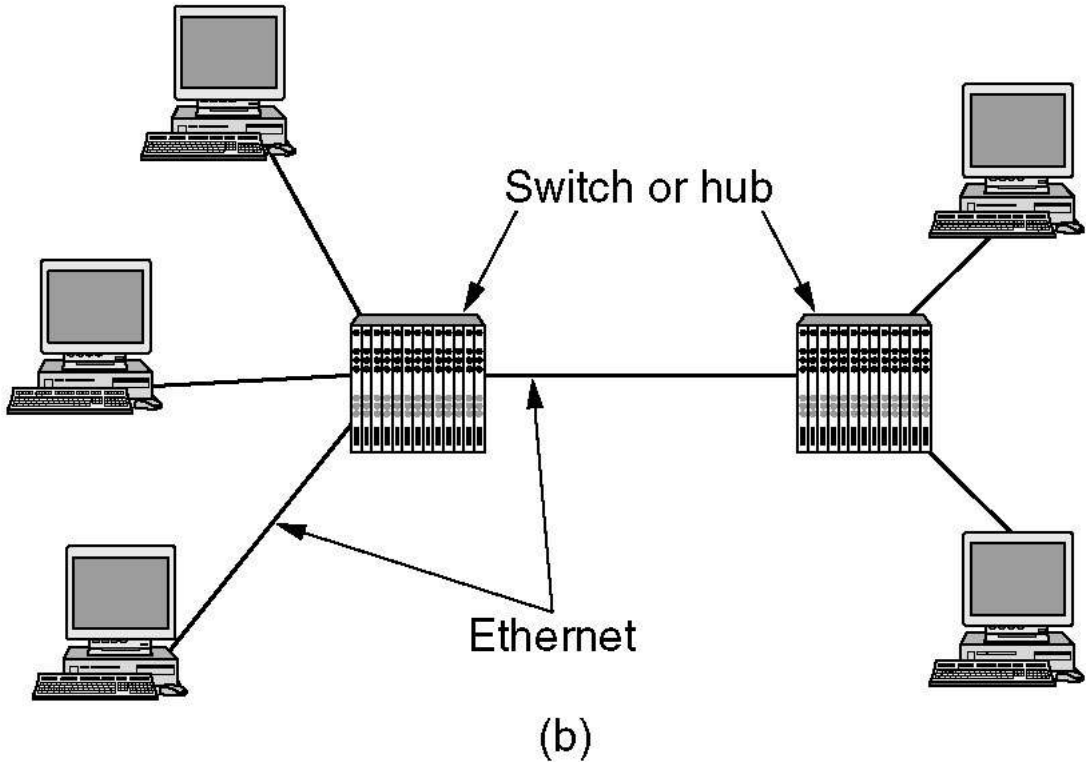
- Còn gọi là chuẩn IEEE 802.3z
- Mở rộng mạng dạng Ethernet lên tốc độ 1000 Mbps
- Giữ cấu trúc frame, giao thức CSMA/CD

Một số loại cáp mạng Gigabit Ethernet

Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550 m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000 m	Single (10 μ) or multimode (50, 62.5 μ)
1000Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP

Hai dạng kết nối mạng Gigabit Ethernet





a. Hai trạm

b. Nhiều trạm

Nhận xét về các loại mạng Ethernet

- Đơn giản
  - Giá thành rẻ
  - Tin cậy
  - Dễ bảo trì
- Hoạt động tốt với bộ giao thức TCP/IP
- Tiếp tục phát triển

4. Mạng Token Ring – 802.5

a. Giới thiệu mạng Token Ring
b. Kết nối
c. Sơ lược hoạt động

a. Giới thiệu mạng Token Ring

- Xuất phát từ mạng Token Ring của IBM

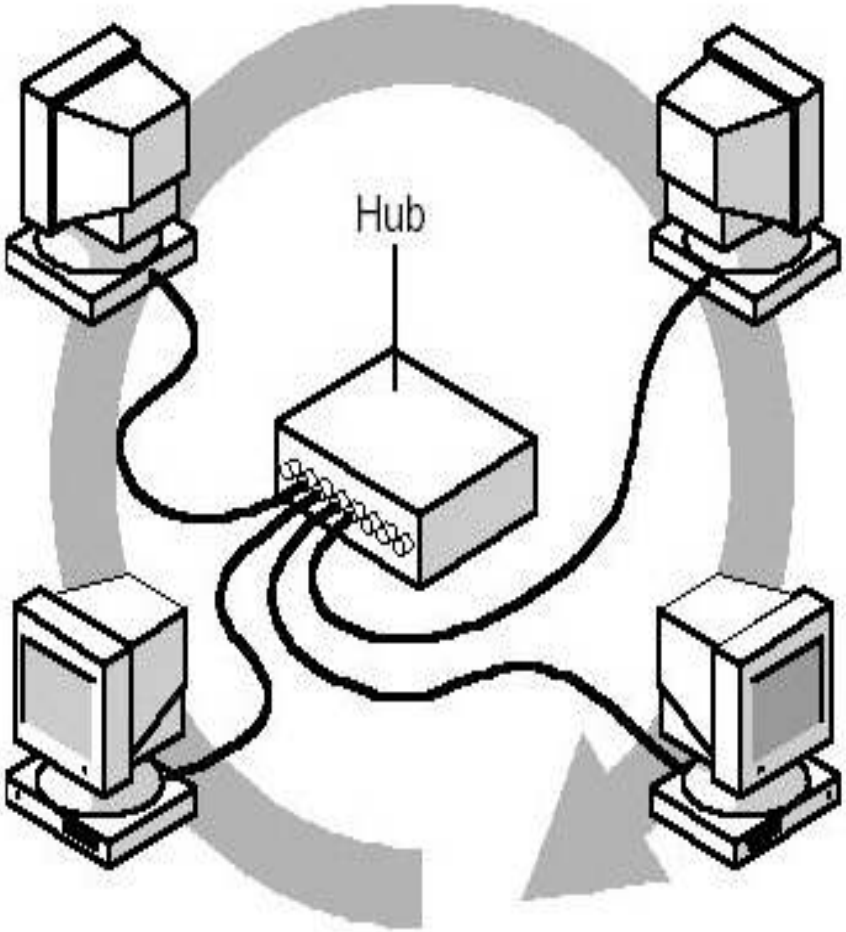
  → SNA (System Networks Architecture)
- Bao gồm các dạng máy tính IBM: PC, Midrange, Mainframe
- Tiêu chuẩn IEEE 802.5

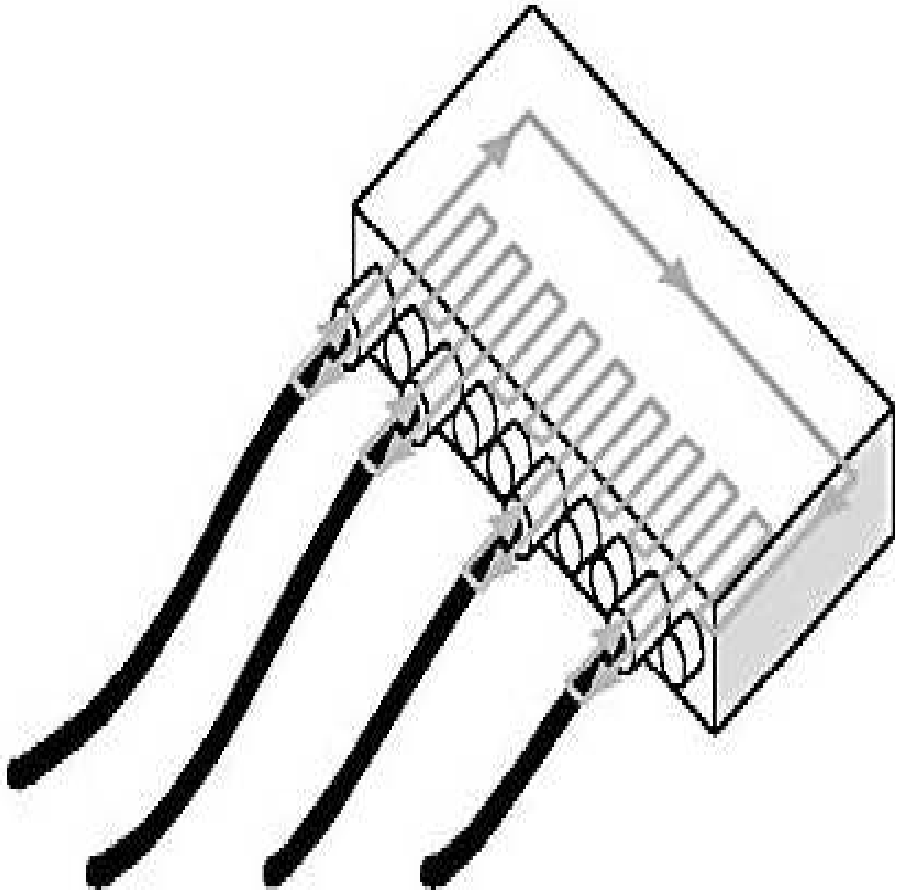
Tốc độ	4/16 Mbps	802.5
	100 Mbps	802.5t
	1000 Mbps	802.5v

b. Kết nối mạng Token Ring

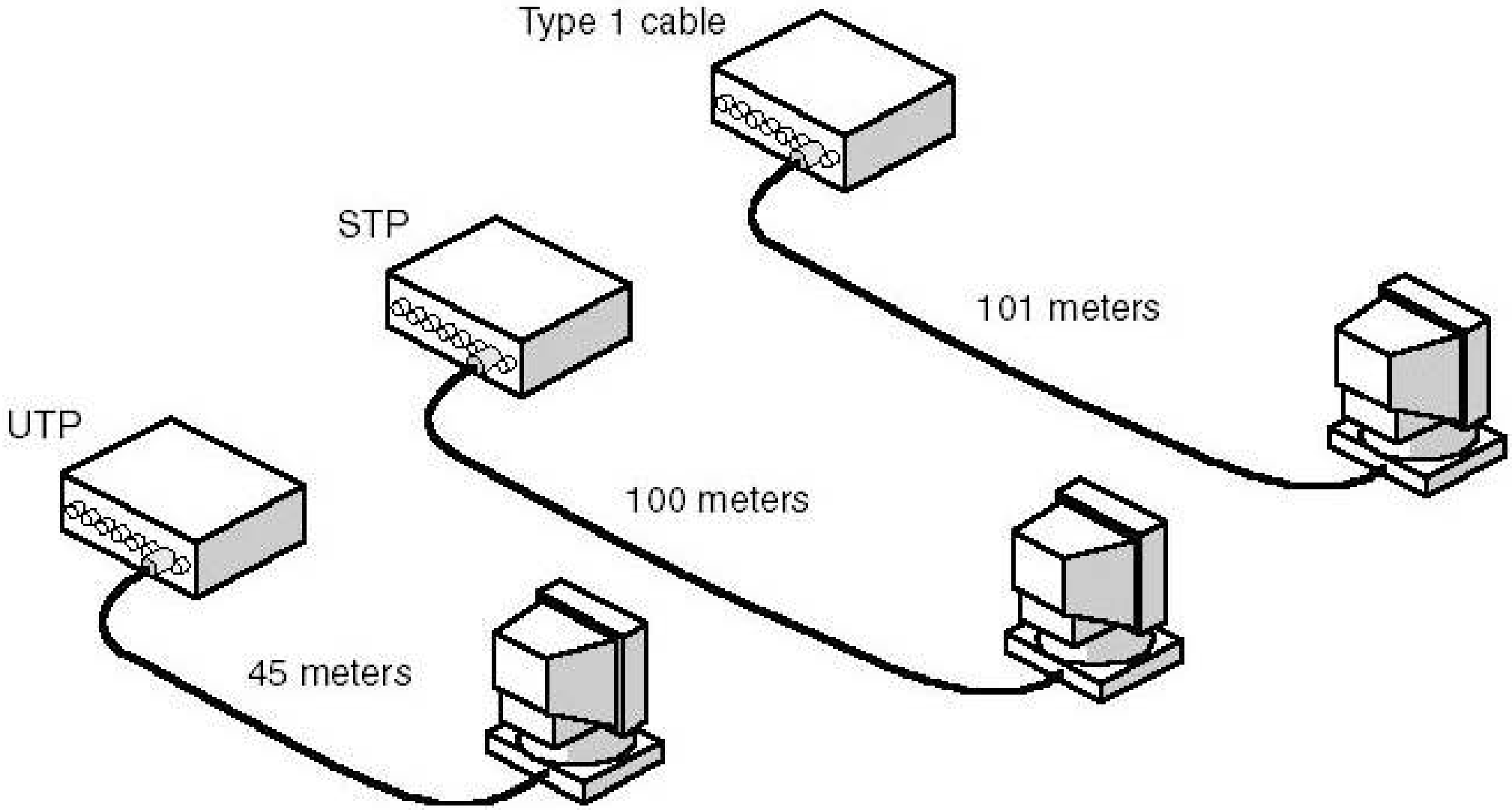
- Dùng Hub, còn gọi là Wire center, MAU (Multistation Access Unit) tạo vòng vật lý
- Token Ring NIC
- UTP, STP với RJ-45

Vòng vật lý dùng Hub





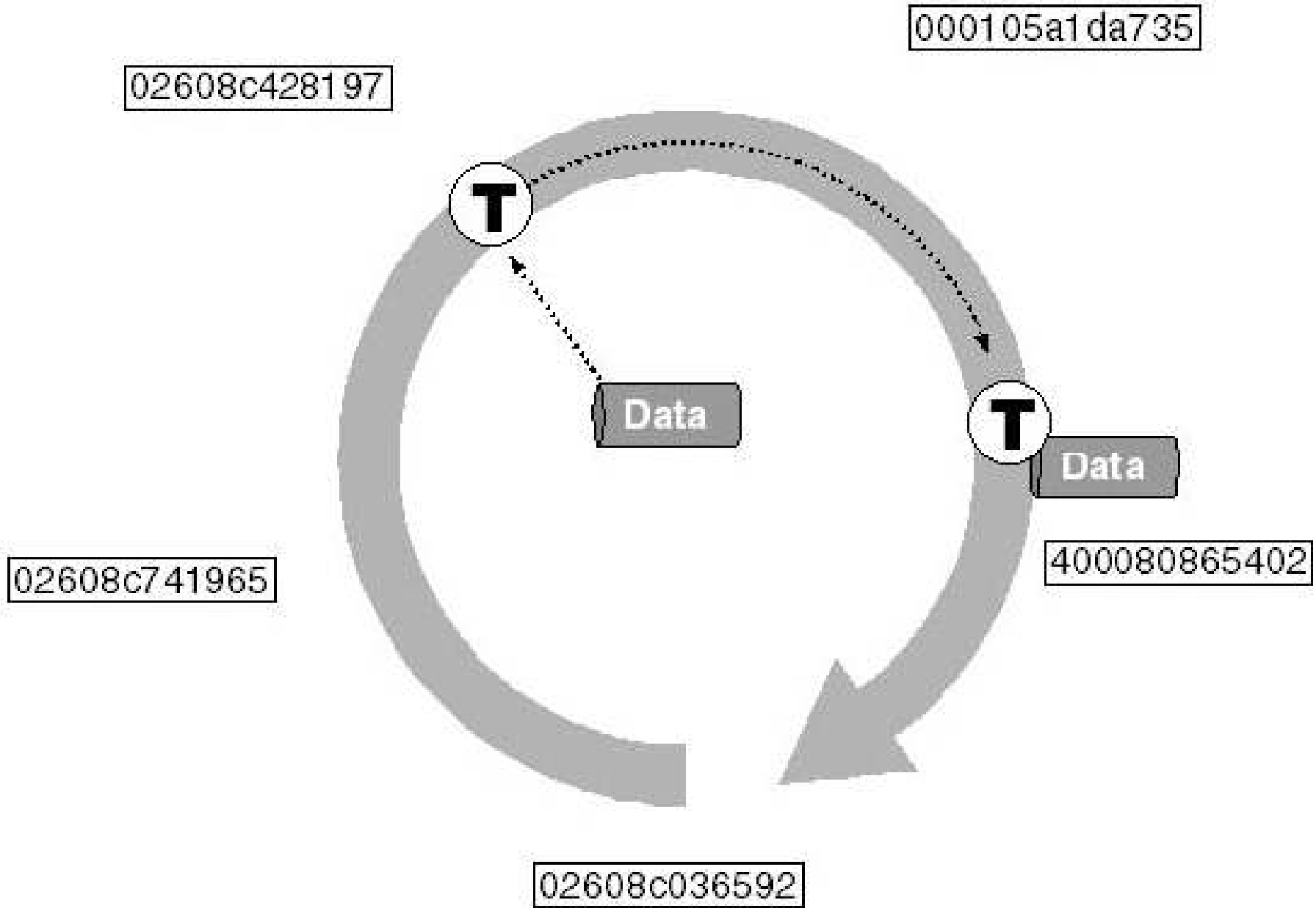
Một số dạng cáp



c. Sơ lược hoạt động mạng Token Ring

- Có 1 frame đặc biệt (token) truyền trên vòng
- Một máy cần gởi frame:
  - Chờ token
  - Truyền data frame
  - Data frame theo vòng đến máy nhận
  - Máy nhận xác nhận trên frame
  - Data frame theo vòng trở về máy gởi
  - Máy gởi hủy frame, gởi lại token

Token xoay trên vòng



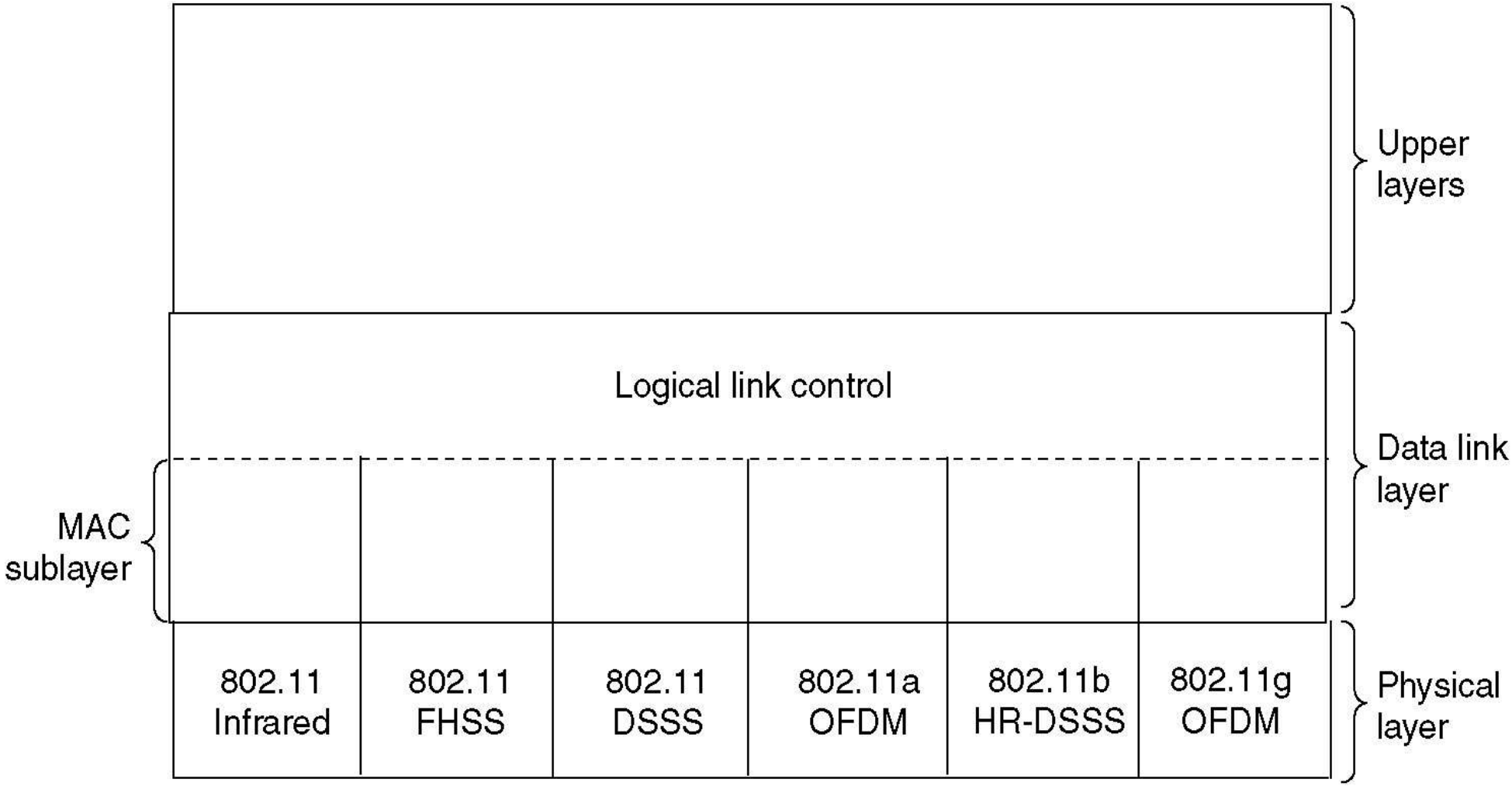
5. Mạng Wireless Ethernet – 802.11

a. Giới thiệu tiêu chuẩn IEEE 802.11
b. Kết nối mạng 802.11
c. Sơ lược hoạt động mạng 802.11

a. Giới thiệu tiêu chuẩn IEEE 802.11

- Là tiêu chuẩn cho mạng cục bộ không dây (Wireless LAN)
- Dùng sóng điện từ với nhiều kỹ thuật cho lớp vật lý
- Các dạng tốc độ
  - 1 → 2 Mbps : 802.11
  - 1 → 11 Mbps : 802.11b (Wi-Fi)
  - 5 Ghz band (~ 54 Mbps): 802.11a
  - 802.11g : tương đương 802.11a

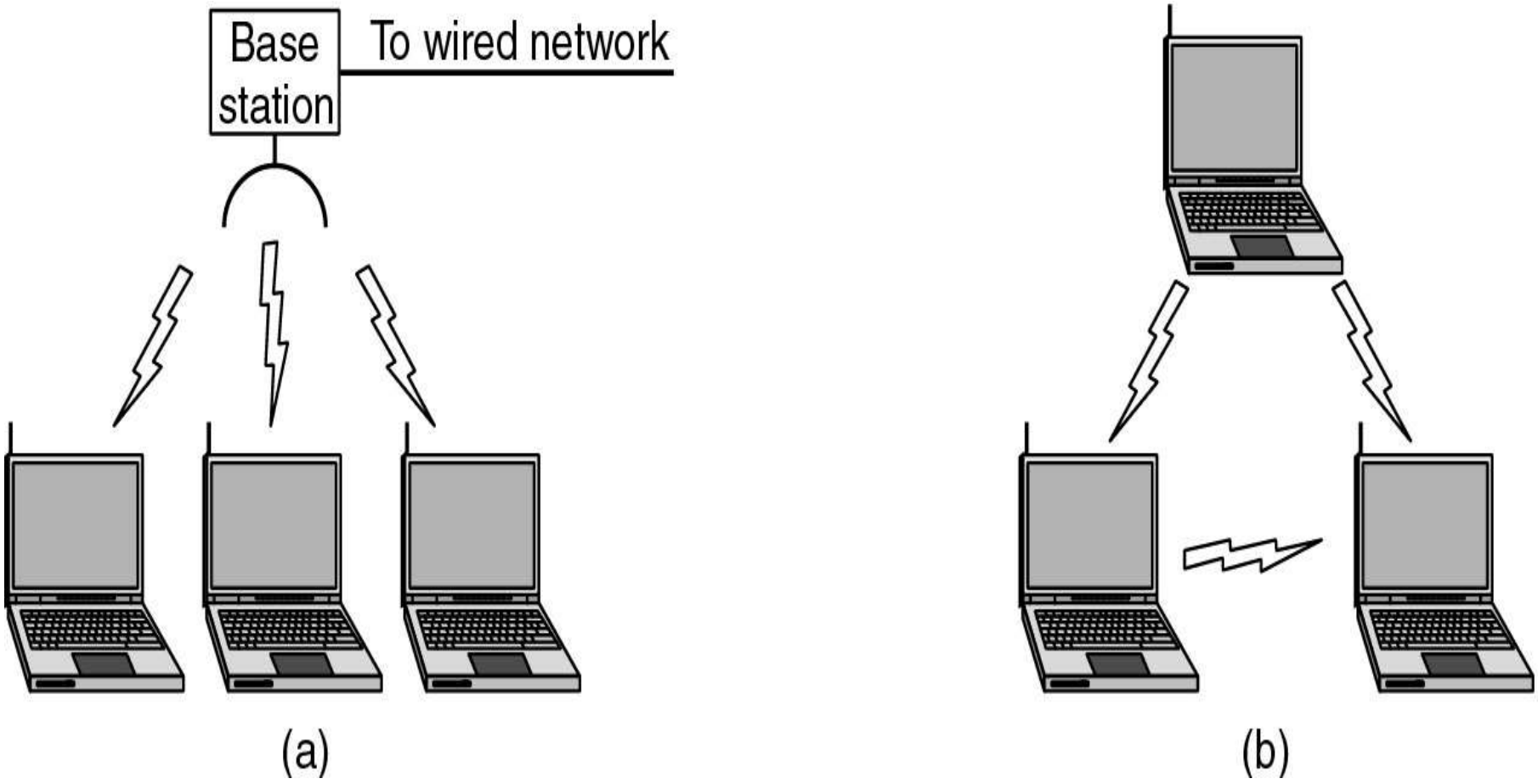
Một phần các giao thức theo chuẩn 802.11



b. Kết nối mạng 802.11

- Card mạng không dây (Wireless NIC)
- Kết nối:
  - Có trạm nền (base station/access point)
  - Ngang hàng (peer nodes / ad hoc)

Hai dạng kết nối mạng không dây



a. Có dùng base station, còn gọi là access point

b. Các máy gởi nhận trực tiếp, ad hoc networking

c. Sơ lược hoạt động mạng 802.11

- Máy trạm phải liên kết (associate) để kết nối vào mạng (access point/peer)
- Máy trạm có thể tách (disassociate) khỏi trạm nền, hay thay đổi trạm nền khác (reassociate)
- Máy trạm có thể cần đăng nhập (authenticate) trước khi trao đổi dữ liệu

Sơ lược hoạt động mạng 802.11 (tt)

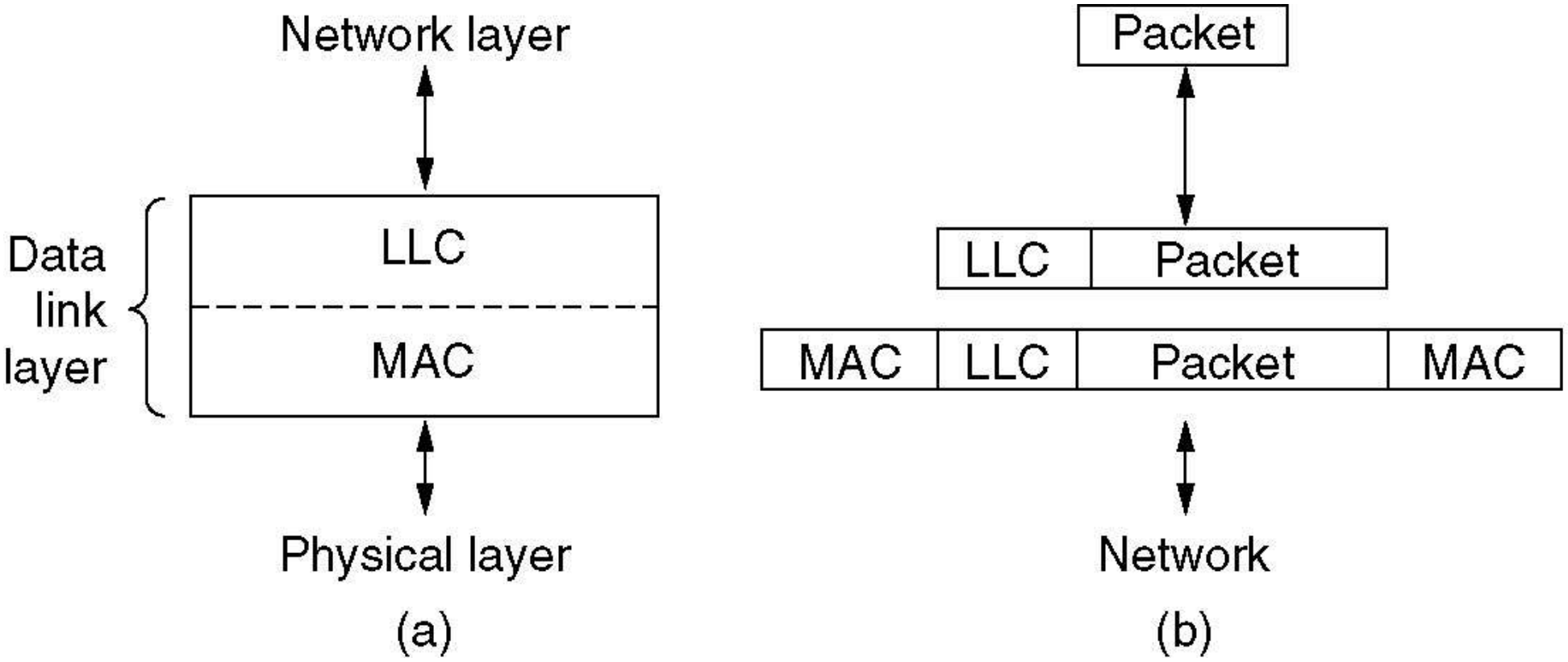
- Sau khi thiết lập kết nối với mạng, mỗi máy có thể gởi frame theo tiêu chuẩn 802.11
- Dùng giao thức CSMA/CA

  (Carrier Sense Multiple Access/Collision Avoidance)
- Khi máy gởi truyền frame, máy nhận gởi ACK

6. Điều khiển liên kết luận lý (LLC)

- Chuẩn IEEE 802.2
- Giao thức LLC ở trên các giao MAC:
  - Che dấu những khác biệt, tạo khuôn dạng và giao diện chung đối với lớp mạng
  - Thực hiện kiểm soát lỗi, kiểm soát lưu lượng nếu cần thiết

Quan hệ giữa các lớp



a. Vị trí lớp con LLC

b. Quan hệ về dữ liệu

Các dịch vụ của lớp LLC

- Unacknowledged connectionless-mode

  Gởi nhận không kiểm soát
  - Có các dạng point-to-point, multicast, broadcast
- Acknowledged connectionless-mode

  Gởi nhận có xác nhận của máy nhận
  - dạng point-to-point
- Connection-mode

  Gởi nhận có thiết lập kết nối

V. Giới thiệu về Bridge, Switch

1. Bridge (cầu nối)
2. Switch (chuyển mạch)

1. Bridge

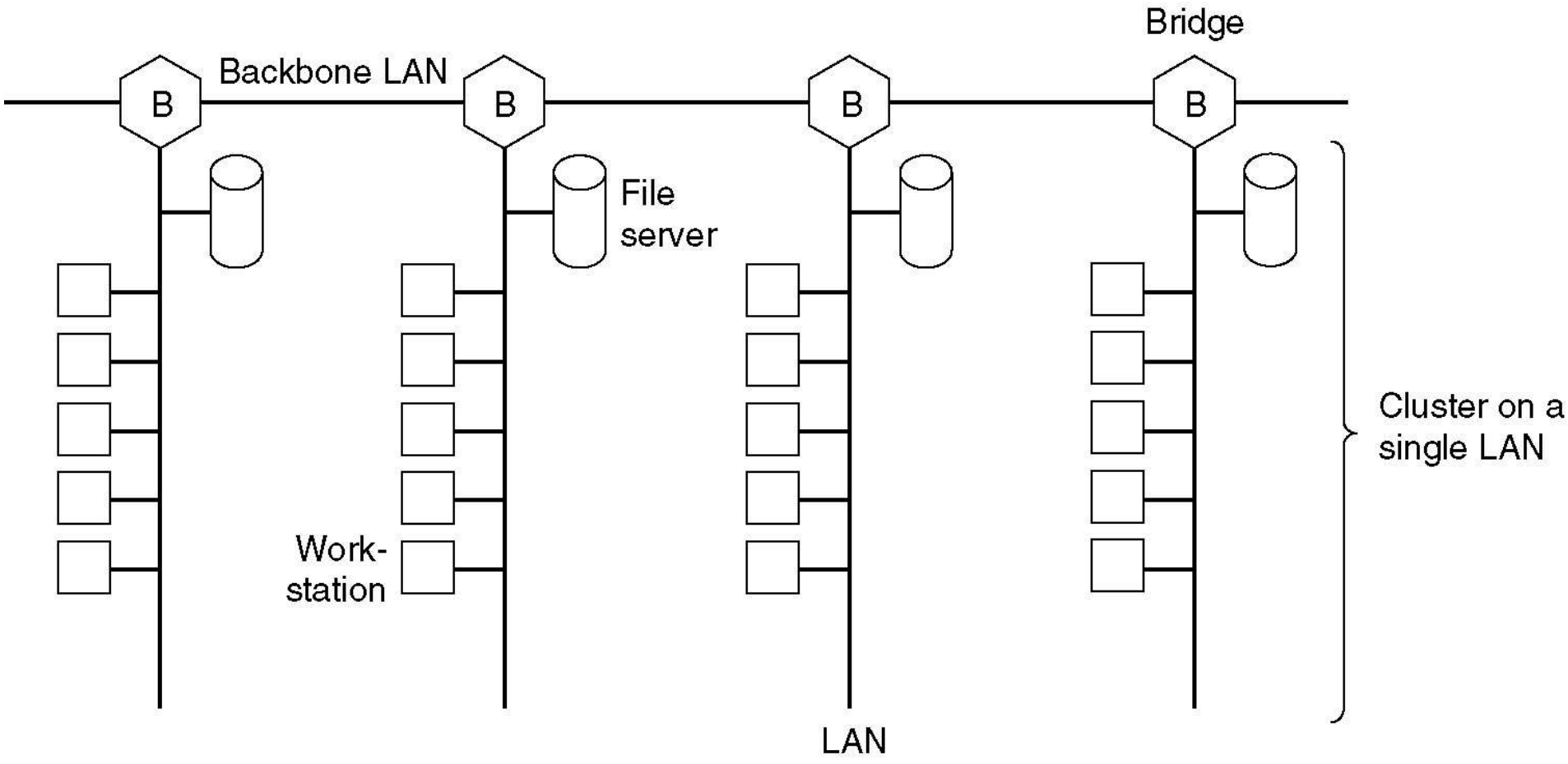
Mục đích:

- Kết nối các mạng LAN khác loại
- Mở rộng khoảng cách giữa các máy
- Chia mạng lớn thành các mạng nhỏ

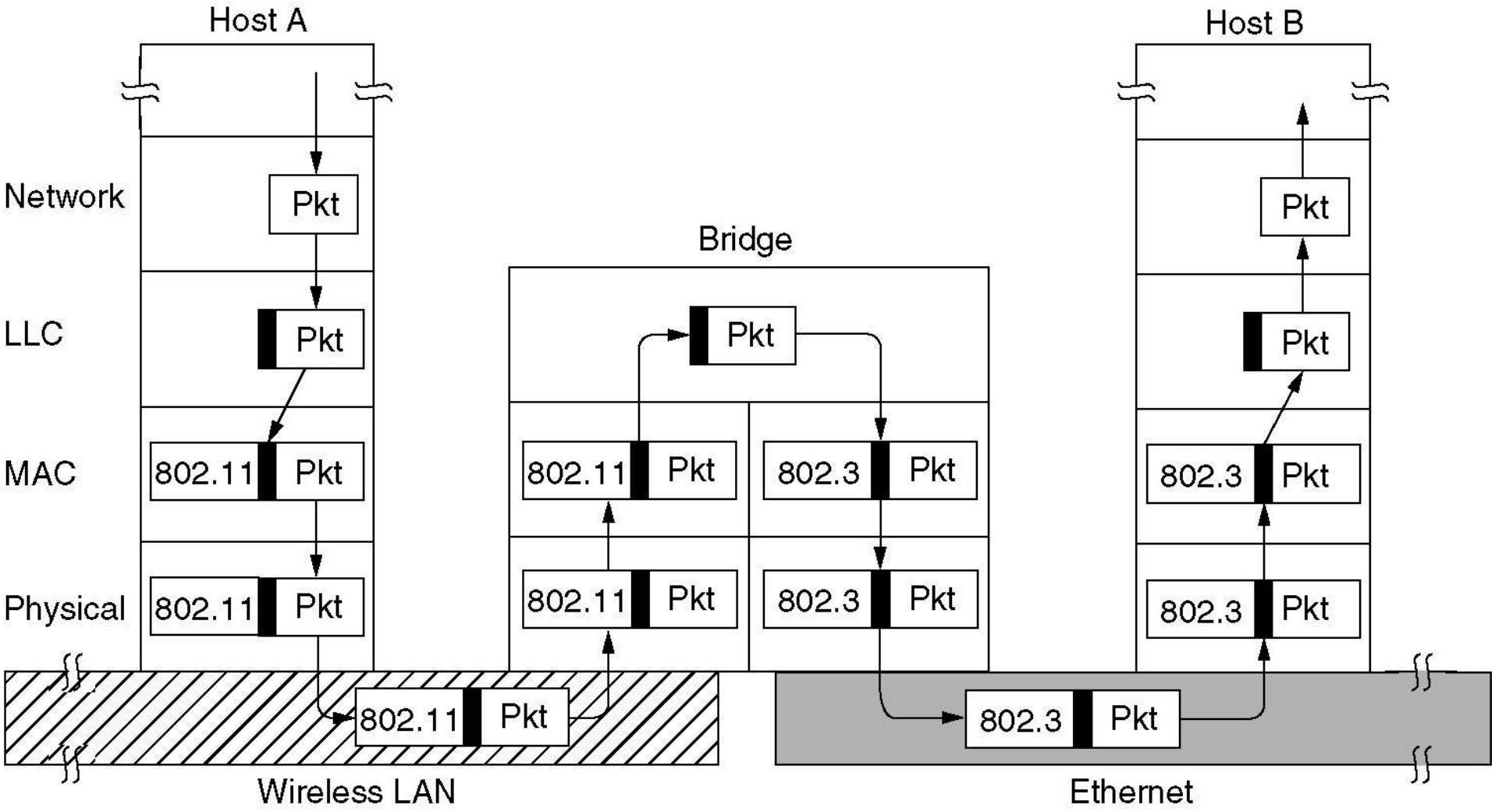
Hoạt động: *dạng store-and-forward*

- Nhận frame từ mạng nguồn
- Thực hiện các xử lý cần thiết
- Chuyển frame đến mạng đích

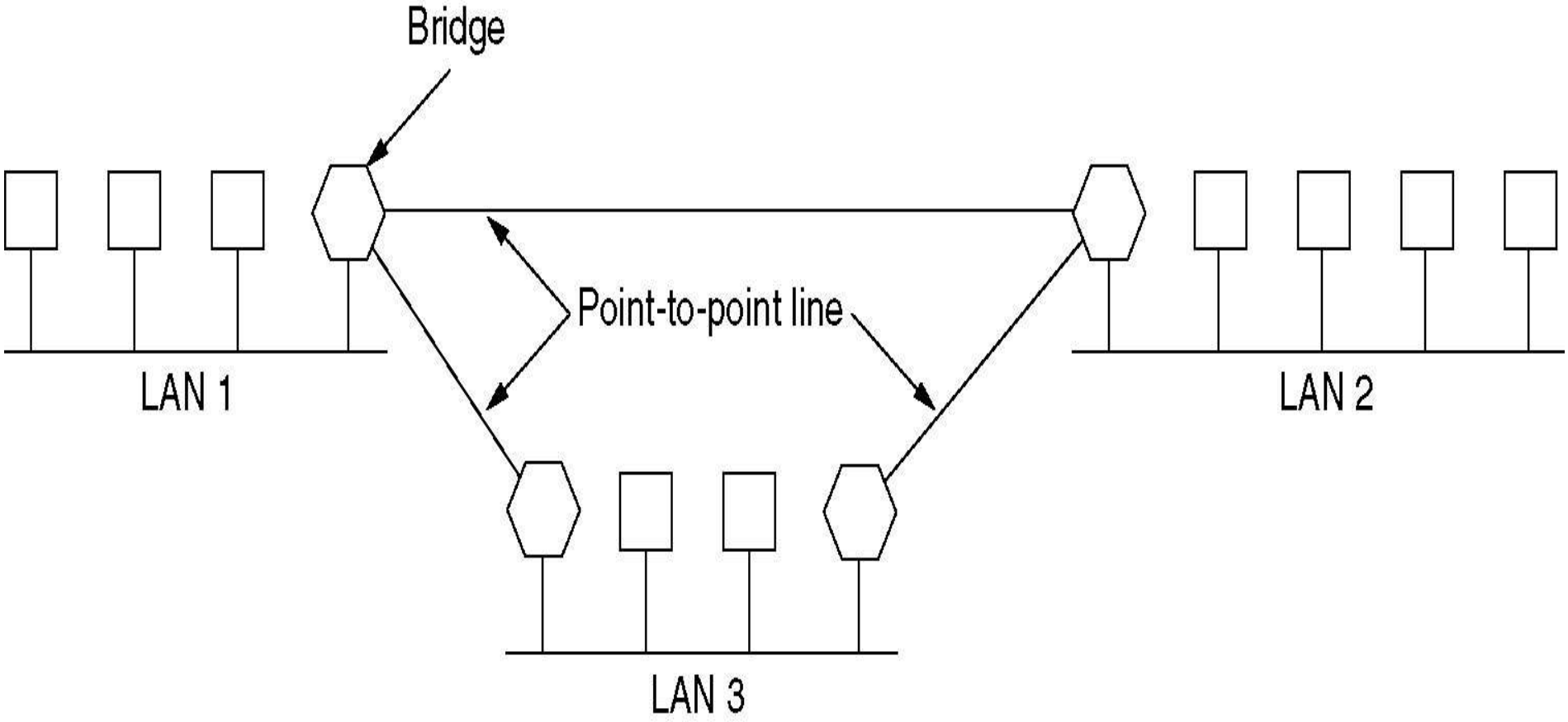
Nhiều LAN kết dùng các bridge



Hoạt động của bridge từ 802.11 sang 802.3



Kết nối các LAN từ xa dùng bridge



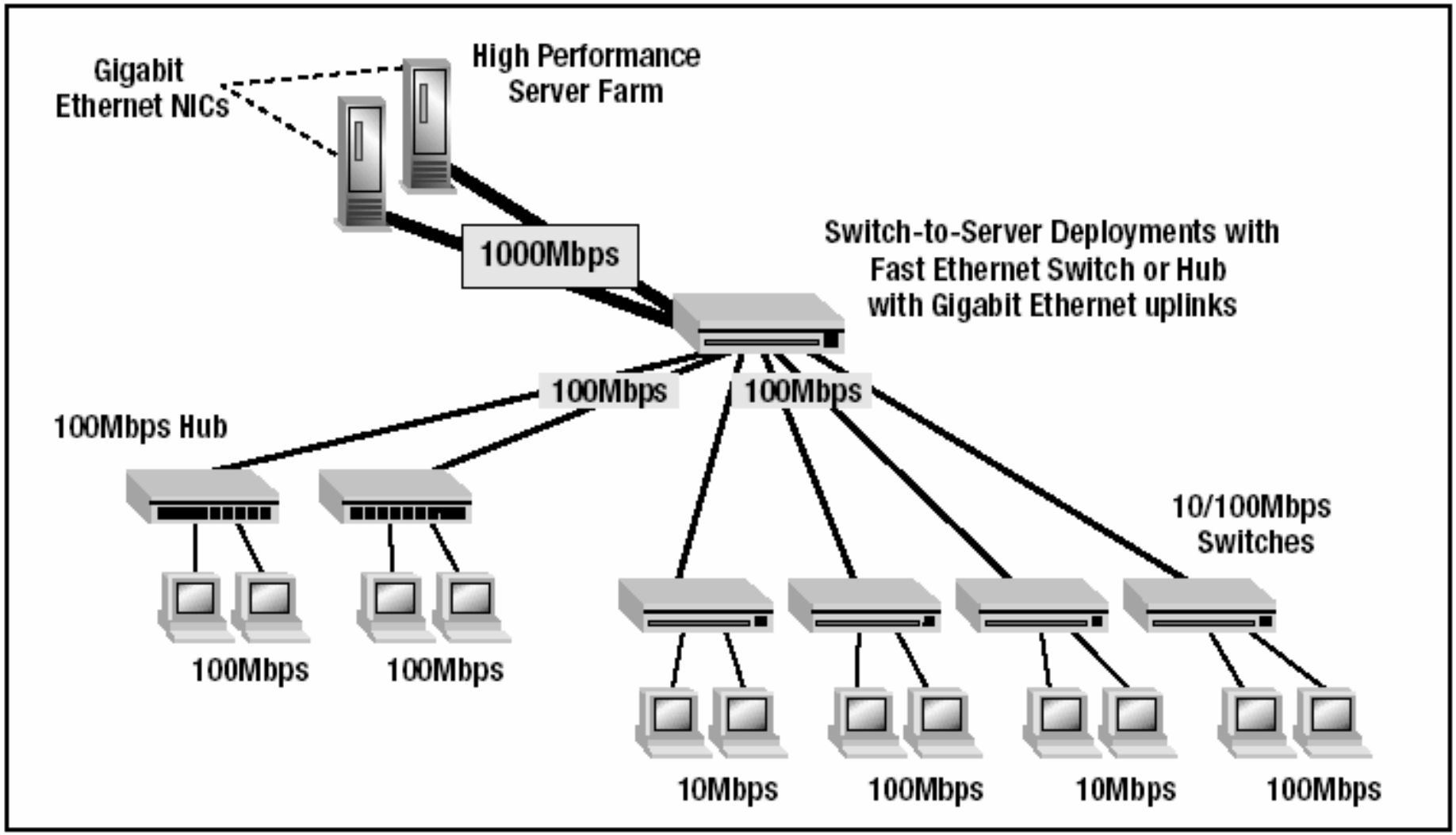
2. Switch

Switch: bridge nhiều port, tốc độ cao

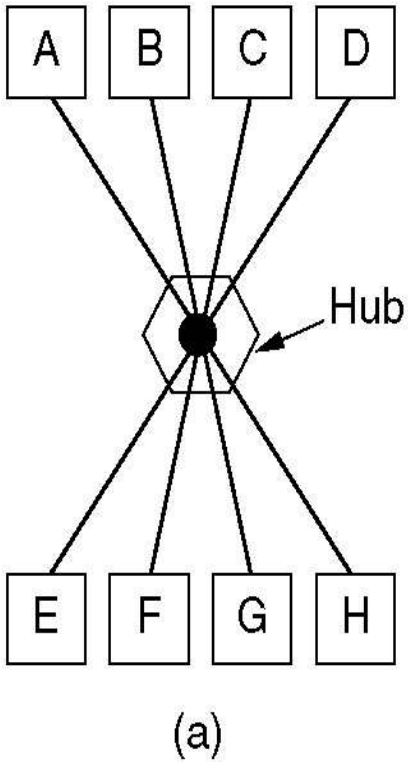
Đặc điểm:

- Tốc độ cao
- Giảm xung đột → chỉ xung đột giữa máy và switch port
- Hoạt động ở chế độ full-duplex
  → không xung đột
- Có khả năng kiểm tra checksum của frame

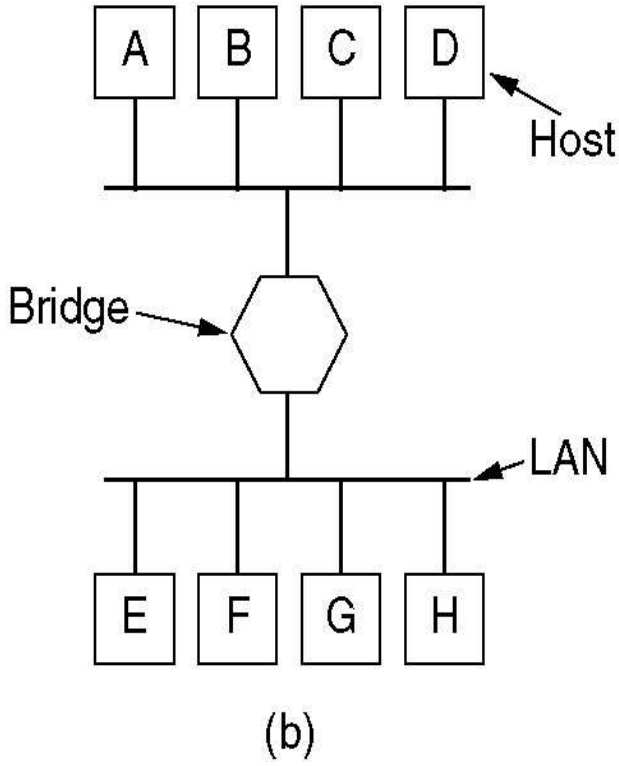
Ví dụ:


Gigabit
Ethernet NICs
High Performance
Server Farm
1000Mbps
Switch-to-Server Deployments with
Fast Ethernet Switch or Hub
with Gigabit Ethernet uplinks
100Mbps
100Mbps
100Mbps Hub
10/100Mbps
Switches
100Mbps
100Mbps
10Mbps
100Mbps
10Mbps
100Mbps

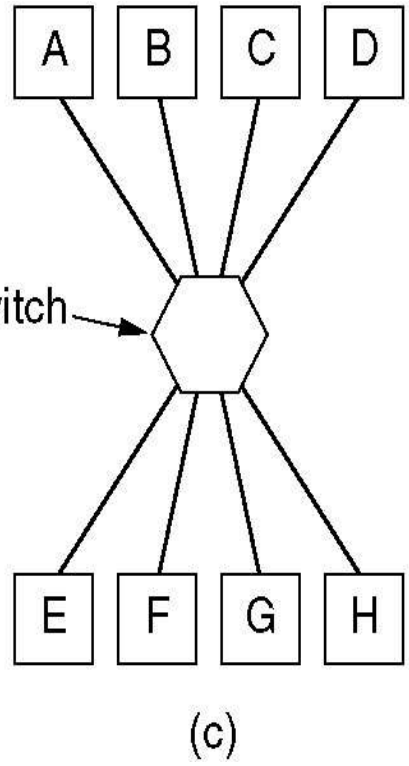
So sánh Hub, Bridge, Switch



(a)



(b)



(c)

a. Hub

b. Bridge

c. Switch

NHẬP MÔN MẠNG MÁY TÍNH

Chương 4

LỚP NETWORK

(LỚP MẠNG)

Nội dung chương 4

I. Các vấn đề thiết kế lớp network
II. Giới thiệu về định tuyến
III. Các vấn đề liên mạng
IV. Lớp network trên mạng TCP/IP
V. Giới thiệu IPv6

I. Các vấn đề thiết kế lớp network

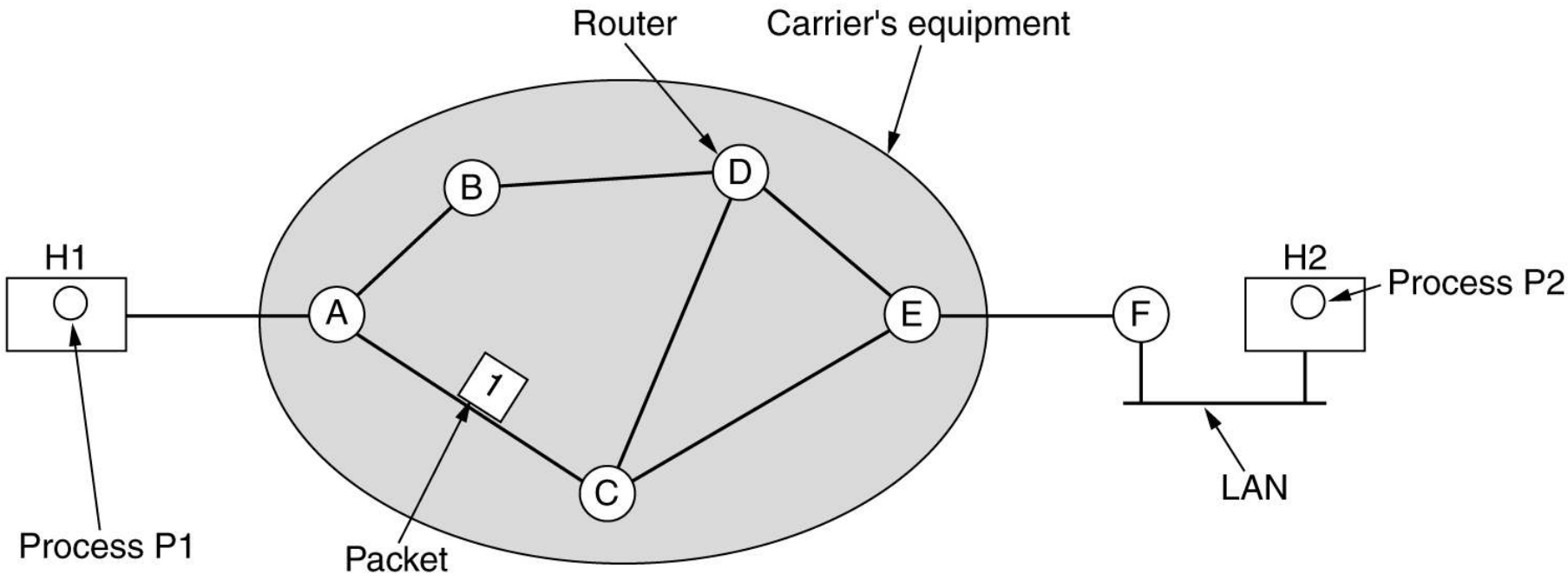
1. Nhiệm vụ lớp Network
2. Các dịch vụ cung cấp cho lớp transport

1. Nhiệm vụ lớp network

- Cung cấp dịch vụ gởi nhận dữ liệu (packet) giữa hai máy bất kỳ

  hai máy bất kỳ có thể trên các mạng khác nhau
- Giải quyết vấn đề định tuyến, liên mạng, định địa chỉ mạng

Môi trường hoạt động lớp network



- Host gởi packet đến router gần nhất
- Các router truyền các packet theo dạng store-and-forward

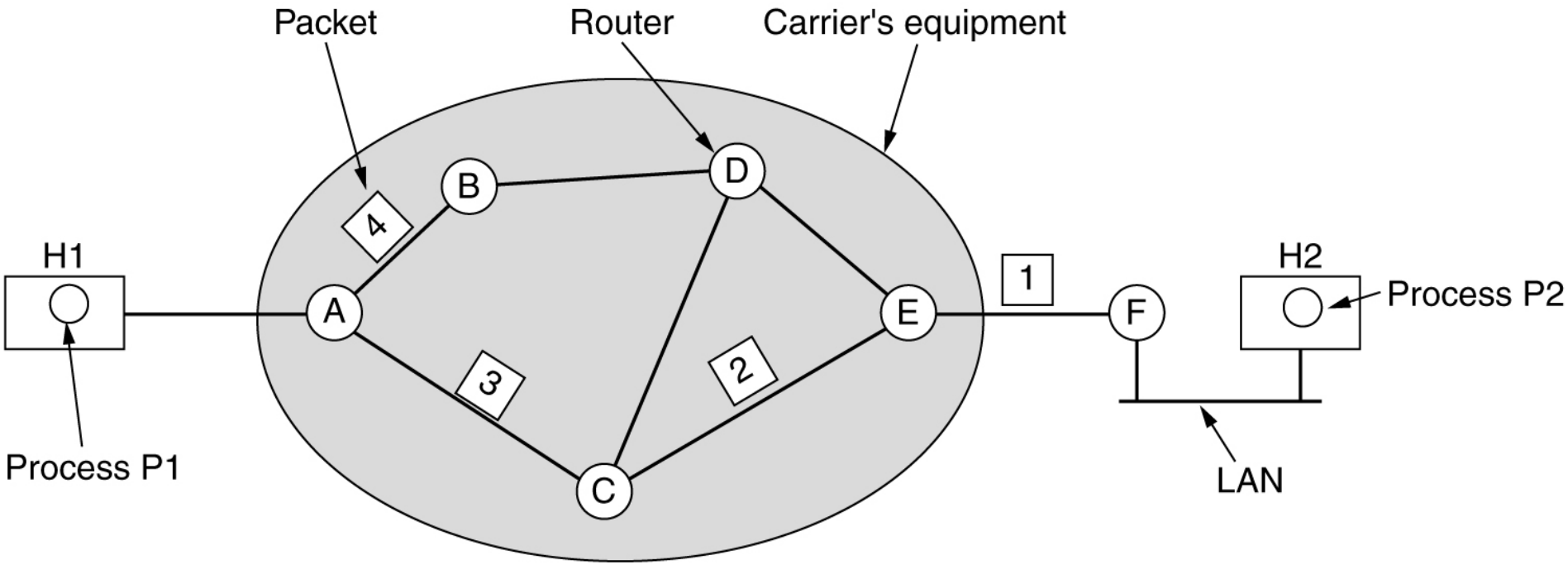
2. Các dịch vụ cung cấp cho lớp transport

- Dịch vụ không kết nối (connectionless)
- Dịch vụ có kết nối (connection-oriented)

Các đặc điểm hai dạng dịch vụ

Vấn đề	Dịch vụ không kết nối	Dịch vụ có kết nối
Thiết lập kết nối	Không cần	Cần → mạch ảo
Định địa chỉ	Mỗi packet chứa địa chỉ nguồn và địa chỉ đích	Mỗi packet chứa thông tin về mạch ảo
Định tuyến	Mỗi packet được định tuyến độc lập	Tuyến được chọn khi thiết lập mạch ảo. Tất cả packet truyền trên tuyến.

Ví dụ: định tuyến dạng không kết nối



A's table

Dest.	initially Line	later Line
A	–	–
B	B	B
C	C	C
D	B	B
E	C	B
F	C	B

C's table

Dest.	Line
A	A
B	A
C	–
D	D
E	E
F	E

E's table

Dest.	Line
A	C
B	D
C	C
D	D
E	–
F	F

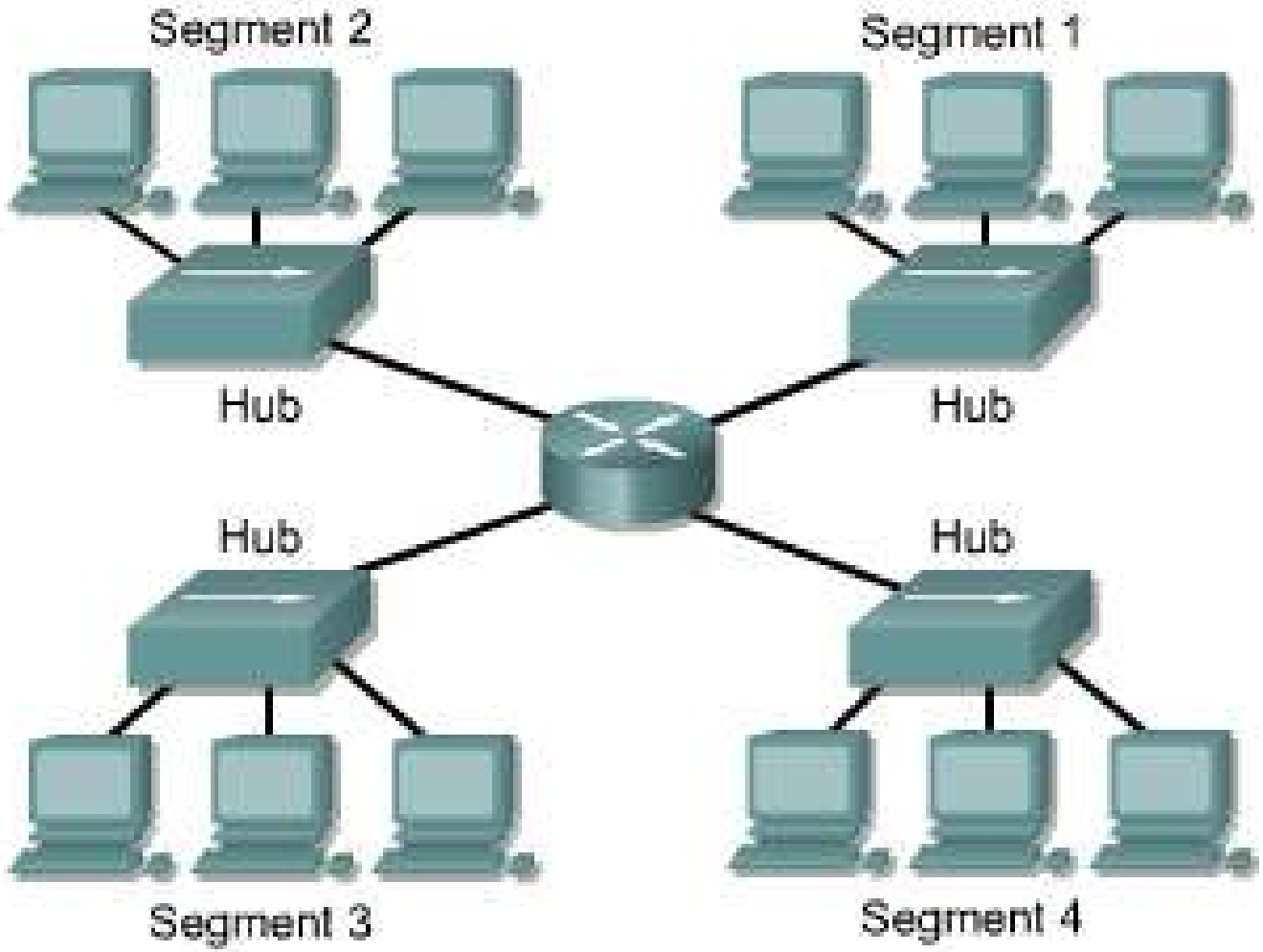
II. Giới thiệu về định tuyến

1. Khái niệm định tuyến
2. Định tuyến tĩnh
3. Định tuyến động

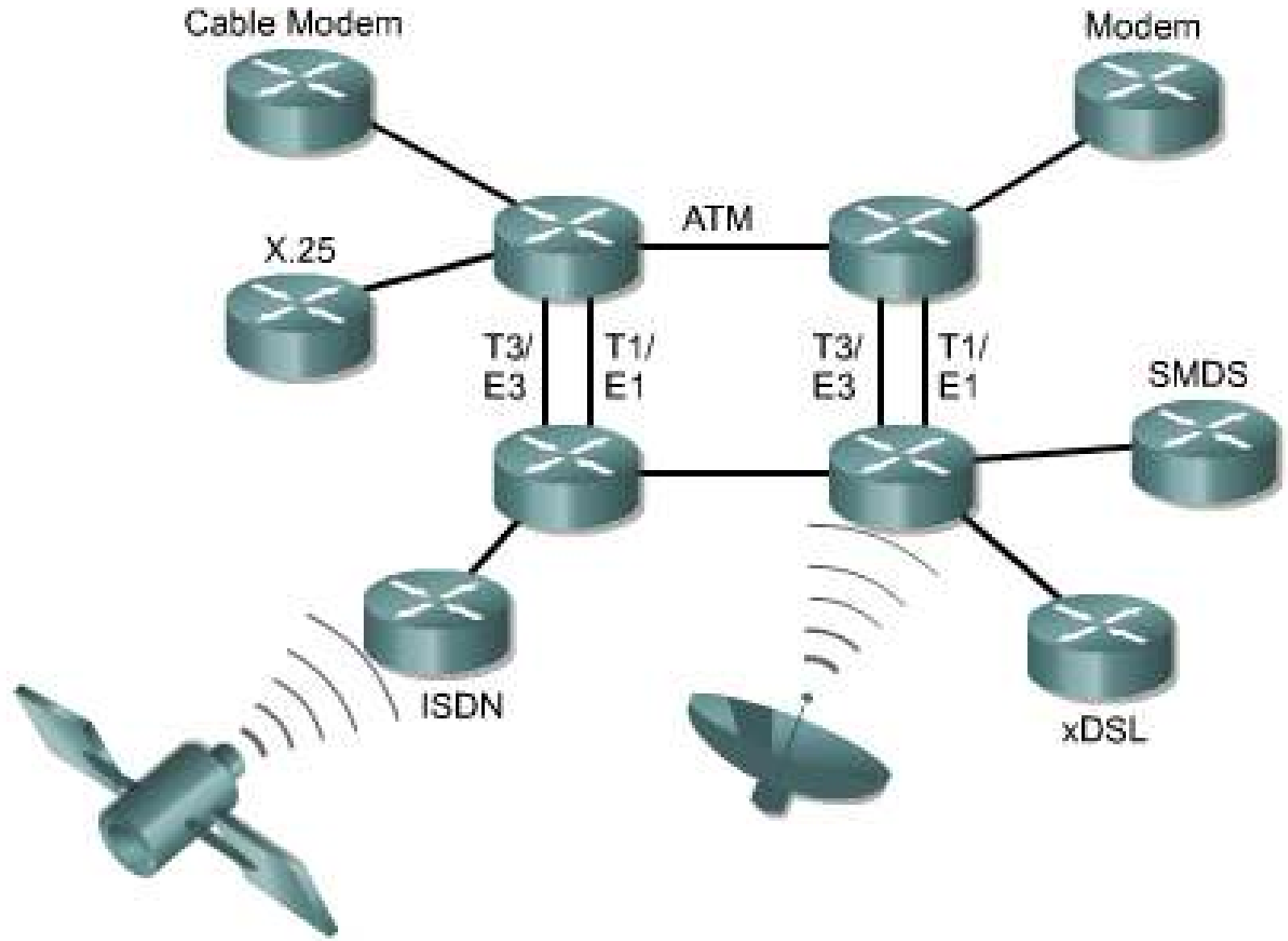
1. Khái niệm định tuyến

- Định tuyến (routing): xác định con đường (tuyến, route) chuyển tiếp dữ liệu từ mạng này sang mạng khác
- Định tuyến là chức năng của lớp network
- Định tuyến được thực hiện tại bộ định tuyến (router)
- Router là thiết bị (hay phần mềm trên một máy tính) kết nối giữa các mạng

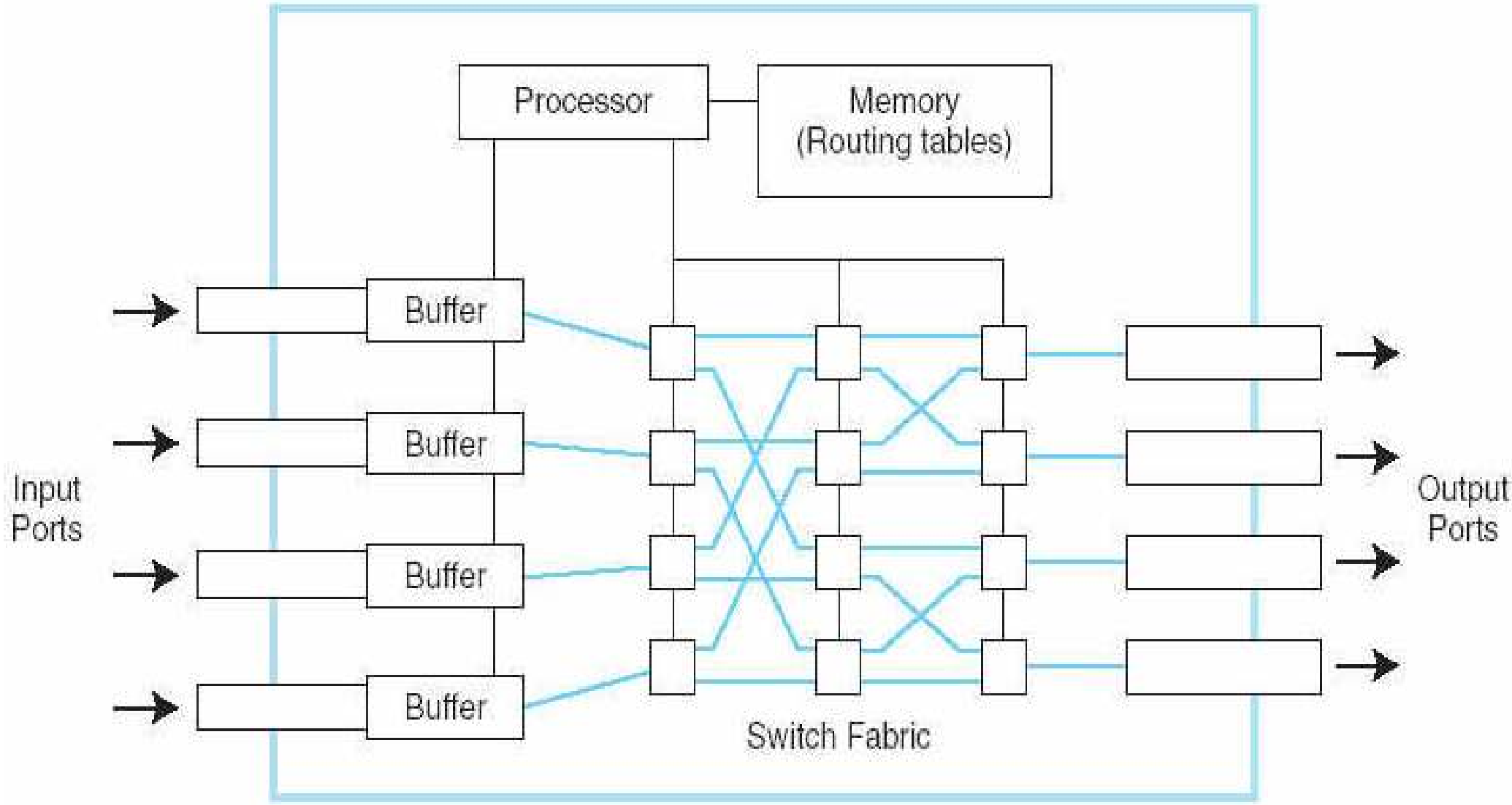
Router kết nối các mạng cục bộ



Router trên mạng miền rộng



Cấu trúc cơ bản router

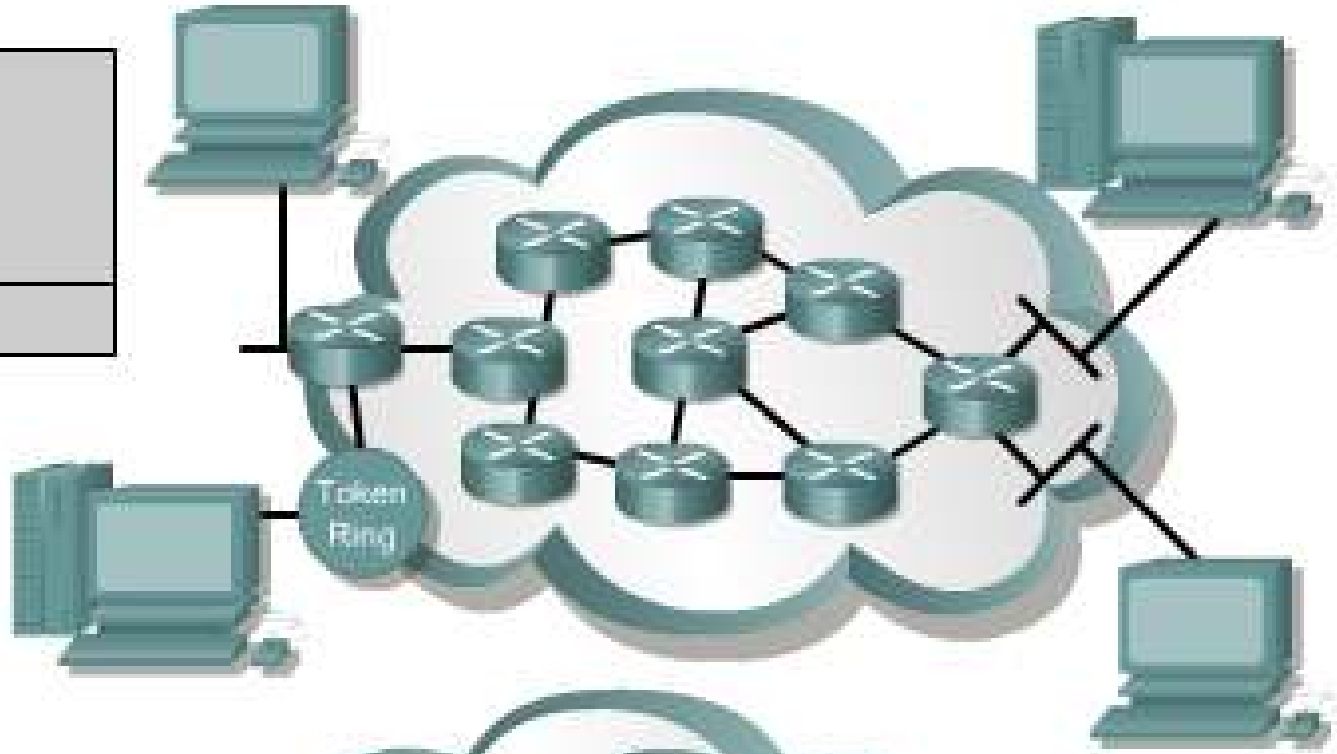


Chức năng router

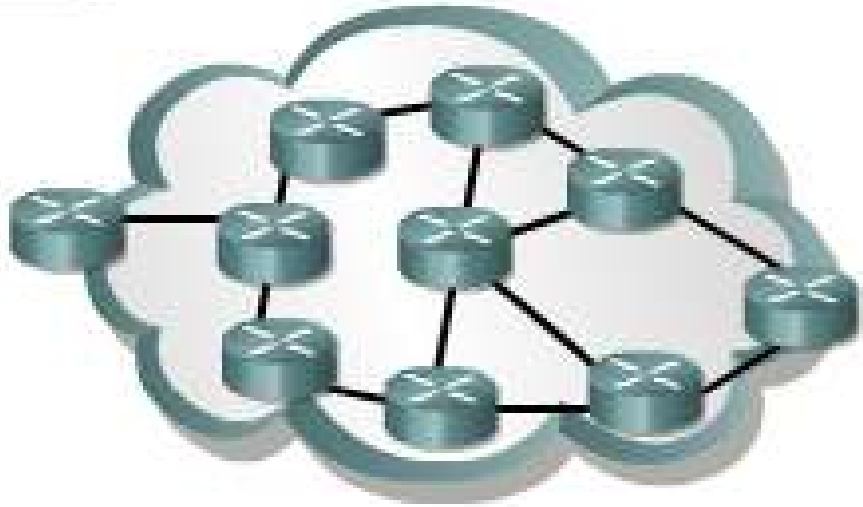
- Duy trì các bảng định tuyến (routing tables), được xây dựng theo các giao thức định tuyến (routing protocol)
- Khi nhận dữ liệu thì dùng bảng định tuyến để xác định ngõ ra

Giao thức được định tuyến (routed protocol)
Giao thức định tuyến (routing protocol)

Routed protocol used between routers to direct user traffic
Examples: IP and IPX



Routing protocol used between routers to maintain tables
Examples: RIP, IGRP, OSPF



Ví dụ: Node 1 cần gởi dữ liệu cho Node 2

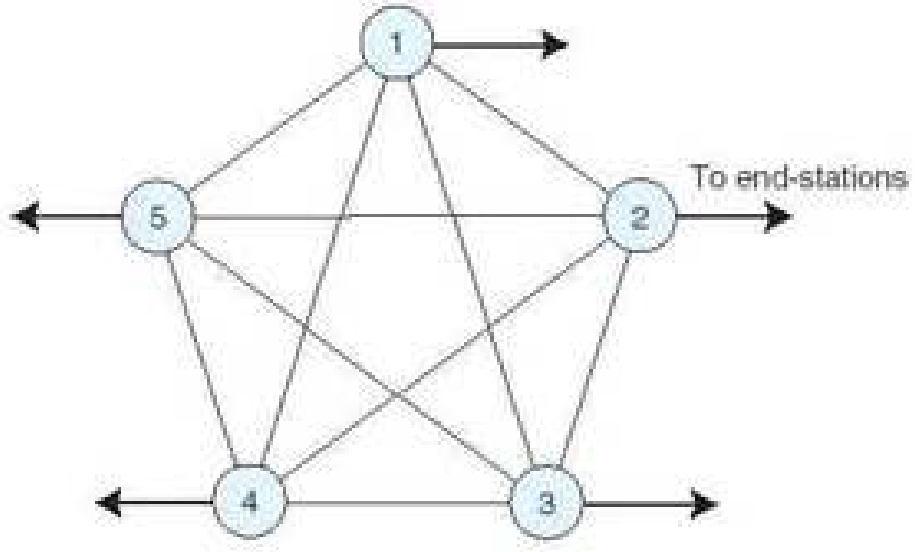
- 1 route với 1 hop

  1 → 2

- 3 routes với 2 hops

  1 → 3 → 2 1 → 4 → 2

  1 → 5 → 2



- 6 routes với 3 hops:

  1 → 3 → 4 → 2 1 → 3 → 5 → 2 1 → 5 → 4 → 2

  1 → 4 → 3 → 2 1 → 5 → 3 → 2 1 → 4 → 5 → 2

- 6 routes với hops:

  1 → 3 → 4 → 5 → 2 1 → 4 → 3 → 5 → 2

  1 → 5 → 4 → 3 → 2 1 → 3 → 5 → 4 → 2

  1 → 4 → 5 → 3 → 2 1 → 5 → 3 → 4 → 2

Các dạng định tuyến

- Định tuyến tĩnh
  - Tuyến do người quản trị mạng thiết lập
- Định tuyến động
  - Tuyến do các router thiết lập động theo các giao thức định tuyến

2. Định tuyến tĩnh

Gồm 3 giai đoạn:

- Người quản trị thiết lập các tuyến
- Tuyến được cài đặt trên router dưới dạng bảng định tuyến
- Các packet được định tuyến theo các tuyến cố định

Định tuyến tĩnh (tt)

- Khi mạng thay đổi, phải xác định lại các tuyến
- Chỉ dùng cho mạng cố định, quy mô nhỏ

- Ví dụ giải thuật định tuyến tĩnh:
  Giải thuật đường dẫn ngắn nhất
  (Shortest Path Routing)
  theo Dijkstra, Moore, …

3. Định tuyến động

- Tuyến được thiết lập tự động đáp ứng sự thay đổi của mạng
- Tuyến có dạng tối ưu
- Giao thức định tuyến là cố định, dữ liệu (bảng định tuyến) thay đổi thông qua việc trao đổi giữa các router

Giải thuật định tuyến

Gồm 2 dạng:

- Distance Vector Routing

  Định tuyến vector khoảng cách
- Link State Routing

  Định tuyến trạng thái liên kết

Định tuyến vector khoảng cách

- Còn gọi là giải thuật Bellman-Ford
- Nguyên tắc:
  - Mỗi router lưu bảng định tuyến cung cấp:
    - Khoảng cách tốt nhất đến đích
    - Đường để đến đích
  - Các router định kỳ trao đổi bảng định tuyến với các router láng giềng, cập nhật bảng định tuyến

Định tuyến vector khoảng cách (tt)

- Khoảng cách: số router trên tuyến

  → Hop count
- Ưu điểm
  - Đơn giản
- Khuyết điểm
  - Thời gian xây dựng bảng định tuyến lớn khi mạng quy mô lớn
  - Dữ liệu trao đổi trên mạng lớn
  - Các tuyến không còn sử dụng có thể tồn tại trên bảng định tuyến

Ví dụ định tuyến vector khoảng cách

- Dùng trên mạng ARPANET/Internet đến 1979 dưới tên RIP

  (Routing Information Protocol)
- Đặc điểm RIP
  - Dạng định tuyến vector khoảng cách
  - Khoảng cách: số hop
  - Packet bị hủy khi hop > 15
  - Định kỳ cập nhật bảng định tuyến: 30 giây

Định tuyến trạng thái liên kết

Công việc của router:

- Tìm các router láng giềng và học địa chỉ mạng của các router láng giềng
- Xác định thời gian trì hoãn, chi phí truyền dữ liệu đến từng láng giềng
- Xây dựng 1 gói cho biết các thông tin trên (link state packet)
- Truyền gói này đến các router khác
- Tính đường dẫn ngắn nhất đến mỗi router khác

Định tuyến trạng thái liên kết(tt)

- Đặc điểm so với định tuyến vector khoảng cách:
  - Đáp ứng nhanh với sự thay đổi của mạng
  - Duy trì cơ sở dữ liệu phức tạp về hình học của toàn mạng
  - Router cần nhiều bộ nhớ hơn, xử lý nhiều hơn
  - Cập nhật thông tin khi có biến cố trên mạng

    → sử dụng ít băng thông hơn

Ví dụ định tuyến trạng thái liên kết

Giao thức OSPF (Open Shortest Path First)

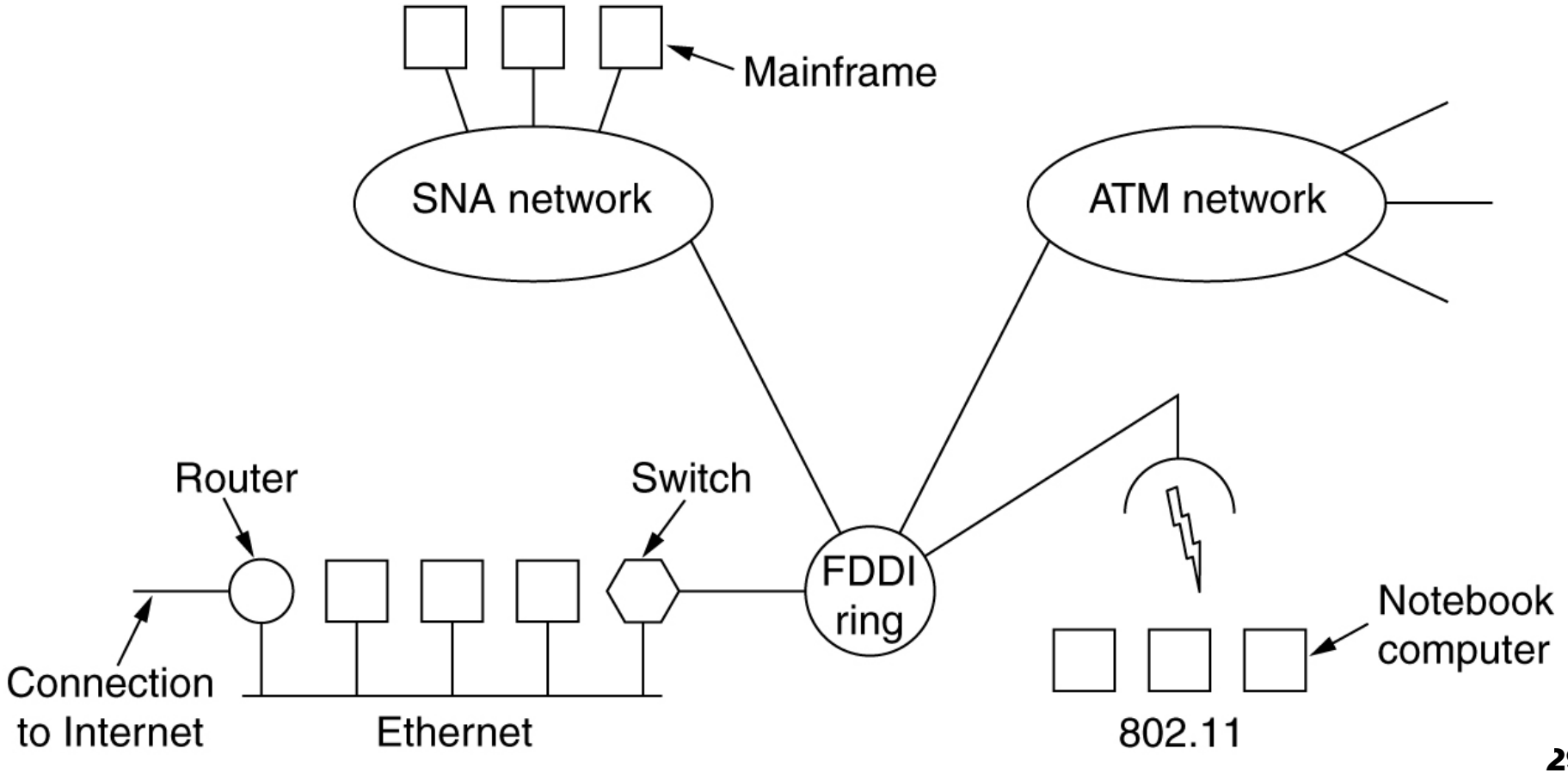
- Dạng định tuyến trạng thái liên kết
- Dùng giải thuật đường dẫn ngắn nhất để xác định các tuyến
- Khi mạng thay đổi thì thông tin trạng thái được gởi tràn ngập (flooding) đến các router láng giềng

III. Các vấn đề liên mạng

1. Khái niệm liên mạng
2. Một số thiết bị liên mạng
3. Khái niệm về tunneling
4. Khái niệm về firewall
5. Khái niệm về mạng riêng ảo

1. Khái niệm liên mạng

- Liên mạng (internetwork): sự kết nối của nhiều mạng



Sự khác nhau của các loại mạng

Thông số	Các khả năng
Dạng dịch vụ	Có kết nối, không kết nối
Các giao thức	IP, IPX, …
Định địa chỉ	Phẳng (IEEE 802), có thứ bậc (IP)
Kích thước gói	Mỗi mạng có max riêng
Kiểm soát lỗi	Truyền tin cậy, có/không có số thứ tự
*********	**********

2. Một số thiết bị liên mạng

- Repeater (bộ lập lại): hoạt động tại lớp physical
- Bridge (cầu nối): hoạt động tại lớp data link
- Switch (bộ chuyển mạch): hoạt động tại lớp data link
- Router (bộ định tuyến): hoạt động tại lớp network

Một số thiết bị liên mạng (tt)

- Gateway (cổng nối): tên gọi tổng quát thiết bị liên mạng
  - Hoạt động tại một lớp

    Router: gateway tại lớp network
  - Hoạt động trên nhiều lớp

3. Khái niệm về tunneling (tạo đường hầm)

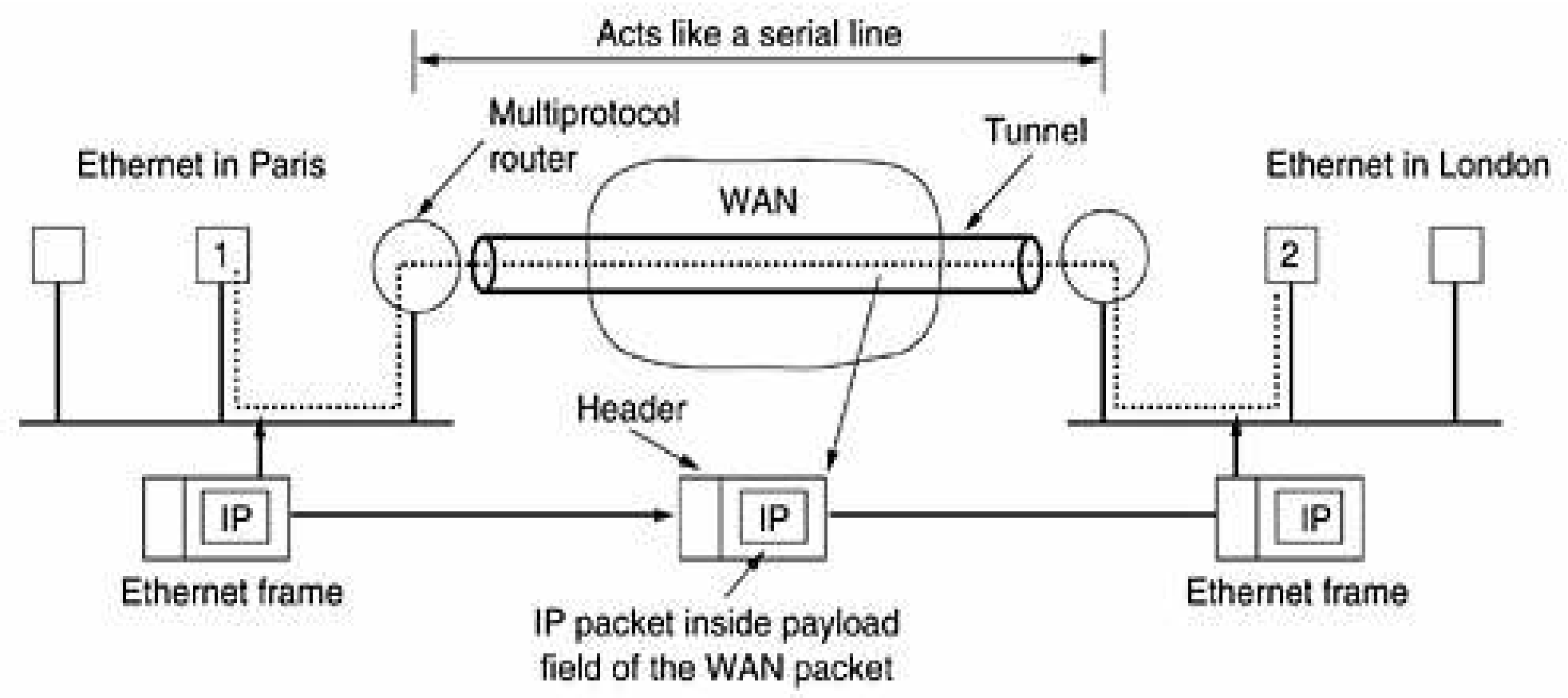
- Xử lý liên mạng tổng quát rất phức tạp
- Trường hợp đơn giản:

  Máy gởi và máy nhận trên hai mạng cùng loại được kết nối bởi một mạng khác loại

  ví dụ: dạng LAN-WAN-LAN

  → sử dụng kỹ thuật tạo đường hầm

Ví dụ tunnel

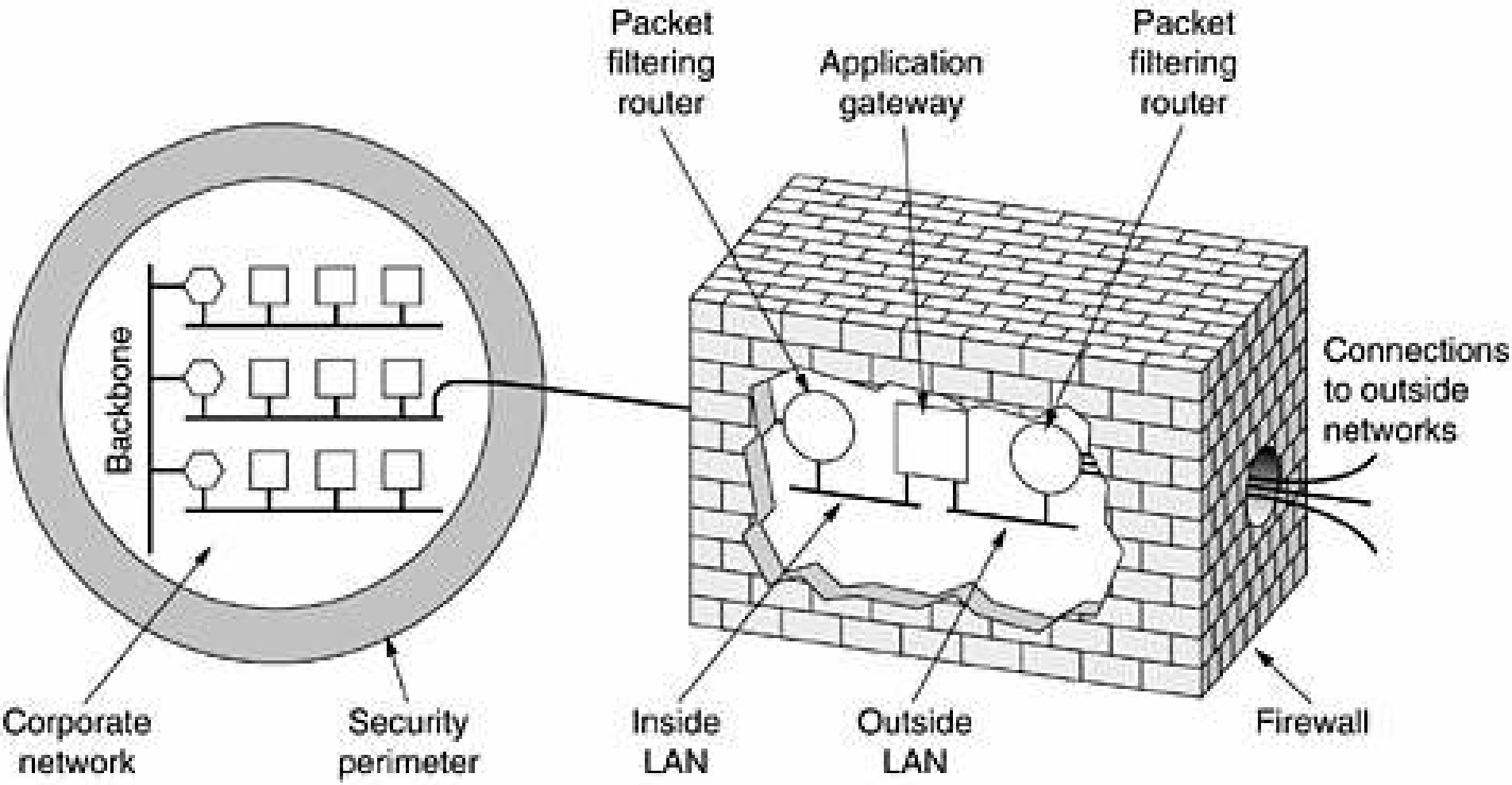


Hai router và mạng WAN đóng vai trò như đường hầm (tunnel) giữa hai mạng Ethernet

4. Khái niệm về firewall

- Là thiết bị liên mạng
- Mục đích: kiểm soát việc trao đổi dữ liệu
- Cấu tạo cơ bản:
  - Router lọc dữ liệu (packet filtering router)
    - Loại bỏ packet theo điều kiện xác định
  - Cổng nối ứng dụng (application gateway)
    - Hoạt động tại lớp ứng dụng, ví dụ Mail gateway
    - Kiểm tra nội dung dữ liệu

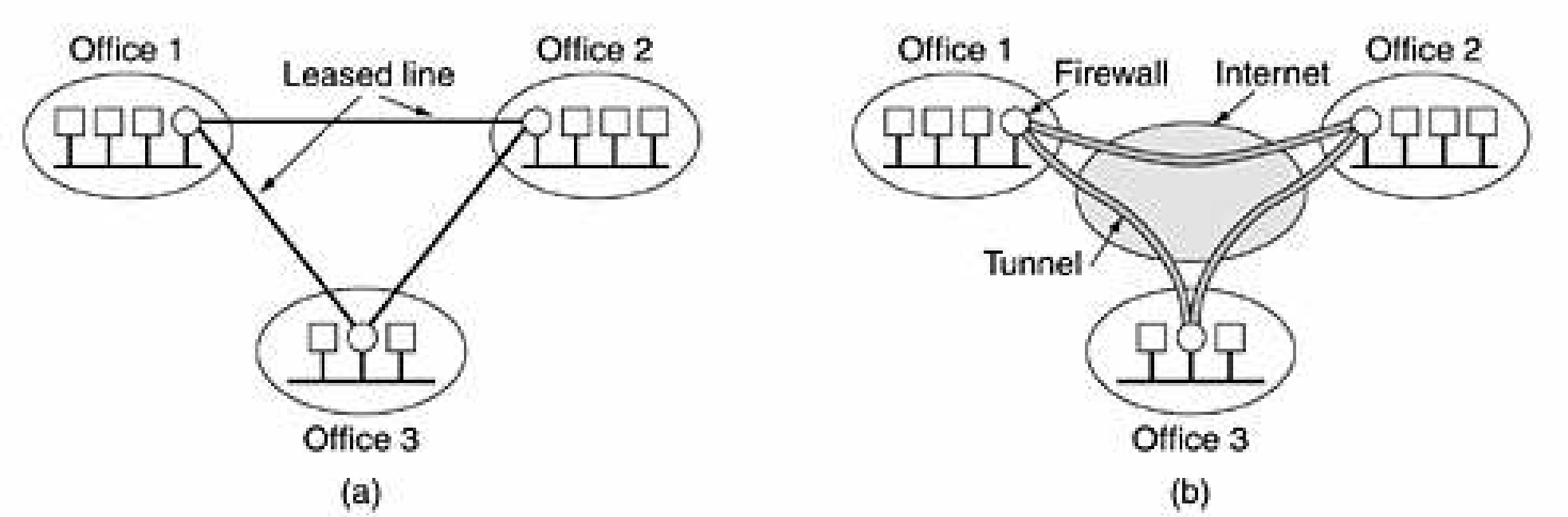
Cấu trúc firewall



5. Khái niệm VPN (mạng riêng ảo)

- Mạng riêng (Private Network): mạng dùng riêng của một tổ chức
- Mạng riêng ảo (VPN, Virtual Private Network) là mạng riêng thiết lập trên nền tảng mạng công cộng với kỹ thuật tunneling và firewall

Mạng riêng ảo



a. Mạng riêng (Private Network)

b. Mạng riêng ảo (VPN)

IV. Lớp network trên mạng TCP/IP

1. Giới thiệu
2. Giao thức IP
3. Địa chỉ IP
4. Các giao thức điều khiển
5. Định tuyến trên Internet

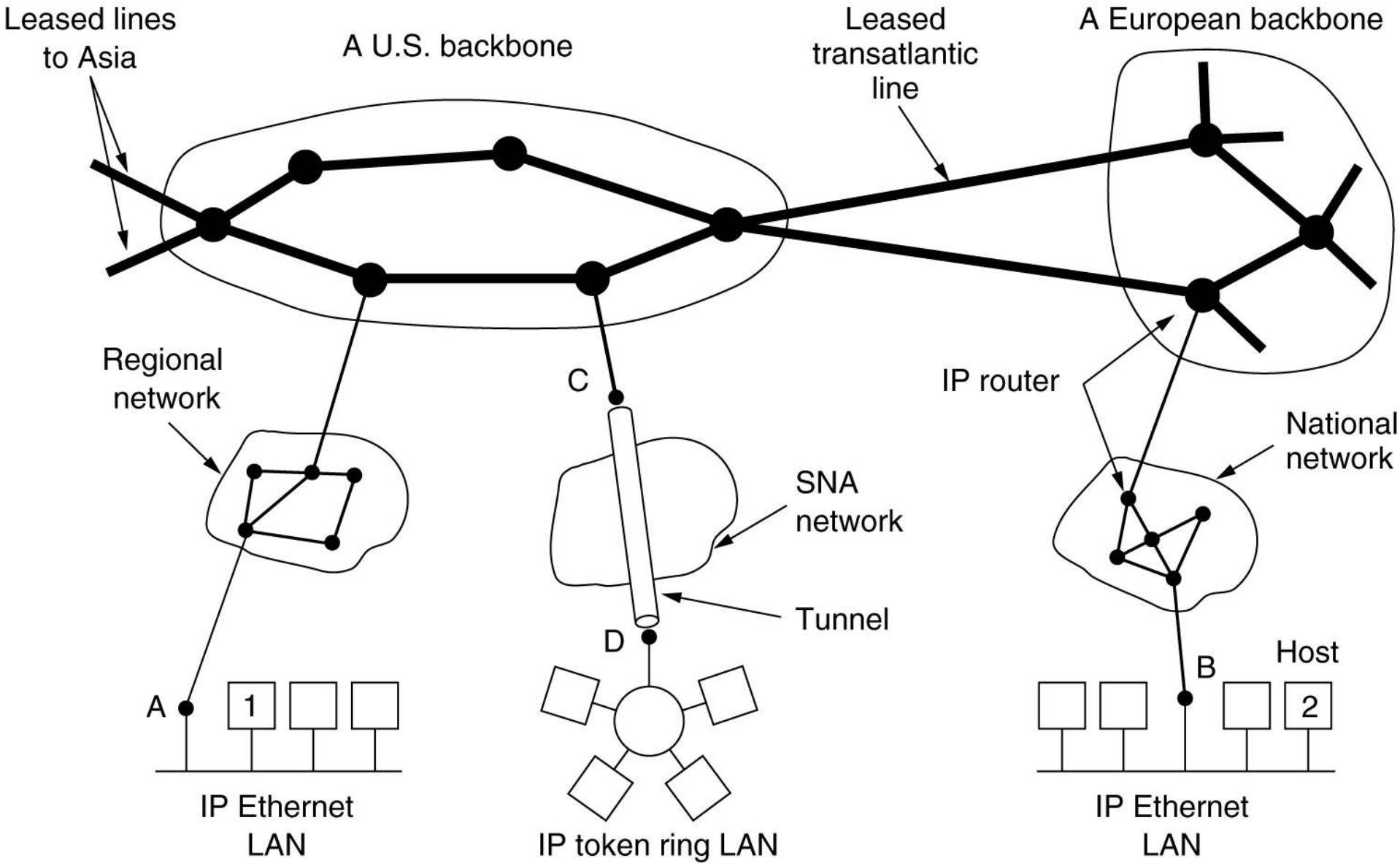
1. Giới thiệu

- Tại lớp network, mạng Internet là sự kết nối của các mạng độc lập
- Lớp network trên mạng TCP/IP gọi là lớp Internet
- Nhiệm vụ lớp Internet: chọn tuyến để truyền dữ liệu (packet) giữa hai máy bất kỳ

Các giao thức trên lớp Internet

- IP (Internet Protocol)
  - Truyền các gói dữ liệu dạng không kết nối
- ARP (Address Resolution Protocol)
  - Chuyển đổi địa chỉ IP thành địa chỉ lớp data link (địa chỉ MAC)
- ICMP (Internet Control Message Protocol)
  - Truyền các thông tin trạng thái, các thông điệp điều khiển
- ……

Mạng Internet: sự kết nối các mạng

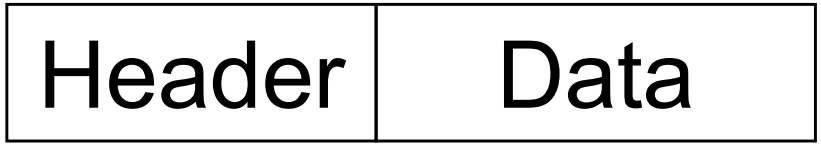


Hoạt động mạng Internet

- Lớp transport nhận dữ liệu từ lớp application, chia thành các gói dữ liệu, giao cho lớp network
- Lớp network truyền các gói dữ liệu đến máy nhận, các gói ban đầu có thể được chia thành các gói nhỏ hơn
- Khi tất cả các gói dữ liệu đến máy nhận, lớp network tạo lại các gói ban đầu, đưa cho lớp transport và đến lớp application

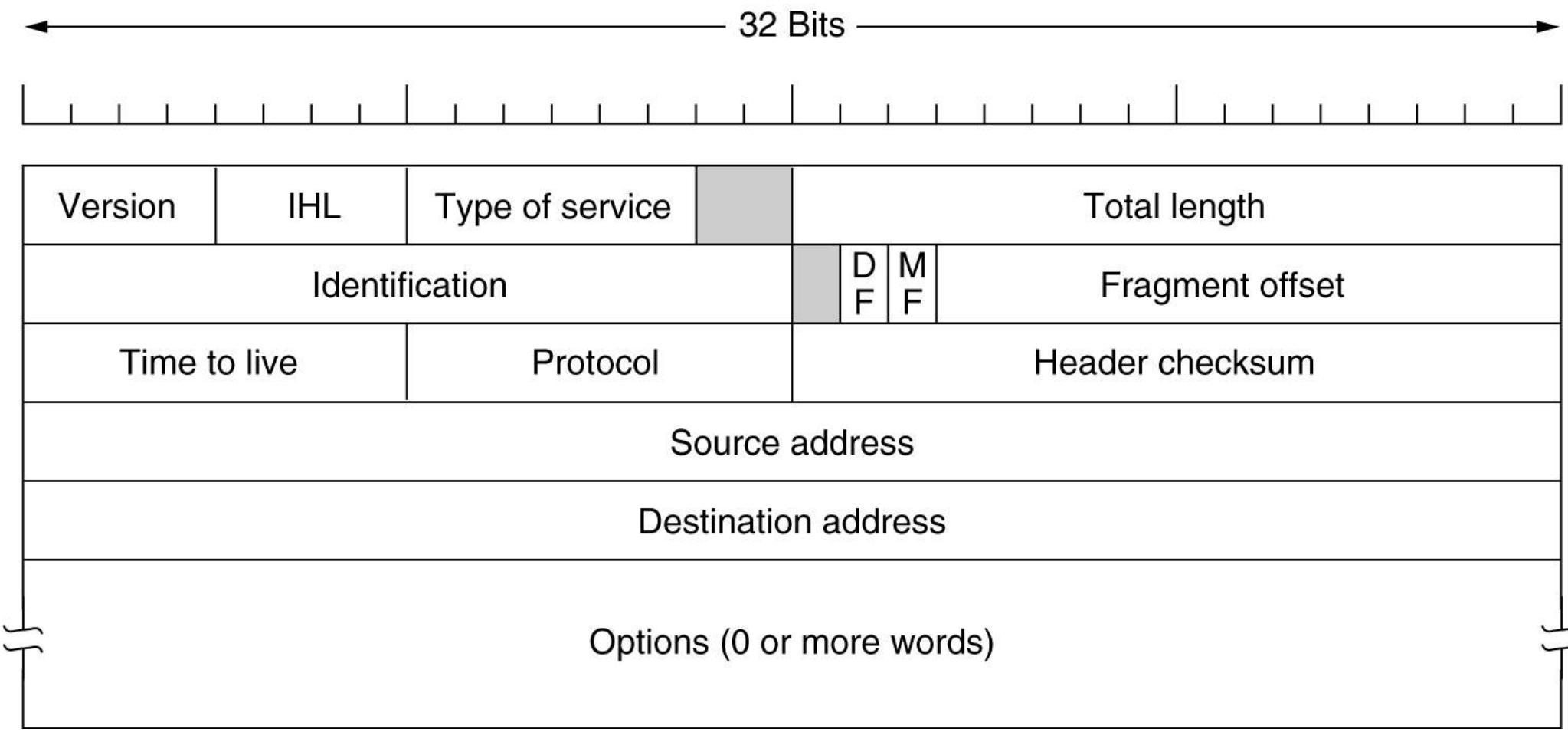
2. Giao thức IP

- Truyền dữ liệu dạng không kết nối
- Đơn vị dữ liệu: gói IP (IP packet)
  - IP Header ≥ 20 bytes
  - IP Data



- Khi chuyển sang mạng khác, gói IP có thể bị chia thành các gói nhỏ hơn

IP header


32 Bits
Version
IHL
Type of service
Total length
Identification
D F
M F
Fragment offset
Time to live
Protocol
Header checksum
Source address
Destination address
Options (0 or more words)

3. Địa chỉ IP

a. Khái niệm
b. Các lớp địa chỉ IP
c. Địa chỉ dành riêng, địa chỉ riêng
d. Subnet
e. CIDR (Classless InterDomain Routing)
f. Đặt địa chỉ IP
g. Dùng chung kết nối Internet

a. Khái niệm

- Mỗi máy, bộ định tuyến có một địa chỉ luận lý lớp network, địa chỉ IP

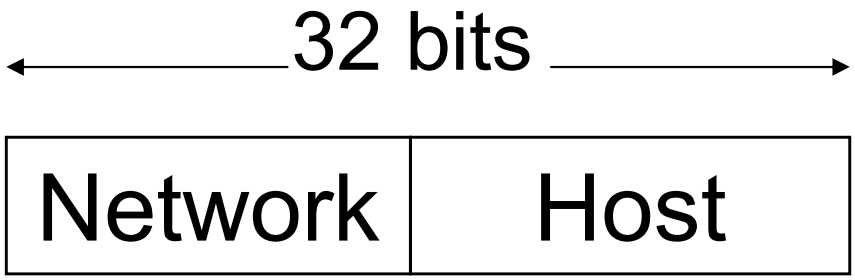
  (IP address)
- Hai máy không thể có cùng địa chỉ IP
- Một máy có thể có nhiều địa chỉ IP nếu kết nối vào nhiều mạng

Địa chỉ IP

- Giá trị nhị phân 32 bit, viết dưới dạng dotted-decimal
- Ví dụ:

  11000000.10101000.00000001.00001000

  192.168.1.8
- Gồm 2 phần
  - Network address
  - Host address



Địa chỉ IP (tt)

- Network addresses do ICANN cấp phát để tránh trùng địa chỉ

  (Internet Corporation for Assigned Names and Numbers)
- ICANN phân quyền cho các vùng, quốc gia, ví dụ VNNIC (VN Network Information Center), và ISPs

Các dạng địa chỉ IP

- Theo lớp (classful addressing)

  → các lớp địa chỉ IP

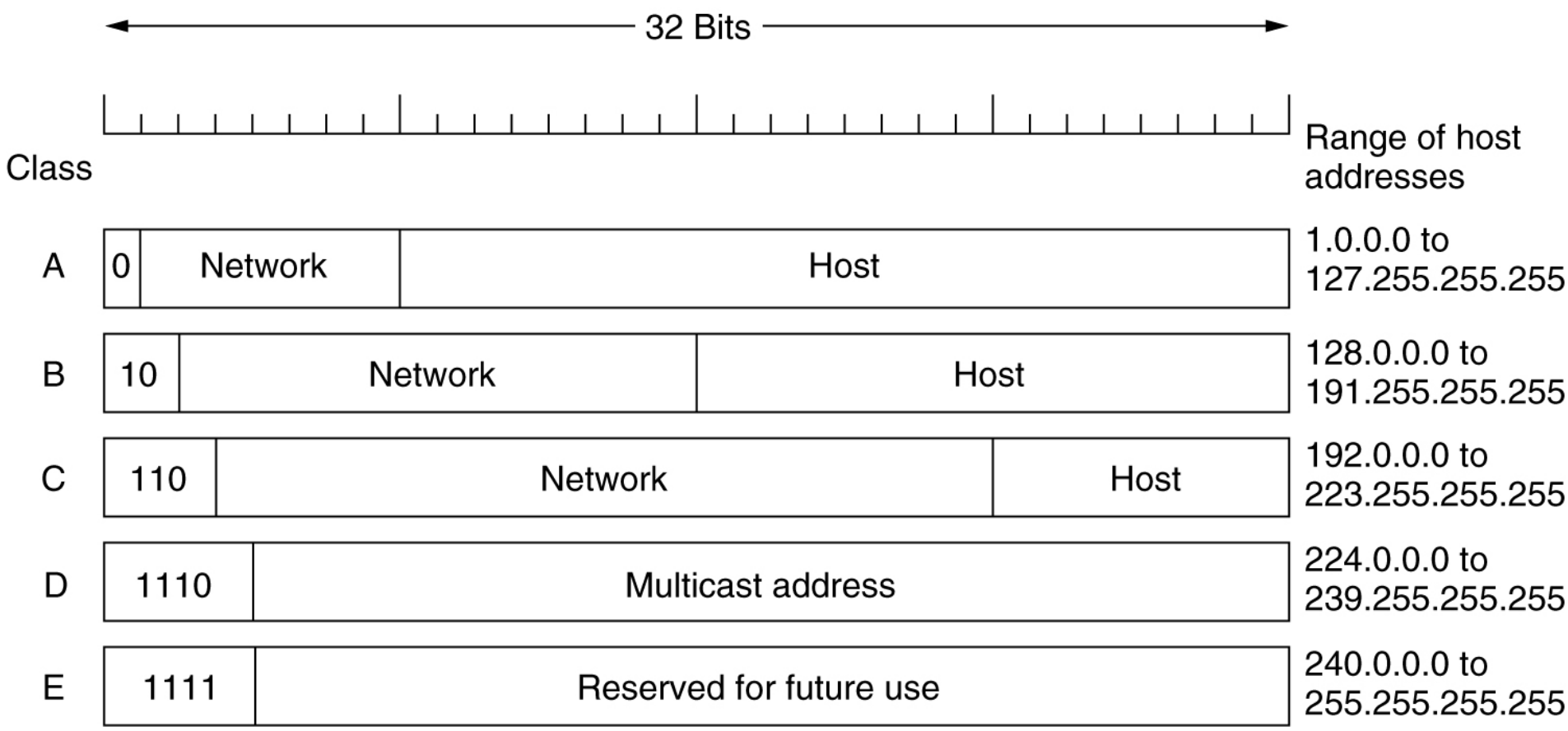
  → không còn sử dụng

- Không theo lớp (classless addressing)

  → dạng CIDR

  (Classless InterDomain Routing)

b. Các lớp địa chỉ IP



c. Địa chỉ dành riêng, địa chỉ riêng

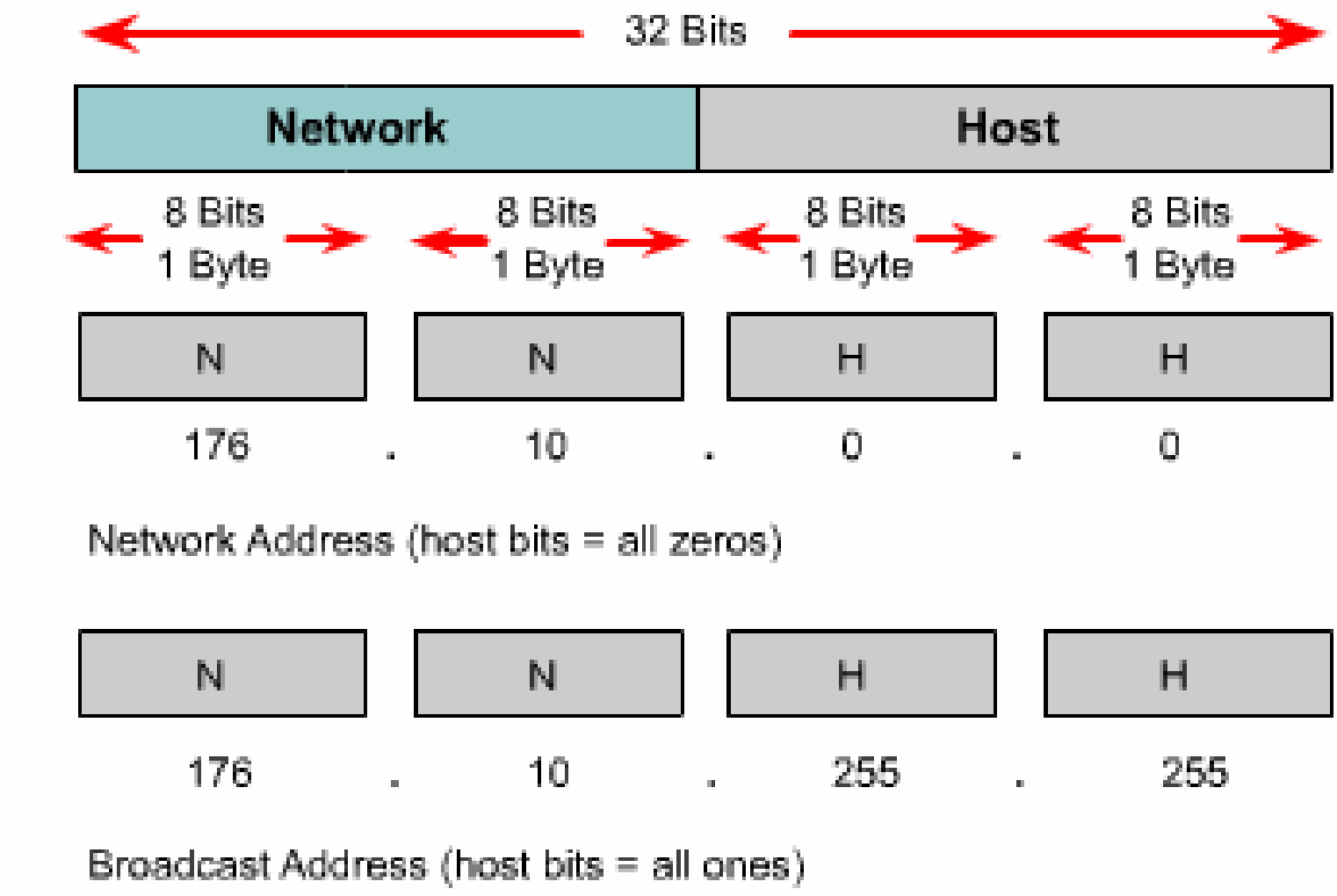
- Địa chỉ dành riêng (reserved addresses): không dùng làm địa chỉ máy
- Địa chỉ riêng (private addresses)

  dùng trên mạng riêng, không cấp phát trên Internet

Địa chỉ dành riêng

- Địa chỉ mạng – Network address
  - Dùng xác định mạng
  - Vùng host toàn bit 0
- Địa chỉ quảng bá – Broadcast address
  - Dùng để gởi packet đến tất cả các máy trên một mạng
  - Vùng host toàn bit 1
- Địa chỉ vòng – Loopback
  - Dùng để kiểm tra
  - 127.x.y.z, giá trị thông dụng 127.0.0.1

Ví dụ



Địa chỉ mạng, địa chỉ quảng bá của một mạng lớp B

Địa chỉ riêng

Lớp A: 10.0.0.0 → 10.255.255.255

Lớp B: 172.16.0.0 → 172.31.255.255

Lớp C: 192.168.0.0 → 192.168.255.255

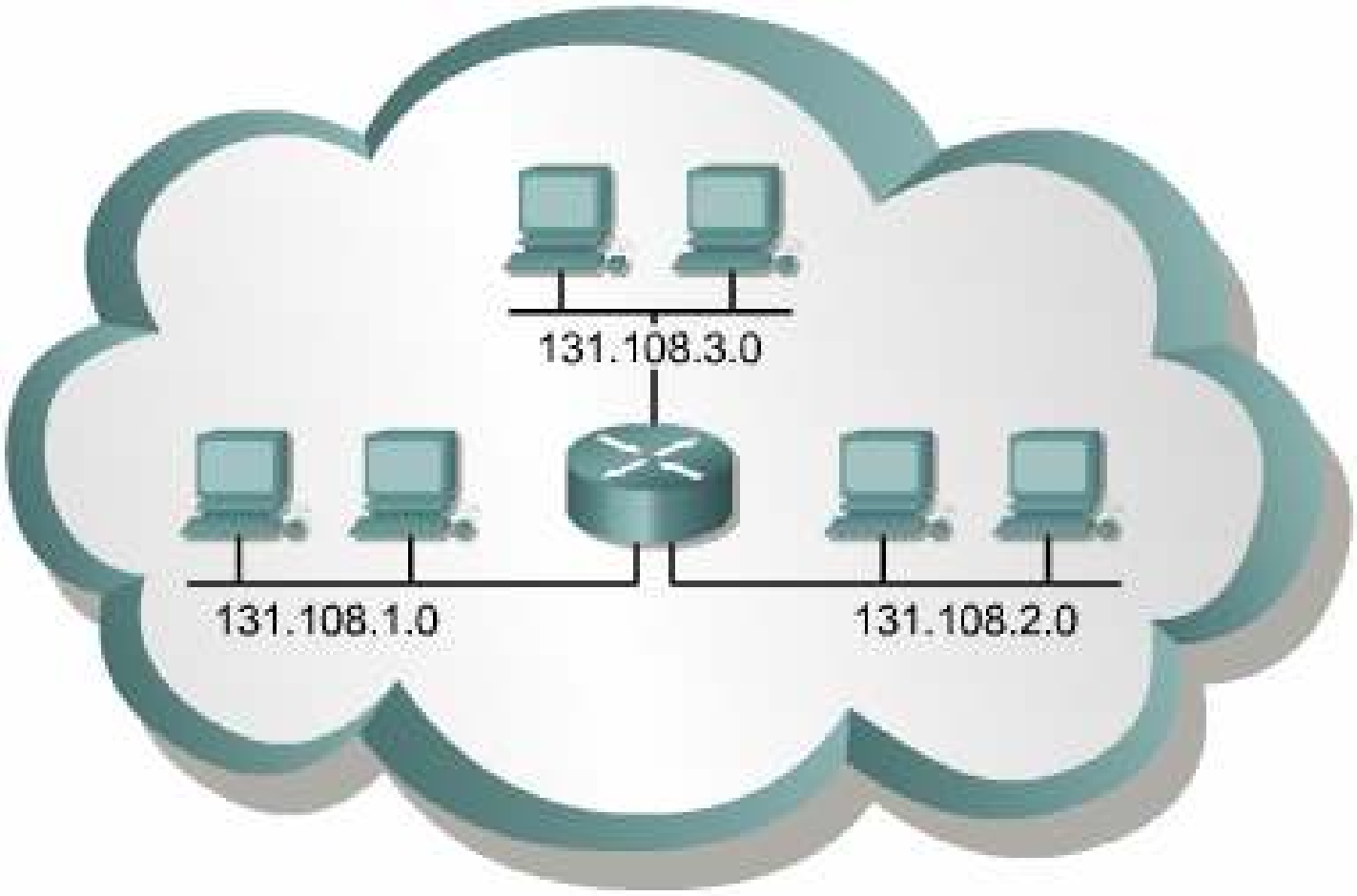
Dùng cho các máy:

- Trên mạng intranet
- Mạng dùng riêng

d. Subnet

- Địa chỉ mạng trong địa chỉ IP là mạng luận lý
- Các máy trên cùng một mạng phải có cùng phần địa chỉ mạng (network) trong địa chỉ IP
- Mạng luận lý không tương ứng với một mạng cục bộ
- Subnetting là kỹ thuật chia mạng nhiều máy thành các mạng nhỏ hơn (subnet)

Ví dụ

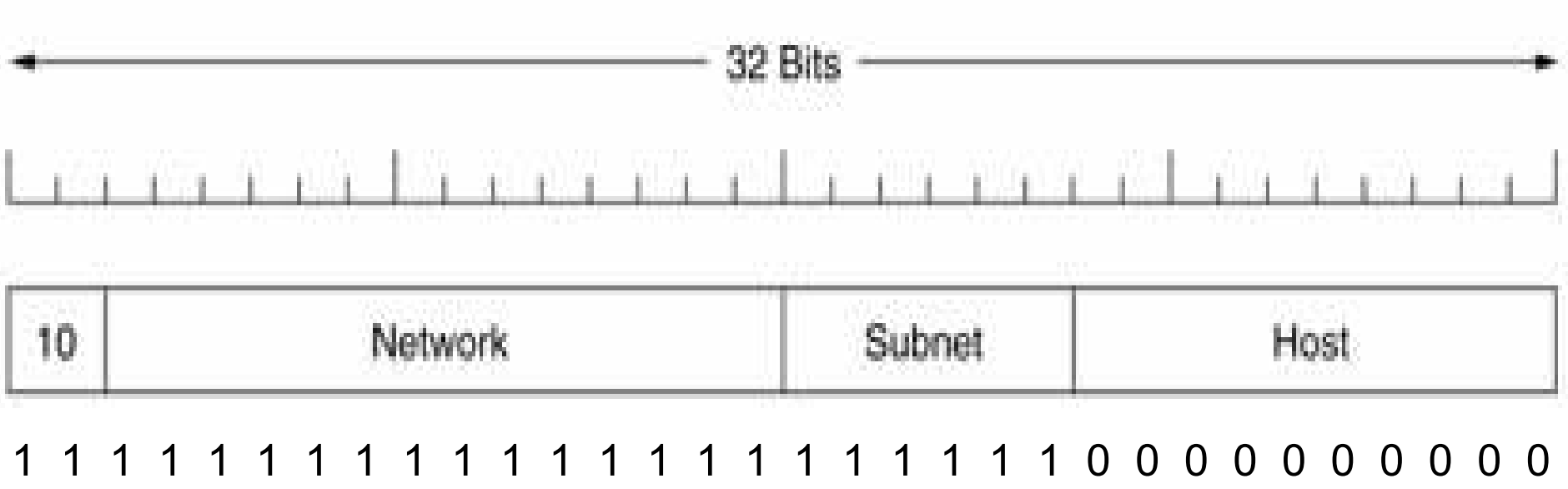


Các subnet 131.108.1.0, 131.109.2.0, 131.108.3.0 trong network 131.108.0.0

Subnet mask

- Trong địa chỉ IP cần có thêm vùng subnet được lấy từ vùng host
- Subnet mask là giá trị xác định số bit của vùng network + vùng subnet trong địa chỉ IP
- Hình thức subnet mask:
  - Dotted-decimal, ví dụ 255.255.252.0
  - Slash: /n, với n là số bit network+subnet
    ví dụ /22

Ví dụ



Một mạng lớp B được chia thành 64 mạng nhỏ

Subnet mask : 255.255.252.0 /22

Xác định giá trị subnet từ địa chỉ IP và subnet mask

- Dùng hàm AND
- Ví dụ:
  - Địa chỉ IP: 130.50.15.6

    10000010.00110010.00001111.00000110
  - Subnet mask: 255.255.252.0 /22

    11111111.11111111.11111100.00000000

  →Subnet: 130.50.12.0

    10000010.00110010.00001100.00000000

e. CIDR

Cấp phát các khối địa chỉ IP:

- có kích thước thay đổi
- không theo lớp địa chỉ
- tồn tại như một mạng trên Internet

Ví dụ

University	First address	Last address	How many	Written as
Cambridge	194.24.0.0	194.24.7.255	2048	194.24.0.0/21
Edinburgh	194.24.8.0	194.24.11.255	1024	194.24.8.0/22
(Available)	194.24.12.0	194.24.15.255	1024	194.24.12/22
Oxford	194.24.16.0	194.24.31.255	4096	194.24.16.0/20

C: 11000010.00011000.00000000.00000000

mask 11111111.11111111.11111000.00000000

E: 11000010.00011000.00001000.00000000

mask 11111111.11111111.11111100.00000000

O: 11000010.00011000.00010000.00000000

mask 11111111.11111111.11110000.00000000

Ví dụ (tt)

- Xét địa chỉ 194.24.17.4

  11000010.00011000.00010001.00000100
- Thực hiện AND với các mask của 3 mạng trên

  → 194.24.17.4 thuộc mạng Oxford

Tác dụng của CIDR

- Sử dụng hiệu quả không gian địa chỉ IP
- Giảm số lượng mạng
  - Nhiều mạng lớp C tồn tại như một mạng
  - Có thể kết hợp nhiều mạng thành một mạng

  Ví dụ: 3 mạng trong ví dụ trên có thể được kết hợp thành một mạng 194.24.0.0/19

f. Đặt địa chỉ IP

- Địa chỉ tĩnh
  - Do administrator đặt
- Địa chỉ động
  - Do DHCP server cấp phát

- Các thành phần
  - IP address
  - Subnet mask
  - Default gateway address, ……

Kiểm tra địa chỉ IP

Các công cụ:

- ipconfig, winipcfg (windows 9x)

  cung cấp các thông tin ip address, subnet mask, default gateway, …

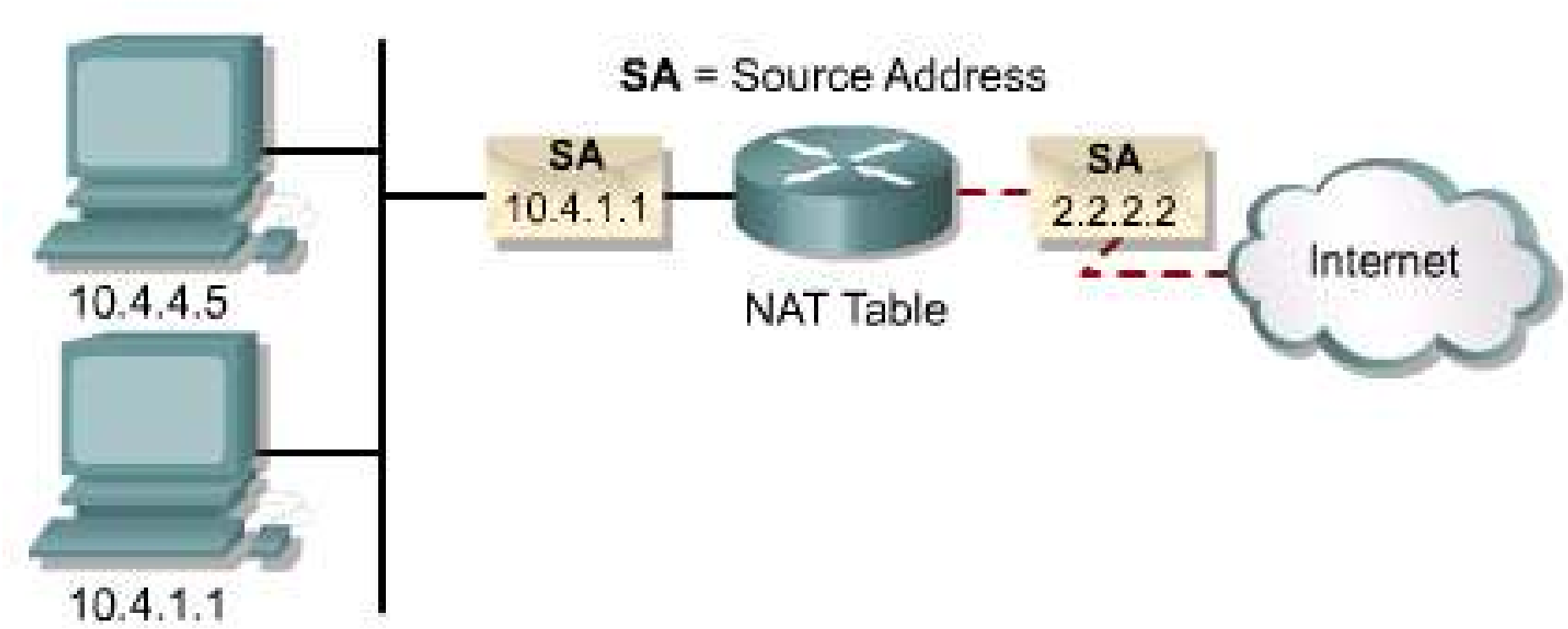
- ping

  kiểm tra kết nối theo IP

g. Dùng chung kết nối Internet (Internet Connection Sharing)

- Các máy trên một LAN, sử dụng địa chỉ IP riêng
- Có một kết nối Internet, sử dụng địa chỉ IP toàn cục
- Cần khối chuyển đổi địa chỉ NAT (Network Address Translation), có thể là:
  - Thiết bị
  - Phần mềm

Ví dụ



Địa chỉ địa phương: 10.4.4.5, 10.4.1.1

Địa chỉ toàn cục: 2.2.2.2

Hoạt động của khối NAT

- Khi một máy X gởi dữ liệu ra ngoài mạng thì gởi đến khối NAT
- Khối NAT thay thế địa chỉ máy gởi trên gói IP bằng địa chỉ toàn cục
- Khi có đáp ứng từ bên ngoài, khối NAT:
  - Nhận dữ liệu
  - Kiểm tra bảng chuyển đổi địa chỉ
  - Thay thế địa chỉ máy nhận trên gói IP bằng địa chỉ máy X

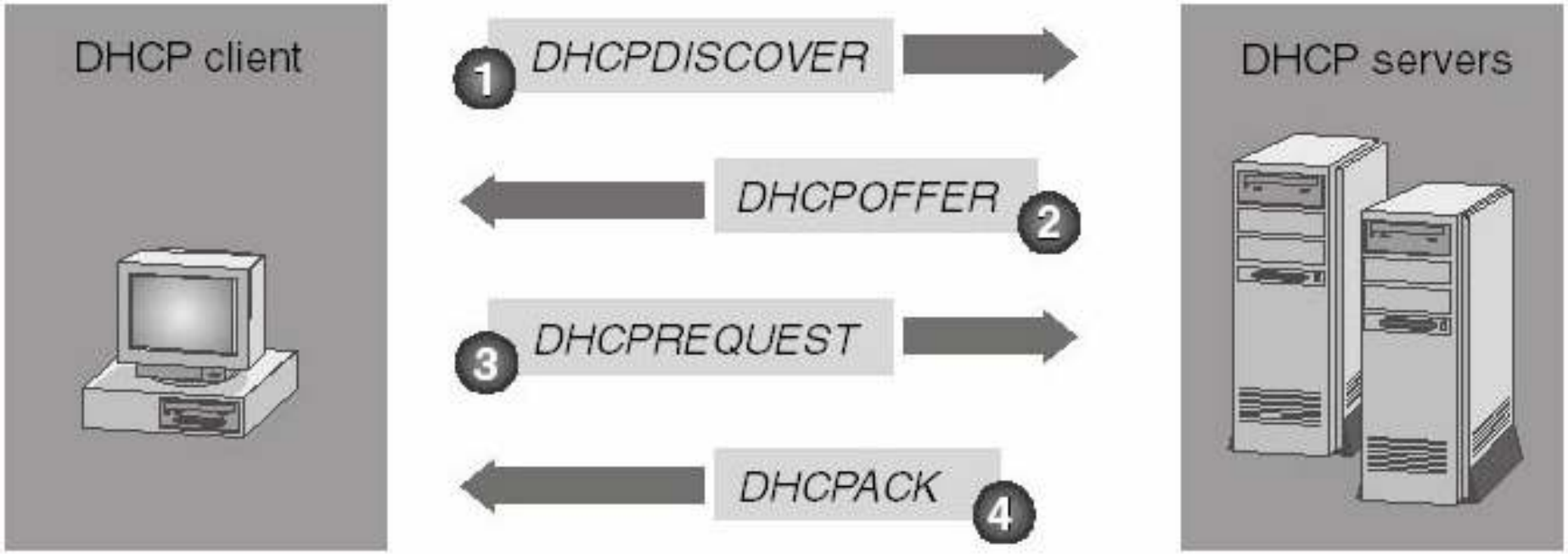
4. Các giao thức điều khiển

a. DHCP
   (Dynamic Host Configuration Protocol)
b. ARP
   (Address Resolution Protocol)
c. ICMP
   (Internet Control Message Protocol)

a. DHCP

- DHCP server cấp các thông số địa chỉ IP cho DHCP Client:
  - IP address
  - Subnet mask
  - Options: gateway address, DNS Server, …
- Mục đích:
  - Đơn giản công việc quản trị mạng
  - Sử dụng hiệu quả địa chỉ IP

Các giai đoạn cấp địa chỉ IP động



DHCPDISCOVER: client tìm server

DHCPOFFER: server cung cấp thông số IP

DHCPREQUEST: client thông báo đã nhận

DHCPACK: server chấp nhận

b. ARP

- Chuyển đổi địa chỉ IP thành địa chỉ MAC để truyền thông bên trong một mạng
- Cần khối thực hiện giao thức ARP
- Khối ARP xây dựng và duy trì một bảng chứa các phần tử (IP address – MAC address)

c. ICMP

- Giao thức IP dùng để gởi dữ liệu
- Giao thức ICMP dùng để gởi các thông báo lỗi và các thông tin điều khiển
- Ví dụ:
  - Thông báo không đến được máy nhận
  - Kiểm tra một máy có tồn tại
- Thông điệp ICMP được gởi trên gói IP

Một số dạng thông điệp ICMP

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

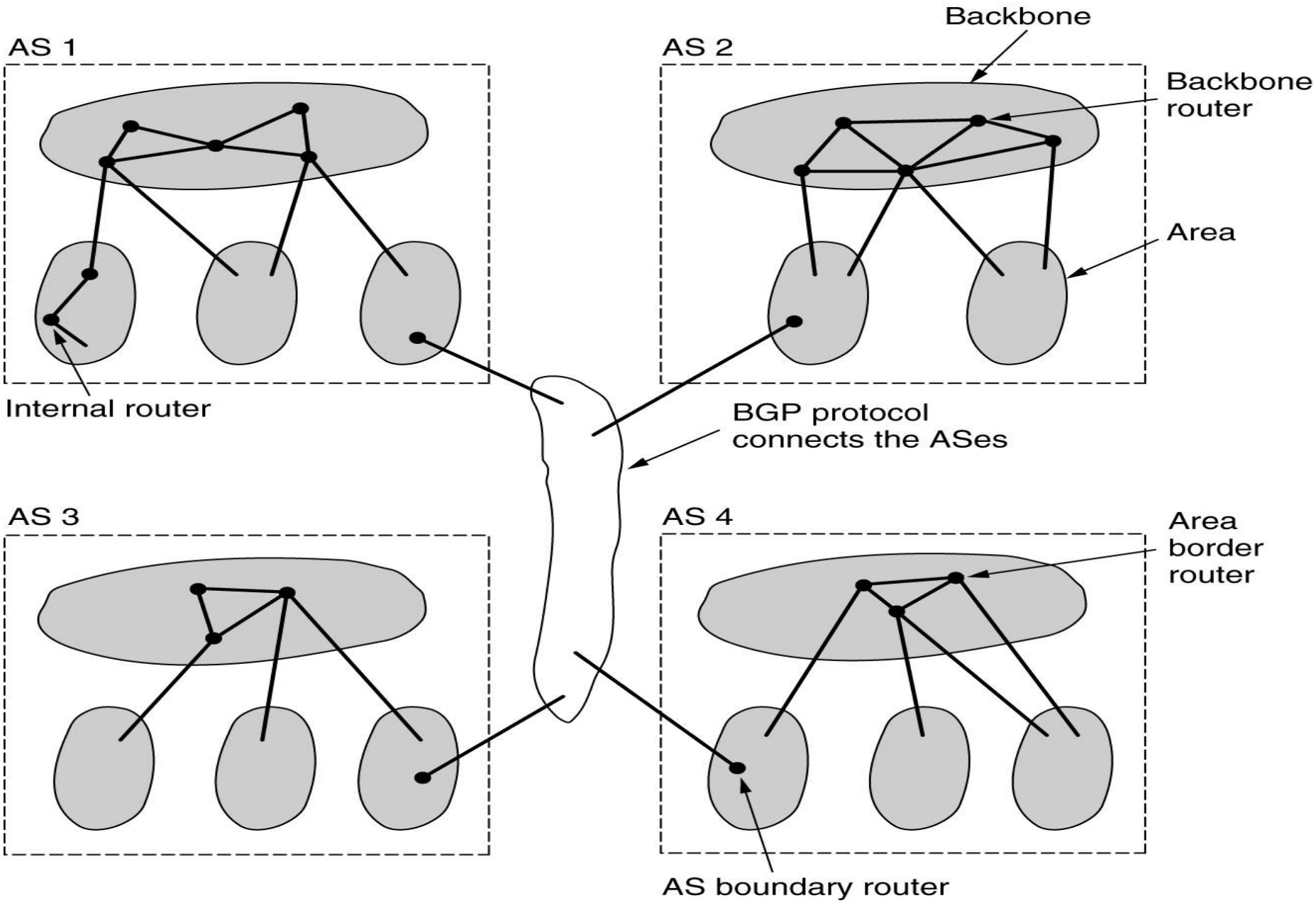
5. Định tuyến trên Internet

- Tại lớp Network, mạng Internet là tập hợp các mạng độc lập (Autonomous System)
- Có 2 dạng giao thức định tuyến:
  - Interior Gateway Protocol

    thực hiện bên trong AS, ví dụ OSPF (Open Shortest Path First)
  - Exterior Gateway Protocol

    thực hiện giữa các AS, ví dụ BGP (Border Gateway Protocol)

Ví dụ


AS 1
AS 2
Backbone
Backbone router
Area
Internal router
BGP protocol connects the ASes
AS 3
AS 4
Area border router
AS boundary router

V. Giới thiệu IPv6

- Dùng 128 bit địa chỉ, viết dưới dạng colon-hexadecimal
- Các đặc điểm chính, so với IPv4:
  - Không gian địa chỉ lớn (~ $3.4*10^{38}$)
  - Phần header đơn giản hơn
  - Hỗ trợ tốt hơn các tùy chọn (options)
  - Bảo mật
  - Chất lượng dịch vụ tốt hơn

NHẬP MÔN MẠNG MÁY TÍNH

Chương 5

LỚP TRANSPORT

(LỚP GIAO VẬN)

Nội dung chương 5

I. Các vấn đề thiết kế lớp transport

II. Lớp transport trên mạng TCP/IP

III. Giới thiệu giao diện lập trình mạng socket

I. Các vấn đề thiết kế lớp transport

1. Nhiệm vụ lớp transport
2. Dịch vụ lớp transport

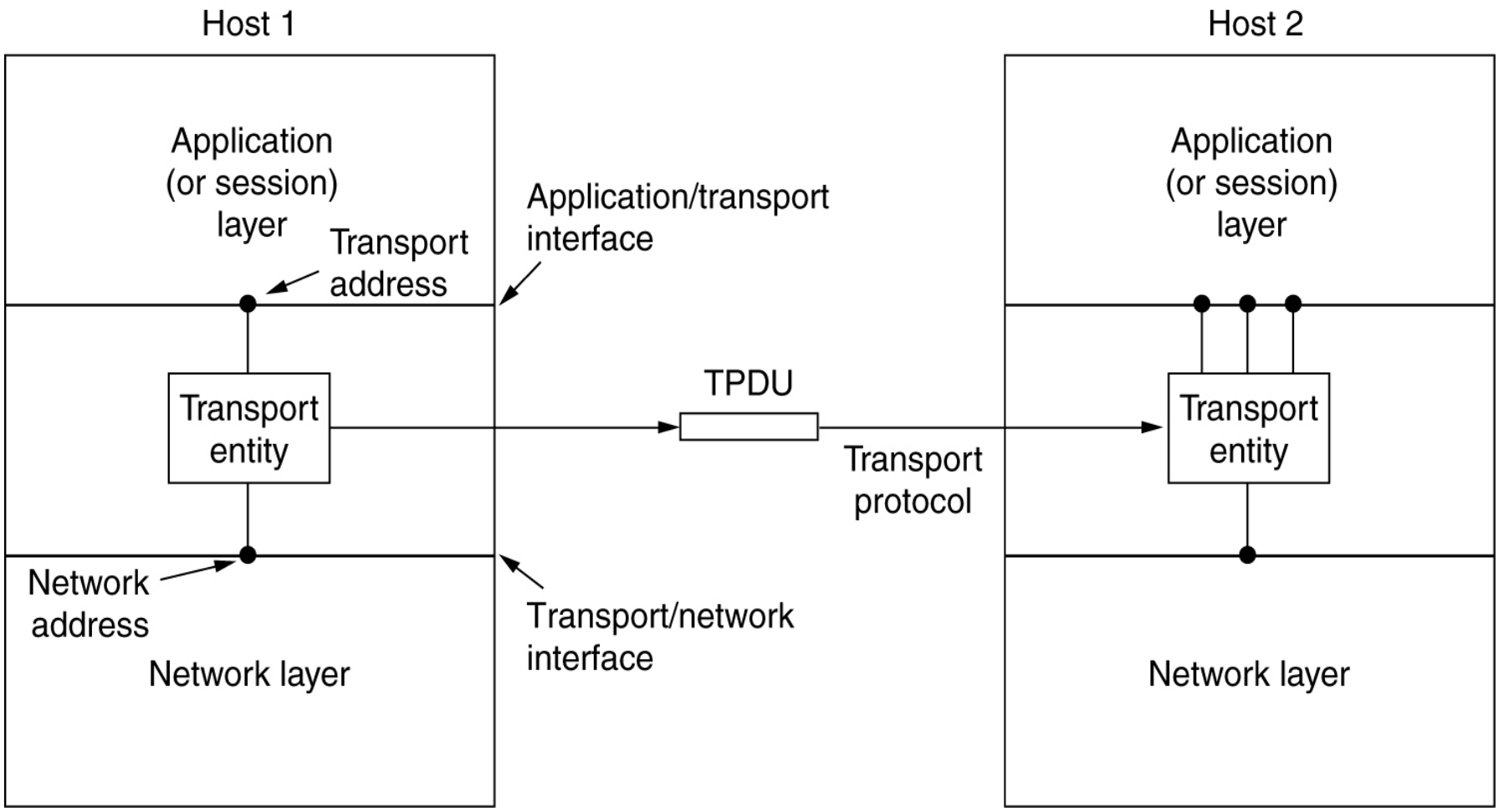
1. Nhiệm vụ lớp transport

- Cung cấp dịch vụ gởi nhận dữ liệu tin cậy giữa các chương trình trên hai máy bất kỳ
- Thực hiện:
  - Chia và ghép dữ liệu từ lớp application
  - Kiểm soát lỗi, kiểm soát lưu lượng
- Lớp transport có vai trò quan trọng trên kiến trúc mạng nhiều lớp

2. Dịch vụ lớp transport

a. Dịch vụ lớp transport
b. Các thao tác cơ sở

a. Dịch vụ lớp transport



Quan hệ giữa các lớp

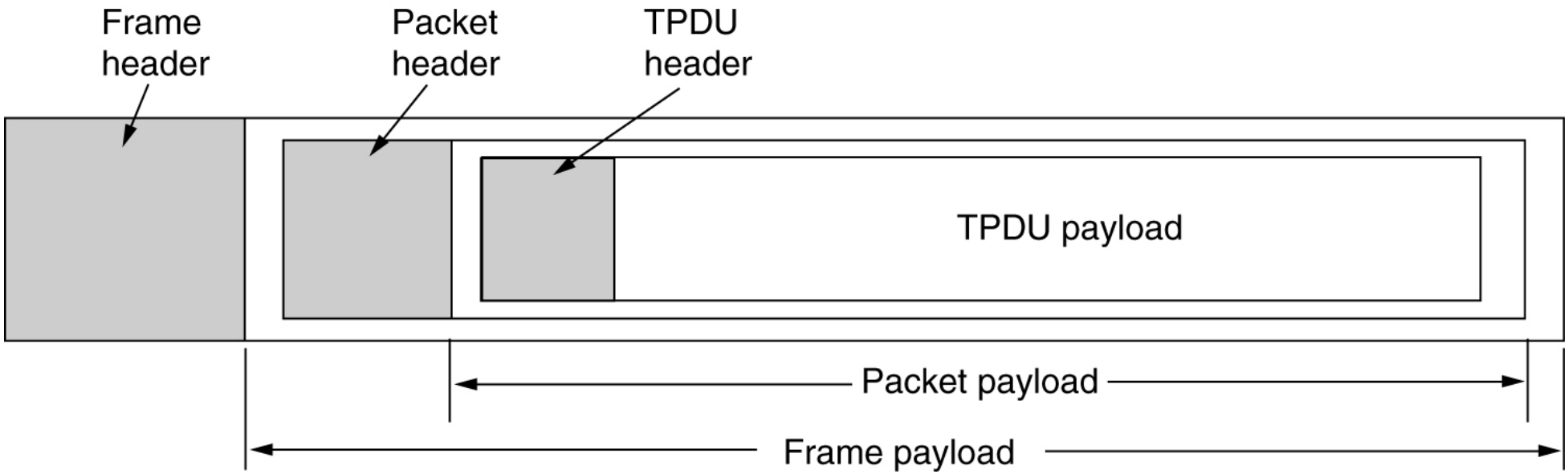
Các thuật ngữ

- Transport entity: thực thể lớp transport
- TPDU (Transport Protocol Data Unit): đơn vị dữ liệu giao thức lớp transport
- Transport address: địa chỉ lớp transport
  - Transport Service Access Point
  - Port (mạng TCP/IP)
- Network address: địa chỉ lớp network
  - Địa chỉ IP (mạng TCP/IP)

Các dạng dịch vụ

- Có kết nối (connection-oriented service)
- Không kết nối (connectionless service)

Đơn vị dữ liệu giao thức lớp transport



TPDU trong packet và frame

b. Các thao tác cơ sở

(Transport service primitives)

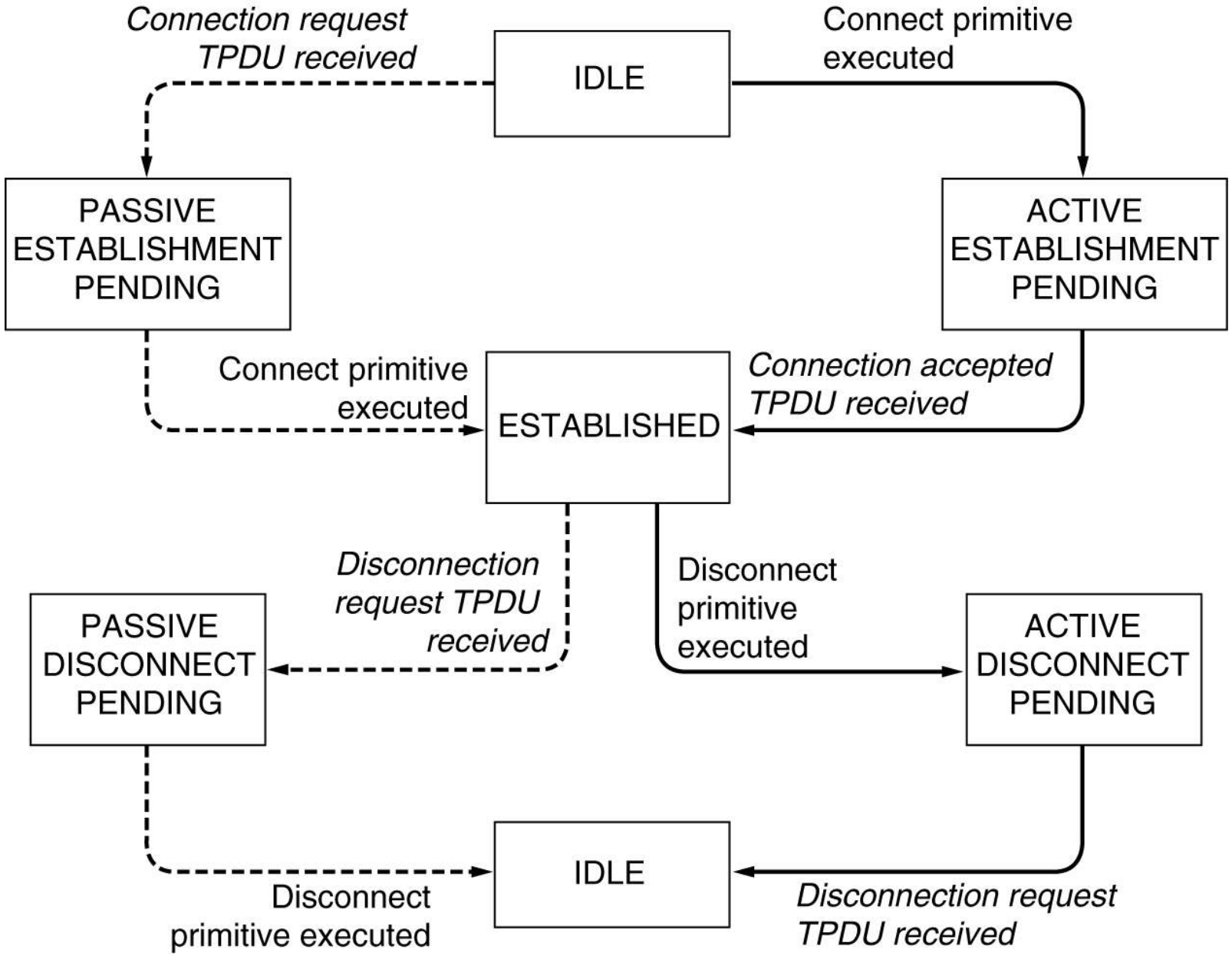
- Các thao tác cơ sở của dịch vụ đơn giản
- Ví dụ:

  Mô hình client-server dạng có kết nối

Các thao tác cơ sở của dịch vụ đơn giản

Primitive	Dữ liệu gởi	Ý nghĩa
LISTEN	Không có	Chờ process khác kết nối
CONNECT	CONNECTION REQUEST	Thiết lập kết nối
SEND	DATA	Gởi dữ liệu
RECEIVE	Không có	Chờ nhận dữ liệu
DISCONNECT	**DISCONNECTION REQUEST**	Yêu cầu hủy kết nối

Mô hình Client-Server dạng có kết nối



II. Lớp transport trên mạng TCP/IP

1. Giao thức TCP
   (Transmission Control Protocol)
2. Giao thức UDP
   (User Datagram Protocol)

1. Giao thức TCP

a. Giới thiệu TCP
b. Mô hình dịch vụ TCP
c. Giao thức TCP
d. TCP segment header
e. Thiết lập kết nối TCP

a. Giới thiệu TCP

- Cung cấp dịch vụ gởi nhận chuỗi byte tin cậy giữa hai chương trình trên mạng có thể không tin cậy
- Thực thể TCP:
  - Thư viện
  - User process
  - Kernel
- Chia dữ liệu từ process ứng dụng, gởi trên các gói IP

b. Mô hình dịch vụ TCP

- Dịch vụ TCP thực hiện trên kết nối TCP (TCP connection)
- Kết nối TCP bao gồm hai đầu cuối (end-point), được gọi là socket
- Socket number (socket address):
  - Địa chỉ IP – 32 bit
  - Port – 16 bit

Port

- Khái niệm trừu tượng → nhiều ứng dụng TCP trên một máy
- Well-known ports: dùng cho các dịch vụ chuẩn, ví dụ:

Port 21: FTP - File Tranfer Protocol

25: SMTP - Email

80: HTTP - Web

Kết nối TCP

- Full-duplex
- Point-to-point
- Byte stream

c. Giao thức TCP

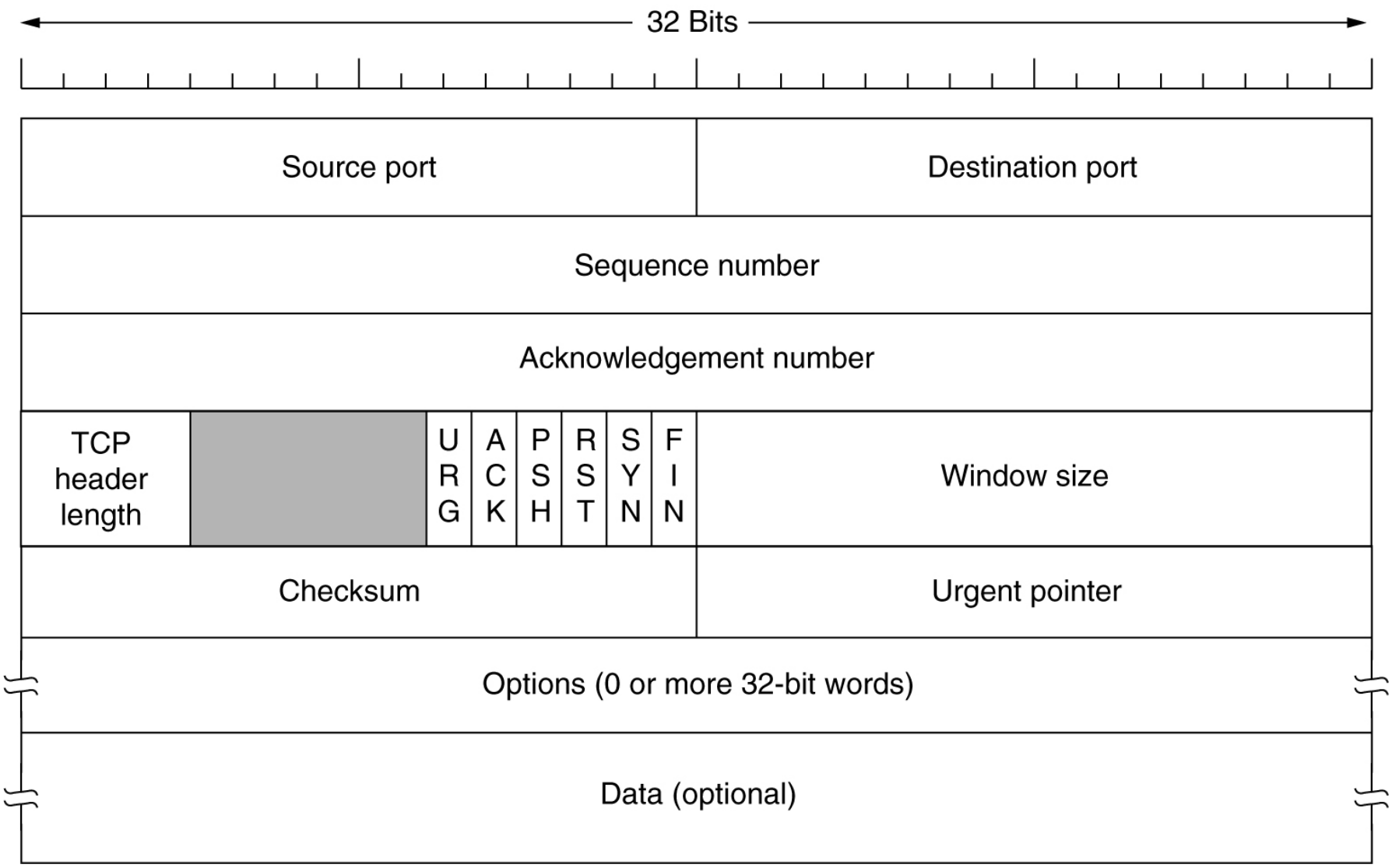
- Đơn vị dữ liệu: TCP segment
  - TCP header ≥ 20 bytes
  - TCP data ≥ 0 bytes
- Kích thước TCP segment bị giới hạn bởi:
  - IP payload (65515 bytes)
  - MTU (Maximum Transfer Unit)

    Ví dụ: MTU mạng Ethernet ~ 1500 bytes

Giao thức TCP (tt)

- Mỗi byte truyền trên kết nối TCP có số thứ tự trình tự (sequence number) 32 bit
- Giao thức cơ bản: sliding window
  - Sender gởi segment, khởi động timer
  - Receiver gởi segment có kèm ACK number là số thứ tự byte chờ nhận tiếp theo
  - Sender sẽ gởi lại nếu không có ACK khi hết thời gian

d. TCP segment header



e. Thiết lập kết nối TCP

Thiết lập kết nối giữa

Host 1 (Client) và Host 2 (Server)

(Three-way handshake)

- Host 1 → Host 2:

  seq=x, ack=0, SYN=1, ACK=0

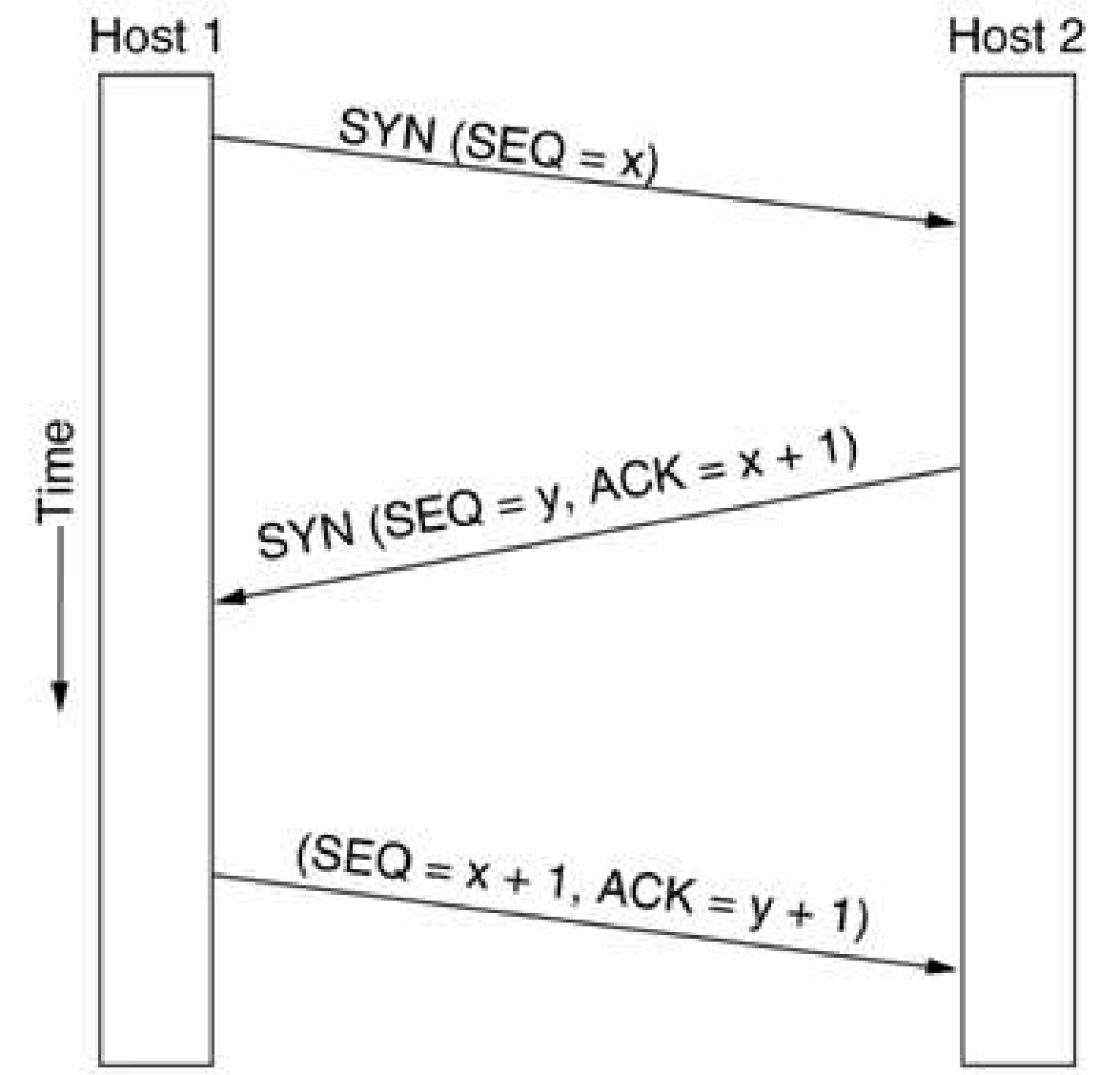
- Host 2 → Host 1:

  seq=y, ack=x+1, SYN=1, ACK=1

- Host 1 → Host 2:

  seq=x+1, ack=y+1, SYN=0, ACK=1

Sơ đồ thiết lập kết nối TCP



Hủy bỏ kết nối TCP

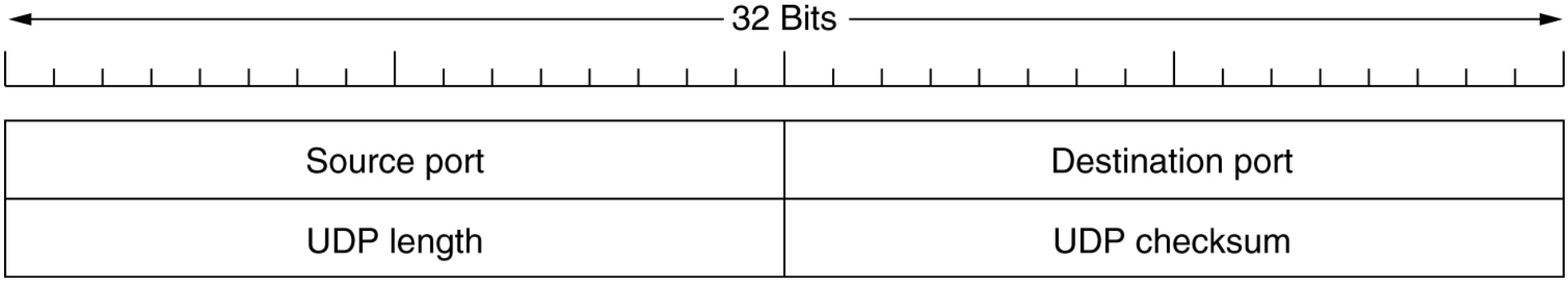
- Gởi TCP segment với FIN=1
- Cần một FIN segment và một ACK segment cho một bên truyền thông

2. Giao thức UDP

- Giao thức dạng không kết nối
- Không có kiểm soát lỗi

  → nếu cần thì thực hiện trên lớp application
- Đơn vị dữ liệu: UDP datagram/segment
  - UDP header: 8 bytes
  - UDP data
- Sử dụng khái niệm port tương tự TCP

UDP header



Source port: địa chỉ port chương trình gởi

Destination port: địa chỉ port chương trình nhận

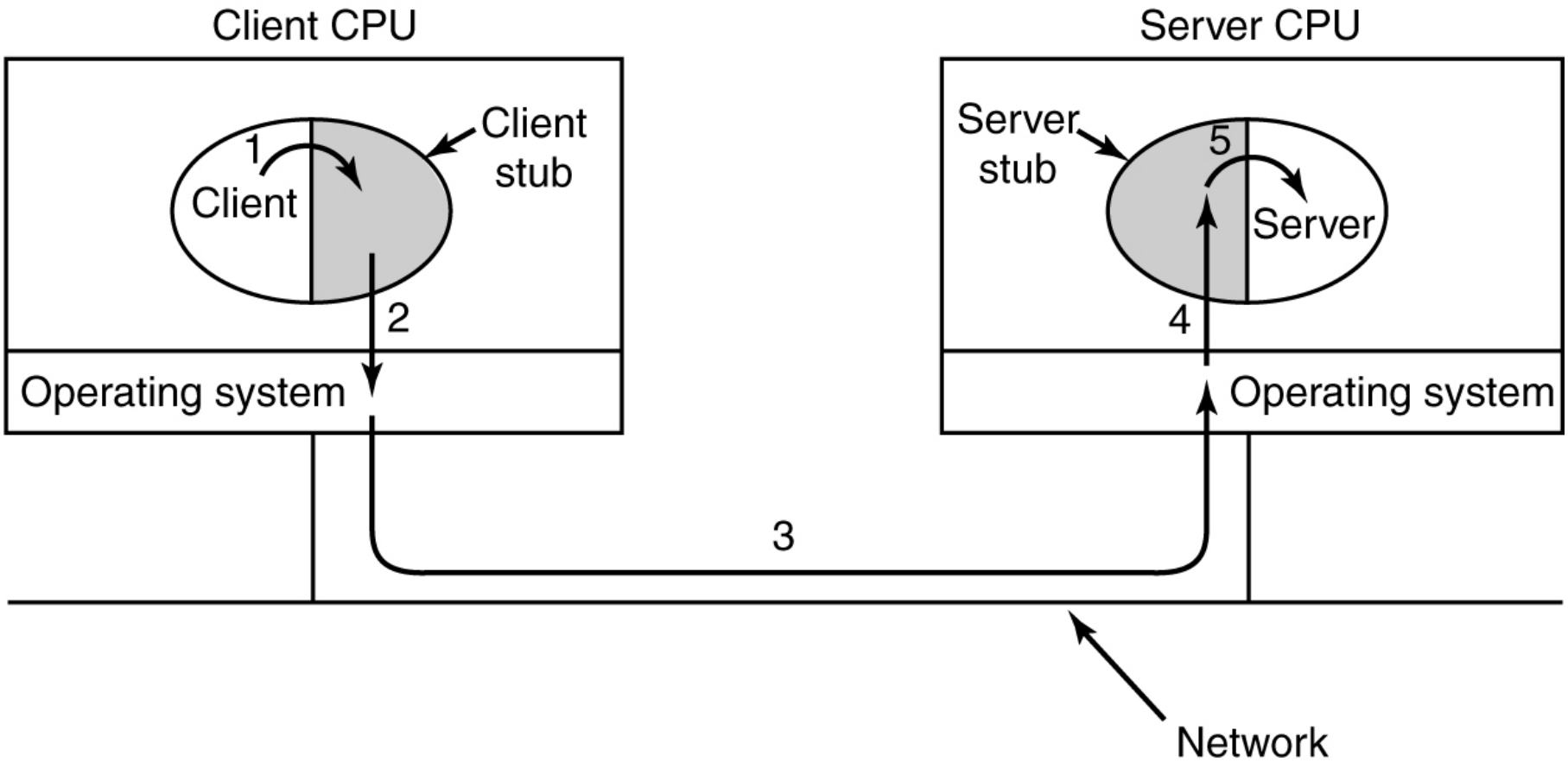
UDP length: kích thước header+data

UDP checksum: phát hiện lỗi cho header+data

Khái niệm RPC (Remote Procedure Call)

- Mô hình hoạt động thông dụng:
  - Một chương trình gởi thông điệp yêu cầu (request) đến chương trình trên máy khác
  - Chờ thông điệp trả lời (reply)
- Trừu tượng hoá mô hình request-reply thành dạng gọi thủ tục từ xa (RPC)
  - Client: nơi gọi thủ tục
  - Server: nơi thực thi thủ tục

Mô hình RPC


Client CPU
Server CPU
Client
Client stub
Server stub
Server
Operating system
Operating system
1
2
3
4
5
Network

III. Giới thiệu giao diện lập trình mạng socket

1. Khái niệm Socket API
2. Giới thiệu Windows Sockets (WinSock)

1. Khái niệm Socket API

- API (Application Programming Interface)

  Giao diện lập trình ứng dụng: tập hợp các hàm cung cấp cho chương trình ứng dụng
- Socket APIs trừu tượng hoá việc truyền thông dạng client/server trên bộ giao thức TCP/IP với mô hình socket
- Socket API có thể sử dụng cho các bộ giao thức khác như IPX/SPX, DECNet, …)

Hai dạng Socket APIs

- Berkeley Sockets (BSD Sockets)

  cung cấp các thao tác cơ sở (primitives) dùng trên UNIX

- Windows Sockets (WinSock)

  Có các mở rộng hỗ trợ cơ chế message-driven của Windows

Ví dụ

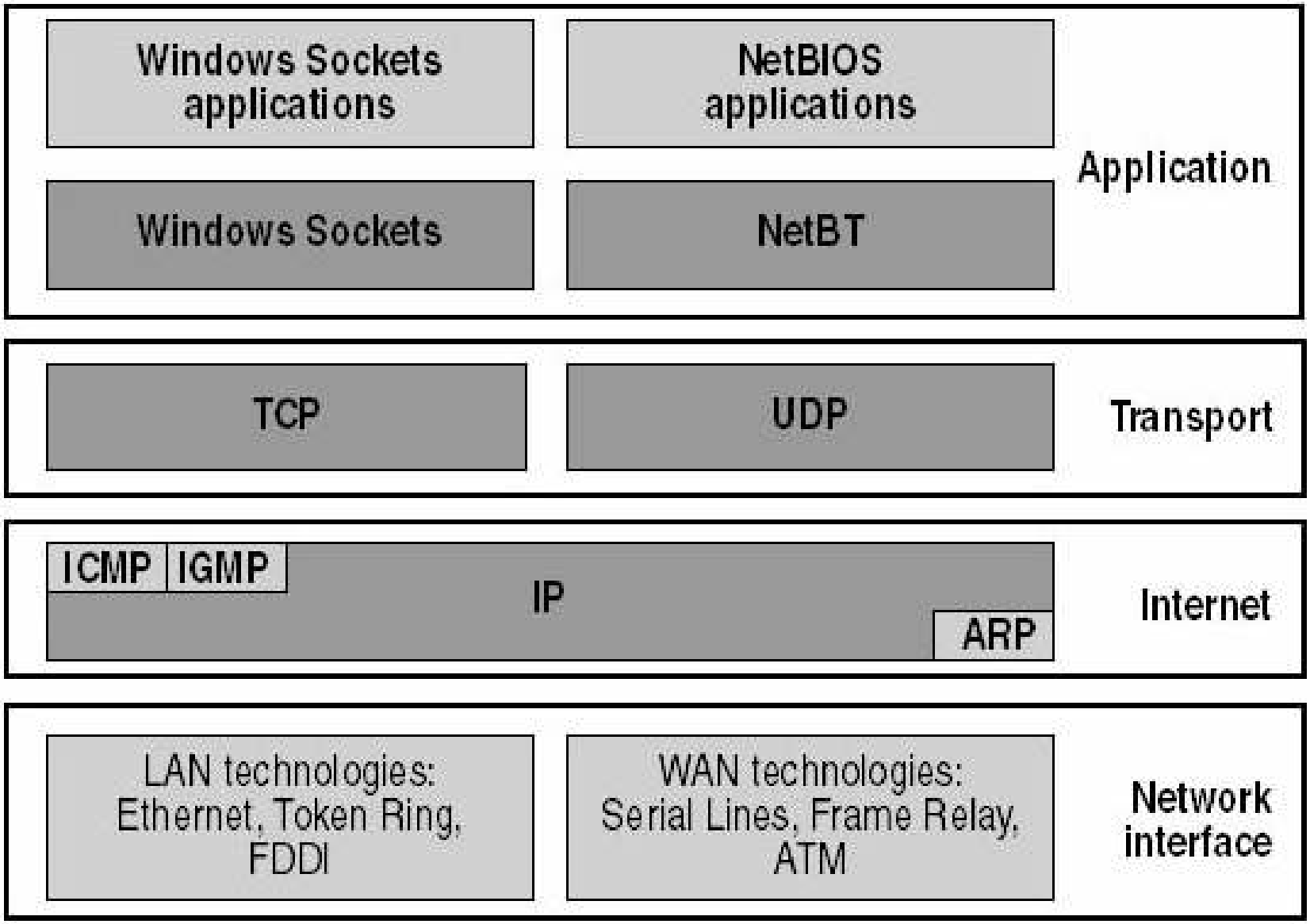
Primitive	Meaning
SOCKET	Create a new communication end point
BIND	Attach a local address to a socket
LISTEN	Announce willingness to accept connections; give queue size
ACCEPT	Block the caller until a connection attempt arrives
CONNECT	Actively attempt to establish a connection
SEND	Send some data over the connection
RECEIVE	Receive some data from the connection
CLOSE	Release the connection

Các thao tác cơ sở trên TCP của BSD sockets

2. Giới thiệu WinSock

- WinSock: giao diện lập trình mạng dùng trên hệ điều hành Windows trên mô hình socket
- Chương trình sử dụng WinSock API, liên kết với thư viện WinSock

Kiến trúc TCP/IP trên Microsoft Windows



Dịch vụ WinSock

- Các thao tác cơ sở
  - Liên kết chương trình ứng dụng với socket
  - Khởi tạo, chấp nhận kết nối
  - Gởi nhận dữ liệu
  - Đóng kết nối
- Các hàm bất đồng bộ
- Các hàm chuyển đổi dữ liệu

Các dạng socket

- Stream socket
  - Trao đổi dữ liệu tin cậy 2 chiều dùng TCP
- Datagram socket
  - Trao đổi dữ liệu 2 chiều dùng UDP

Socket được định nghĩa theo:

- Giao thức sử dụng
- Địa chỉ

NHẬP MÔN MẠNG MÁY TÍNH

Chương 6

LỚP APPLICATION

(LỚP ỨNG DỤNG)

Nội dung chương 6

I. Giới thiệu

II. Domain Name System (DNS)

III. Telnet

IV. File Tranfer Protocol (FTP)

V. E-Mail

VI. World Wide Web (WWW)

I. Giới thiệu

- Chương trình ứng dụng thực hiện các dịch vụ mạng
- Dịch vụ được đặc tả bởi giao thức
- Các dịch vụ chuẩn trên mạng TCP/IP:
  - DNS
  - FTP
  - SMTP
  - HTTP
  - ……

II. Domain Name System (DNS)

1. Giới thiệu DNS
2. Không gian tên DNS
3. Dữ liệu DNS
4. Name servers

1. Giới thiệu DNS

- DNS là sơ đồ đặt tên:
  - Dạng text
  - Có thứ bậc
  - Cơ sở dữ liệu tên được quản lý phân bố
- Dùng để ánh xạ tên máy với địa chỉ IP, có thể dùng cho mục đích khác
- Được định nghĩa trong RFC 1034, 1035

Hoạt động dạng đơn giản

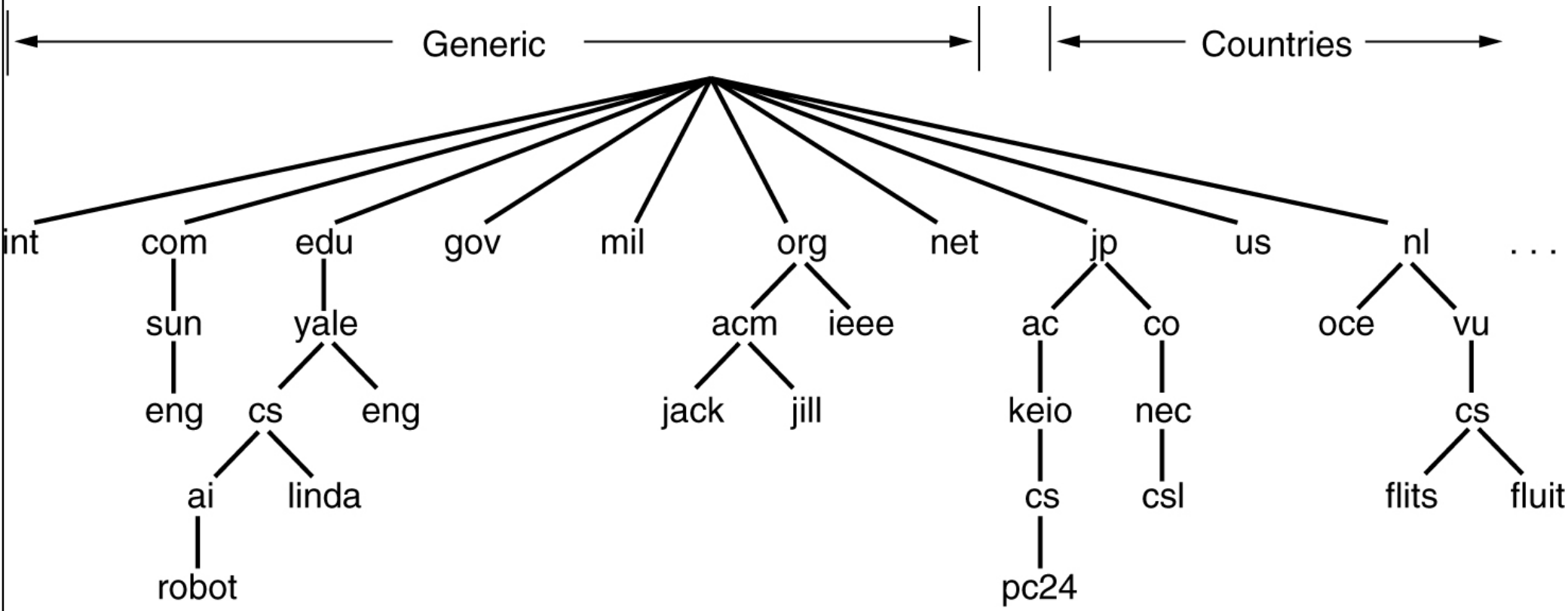
Chương trình ứng dụng cần địa chỉ IP của một tên máy:

- Gọi hàm thư viện resolver (DNS client), tham số là tên máy
- Resolver gởi yêu cầu đến DNS server
- DNS server trả địa chỉ IP cho resolver
- Resolver trả địa chỉ IP cho chương trình ứng dụng

2. Không gian tên DNS

- Cấu trúc cây
- Có các top-level domain
- Trong top-level domain chia thành các subdomain
- Trong subdomain có thể chia thành các domain cấp thấp hơn

Một phần không gian tên DNS



Ví dụ: eng.sun.com

robot.ai.cs.yale.edu

www.vnn.vn

Top-level domain (tên miền cấp 1)

Gồm 2 phần:

- Tên miền quốc gia

  (Country code top-level domains)
  - Theo ISO 3166
  - Ví dụ: .vn, .fr, …
- Tên miền chung

  (Generic top-level domains)
  - Do ICANN/IANA quy định

  (Internet Assigned Numbers Authority)

Tên miền chung

- com (commercial)
- edu (educational institutions)
- gov (US gorvernment)
- int (international organizations)
- mil (US armed forces)
- net (network providers)
- org (nonprofit organizations)

Tên miền chung (tt)

- biz (businesses)
- info (information)
- name (people's name)
- pro (professions)

Tên miền dành riêng

- aero (aerospace industry)
- coop (co-operatives)
- museum (museums)

3. Dữ liệu DNS

- Bao gồm các mẩu tin (resource record)
- Cấu trúc mẩu tin: có 5 trường
  - Domain_name: tên miền
  - Time_to_live: thời gian ổn định của mẩu tin
  - Class: luôn là IN (Internet)
  - Type: loại mẩu tin
  - Value: giá trị

Dữ liệu DNS (tt)

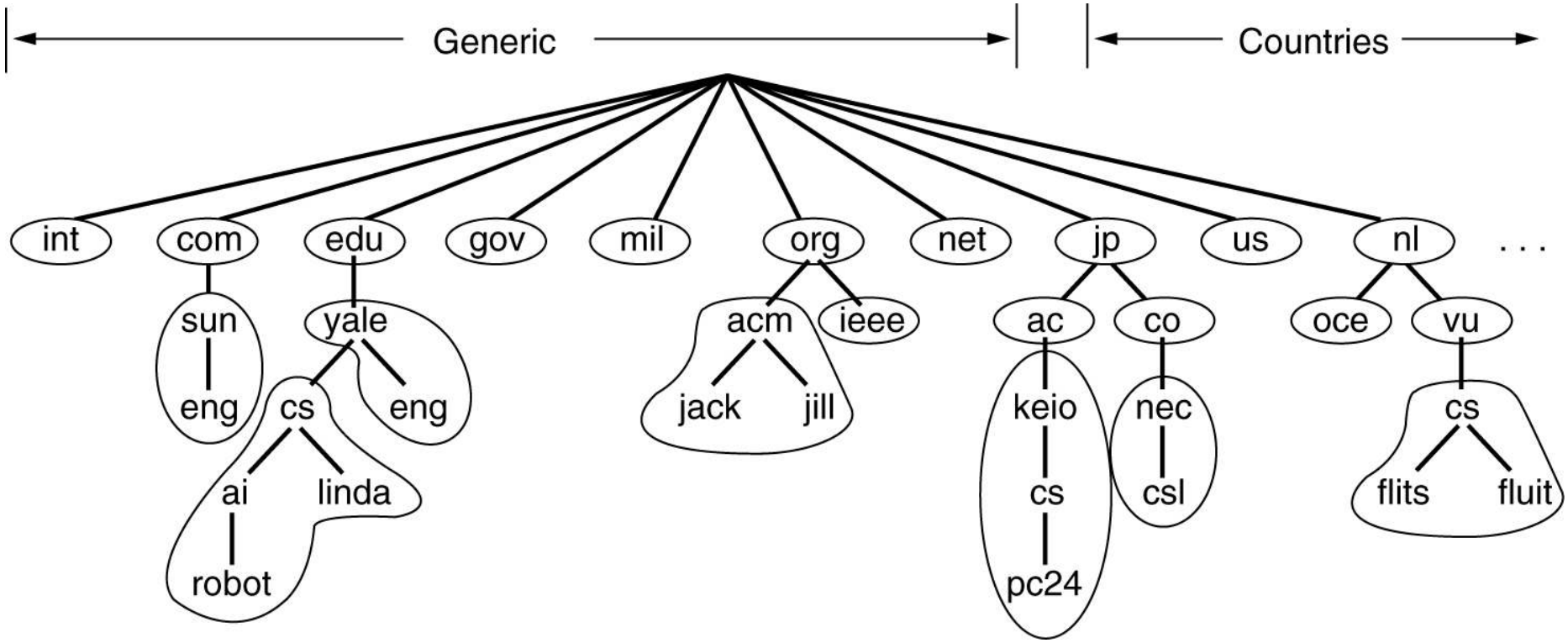
Loại (Type)	Ý nghĩa	Giá trị (Value)
SOA	Start of Authority	Các thông số của vùng
NS	Name Server	Tên của Name Server
A	IP address	Số nguyên 32 bit

Một số loại mẩu tin dữ liệu DNS

4. Name servers

- Không gian tên DNS được chia thành các vùng (zones) rời nhau
- Mỗi vùng được quản lý bởi các name server:
  - Primary name server
  - Các secondary name server

Ví dụ các vùng

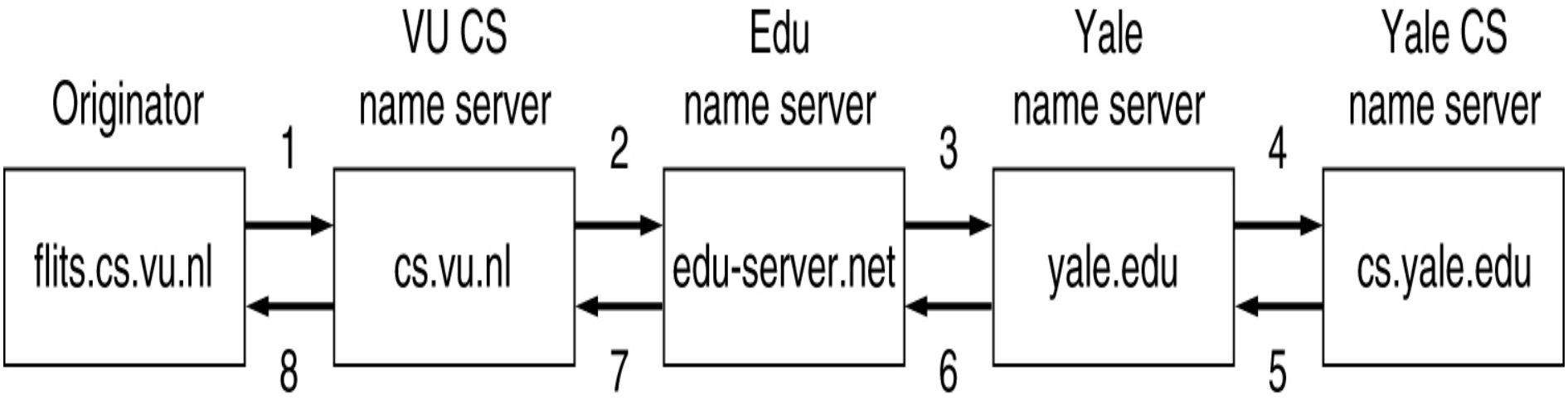


Hoạt động của DNS

Resolver cần địa chỉ IP của một tên máy:

- Resolver gởi yêu cầu đến local name server
- Nếu có thông tin, local name server cung cấp mẩu tin cho resolver
- Nếu không có thông tin, local name server gởi yêu cầu đến top-level name server tương ứng, để có thông tin từ name server lưu mẩu tin cần tìm

Ví dụ



Máy flits.cs.vu.nl cần địa chỉ IP của máy linda.cs.yale.edu

III.Telnet

- Là ứng dụng chuẩn dạng có kết nối trên mạng TCP/IP
- Cho phép Telnet client (local host) đăng nhập vào Telnet server (remote host) tại port 23 và thực thi các lệnh trên dòng lệnh

  →sử dụng Network Virtual Terminal (NVT)

  →client system có thể khác server system
- Được định nghĩa trong RFC 854, 855

Hoạt động telnet

- Truyền các phím ấn từ local host đến remote host
- Xử lý trên remote host
- Truyền màn hình kết quả cho local host

Các dạng tương tự telnet

- VNC (Virtual Network Computer)
- Terminal Service
- Remote shell (RSH)
- Remote execution (REXEC)

IV.File Transfer Protocol (FTP)

1. Khái niệm
2. Mô hình FTP

1. Khái niệm

- FTP là dịch vụ cho phép FTP client kết nối với FTP server để truyền và quản lý file
- Các tính chất:
  - Truy xuất dạng tương tác
  - Có 2 chế độ truyền: nhị phân và văn bản
  - Client phải cung cấp username, password
    anonymous user: không cần password
- Được định nghĩa trong RFC 959

FTP Client

- Có 2 dạng:
  - Văn bản: dùng các lệnh FTP tại dòng lệnh ftp, get, close, quit, …
  - Đồ hoạ: thao tác trên file như chương trình quản lý file

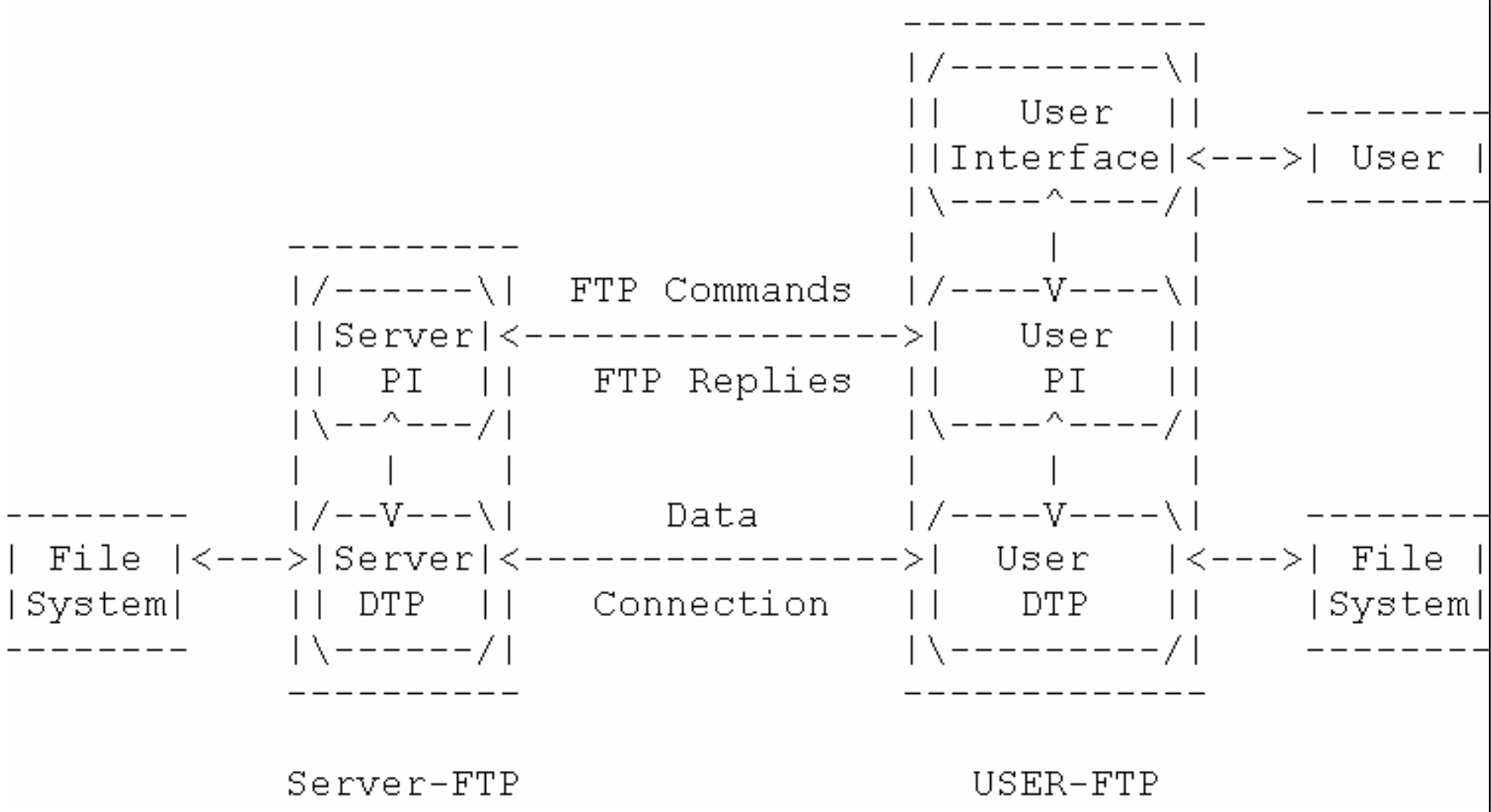
TFTP (Trivial FTP)

- Dạng không kết nối (dùng UDP)
- Tốc độ cao hơn FTP
- Không tin cậy
- Ít chức năng hơn FTP

Các dịch vụ tương tự FTP

- Web Browser có thể thực hiện các chức năng của FTP Client
- Gopher
  - Truyền file dạng phân bố
  - Giao diện menu
  - Kết hợp với các dịch vụ tìm kiếm

2. Mô hình FTP



PI: Protocol Interface, DTP: Data Transfer Process

Mô hình FTP (tt)

Gồm 2 loại kết nối:

- FTP control
  - Server port 21, client port (>1023)
  - Được thiết lập và duy trì trong phiên làm việc FTP
- FTP data
  - Server port 20, client port như FTP control
  - Được thiết lập khi có truyền file, và kết thúc tự động

V. Electronic Mail

1. Khái niệm
2. Kiến trúc hệ thống mail
3. Khuôn dạng mail
4. Các giao thức truyền mail
5. Webmail

1. Khái niệm

- Hệ thống mail:
  - Cho phép gởi nhận thông tin bất đồng bộ giữa hai người hay hai nhóm người
  - Cung cấp phương tiện tạo, truyền, xử lý các thông tin
- Có nhiều hệ thống mail
- Internet mail:
  - Khuôn dạng mail theo RFC 822, 2822
  - Giao thức truyền mail theo RFC 821, 2821

2. Kiến trúc hệ thống mail

Gồm 2 thành phần

- User Agents – UA
  - Chương trình địa phương phía user (Local program)
  - Cung cấp các phương tiện tương tác với hệ thống mail
- Message Transfer Agents –MTA
  - Chương trình thường trú phía server (System daemon)
  - Thực hiện việc truyền mail

Các chức năng cơ bản của hệ thống mail

- Tạo mail – Composition
- Truyền mail – Transfer
- Thông báo kết quả cho người gởi – Reporting
- Thông báo trạng thái cho người nhận – Displaying
- Xử lý mail đã nhận – Disposition

Tổ chức hệ thống mail

Có các mailbox:

- Inbox (Incoming mailbox)
- Outbox (Outgoing mailbox)

Các dạng mailbox đặc biệt:

- Bulk
  - Chứa thư rác – spam/junk e-mail
- Sent
- …

Tổ chức hệ thống mail (tt)

Hỗ trợ về địa chỉ mail:

- Mailing list
- Address book

Địa chỉ mail – Mail account

- local-part@domain
- mailbox@host

3. Khuôn dạng mail

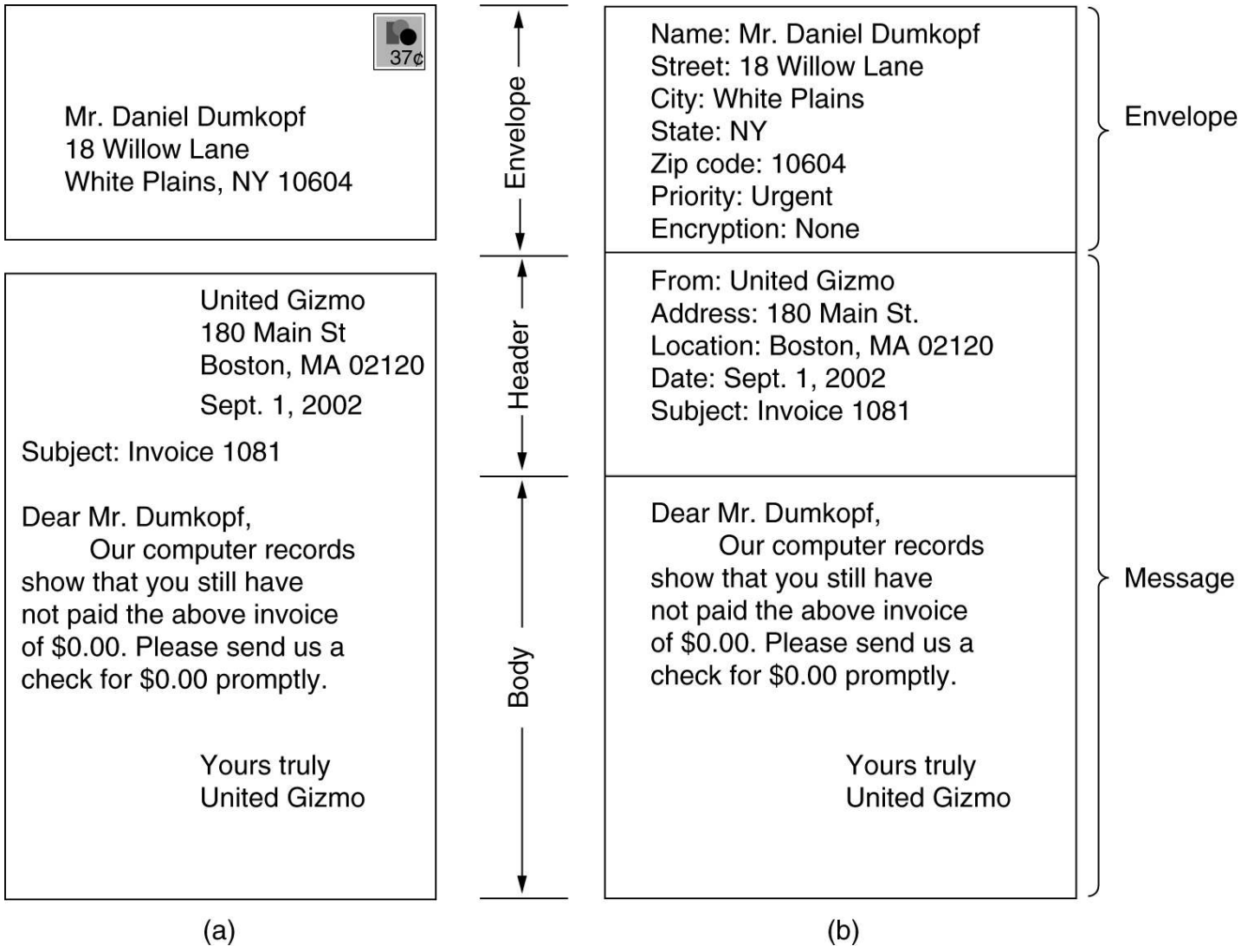
Gồm các phần:

- Envelope – Bao thư/phong bì
- Message – Thông điệp
  - Header: các thông tin điều khiển
  - Body: nội dung

Tiêu chuẩn khuôn dạng mail

- Internet message format - RFC 822/2822
- MIME – RFC 2045-2049
  Multipurpose Internet Mail Extensions

Ví dụ



a. Thư trên giấy b. Thư điện tử

Khuôn dạng mail theo RFC 822

- Không phân biệt phần envelope và phần header, gọi chung là header
- Phần body là tùy ý

Các thành phần chính trên RFC 822 header

To:	Địa chỉ mail các người nhận chính
Cc:	Cacbon copy Địa chỉ mail các người nhận phụ
Bcc:	Blind cacbon copy Địa chỉ mail các người nhận ẩn
From:	Tên người tạo mail
Sender:	Địa chỉ mail người gởi
Subject	Nội dung tóm tắt
.....	.....

MIME

- Mở rộng khuôn dạng thông điệp theo RFC 822:
  - Nội dung thông điệp với các bộ ký tự khác ASCII
  - Nội dung thông điệp không là ký tự (hình ảnh, âm thanh, …)
  - Thông điệp có nhiều phần (multi-part)
  - Phần header với ký tự khác ASCII

Mở rộng phần header

Header	Ý nghĩa
MIME-Version	Phiên bản MIME
Content-Description	Mô tả nội dung
Content-ID	Số thứ tự
Content-Transfer-Encoding	Dạng mã hoá của nội dung
Content-Type	Loại và khuôn dạng của nội dung

Một số loại dữ liệu theo MIME

Type	Subtype	Description
Text	Plain	Unformatted text
	Enriched	Text including simple formatting commands
Image	Gif	Still picture in GIF format
	Jpeg	Still picture in JPEG format
Audio	Basic	Audible sound
Video	Mpeg	Movie in MPEG format
Application	Octet-stream	An uninterpreted byte sequence
	Postscript	A printable document in PostScript
Message	Rfc822	A MIME RFC 822 message
	Partial	Message has been split for transmission
	External-body	Message itself must be fetched over the net
Multipart	Mixed	Independent parts in the specified order
	Alternative	Same message in different formats
	Parallel	Parts must be viewed simultaneously
	Digest	Each part is a complete RFC 822 message

Ví dụ

```
From: elinor@abcd.com
To: carolyn@xyz.com
MIME-Version: 1.0
Message-Id: <0704760941.AA00747@abcd.com>
Content-Type: multipart/alternative; boundary=qwertyuiopasdfghjklzxcvbnm
Subject: Earth orbits sun integral number of times

This is the preamble. The user agent ignores it. Have a nice day.

--qwertyuiopasdfghjklzxcvbnm
Content-Type: text/enriched

Happy birthday to you
Happy birthday to you
Happy birthday dear <bold> Carolyn </bold>
Happy birthday to you

--qwertyuiopasdfghjklzxcvbnm
Content-Type: message/external-body;
        access-type="anon-ftp";
        site="bicycle.abcd.com";
        directory="pub";
        name="birthday.snd"

content-type: audio/basic
content-transfer-encoding: base64
--qwertyuiopasdfghjklzxcvbnm--
```

4. Các giao thức truyền mail

- SMTP - Simple Mail Transfer Protocol

  MTA → MTA, UA → MTA
- POP3 - Post Office Protocol version 3

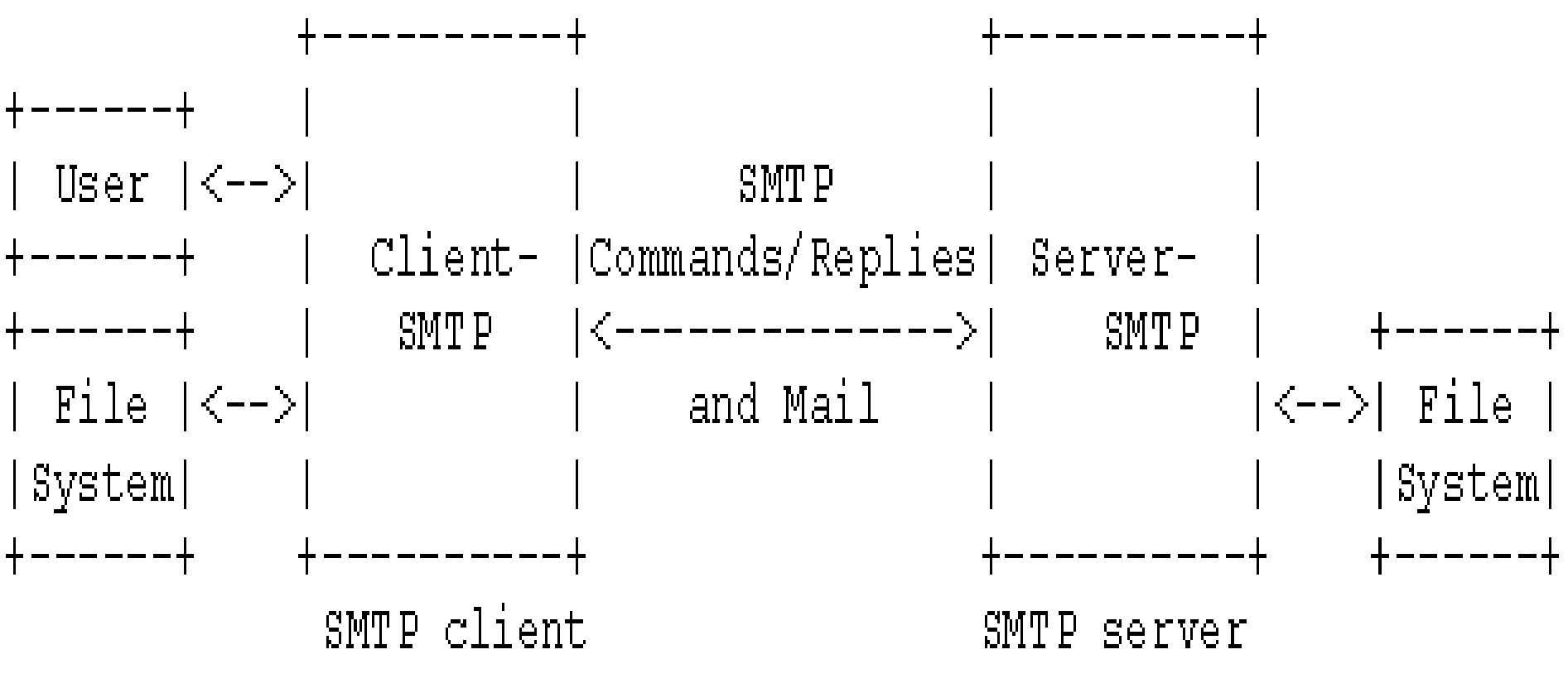
  MTA → UA
- IMAP-Internet Message Access Protocol

  MTA → UA

SMTP

- Được định nghĩa trong RFC 821, 2821
- Dạng client-server
- SMTP client thiết lập kết nối TCP với SMTP server tại port 25
- Nếu SMTP server đồng ý nhận mail:
  - SMTP client gởi địa chỉ người gởi, người nhận
  - SMTP client gởi mail
  - SMTP server gởi ACK
  - Hủy kết nối

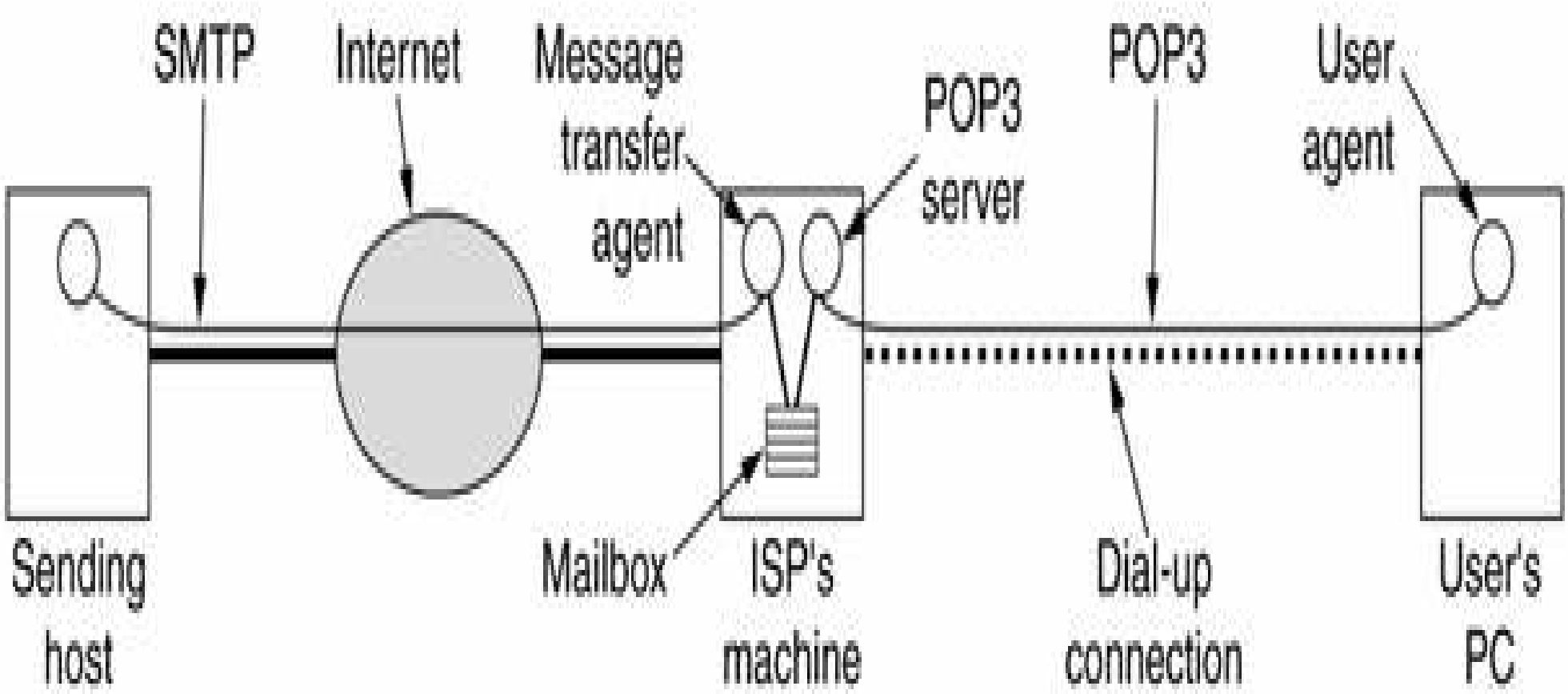
Mô hình SMTP


User
File
System
Client-
SMTP
SMTP
Commands/Replies
and Mail
Server-
SMTP
SMTP
File
System
SMTP client
SMTP server

POP3

- Được định nghĩa trong RFC 1939, 2449
- Dùng lấy mail từ remote mailbox về máy địa phương
- Client thiết lập kết nối TCP với server tại port 110

Mô hình POP3


SMTP
Internet
Message transfer agent
POP3 server
POP3
User agent
Sending host
Mailbox
ISP's machine
Dial-up connection
User's PC

Các giai đoạn hoạt động POP3

- Authorization – Cho phép
  - Client gởi username, password
- Transaction – Giao dịch
  - Client yêu cầu nội dung mail và xoá mail tại server
  - Server gởi các mail
- Update – Cập nhật
  - Client gởi lệnh thoát (quit)
  - Server xoá các mail, hủy kết nối

IMAP

- Được định nghĩa trong RFC 2060
- Quản lý mail tập trung tại server, không di chuyển về máy địa phương như POP3

  → có thể truy xuất từ nhiều máy
- Client thiết lập kết nối TCP với server tại port 143

Các đặc điểm của IMAP

- Cho phép tạo, xoá, xử lý nhiều mailbox tại server
- Có thể truy xuất từng phần của mail
- Có thể truy xuất mail theo thuộc tính

5. Webmail

- Web site cung cấp dịch vụ mail
- Có MTA tại port 25, nhận các kết nối SMTP
- User dùng các form trên trang web để tương tác với hệ thống:
  - Đăng nhập - Login
  - Liệt kê các mail box
  - Đọc, xoá, soạn thảo, …mail

VI. World Wide Web

1. Khái niệm
2. Kiến trúc hệ thống Web
3. Trang web tĩnh
4. Trang web động
5. Giao thức HTTP
6. Web không dây

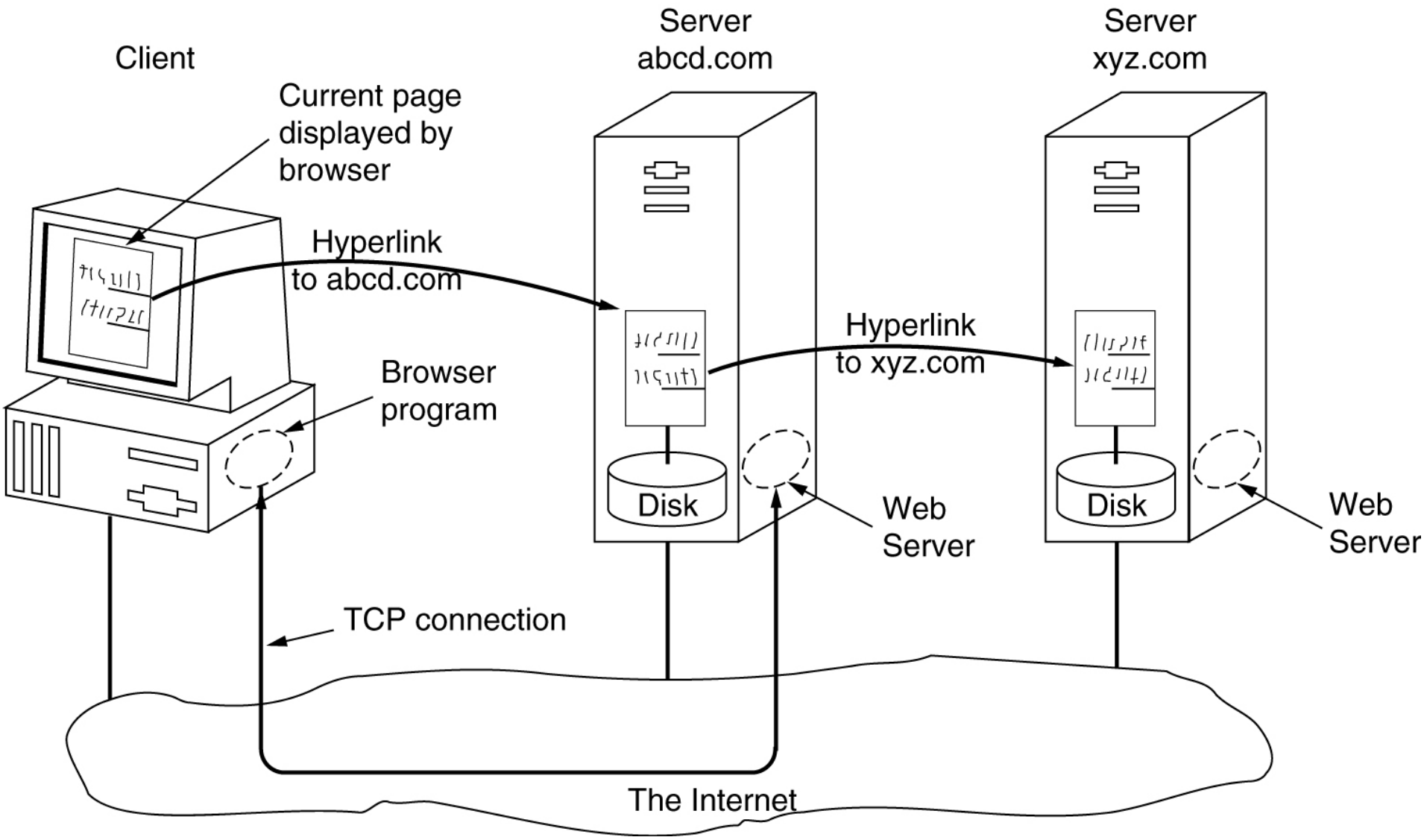
1. Khái niệm

- Web là dịch vụ truy xuất các văn bản có liên kết, trang web, từ các máy trên mạng Internet
- Do Tim Berners-Lee thiết kế năm 1989 tại CERN (trung tâm nghiên cứu hạt nhân châu Âu)
- Năm 1994, CERN và MIT thành lập tổ chức World Wide Web Consortium (www.w3c.org) để phát triển Web

2. Kiến trúc hệ thống Web

a. Hoạt động phía client
b. Hoạt động phía server
c. Tên trang web
d. Cookies

Mô hình dịch vụ Web



a. Hoạt động phía Client

- Web browser: chương trình hiển thị các trang web phía client
- Hoạt động web browser:
  - Lấy trang web được yêu cầu
  - Thông dịch nội dung trang web
  - Hiển thị trên màn hình
- Tên trang web có dạng URL (Uniform Resource Locator)

  Ví dụ: http://www.itu.org/home/index.html

Ví dụ: web browser lấy và hiển thị trang web http://www.itu.org/home/index.html

1. Browser xác định URL
2. Browser yêu cầu DNS cung cấp địa chỉ IP máy www.itu.org
3. DNS trả lời 156.106.192.32
4. Browser thiết lập kết nối TCP port 80 với máy 156.106.192.32
5. Browser gởi yêu cầu file /home/index.html
6. Server www.itu.org gởi file /home/index.html
7. Hủy kết nối TCP
8. Browser hiển thị phần text trong file index.html
9. Browser lấy và hiển thị các hình ảnh trong file (nếu có)

Các chức năng của browser

- Duyệt các trang web: back, forward, history, favorites/bookmarks
- Lưu trang web thành file, in
- Cache các trang web trên đĩa địa phương → hoạt động offline

Plug-in

- Mở rộng khả năng của browser
- Đoạn chương trình lưu trong thư mục plug-in
- Được browser gọi khi cần hiển thị các loại dữ liệu không là html, ví dụ PDF

b. Hoạt động phía server

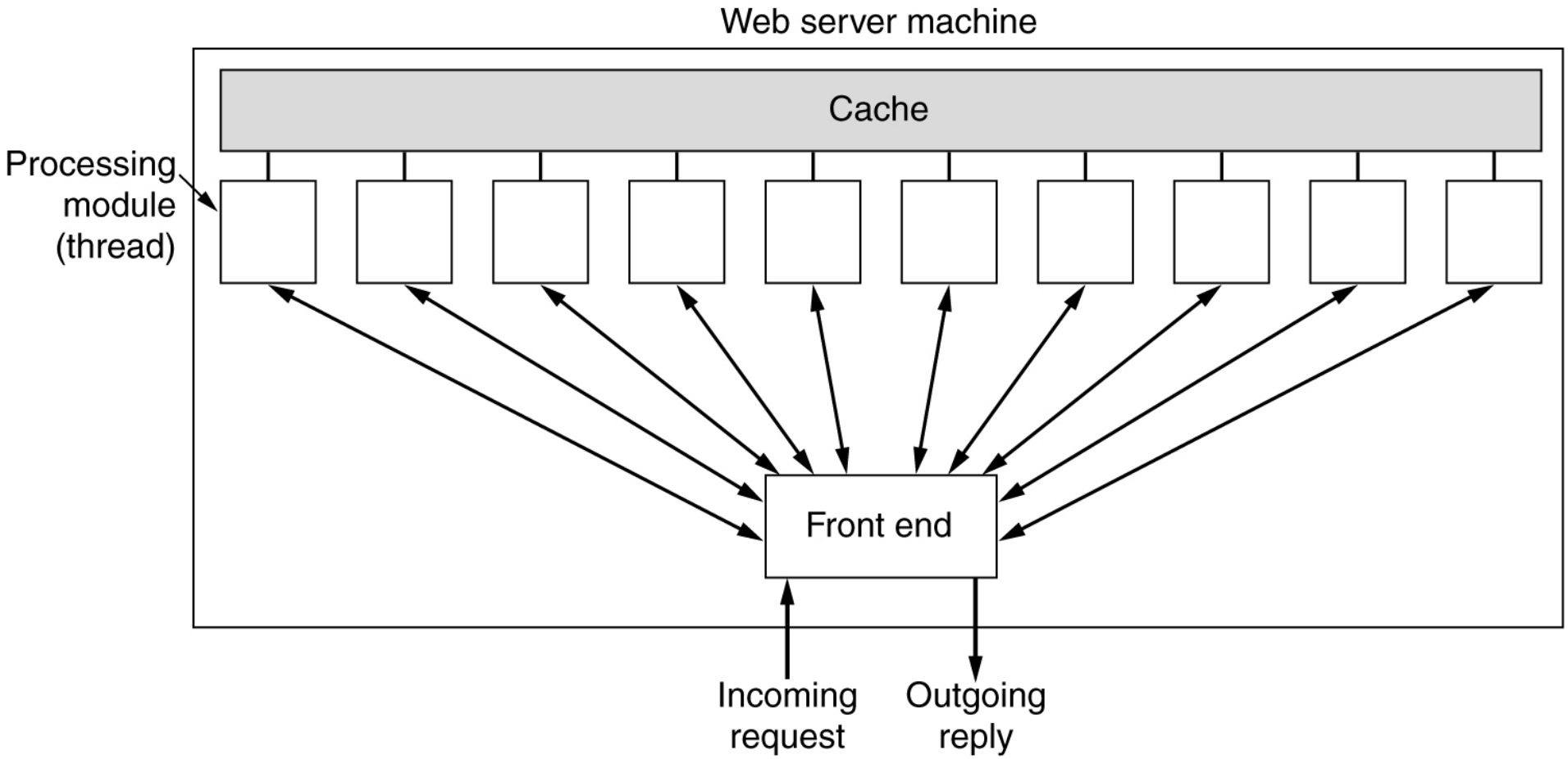
- Web server chờ kết nối TCP tại port 80
- Hoạt động web server:
  - Chấp nhận kết nối từ client (web browser)
  - Nhận tên file được yêu cầu
  - Lấy file (từ đĩa)
  - Gởi file cho client
  - Hủy kết nối

Tăng tốc độ web server

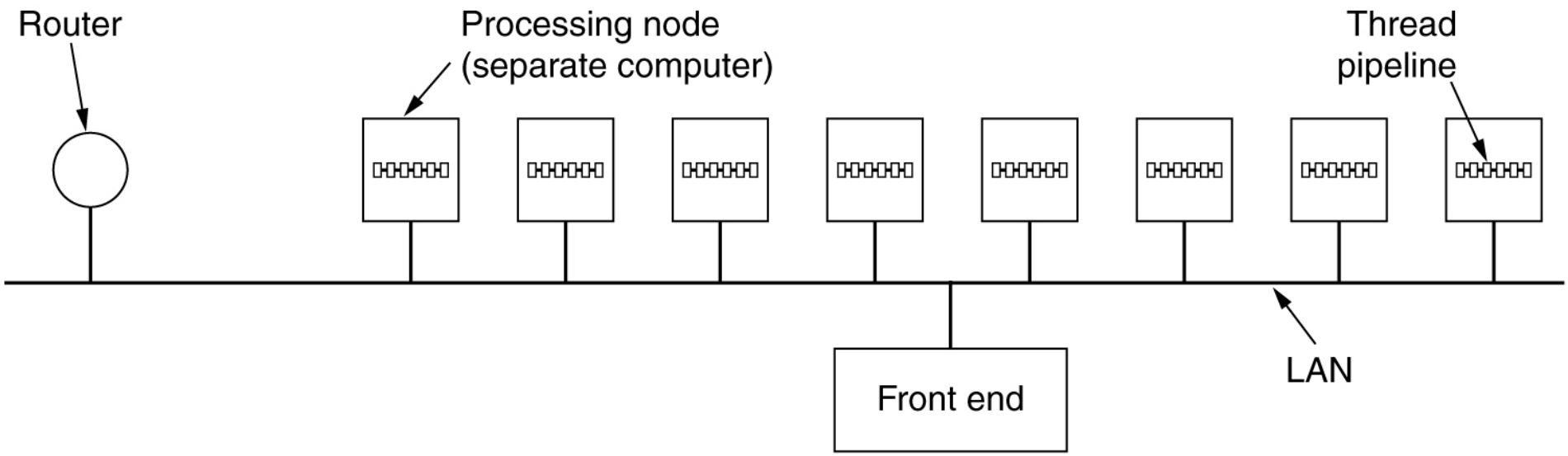
Hai kỹ thuật:

- Dùng cache và server đa luồng
- Dùng nhiều máy làm web server (server farm)

Web server dạng đa luồng



Nhiều máy làm web server



c. Tên trang web

- Theo URL (Uniform Resource Locator)

  Tên_giao_thức://tên_máy/tên_file
  - Tên_file: tên file địa phương
  - Tên_máy: theo DNS
  - Tên_giao_thức: có nhiều loại giao thức
- Web browser có thể dùng cho nhiều dịch vụ với URL

Thành phần tên_giao_thức trong URL

Name	Used for	Example
http	Hypertext (HTML)	http://www.cs.vu.nl/~ast/
ftp	FTP	ftp://ftp.cs.vu.nl/pub/minix/README
file	Local file	file:///usr/suzanne/prog.c
news	Newsgroup	news:comp.os.minix
news	News article	news:AA0134223112@cs.utah.edu
gopher	Gopher	gopher://gopher.tc.umn.edu/11/Libraries
mailto	Sending e-mail	mailto:JohnUser@acm.org
telnet	Remote login	telnet://www.w3.org:80

d. Cookies

- Chứa thông tin trạng thái của phiên làm việc giữa web server và web browser
- Là chuỗi ký tự lưu thành file tại máy client
- Khi gởi trang web cho client, server có thể gởi kèm cookies để lưu các thông tin trạng thái
- Khi gởi yêu cầu đến server, browser sẽ gởi kèm cookies (nếu có)

Ví dụ cookies

Domain	Path	Content	Expires	Secure
toms-casino.com	/	CustomerID=497793521	15-10-02 17:00	Yes
joes-store.com	/	Cart=1-00501;1-07031;2-13721	11-10-02 14:22	No
aportal.com	/	Prefs=Stk:SUNW+ORCL;Spt:Jets	31-12-10 23:59	No
sneaky.com	/	UserID=3627239101	31-12-12 23:59	No

3. Trang web tĩnh

a. HTML
b. Forms
c. XML

a. HTML (HyperText Markup Language)

- Trang web được tạo theo ngôn ngữ HTML (ngôn ngữ đánh dấu siêu văn bản)
- Nội dung trang web có thể bao gồm:
  - Văn bản
  - Hình ảnh
  - Âm thanh, hình ảnh động
  - Các siêu liên kết (hyperlink)

Đặc điểm HTML

- Là ứng dụng SGML

  (Standard Generalized Markup Language)
- Bao gồm các lệnh định dạng, gọi là tag

  Ví dụ: boldface
- Các browser có thể định dạng lại cho phù hợp với môi trường
- Có các tiêu chuẩn HTML 1.0, 2.0, …, 4.0

  XHTML (eXtended HTML)

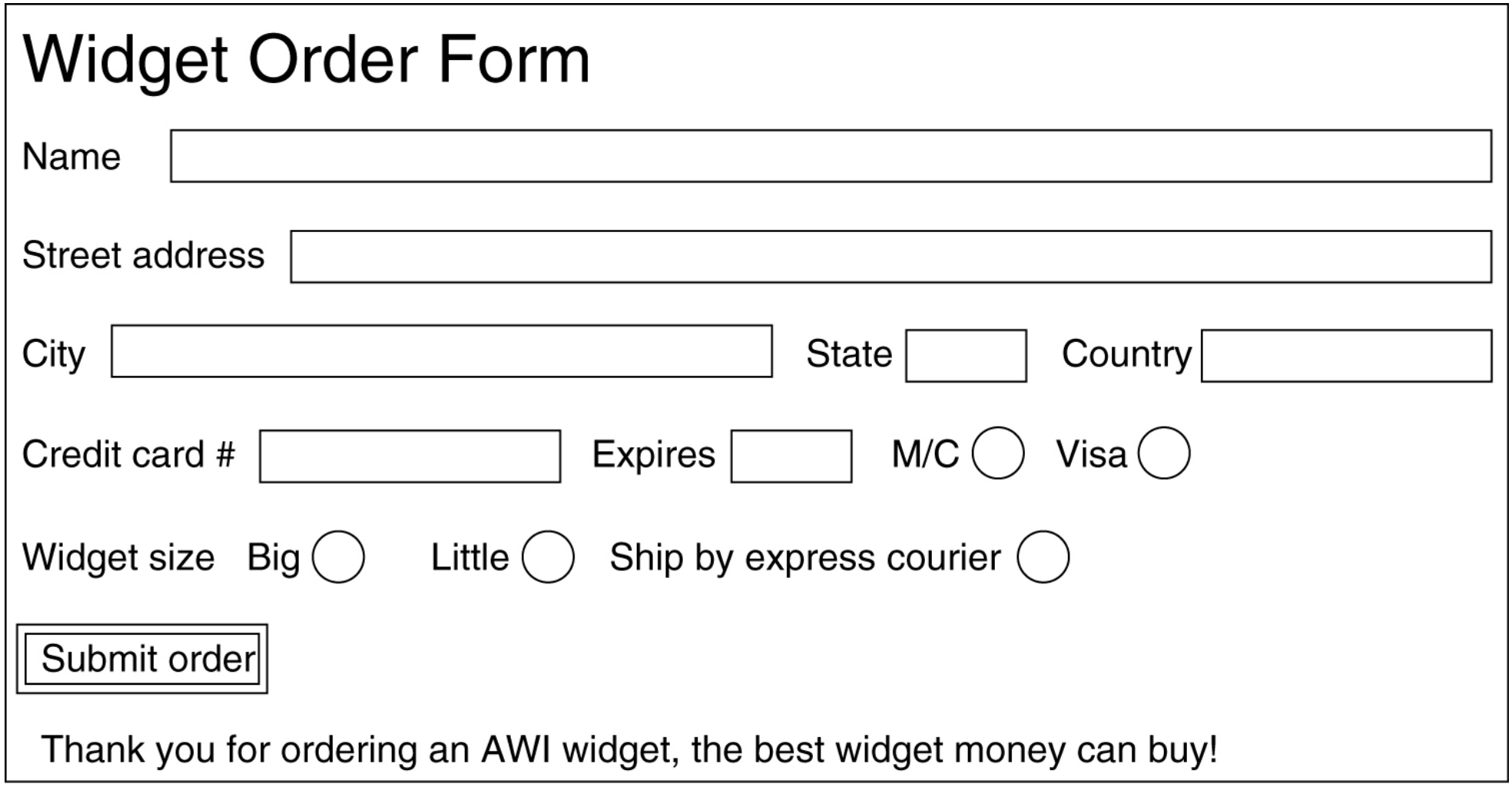
Một số lệnh định dạng

Tag	Description
<html> ... </html>	Declares the Web page to be written in HTML
<head> ... </head>	Delimits the page's head
<title> ... </title>	Defines the title (not displayed on the page)
<body> ... </body>	Delimits the page's body
<h *n*> ... </h*n*>	Delimits a level *n* heading
...	Set ... in boldface
...	Set ... in italics
...	Center ... on the page horizontally
...	Brackets an unordered (bulleted) list
...	Brackets a numbered list
	Starts a list item (there is no)
 	Forces a line break here
<p>	Starts a paragraph
<hr>	Inserts a Horizontal rule
<img src="...">	Displays an image here
 ... 	Defines a hyperlink

b. Forms

- Có từ HTML 2.0
- Form bao gồm các nút ấn (button), hộp (boxes) cho phép user nhập thông tin, lựa chọn
- Dữ liệu trên form được gởi lại server dưới dạng string

Ví dụ form


Widget Order Form
Name
Street address
City
State
Country
Credit card #
Expires
M/C
Visa
Widget size
Big
Little
Ship by express courier
Submit order
Thank you for ordering an AWI widget, the best widget money can buy!

c. XML (eXtensible Markup Language)

- Mục đích:
  - Thể hiện cấu trúc trang web
  - Mô tả thông tin
  - Có thể dùng cho các loại ứng dụng khác
- Cần cơ chế hiển thị thông tin XML trên browser dạng HTML, ví dụ XSL (eXtensible Style Language)

Ví dụ văn bản XML

```
<?xml version="1.0" ?>
<?xml-stylesheet type="text/xsl" href="b5.xsl"?>

<book_list>

<book>
   <title> Computer Networks, 4/e </title>
   <author> Andrew S. Tanenbaum </author>
   <year> 2003 </year>
</book>

<book>
   <title> Modern Operating Systems, 2/e </title>
   <author> Andrew S. Tanenbaum </author>
   <year> 2001 </year>
</book>

<book>
   <title> Structured Computer Organization, 4/e </title>
   <author> Andrew S. Tanenbaum </author>
   <year> 1999 </year>
</book>

</book_list>
```

4. Trang web động

- Trang web tĩnh:
  - Client gởi yêu cầu là tên file
  - Server gởi file đã có
- Trang web động
  - Nội dung trang web được tạo theo yêu cầu, thay vì đã có trên đĩa
- Có 2 dạng:
  - Tạo trang web động tại server
  - Tạo trang web động tại client

Tạo trang web động tại server

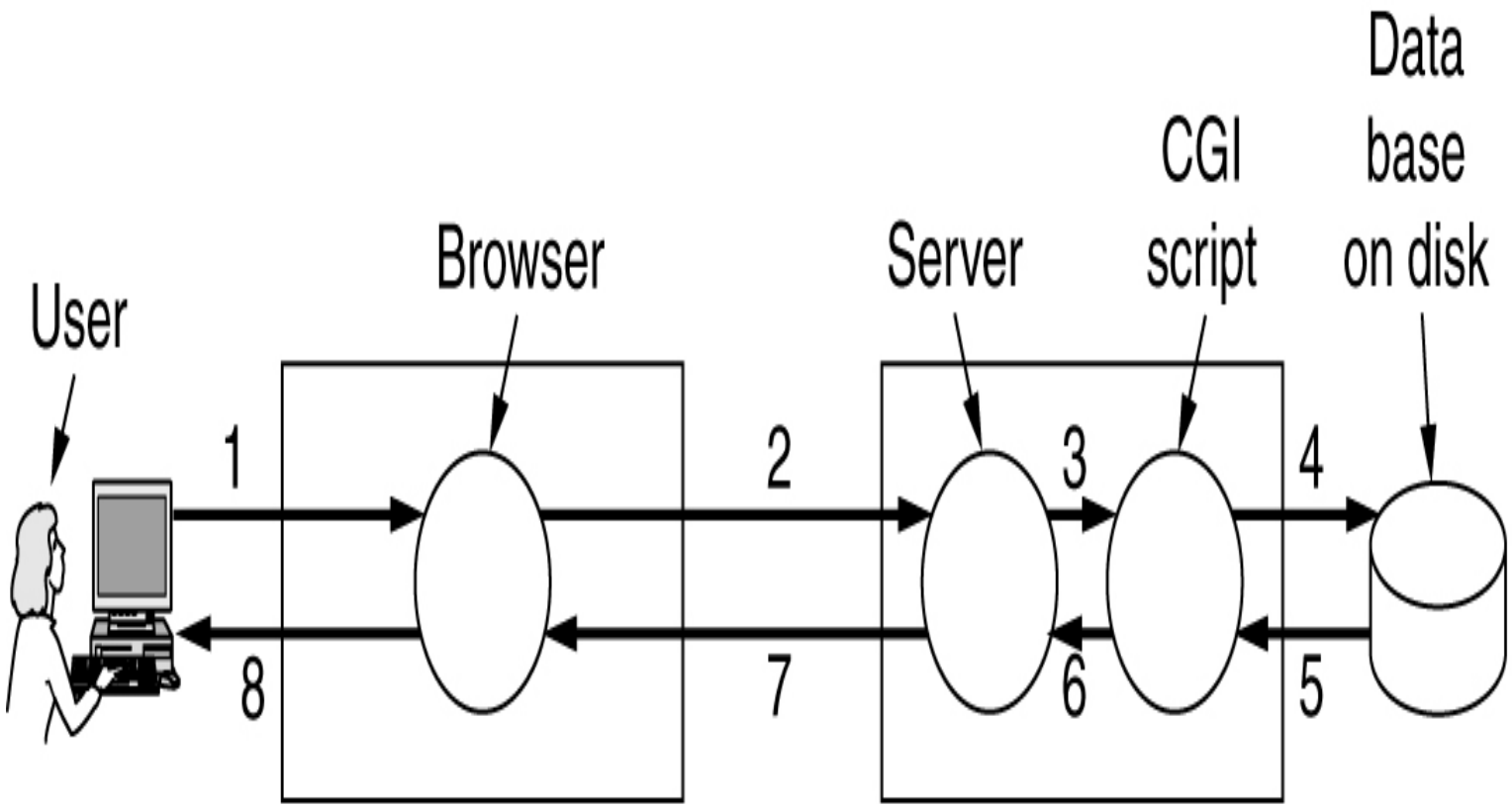
Có các dạng:

- CGI (Common Gateway Interface)

  với các script, ví dụ Perl, Python, …
- Dùng các dạng script trong trang web

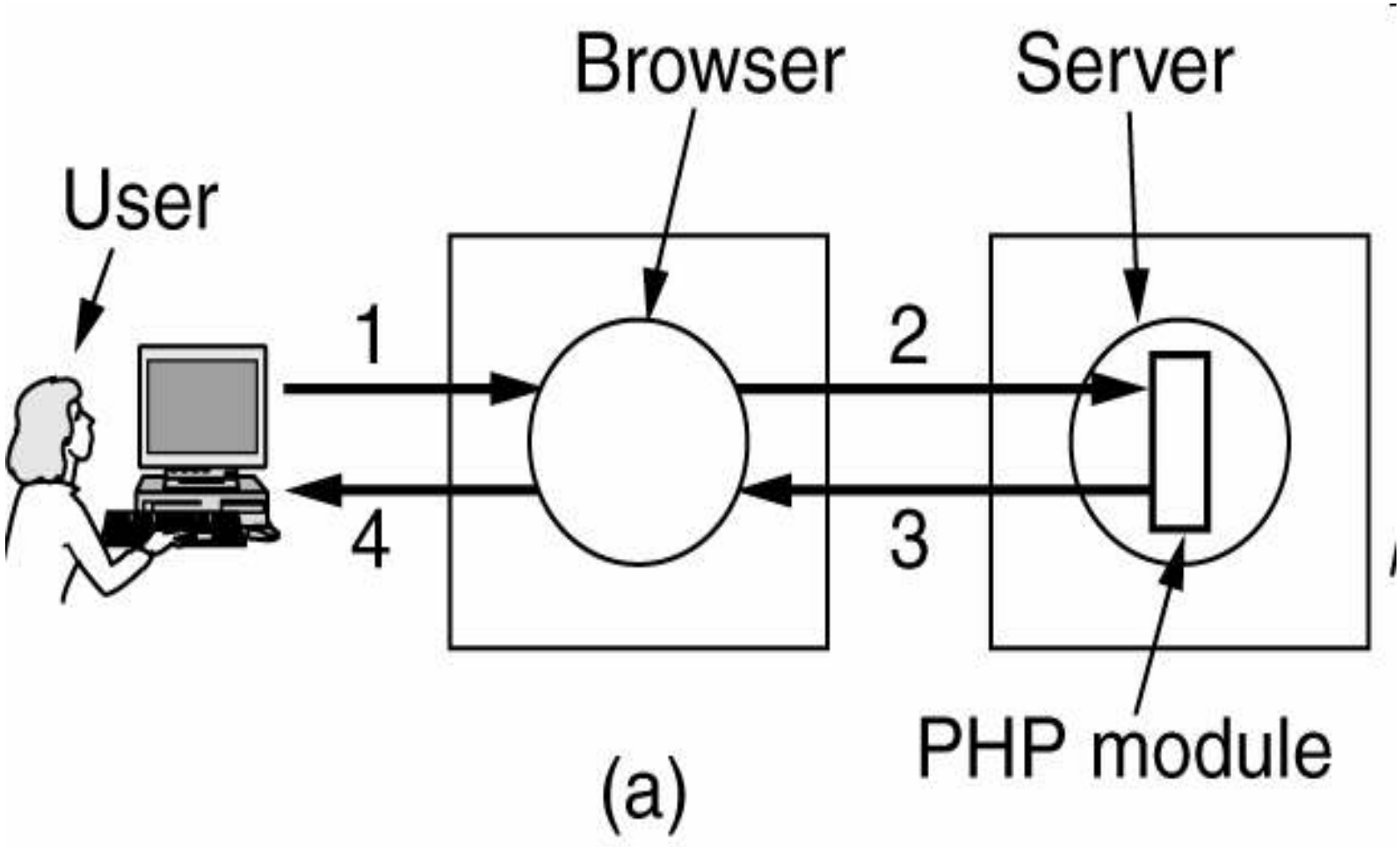
  (HTML-embedded scripting language)
  - PHP (PHP: Hypertext Preprocessor)
  - JSP (JavaServer Pages)
  - ASP (Active Server Pages)

Ví dụ: các bước xử lý form dùng CGI



1. User fills in form
2. Form sent back
3. Handed to CGI
4. CGI queries DB
5. Record found
6. CGI builds page
7. Page returned
8. Page displayed

Ví dụ: tạo trang web động với PHP



Tạo trang web động tại client

- Dùng các script trong trang web, thực hiện tại máy client để tương tác trực tiếp với user
- Các công nghệ thông dụng
  - Javascript: client-side scripting language
  - JavaApplets
  - Microsoft ActiveX control

5. Giao thức HTTP
(HyperText Transfer Protocol)

- Được định nghĩa trong RFC 2616
- Quy định các dạng thông điệp trao đổi giữa web browser và web server
- Mỗi tương tác bao gồm:
  - Yêu cầu từ browser dạng ASCII
  - Đáp ứng từ server dạng tương tự MIME
- Yêu cầu (request) còn gọi là lệnh (command, method) và có đáp ứng (response)

Một số dạng yêu cầu HTTP

Method	Description
GET	Request to read a Web page
HEAD	Request to read a Web page's header
PUT	Request to store a Web page
POST	Append to a named resource (e.g., a Web page)
DELETE	Remove the Web page
TRACE	Echo the incoming request
CONNECT	Reserved for future use
OPTIONS	Query certain options

Đáp ứng HTTP

Bao gồm:

- Dòng trạng thái
- Thông tin (1 phần hay toàn bộ trang web)

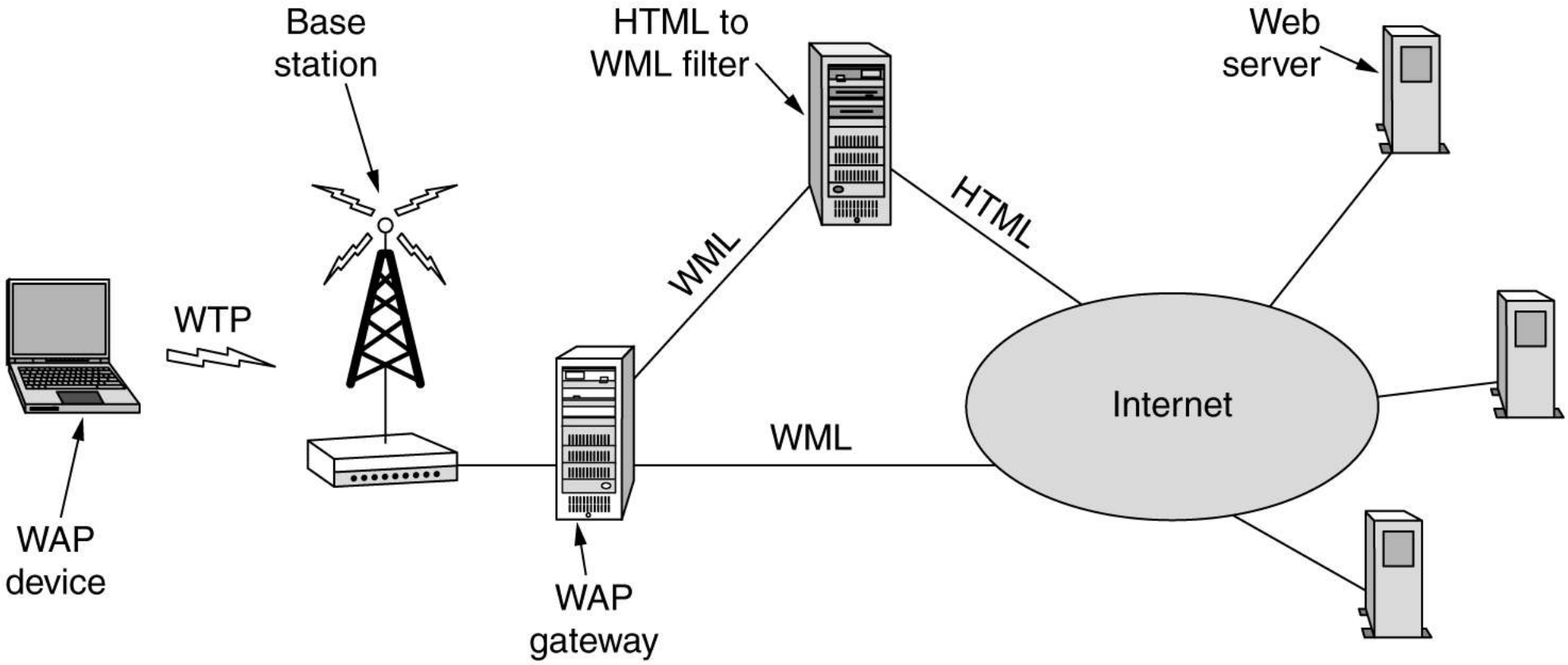
Một số mã trạng thái:

Code	Meaning	Examples
1xx	Information	100 = server agrees to handle client's request
2xx	Success	200 = request succeeded; 204 = no content present
3xx	Redirection	301 = page moved; 304 = cached page still valid
4xx	Client error	403 = forbidden page; 404 = page not found
5xx	Server error	500 = internal server error; 503 = try again later

6. Web không dây (Wireless web)

- Cung cấp dịch vụ truy cập web dạng không dây cho điện thoại di động, PDA (Personal Digital Assistant), máy tính xách tay
- Đặc điểm:
  - Tốc độ truyền thấp
  - Bộ nhớ ít
  - Màn hình kích thước nhỏ
- Tiêu chuẩn thông dụng
  - WAP (Wireless Application Protocol)

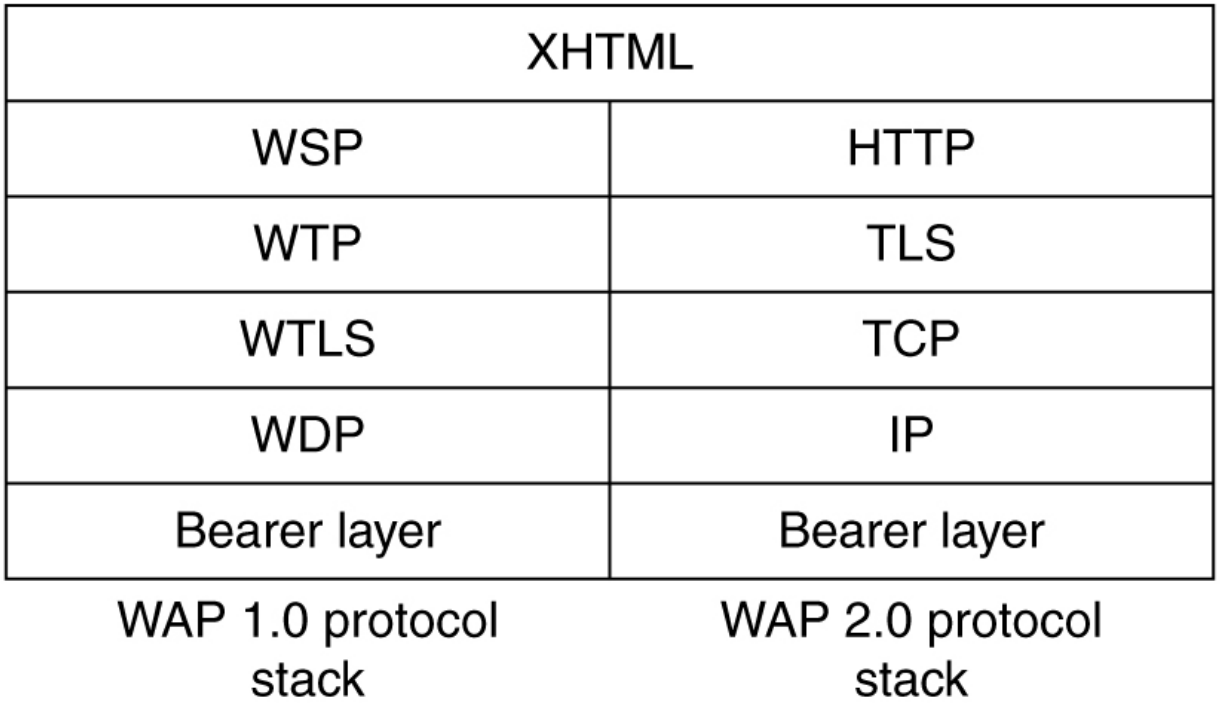
Kiến trúc hệ thống WAP



WTP: Wireless Transaction Protocol

WML: Wireless Markup Language

Bộ giao thức WAP 2.0



WSP: Wireless Session Protocol

WTP: Wireless Transaction Protocol

WTLS: Wireless Transport Layer Security

WDP: Wireless Datagram Protocol

NHẬP MÔN MẠNG MÁY TÍNH

Chương 7

GIỚI THIỆU QUẢN TRỊ MẠNG

VÀ

AN TOÀN THÔNG TIN MẠNG

Nội dung chương 7

I. Giới thiệu về quản trị mạng

II. Giới thiệu về an toàn thông tin mạng

I. Giới thiệu về quản trị mạng

1. Khái niệm
2. Các bước thiết lập mạng cục bộ
3. Ví dụ Windows 2000 Server

1. Khái niệm

- Các loại mạng: WAN, LAN
- Các loại LAN:
  - Peer-to-peer
  - Server-based
  - Dạng tổ hợp
- Quản trị mạng có tính chất động:
  - Quy mô mạng thay đổi
  - Công dụng mạng thay đổi

Công dụng mạng

- Chia sẻ tài nguyên
- Truy xuất có kiểm soát tài nguyên
- Môi trường truyền thông
- Quản lý các hệ thống máy tính tốt hơn

2. Các bước thiết lập mạng cục bộ

a. Lập kế hoạch
b. Hiện thực mạng
c. Quản trị mạng

a. Lập kế hoạch

Các bước lập kế hoạch:

- Thu thập dữ liệu cần thiết
- Khảo sát các khả năng hiện thực
- Chọn giải pháp tốt nhất về giá cả và hiệu suất

Thông số mạng LAN

- Loại mạng
- Kiến trúc mạng
- Môi trường truyền vật lý
- Giao thức mạng
- Phần mềm mạng
- An toàn dữ liệu

b. Hiện thực mạng

- Cài đặt
- Kiểm tra
- Tập huấn, đào tạo

Cài đặt

- Cài đặt phần cứng
- Cài đặt hệ điều hành mạng
  - Hệ điều hành mạng độc lập
  - Phần mềm mạng thêm vào hệ điều hành đã có
- Cài đặt các dịch vụ mạng
- Cài đặt các ứng dụng
  - Ứng dụng mạng dạng multiuser
  - Ứng dụng dùng chung

Kiểm tra

Kiểm tra các thành phần bằng cách cô lập và kiểm tra:

- Các máy tính server
- Các máy tính Client/Workstation
- Các thiết bị ngoại vi
- Môi trường truyền vật lý
- Phần mềm client, phần mềm server

Tập huấn, đào tạo

Mục đích:

- Sử dụng mạng hiệu quả
- Hoạt động ổn định

Đối tượng tập huấn, đào tạo:

- Administrators – Người quản trị
- Users – Người sử dụng

c. Quản trị mạng

- Quản trị user
  - Tạo và duy trì các tài khoản user
- Quản lý tài nguyên
  - Hiện thực, hỗ trợ sử dụng tài nguyên
- Quản lý cấu hình
  - Bảo trì, mở rộng thông tin cấu hình
- Quản trị hiệu suất
  - Kiểm tra hoạt động mạng, tăng hiệu suất
- Bảo trì
  - Ngăn chặn, phát hiện, giải quyết lỗi

3. Ví dụ Windows 2003 Server

a. Các dạng Windows 2003
b. Cài đặt Windows 2003 Server
c. Quản lý users, groups
d. Thiết lập cấu hình các giao thức mạng
e. Thiết lập cấu hình các dịch vụ ứng dụng

a. Các dạng Windows 2003 Server

- Windows Server 2003 Standard Edition
- Windows Server 2003 Enterprise Edition
- Windows Server 2003 Datacenter Edition
- Windows Server 2003 Web Edition

Windows Server 2003 Standard Edition

- Dùng cho doanh nghiệp nhỏ, trung bình
- Hỗ trợ đến 4 CPU, 4GB RAM
- Có thể là File/Print/Web/Application Servers
- Có thể là Domain Controller

Windows Server 2003 Enterprise Edition

- Có các khả năng như bản Standard
- Hỗ trợ đến 8 CPU, 32GB RAM – 32 bit

  Hỗ trợ đến 8 CPU, 64GB RAM – 64 bit
- Hỗ trợ ghép cụm (clustering) 8 nodes

Windows Server 2003 Datacenter Edition

- Phát hành với phần cứng
- Có các khả năng như bản Enterprise
- Hỗ trợ đến 32 CPU, 64GB RAM – 32 bit

  Hỗ trợ đến 32 CPU, 512GB RAM – 64 bit

Windows Server 2003 Web Edition

- Sử dụng cho:
  - Web applications
  - Web pages
  - XML services
- Hỗ trợ ASP.NET, .NET framework
- Hỗ trợ đến 2 CPU, 2GB RAM
- Không có một số chức năng như Domain Controller, Remote Installation Service, DNS services, …

Vai trò của Windows 2003 Server

- Member Server: thành viên của domain, không lưu trữ thông tin directory
- Domain Controller: lưu trữ thông tin domain, cung cấp dịch vụ kiểm chứng
- Stand-alone Server: không tham gia domain, tự kiểm chứng các yêu cầu đăng nhập

b. Cài đặt Windows 2003 Server

Các yêu cầu trước khi cài đặt:

- Yêu cầu về phần cứng, tương thích phần cứng
- Phân vùng đĩa, chọn hệ thống file
- Bản quyền CAL (Client Access License)
  - Per-server: CAL cấp cho server
  - Per-seat: mỗi máy truy xuất Server có CAL
- Chọn vai trò của server

Các dạng cài đặt

- Cài đặt từ các đĩa mềm khởi động
- Cài đặt từ CDROM có thể khởi động
- Cài đặt từ đĩa cứng, từ mạng

c. Quản lý users, groups

- Sử dụng các công cụ Active Directory
- User accounts – User credentials
  - Cho phép user đăng nhập vào máy tính hay đăng nhập vào mạng
- Group account
  - Là tập hợp các user accounts
  - Giúp đơn giản hoá các thao tác quản trị
  - Không thể đăng nhập bằng group account

d. Thiết lập cấu hình các giao thức mạng

Windows 2003 hỗ trợ nhiều bộ giao thức:

- TCP/IP
- IPX/SPX
- Apple Talk

Thiết lập cấu hình TCP/IP

- Đặt địa chỉ IP
  - IP tĩnh
  - IP động
- DHCP Server
- DNS Server, DNS Client

e. Thiết lập cấu hình dịch vụ ứng dụng

- Các dịch vụ ứng dụng mở rộng chức năng của hệ điều hành mạng
- Windows 2003 có các dịch vụ:
  - IIS (Internet Information Services) với Web server, FTP server
  - Terminal service
  - …

II. Giới thiệu về an toàn thông tin mạng

1. Khái niệm
2. Các dạng tấn công
3. Các kỹ thuật an toàn

1. Khái niệm

Sự an toàn (security) liên quan 2 vấn đề:

- Mất dữ liệu
  - Lỗi thiết bị
  - Lỗi phần mềm
  - Lỗi do con người
- Xâm nhập trái phép
  - Truy xuất không hợp lệ
  - Giả mạo
  - .....

Các mục tiêu của an toàn mạng

- Tính bí mật – Confidentiality
  - Bảo vệ dữ liệu trước các truy xuất không hợp lệ
- Tính toàn vẹn – Integrity
  - Không thay đổi hay mất dữ liệu do truy xuất không hợp lệ
- Tính sẵn sàng – Availability
  - Hệ thống hoạt động liên tục

2. Các dạng tấn công

a. Các nhược điểm về an toàn (Vulnerability / Weaknesses)
b. Một số dạng tấn công

a. Các nhược điểm về an toàn

- Nhược điểm công nghệ
  - Bộ giao thức TCP/IP không an toàn
  - Các hệ điều hành không hoàn thiện
  - Các thiết bị mạng như router, firewall, … không tuyệt đối an toàn
- Nhược điểm về cấu hình
  - Administrator thiết lập cấu hình mạng không an toàn
- Nhược điểm trong quản trị, sử dụng mạng

b. Một số dạng tấn công

- Reconnaissance – Do thám
  - Thu thập thông tin hệ thống bất hợp lệ
- Eavesdropping – Nghe trộm
  - Nghe trộm dữ liệu trên mạng phục vụ các dạng tấn công khác
- Password Attacks
  - Truy xuất tài nguyên không được phép (vì không có password hợp lệ)

Một số dạng tấn công (tt)

- Masquerade/IP spoofing
  - Giả dạng user hợp lệ
- Back doors
  - Tạo đường vào hệ thống không hợp lệ phục vụ các dạng tấn công khác
- Session replay
  - Lưu chuỗi packet hay chuỗi lệnh ứng dụng và sử dụng lại để truy xuất không hợp lệ

Một số dạng tấn công (tt)

- Denial of Service (DoS)
  - Ngăn cản người sử dụng hợp lệ bằng cách tiêu thụ tất cả tài nguyên hệ thống
  - Ví dụ: Ping of death, SYN flood, E-mail bombs, malicious applets, …
- Distributed Denial of Service (DDoS)
  - Làm nghẽn mạch đường truyền bằng các thông tin giả mạo
- ……

3. Các kỹ thuật an toàn

- An toàn mạng là công việc thường xuyên thực hiện dựa trên các chính sách an toàn
- Các kỹ thuật liên quan phần cứng
  - An toàn vật lý cho thiết bị
  - Dùng thiết bị dự phòng (RAID, Mirror, …)
  - Dùng các máy trạm không đĩa (diskless workstation)
- Các kỹ thuật cơ sở cho giải pháp phần mềm
  - Mã hoá dữ liệu (data encryption)
  - Kiểm chứng (authentication)

Các giai đoạn trong chính sách an toàn

- Bảo vệ hệ thống – Secure
  - Kiểm chứng, cấp quyền truy xuất
  - Firewalls
  - Sửa chữa các nhược điểm
- Giám sát hệ thống – Monitor
  - Phát hiện các xâm nhập không hợp lệ
- Kiểm tra hoạt động – Test
- Cải tiến các kỹ thuật bảo vệ hệ thống – Improve