

BÀI GIẢNG
MÔN: MẠNG MÁY TÍNH

Biên soạn: Vũ Quốc Oai

GIỚI THIỆU MÔN HỌC

- Mục đích của môn học
 - Kiến thức cơ bản về mạng máy tính
 - Mô hình tham khảo OSI
 - Mô hình TCP/IP
- Thời lượng: 5 buổi học

GIỚI THIỆU MÔN HỌC

- Nội dung môn học
 - Chương 1: Tổng quan về mạng máy tính
 - Chương 2: Cấu trúc của mạng
 - Chương 3: Phương tiện truyền dẫn và thiết bị mạng
 - Chương 4: Data link
 - Chương 5: TCP/IP
 - Chương 6: Khái niệm cơ bản về bảo mật mạng
 - Bài tập

CHƯƠNG 1: TỔNG QUAN VỀ MẠNG MÁY TÍNH

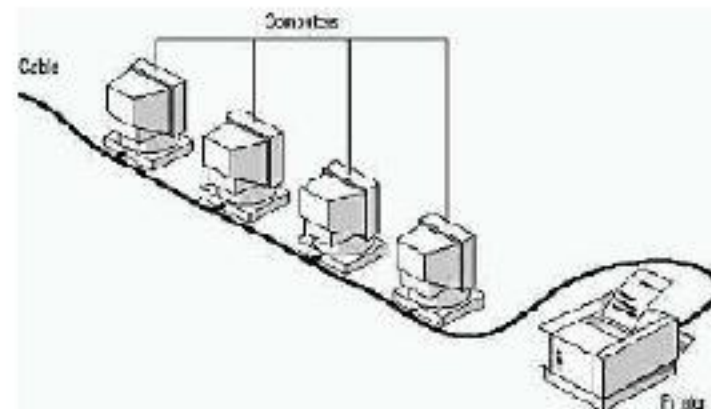
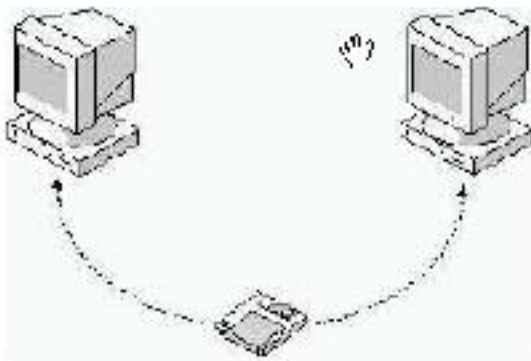
- Khái niệm về mạng máy tính
- Ứng dụng của mạng máy tính
- Phân loại mạng máy tính
- Mô hình OSI

Khái niệm về mạng máy tính

- Một tập hợp của các máy tính độc lập được kết nối bằng một cấu trúc nào đó.
- Hai máy tính được gọi là kết nối nếu chúng có thể trao đổi thông tin.
- Kết nối có thể là dây đồng, cáp quang, sóng ngắn, sóng hồng ngoại, truyền vệ tinh...

Ứng dụng của mạng máy tính

- Chia sẻ thông tin
- Chia sẻ phần cứng và phần mềm
- Quản lý tập trung

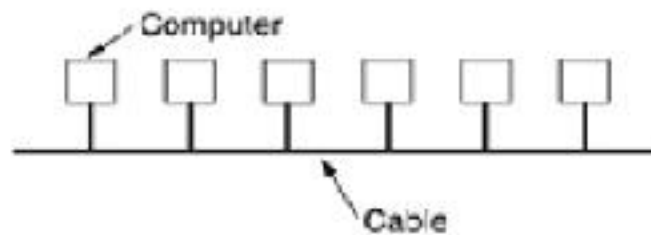


Phân loại mạng máy tính

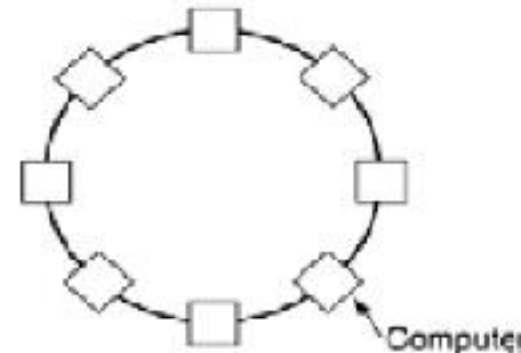
- Cách phân loại mạng máy tính được sử dụng phổ biến nhất là dựa theo khoảng cách địa lý của mạng: Lan, Man, Wan.
- Theo kỹ thuật chuyển mạch mà mạng áp dụng: mạng chuyển mạch kênh, mạng chuyển mạch thông báo, mạng chuyển mạch gói.
- Theo cấu trúc mạng: hình sao, hình tròn, tuyến tính...
- Theo hệ điều hành mà mạng sử dụng: Windows, Unix, Novell...

LANs (Local Area Networks)

- Có giới hạn về địa lý
- Tốc độ truyền dữ liệu cao
- Tỷ lệ lỗi khi truyền thấp
- Do một tổ chức quản lý
- Sử dụng kỹ thuật Ethernet hoặc Token Ring
- Các thiết bị thường dùng trong mạng là Repeater, Bridge, Hub, Switch, Router.

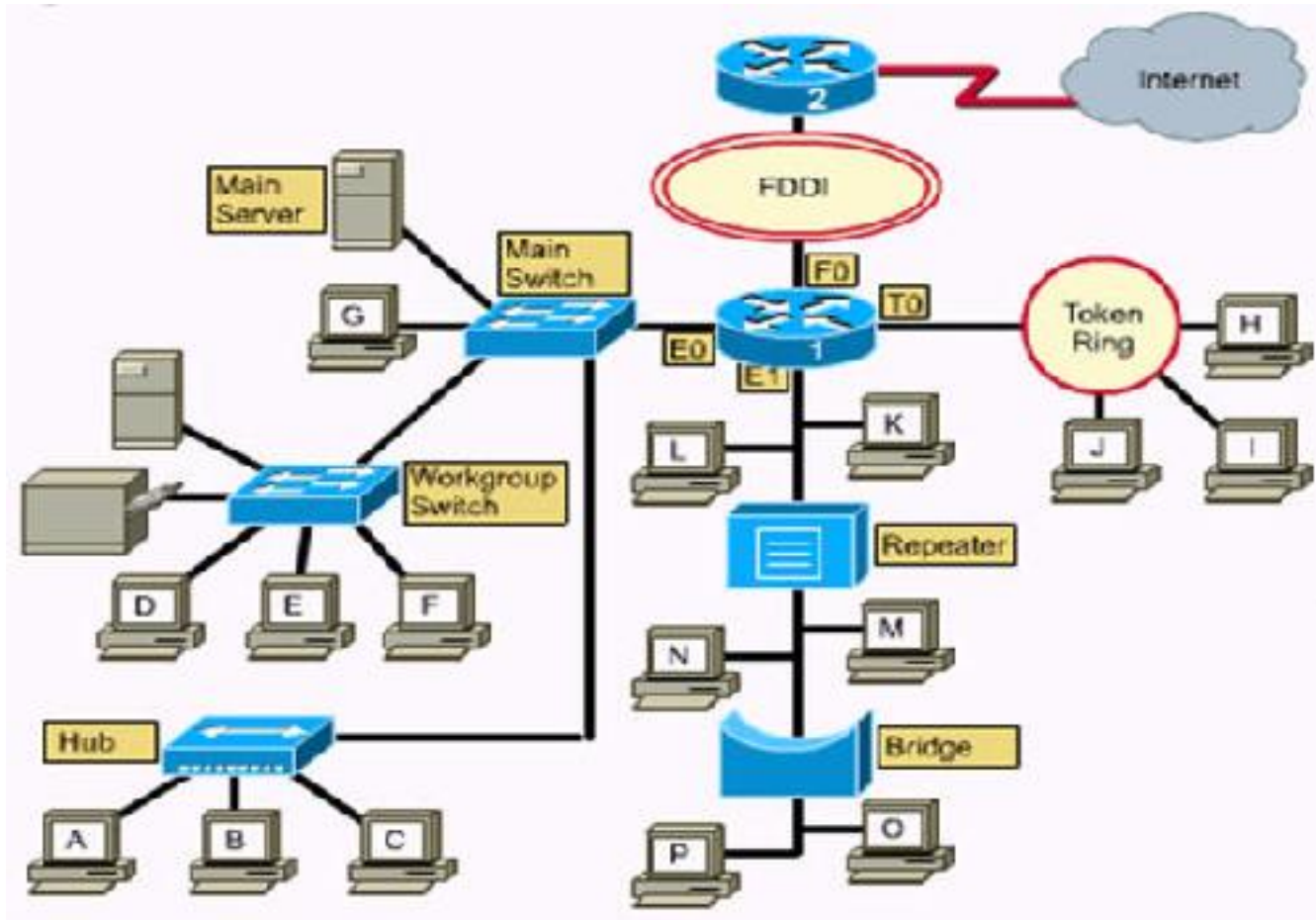


802.3 Ethernet



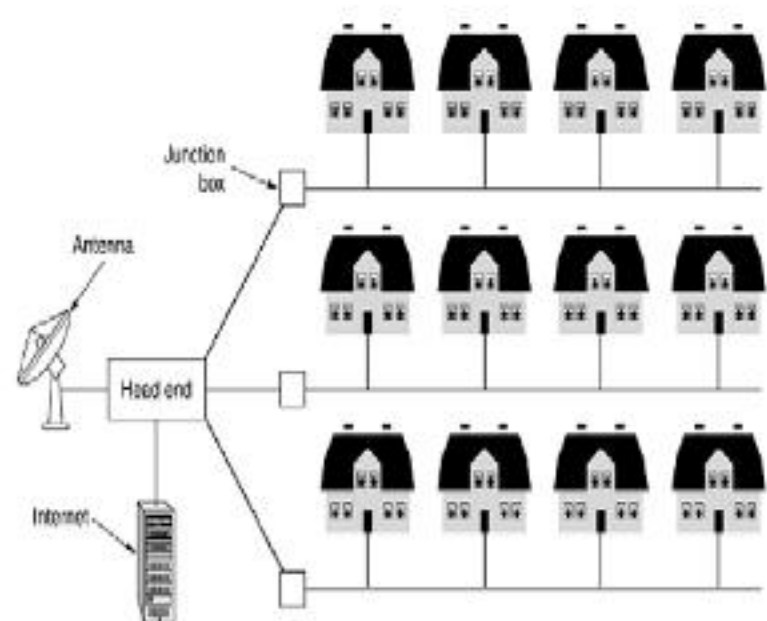
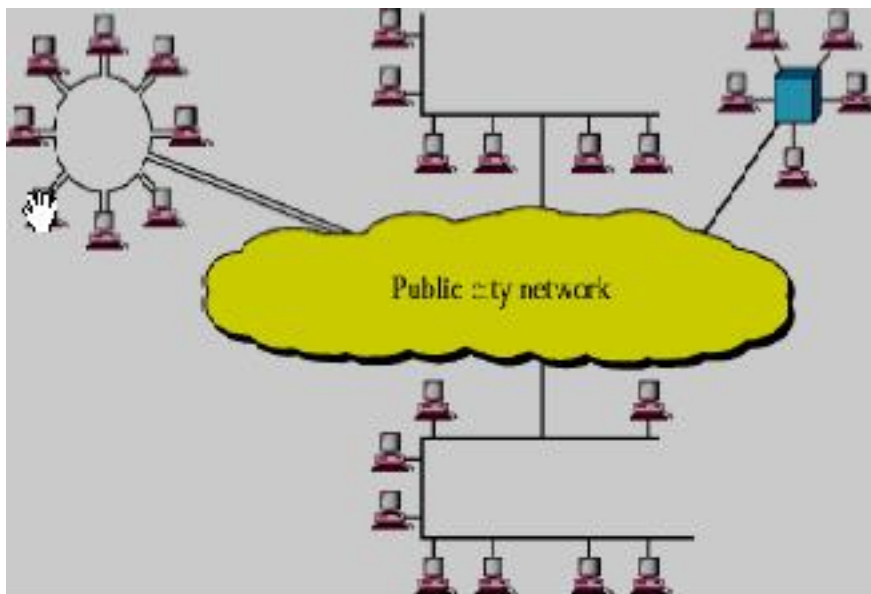
802.5 Token Ring

LANs



MANs (Metropolitan Area Networks)

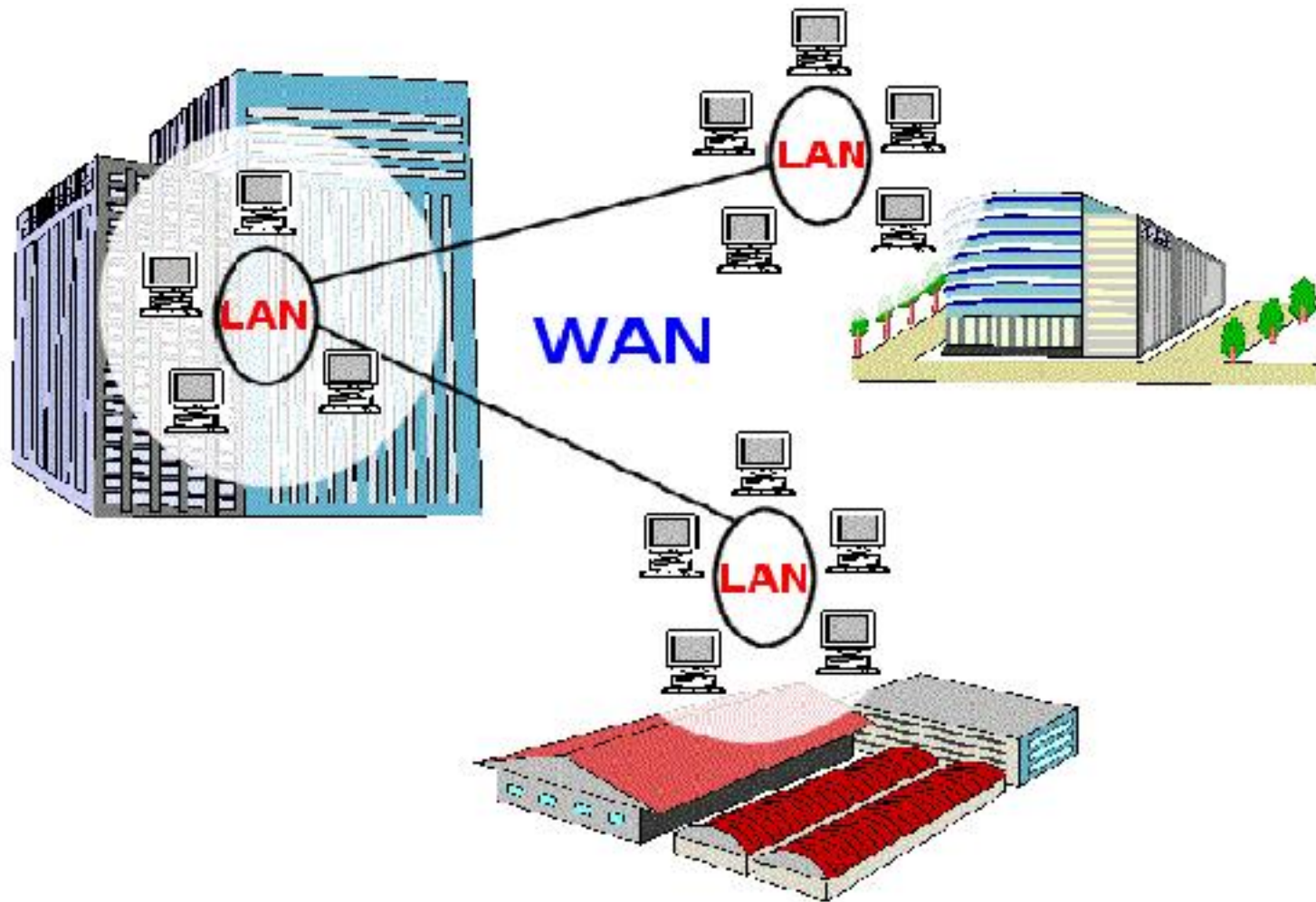
- Có kích thước vùng địa lý lớn hơn LAN
- Do một tổ chức quản lý
- Thường dùng cáp đồng trục hoặc cáp quang



WANs (Wide Area Networks)

- Là sự kết nối nhiều LAN
- Không có giới hạn về địa lý
- Tốc độ truyền dữ liệu thấp
- Do nhiều tổ chức quản lý
- Sử dụng các kỹ thuật Modem, ISDN, DSL, Frame Relay, ATM

WANs (Wide Area Networks)



Mạng không dây (Wireless Networking)

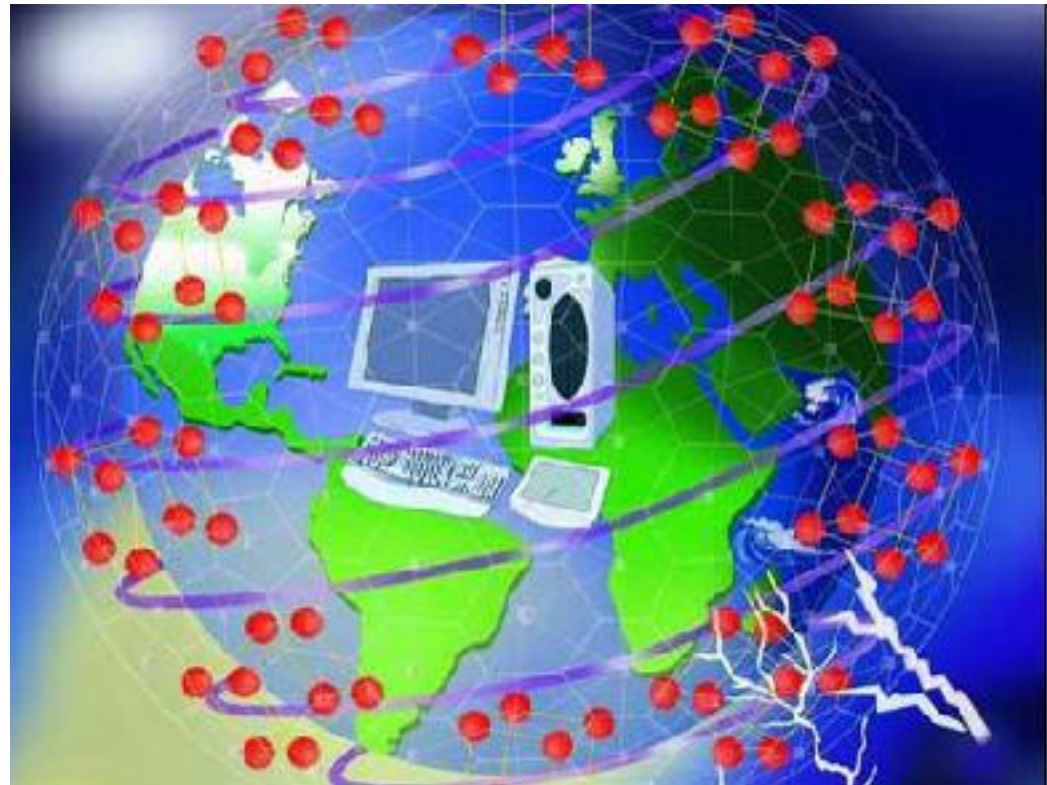
- Do tổ chức IEEE xây dựng và được tổ chức Wi-fi Alliance đưa vào sử dụng trên toàn thế giới.
- Có các tiêu chuẩn: chuẩn 802.11a, chuẩn 802.11b, chuẩn 802.11g (sử dụng phổ biến ở thị trường Việt Nam), chuẩn 802.11n (mới có).
- Thiết bị cho mạng không dây gồm 2 loại: card mạng không dây và bộ tiếp sóng/điểm truy cập (Access Point - AP).

Mạng không dây



Internet

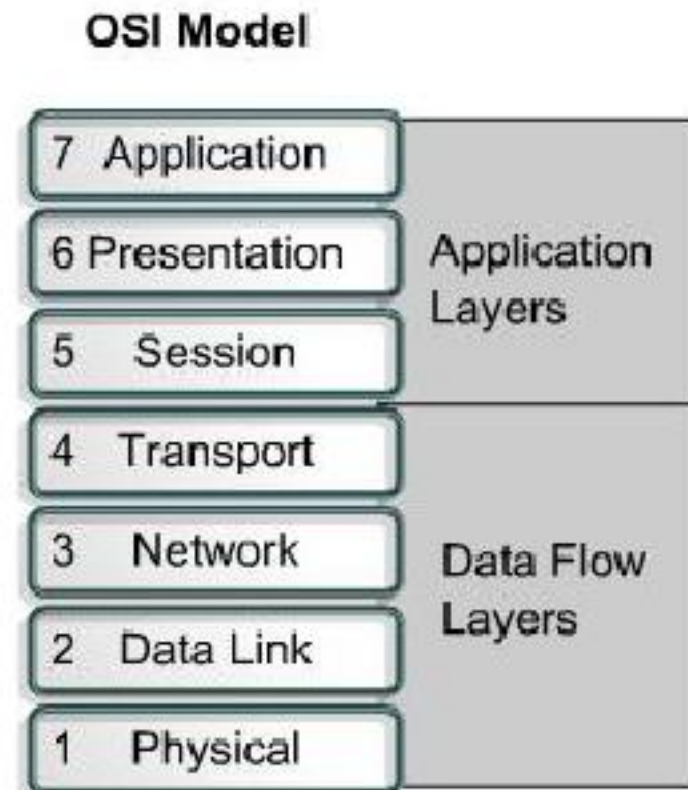
Một hệ thống mạng của các máy tính được kết nối với nhau qua hệ thống viễn thông trên phạm vi toàn thế giới để trao đổi thông tin.



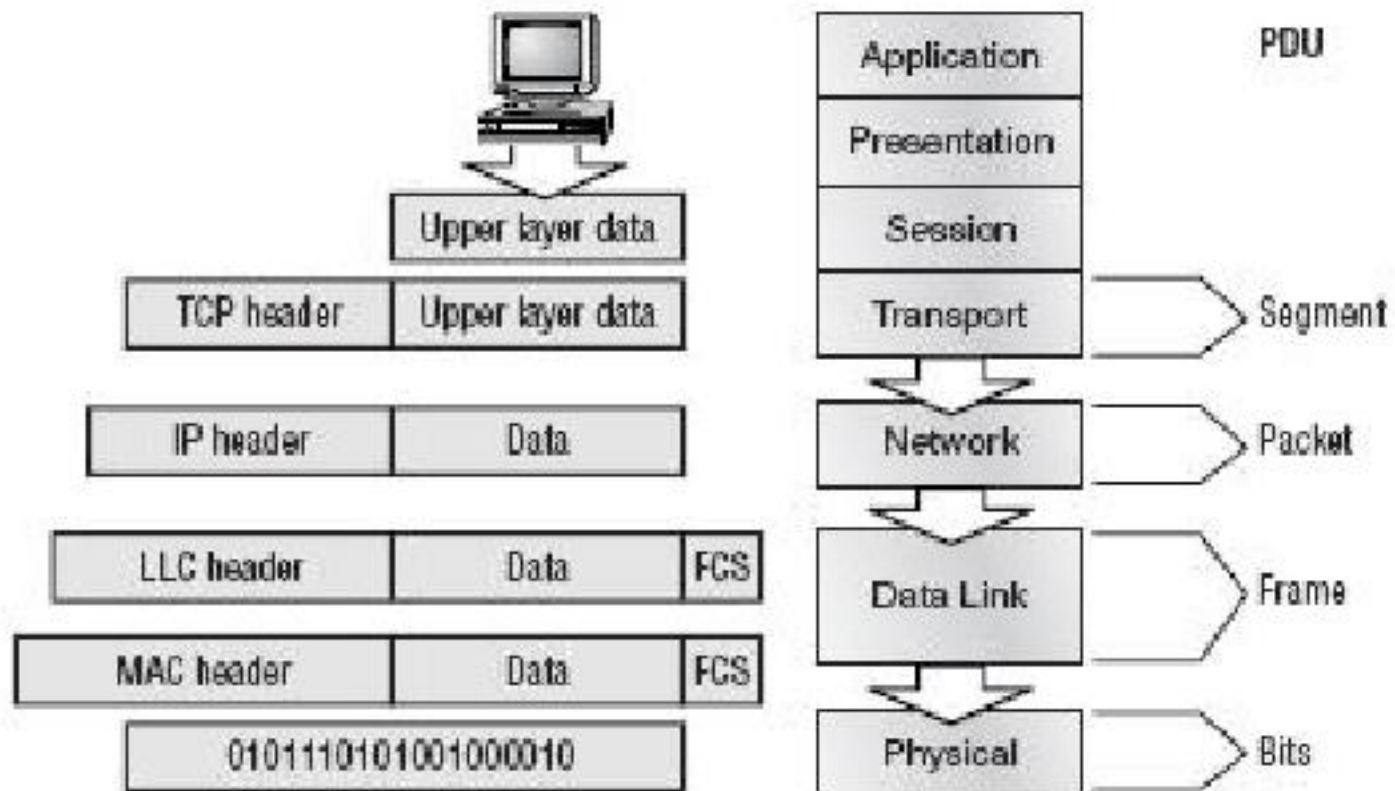
Mô hình OSI

(Open Systems Interconnection)

- Lý do hình thành: Sự gia tăng mạnh mẽ về số lượng và kích thước mạng dẫn đến hiện tượng bất tương thích giữa các mạng.
- Ưu điểm của mô hình OSI:
 - Giảm độ phức tạp
 - Chuẩn hóa các giao tiếp
 - Đảm bảo liên kết hoạt động
 - Đơn giản việc dạy và học

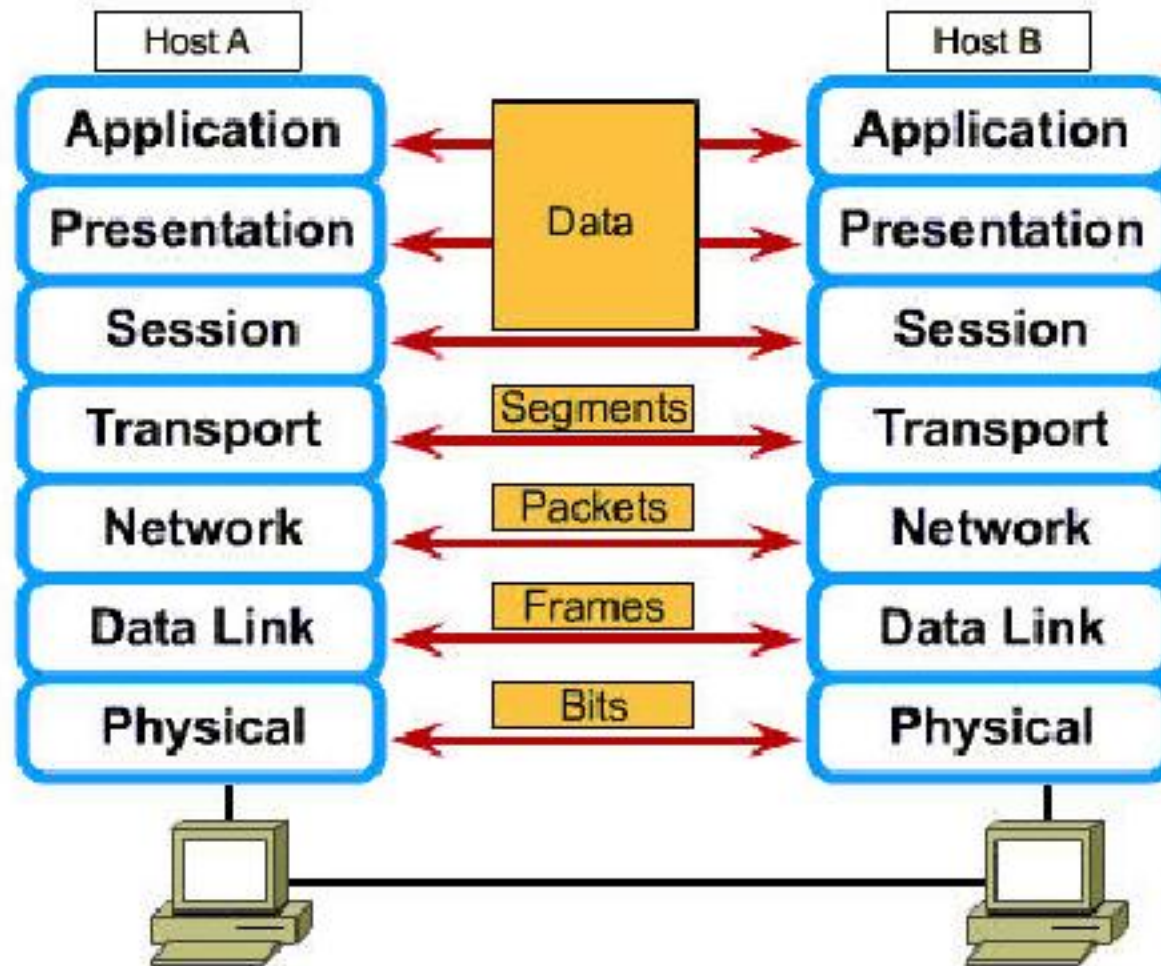


Mô hình OSI

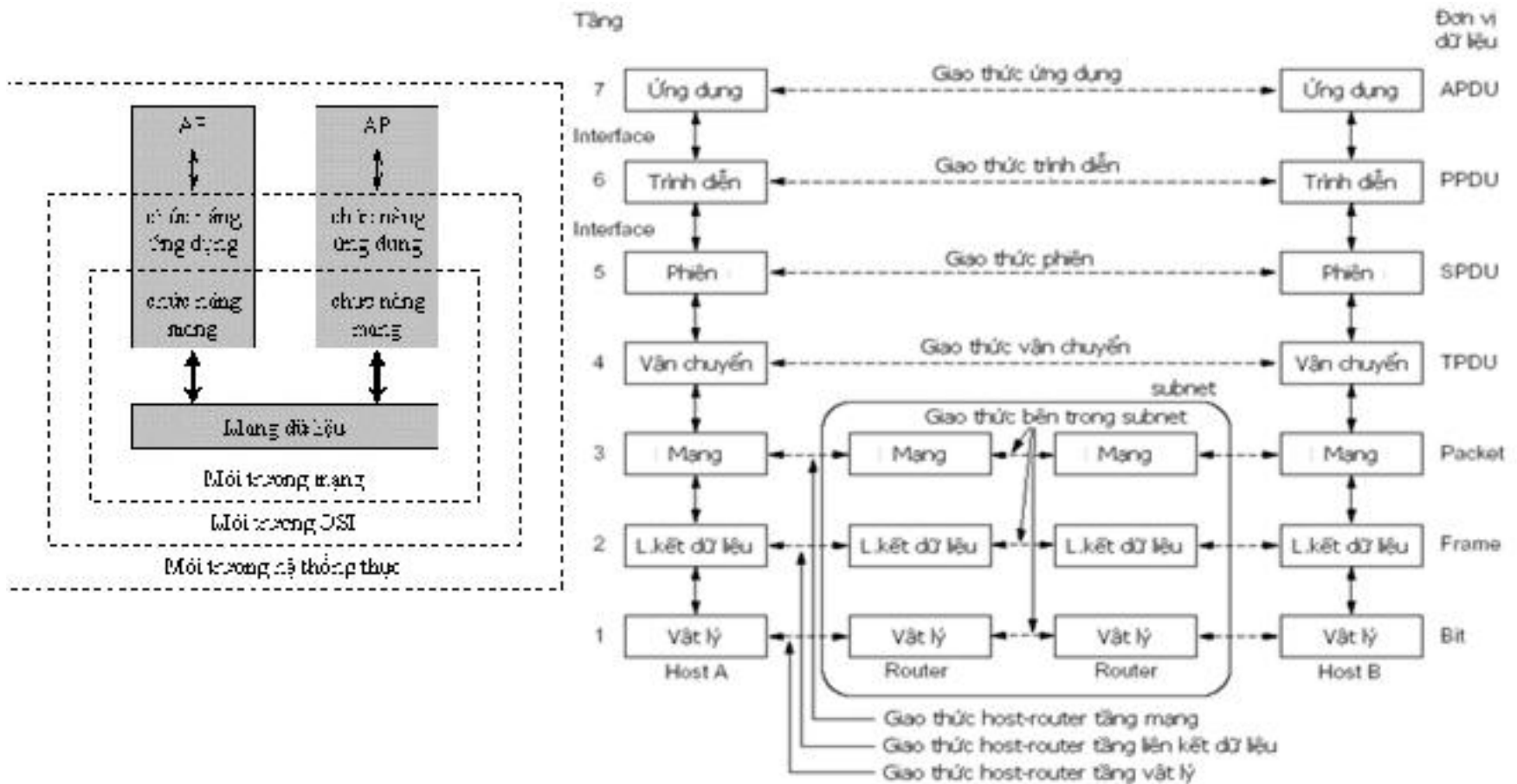


Đóng gói dữ liệu trên mạng

Mô hình OSI



Mô hình OSI



Mô hình OSI



Truyền dẫn nhị phân

- Dây, đầu nối, điện áp
- Tốc độ truyền dữ liệu
- Phương tiện truyền dẫn
- Chế độ truyền dẫn (simplex, half-duplex, full-duplex)

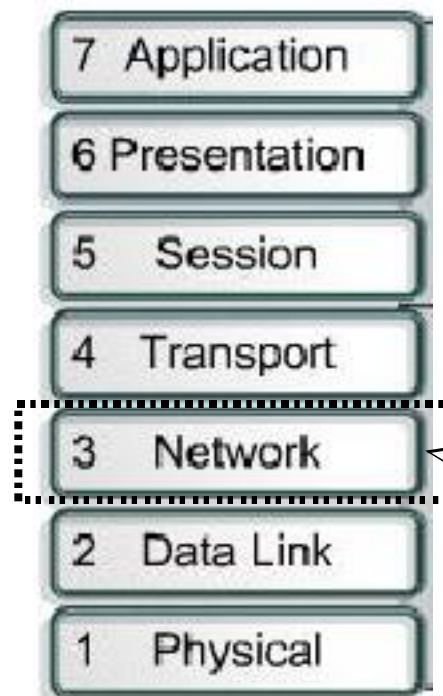
Mô hình OSI



Điều khiển liên kết, truy xuất đường truyền

- Đóng Frame
- Ghi địa chỉ vật lý
- Điều khiển luồng
- Kiểm soát lỗi, thông báo lỗi

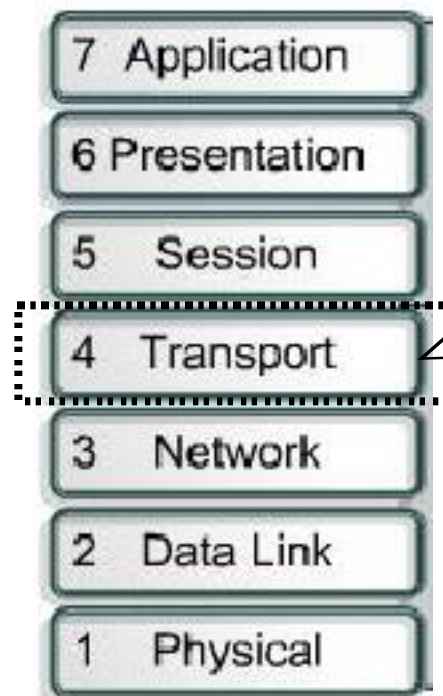
Mô hình OSI



Địa chỉ mạng và xác định đường đi tốt nhất

- Tin cậy
- Địa chỉ luận lý, topo mạng
- Định tuyến (tìm đường đi) cho gói tin

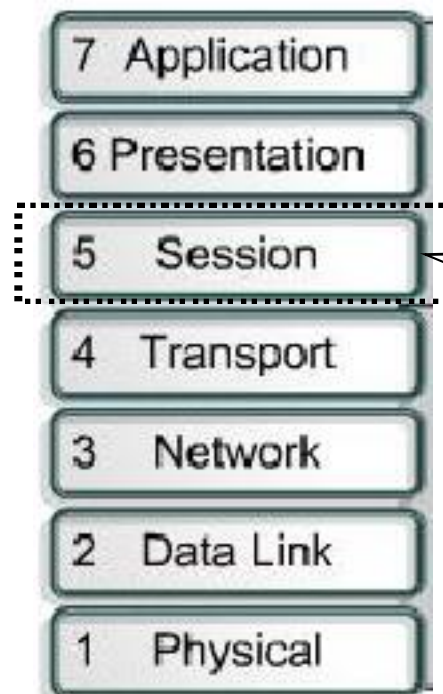
Mô hình OSI



Kết nối end-to-end

- Vận chuyển giữa các host
- Vận chuyển tin cậy
- Thiết lập, duy trì, kết nối các mạch ảo
- Phát hiện lỗi, phục hồi thông tin và điều khiển luồng

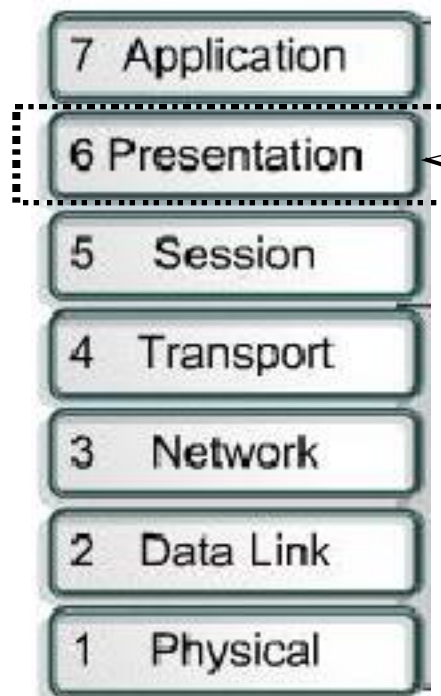
Mô hình OSI



Truyền thông liên host

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

Mô hình OSI



Trình bày dữ liệu

- Định dạng dữ liệu
- Cấu trúc dữ liệu
- Mã hóa
- Nén dữ liệu

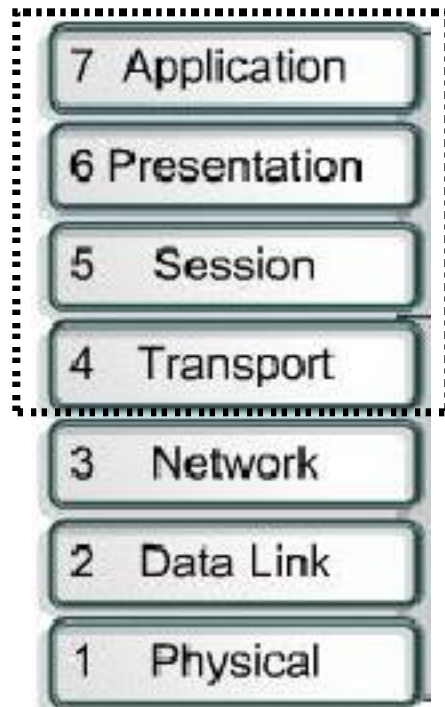
Mô hình OSI



Các quá trình mạng của ứng dụng

- Xác định giao diện giữa người sử dụng và môi trường OSI
- Cung cấp các dịch vụ mạng cho các ứng dụng như email, truyền file...

Mô hình OSI



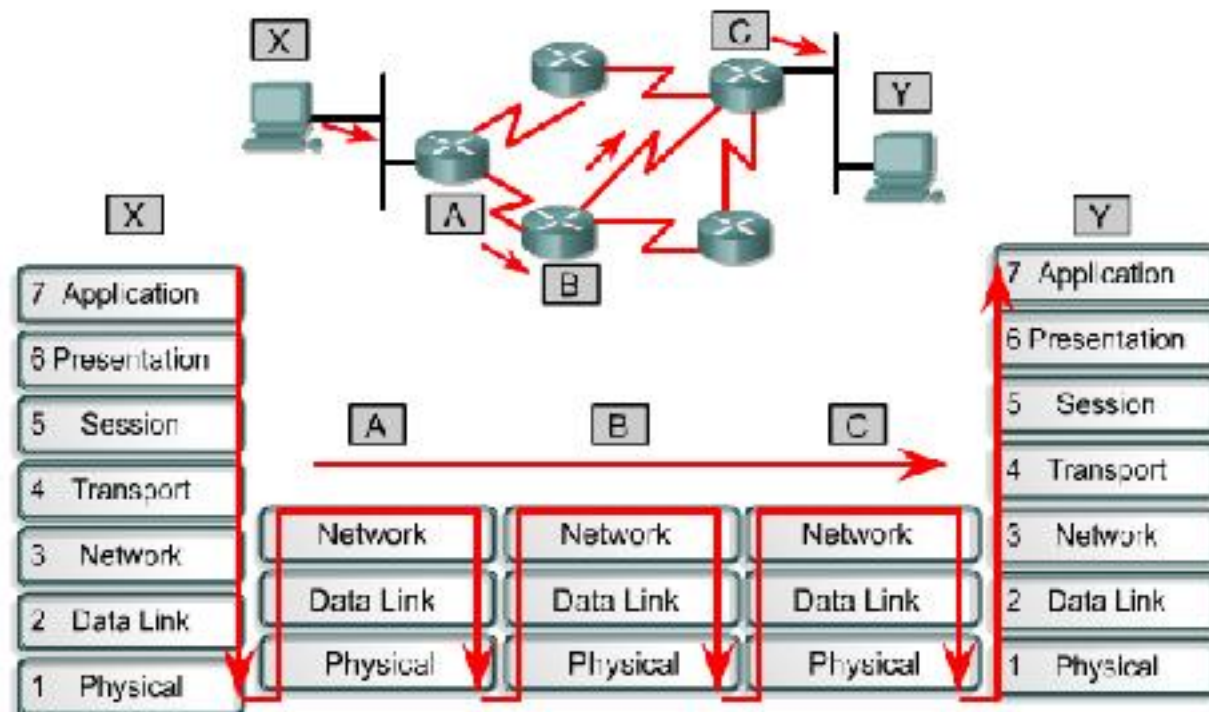
Những lớp này chỉ tồn tại trong máy tính nguồn và máy tính đích

Mô hình OSI



Những lớp này quản lý thông tin di chuyển trong mạng LAN hoặc WAN giữa máy tính nguồn và máy tính đích

Dòng dữ liệu trên mạng



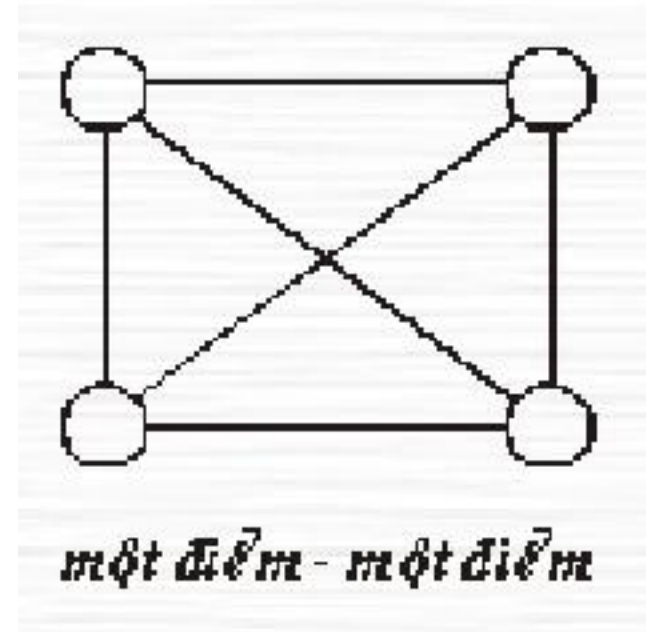
Data flow in a network focuses on layers one, two and three of the OSI model. This is after being transmitted by the sending host and before arriving at the receiving host.

CHƯƠNG 2: CẤU TRÚC MẠNG (TOPOLOGY)

- Phương thức nối mạng
- Cấu trúc vật lý của mạng
- Giao thức truy cập đường truyền trên mạng LAN

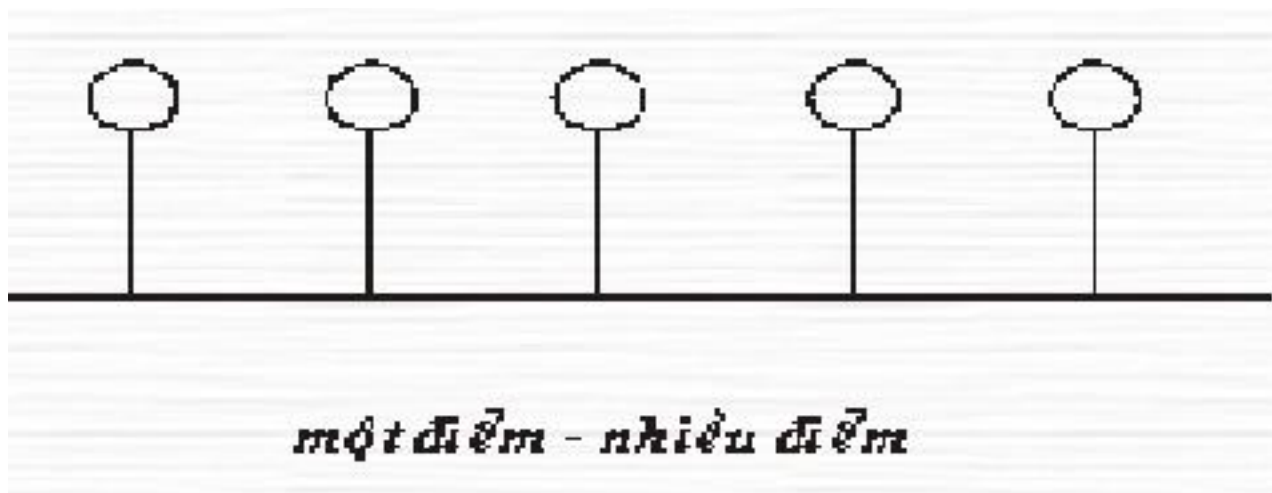
Phương thức nối mạng

- Point-to-point (điểm – điểm): các đường truyền riêng biệt được thiết lập để nối các cặp máy tính lại với nhau.

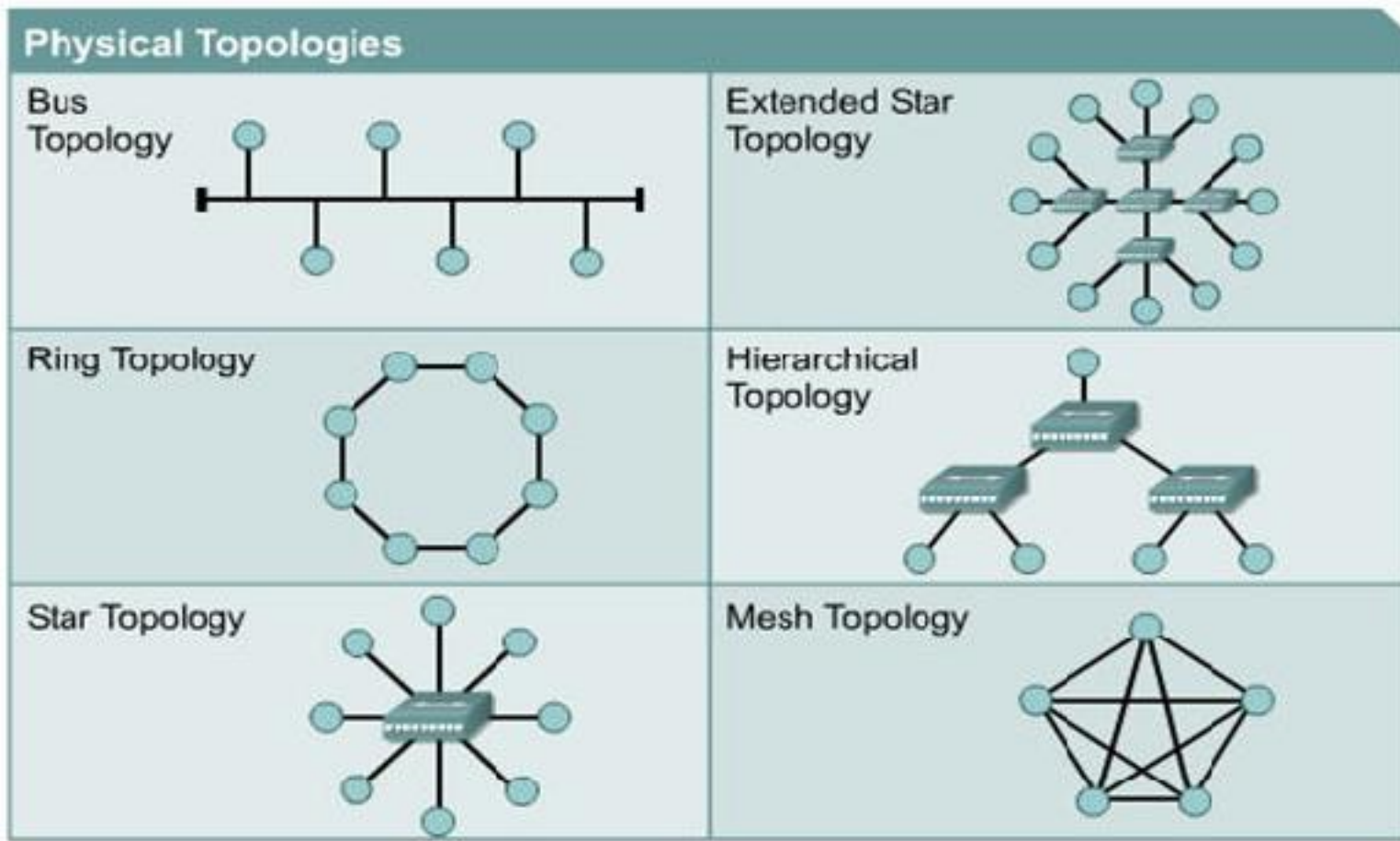


Phương thức nối mạng

- Broadcast (một điểm - nhiều điểm): tất cả các trạm phân chia chung một đường truyền vật lý.

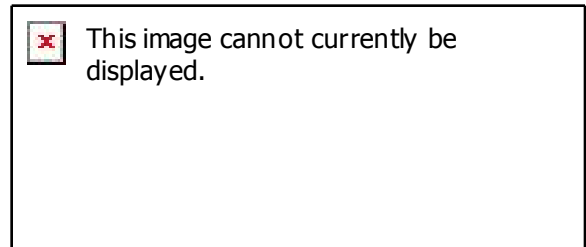
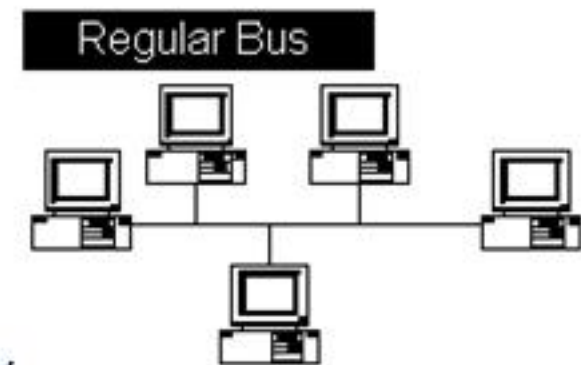


Cấu trúc vật lý của mạng LAN



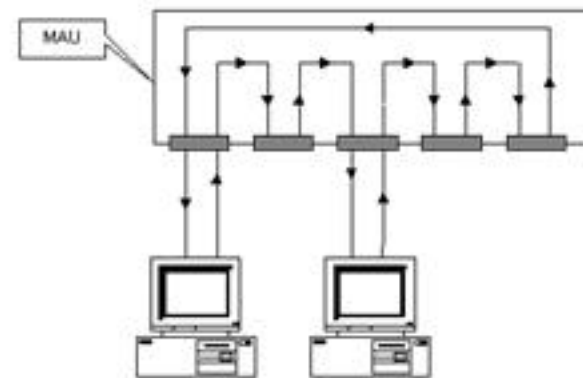
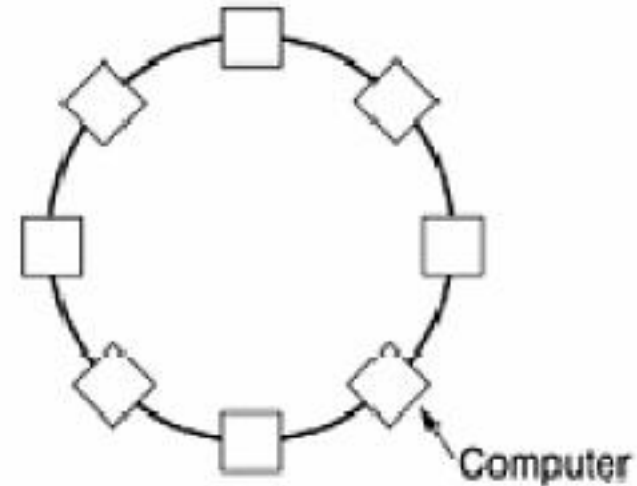
Dạng đường thẳng (Bus Topology)

- Ưu điểm
 - Dễ dàng cài đặt và mở rộng
 - Chi phí thấp
 - Một máy hỏng không ảnh hưởng đến các máy khác.
- Hạn chế
 - Khó quản trị và tìm nguyên nhân lỗi
 - Giới hạn chiều dài cáp và số lượng máy tính
 - Hiệu năng giảm khi có máy tính được thêm vào
 - Một đoạn cáp backbone bị đứt sẽ ảnh hưởng đến toàn mạng



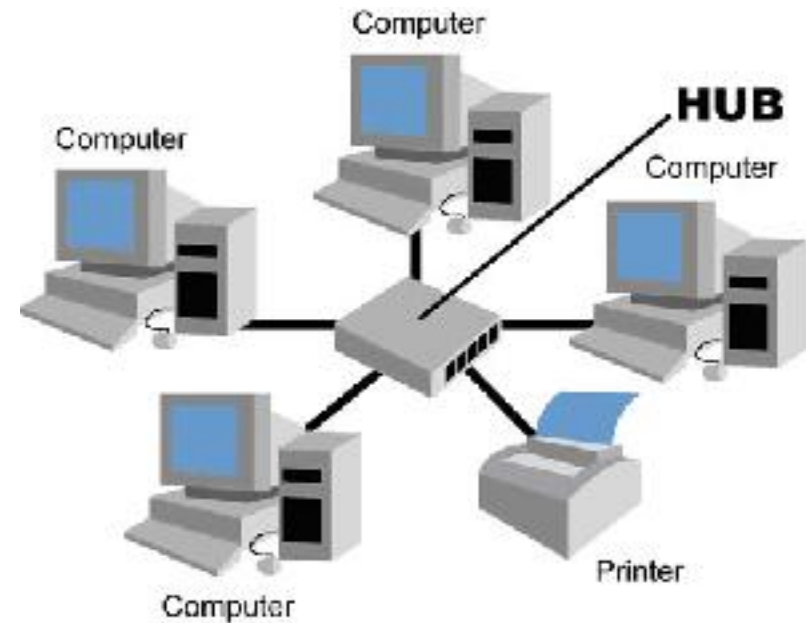
Dạng vòng tròn (Ring Topology)

- Ưu điểm
 - Sự phát triển của hệ thống không tác động đáng kể đến hiệu năng
 - Tất cả các máy tính có quyền truy cập như nhau
- Hạn chế
 - Chi phí thực hiện cao
 - Phức tạp
 - Khi một máy có sự cố thì có thể ảnh hưởng đến các máy tính khác



Dạng hình sao (Star Topology)

- Ưu điểm
 - Dễ dàng bổ sung hay loại bỏ bớt máy tính
 - Dễ dàng theo dõi và giải quyết sự cố
 - Có thể phù hợp với nhiều loại cáp khác nhau
- Hạn chế
 - Khi hub không làm việc, toàn mạng cũng sẽ không làm việc
 - Sử dụng nhiều cáp



Giao thức truy cập đường truyền trên mạng LAN

Hai loại giao thức: ngẫu nhiên và có điều khiển

– Ngẫu nhiên

- Giao thức chuyển mạch
- Giao thức đường dây đa truy cập với cảm nhận va chạm

– Có điều khiển

- Giao thức dùng thẻ bài vòng (Token Ring)
- Giao thức dùng thẻ bài cho dạng đường thẳng (Token Bus)

Giao thức truy cập đường truyền trên mạng LAN

- Giao thức chuyển mạch (yêu cầu và chấp nhận)
Khi máy tính yêu cầu, nó sẽ được thêm nhập vào đường cáp nếu mạng không bận, ngược lại sẽ bị từ chối.

Giao thức truy cập đường truyền trên mạng LAN

- Giao thức đường dây đa truy cập với cảm nhận va chạm (Carrier Sense Multiple Access/with Collision Detection)
 - Gói dữ liệu chỉ được gửi nếu đường truyền rảnh, ngược lại mỗi trạm phải đợi theo một trong 3 phương thức:
 - Chờ đợi một thời gian ngẫu nhiên rồi lại bắt đầu kiểm tra đường truyền
 - Kiểm tra đường truyền liên tục cho đến khi đường truyền rảnh
 - Kiểm tra đường truyền với xác suất p ($0 < p < 1$)

Giao thức truy cập đường truyền trên mạng LAN

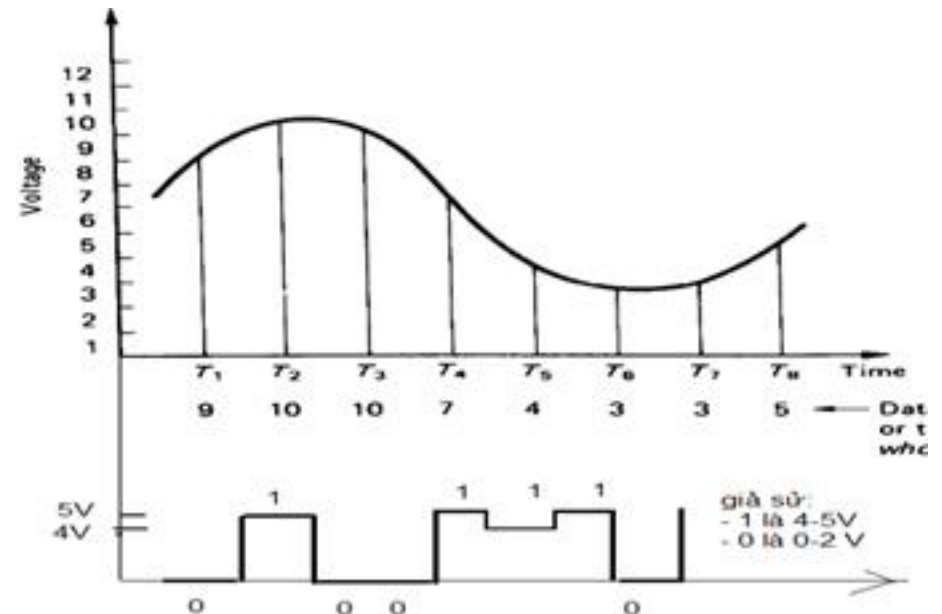
- Giao thức dùng thẻ bài vòng (Token Ring)
 - Thẻ bài là một đơn vị dữ liệu đặc biệt có một bit biểu diễn trạng thái bận hoặc rảnh.
 - Thẻ bài chạy vòng quanh trong mạng.
 - Trạm nào nhận được thẻ bài rảnh thì có thể truyền dữ liệu.
- Giao thức dùng thẻ bài cho dạng đường thẳng (Token bus)
 - Tạo ra một vòng logic (vòng ảo) và thực hiện giống Token Ring.

CHƯƠNG 3: PHƯƠNG TIỆN TRUYỀN DẪN VÀ CÁC THIẾT BỊ LIÊN KẾT MẠNG

- Môi trường truyền dẫn
- Phương tiện truyền dẫn
- Các thiết bị liên kết mạng

Môi trường truyền dẫn

- Là phương tiện vật lý cho phép truyền tải tín hiệu giữa các thiết bị.
- Hai loại phương tiện truyền dẫn chính:
 - Hữu tuyến
 - Vô tuyến
- Hệ thống sử dụng hai loại tín hiệu:
 - Digital
 - Analog



Các đặc tính của phương tiện truyền dẫn

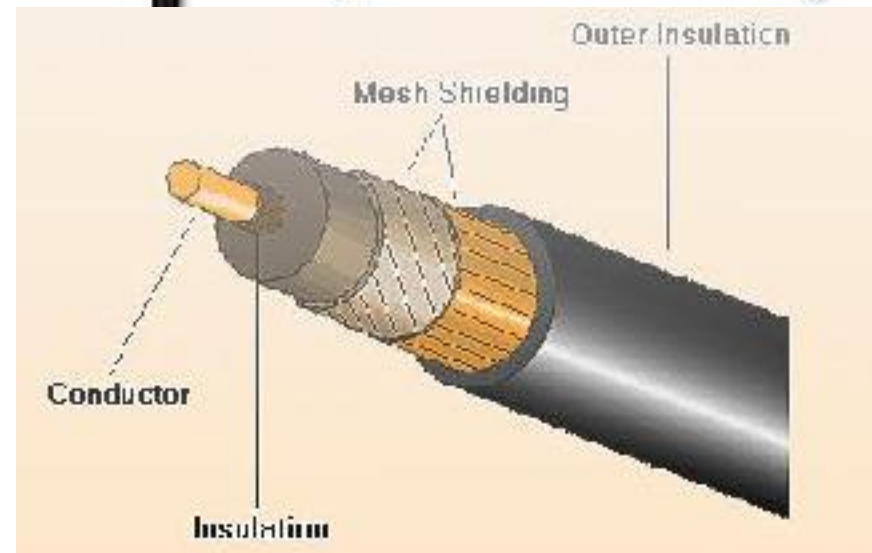
- Chi phí
- Yêu cầu cài đặt
- Băng thông (bandwidth).
- Băng tần (baseband, broadband)
- Độ suy dần (attenuation).
- Nhiễu điện từ (Electromagnetic Interference - EMI)
- Nhiễu xuyên kênh (crosstalk)

Phương tiện truyền dẫn

- Cáp đồng trục
- Cáp xoắn đôi
- Cáp quang
- Wireless

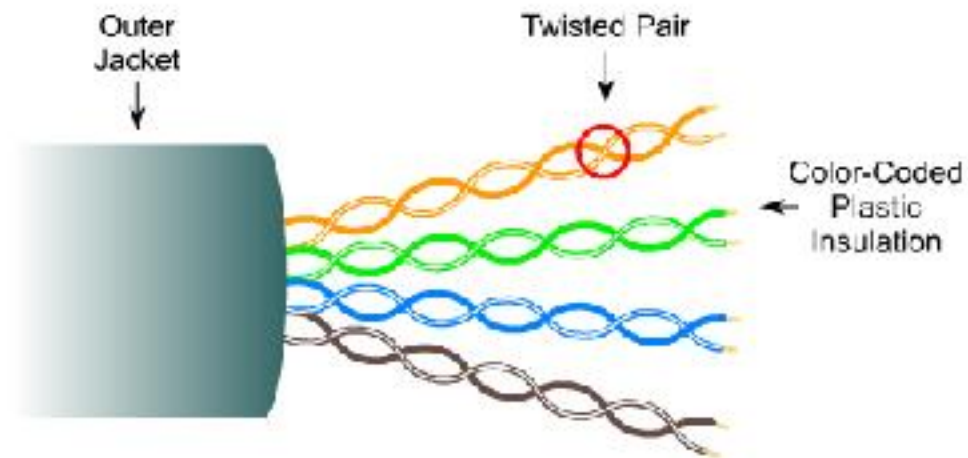
Cáp đồng trục (coaxial)

- Cấu tạo
- Phân loại
 - Thinnet/Thicknet
 - Baseband/
Broadband
- Thông số kỹ thuật
 - Chiều dài cáp
 - Tốc độ truyền
 - Nhiễu
 - Lắp đặt/bảo trì
 - Giá thành
 - Kết nối



Cáp xoắn đôi

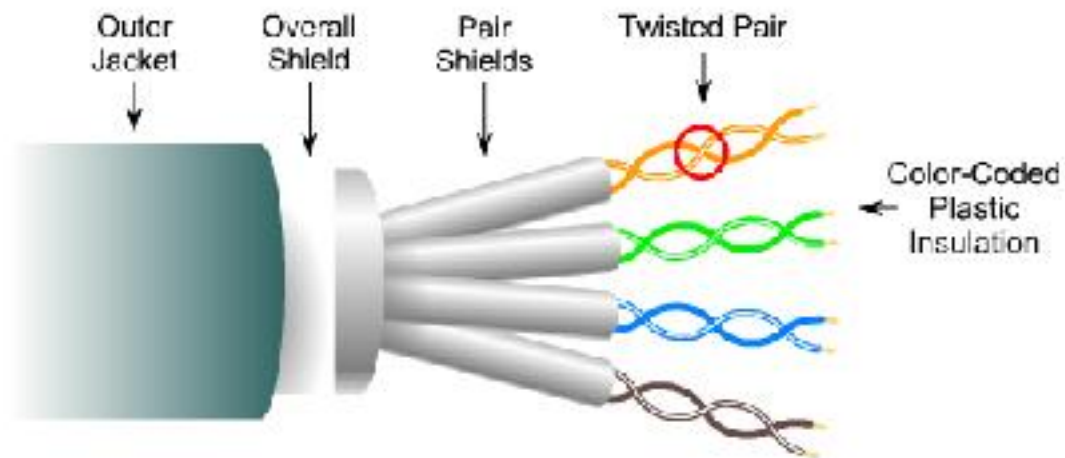
Unshielded Twisted Pair (UTP) Cable



- Speed and throughput: 10 - 100 - 1000 Mbps (depending on the quality/category of cable)
- Average \$ per node: Least Expensive
- Media and connector size: Small
- Maximum cable length: 100m

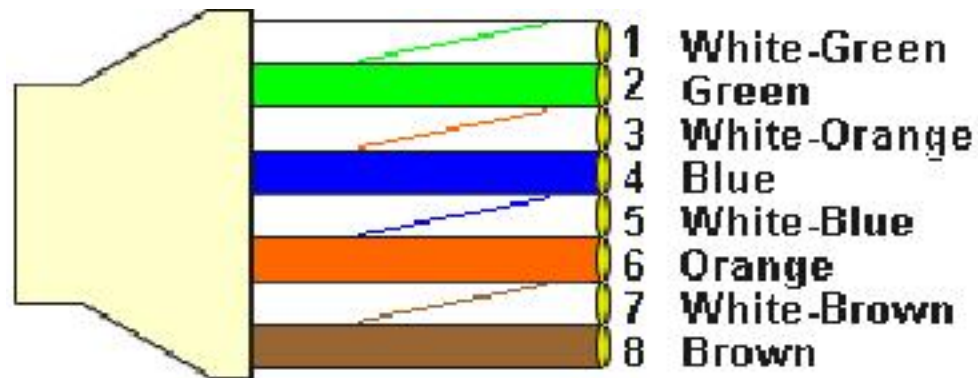
Cáp xoắn đôi

Shielded Twisted Pair (STP) Cable

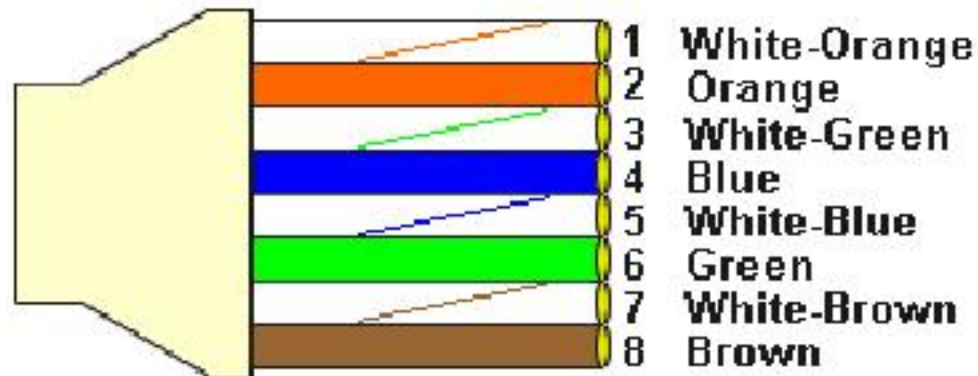


- Speed and throughput: 10 - 100 Mbps
- Average \$ per node: Moderately Expensive
- Media and connector size: Medium to Large
- Maximum cable length: 100m

Chuẩn cáp 568A & 568B

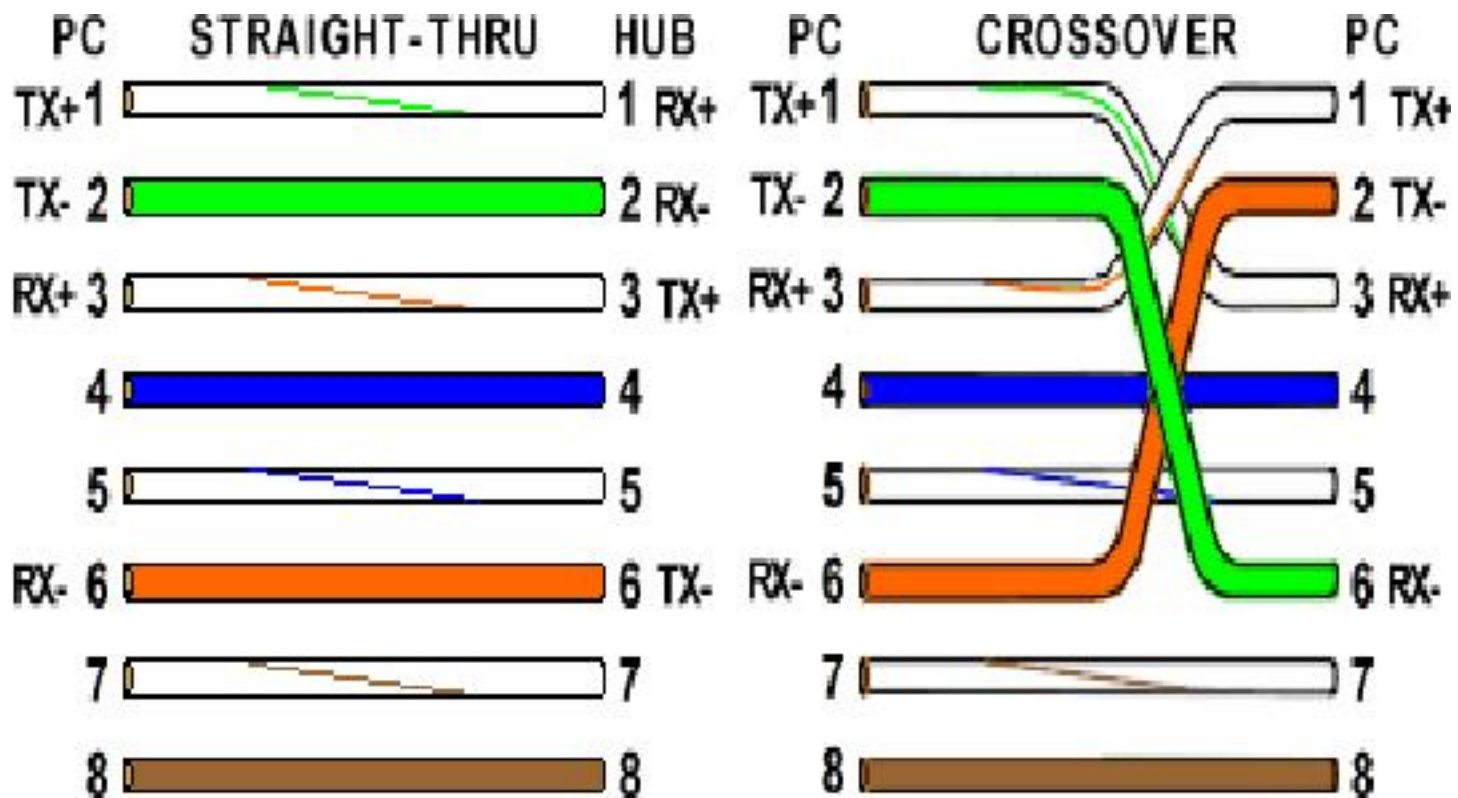


568A CABLE END



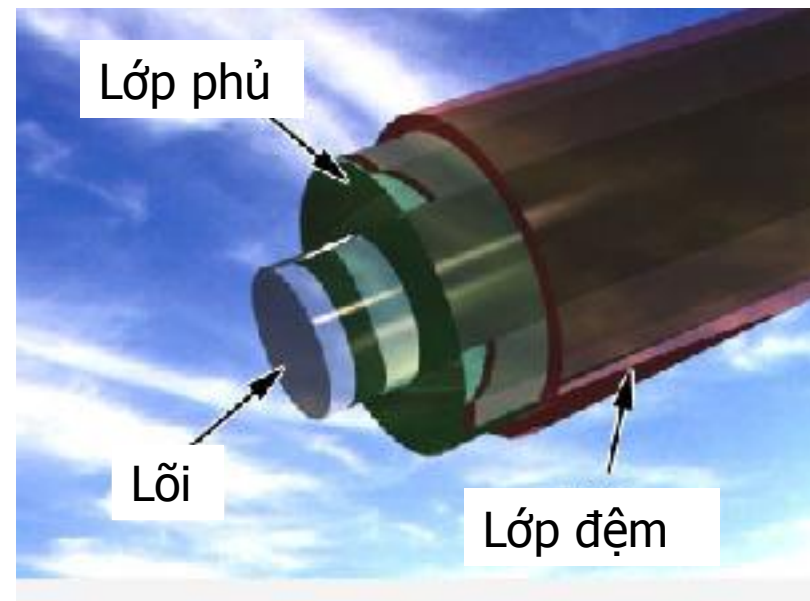
568B CABLE END

Phương thức bấm Cáp

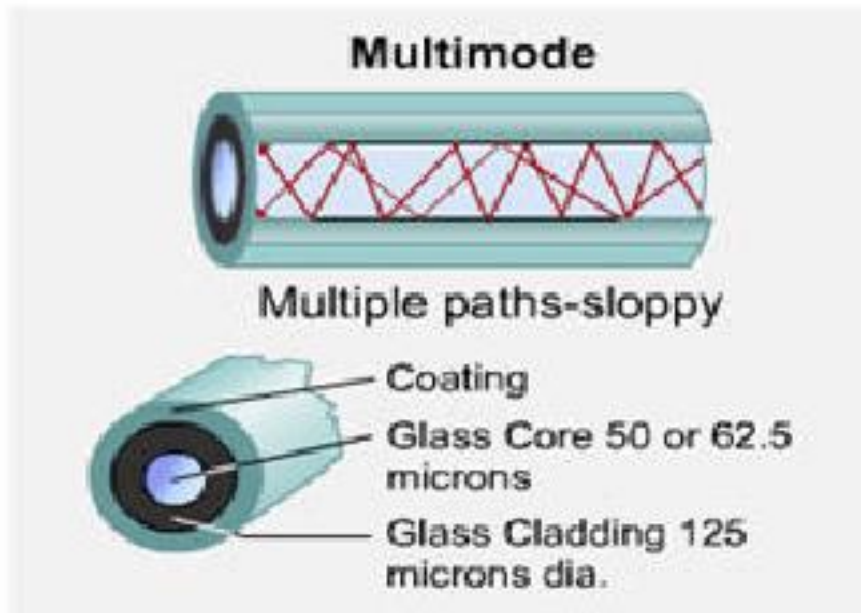
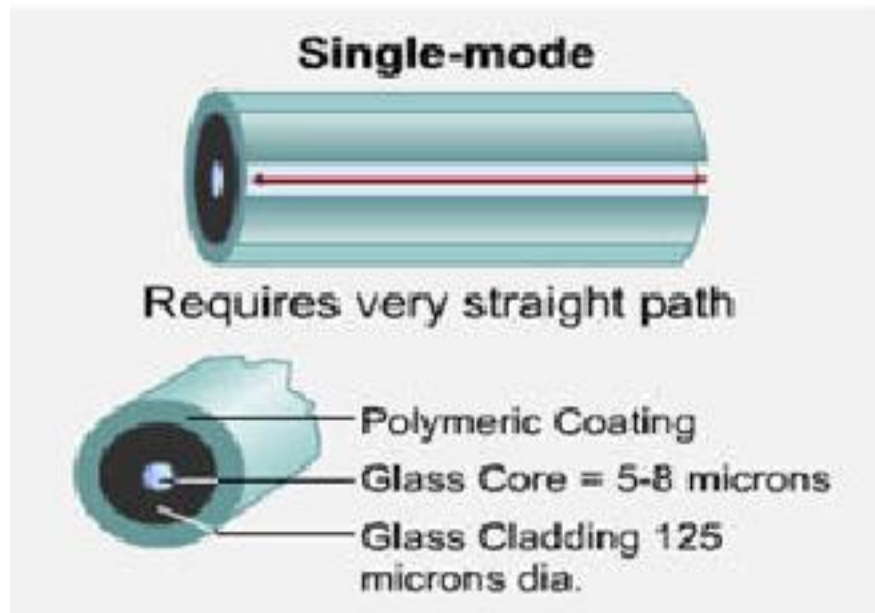


Cáp quang (Fiber optic)

- Thành phần & cấu tạo
 - Dây dẫn
 - Nguồn sáng (LED, Laser)
 - Đầu phát hiện (Photodiode, photo transistor)
- Phân loại
 - Multimode stepped index
 - Multimode graded index
 - Single mode (mono mode)
- Thông số kỹ thuật
 - Chiều dài cáp
 - Tốc độ truyền
 - Nhiều
 - Lắp đặt/bảo trì
 - Giá thành
 - Kết nối



Cáp quang (Fiber optic)

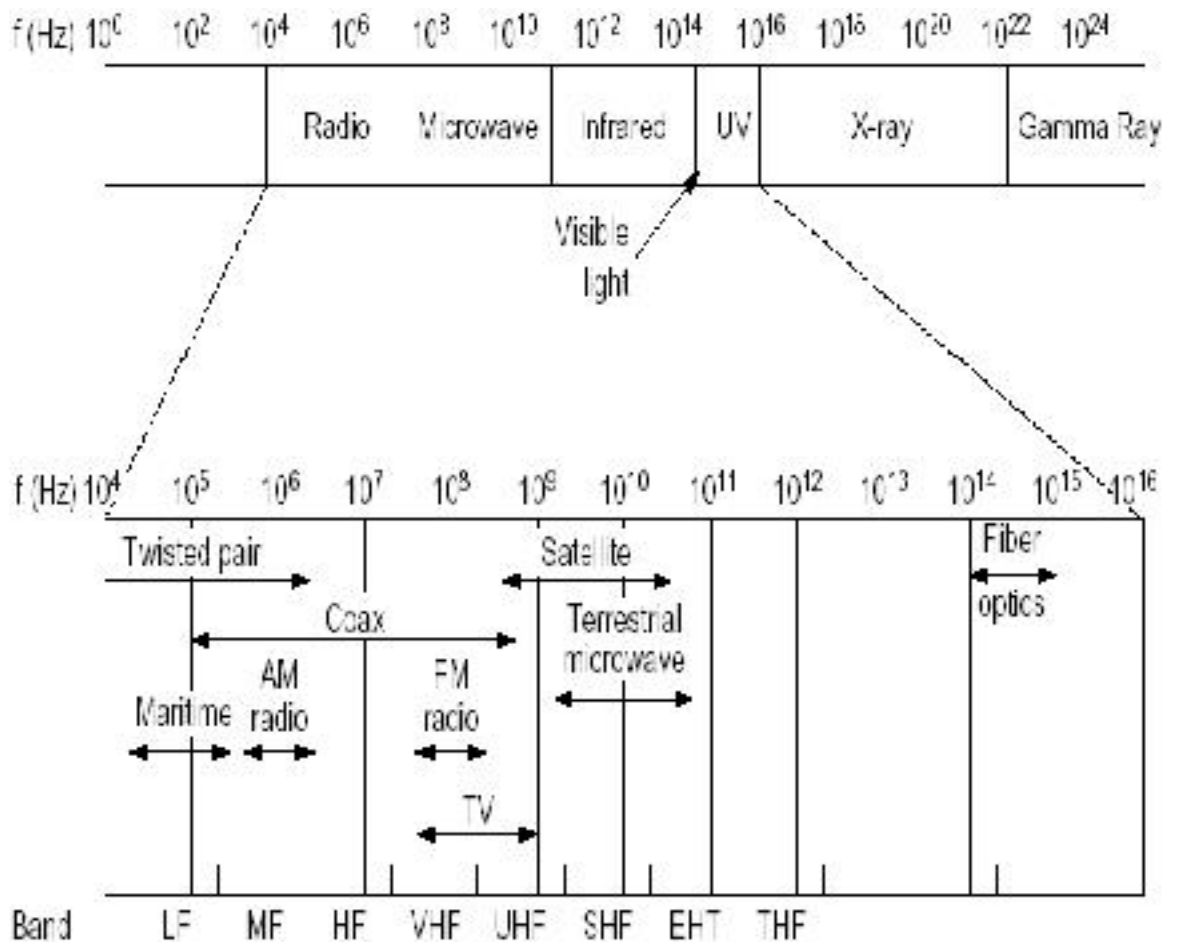


Thông số cơ bản của các loại cáp

| Cáp | Chiều dài cáp tối đa | Tốc độ truyền | Lắp đặt | Nhiều | Giá thành |
|--------------|----------------------|---------------|---------|-------|-----------|
| UTP | 100 m | 10-100 Mbps | Dễ | Cao | Thấp nhất |
| STP | 100 m | 16-500 Mbps | Khá dễ | Thấp | Vừa phải |
| Thinnet | 185 m | 10 Mbps | Dễ | Thấp | Thấp |
| Thicknet | 500 m | 10 Mbps | Khó | Thấp | Cao |
| Fiber optics | 2000 m | 2 Gbps | Khó | Không | Đắt |

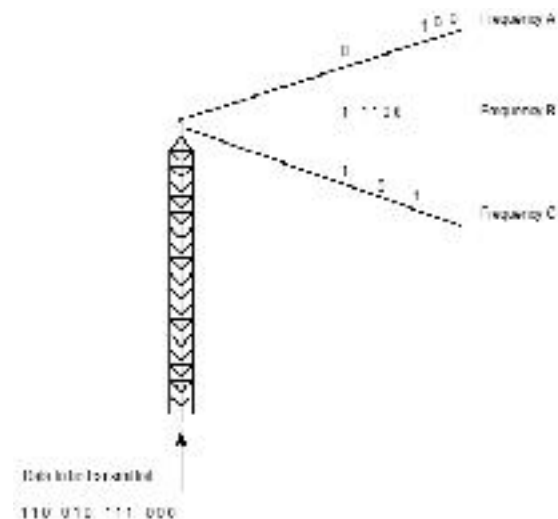
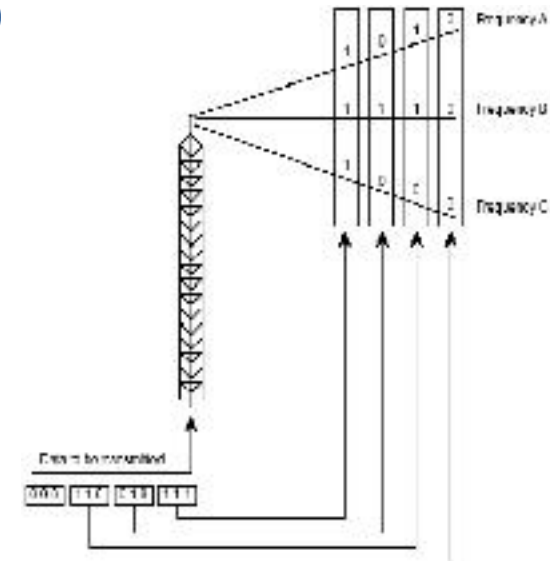
Wireless

- Wireless?
- Các kỹ thuật
 - Radio
 - Microwave
 - Infrared
 - Lightwave



Radio

- Đặc điểm
 - Tần số
 - Thiết bị: antenna, transceiver
- Phân loại
 - Single-Frequency
 - Low power
 - High power
 - Spread-Spectrum
 - Direct-sequence modulation
 - Frequency-hopping



Microwave (sóng cực ngắn)

- Đặc điểm
- Phân loại
 - Terrestrial Microwave
 - Satellite Microwave
- Thông số

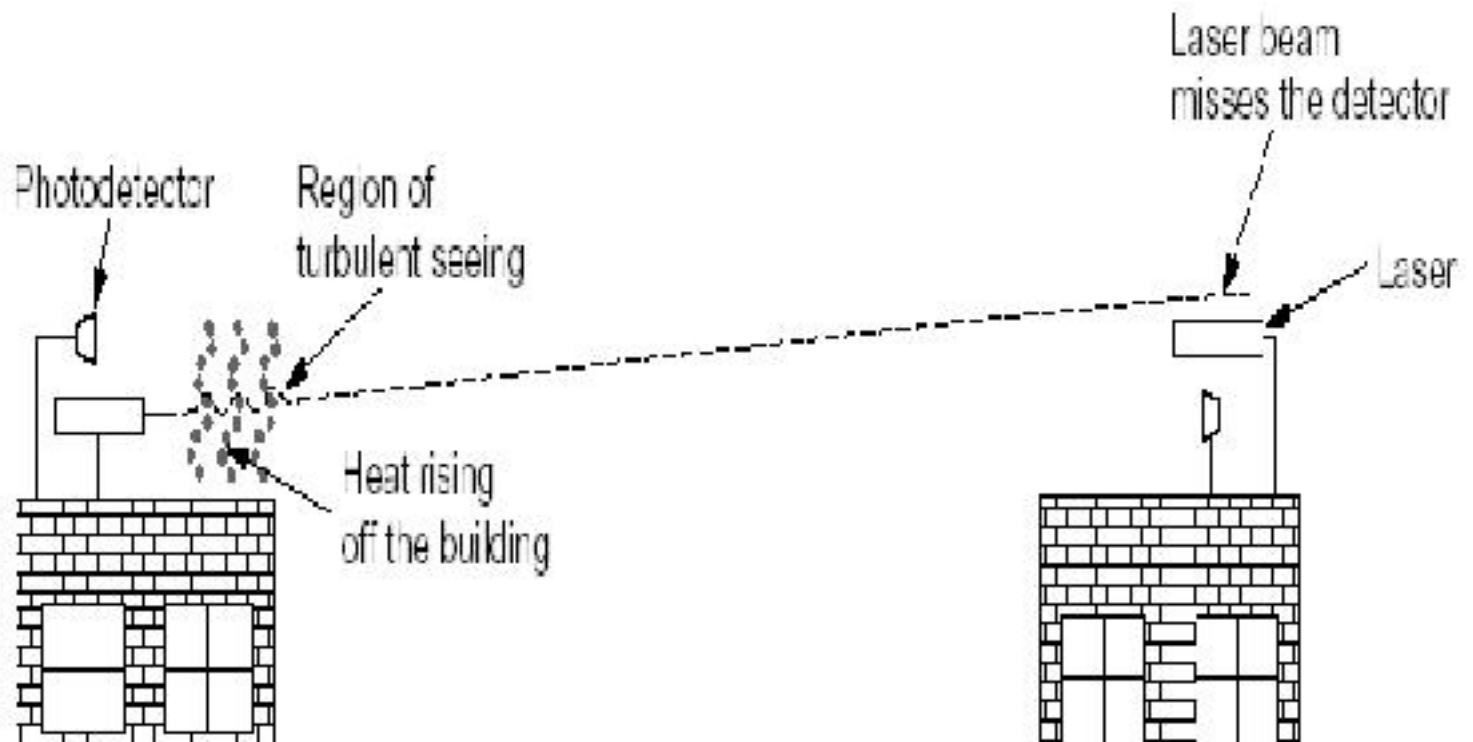
| | Terrestrial Microwave | Satellite Microwave |
|--------------------|---|-------------------------------|
| Tần số | 4-6 GHz, 21-23 GHz | 11-14 GHz |
| Khoảng cách truyền | Phụ thuộc công suất và tần số phát (có thể vài chục km) | Toàn cầu |
| Tốc độ truyền | 1-10 Mbps | 1-10 Mbps |
| Lắp đặt / bảo trì | Khá nhỏ | Khó |
| Nhiều | Phụ thuộc thiết bị, thời tiết | Phụ thuộc thiết bị, thời tiết |
| Giá | Khá cao | Rất cao |
| Bảo mật | Thấp (thường được mã hóa) | Thấp (thường được mã hóa) |

Infrared (Sóng hồng ngoại)

- Đặc điểm
- Phân loại
 - Point-to-point Infrared
 - Broadcast Infrared
- Thông số

| | Point-to-point Infrared | Broadcast Microwave |
|--------------------|--|------------------------------------|
| Tần số | 100-1000 GHz | 100 GHz - 1000 THz |
| Khoảng cách tối đa | Cả bề và ken | Vài chục mét |
| Tốc độ truyền | 100 Mbps - 10 Mbps | Khả năng 1 Mbps |
| Lắp đặt / bảo trì | Vừa phải | Dễ |
| Khấu | Không chấu điện, bị nhiễu ánh sáng | Không chấu điện, bị nhiễu ánh sáng |
| Giá | Tương đương thiết bị | Không cao |
| Bức xạ | Ca (do line-of-sight và độ dải sáng hẹp) | Thấp |









Lightwave



Các thiết bị liên kết mạng

- Card mạng (Network Interface Card - NIC)
- Modem
- Repeater (Bộ chuyển tiếp)
- Hub (Bộ tập trung)
- Bridge (Cầu nối)
- Switch (Bộ chuyển mạch)
- Router (Bộ định tuyến)
- Gateway (Cổng nối)

Biểu diễn của các thiết bị mạng trong sơ đồ mạng

| Network Devices | |
|--|---|
| Repeater  | Bridge  |
| 10BASE-T Hub  | Workgroup Switch  |
| 100BASE-T Hub  | Router  |
| Hub  | Network Cloud  |

Card mạng

- Kết nối giữa máy tính và cáp mạng để phát hoặc nhận dữ liệu với các máy tính khác thông qua mạng.
- Kiểm soát luồng dữ liệu giữa máy tính và hệ thống cáp.
- Mỗi NIC (Network Interface Adapter Card) có một mã duy nhất gọi là địa chỉ MAC (Media Access Control). MAC address có 6 byte, 3 byte đầu là mã số nhà sản xuất, 3 byte sau là số serial của card.

Ca

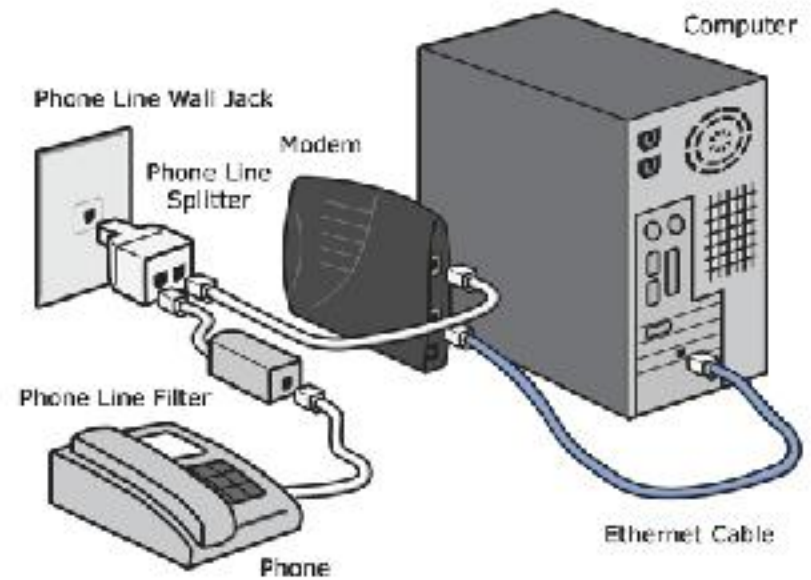
| Organizational Unique Identifier (OUI) | Vendor Assigned (NIC Cards, Interfaces) |
|--|---|
| 24 bits | 24 bits |
| 6 hex digits | 6 hex digits |
| 00 60 2F | 3A 07 BC |
| Cisco | particular device |



Modem

- Là tên viết tắt của hai từ điều chế (MOdulation) và giải điều chế (DEModulation).
- Điều chế tín hiệu số (Digital) sang tín hiệu tương tự (Analog) để gửi theo đường điện thoại và ngược lại.
- Có 2 loại là Internal và External.

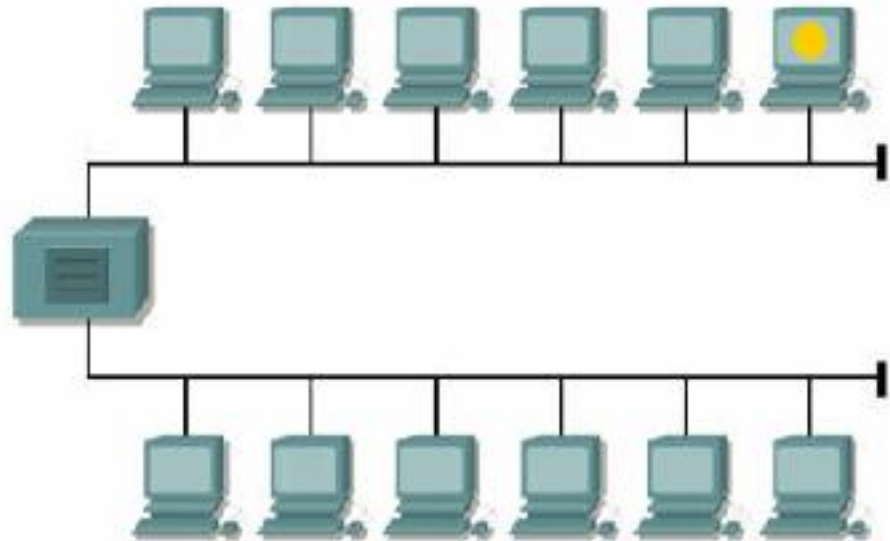
Modem



Repeater (bộ chuyển tiếp)

- Khuếch đại, phục hồi các tín hiệu đã bị suy thoái do tổn thất năng lượng trong khi truyền.
- Cho phép mở rộng mạng vượt xa chiều dài giới hạn của một môi trường truyền.
- Chỉ được dùng nối hai mạng có cùng giao thức truyền thông.
- Hoạt động ở lớp Physical.

Repeater (bộ chuyển tiếp)

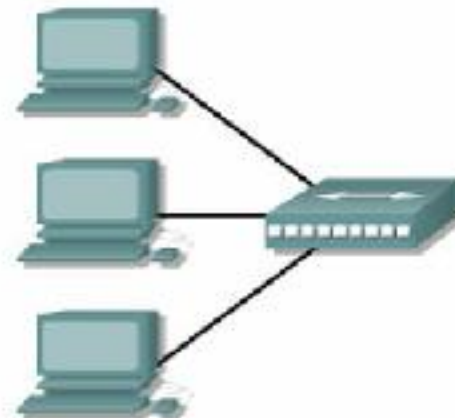
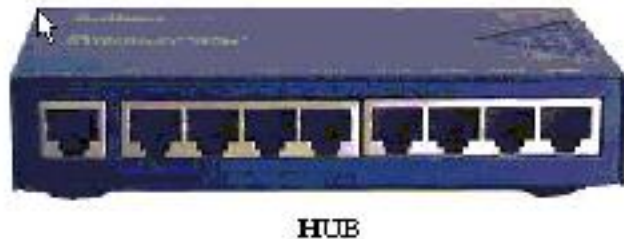


Hub (bộ tập trung)

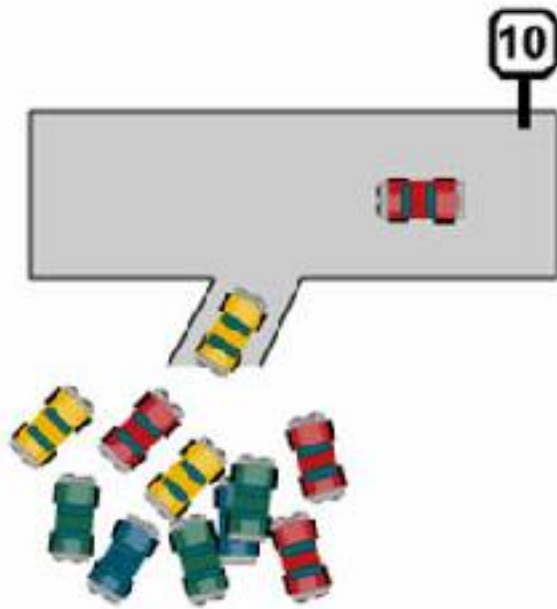
- Chức năng như Repeater nhưng mở rộng hơn với nhiều đầu cắm các đầu cáp mạng.
- Tạo ra điểm kết nối tập trung để nối mạng theo kiểu hình sao.
- Tín hiệu được phân phối đến tất cả các kết nối.
- Có 3 loại Hub: thụ động, chủ động, thông minh.

Hub (bộ tập trung)

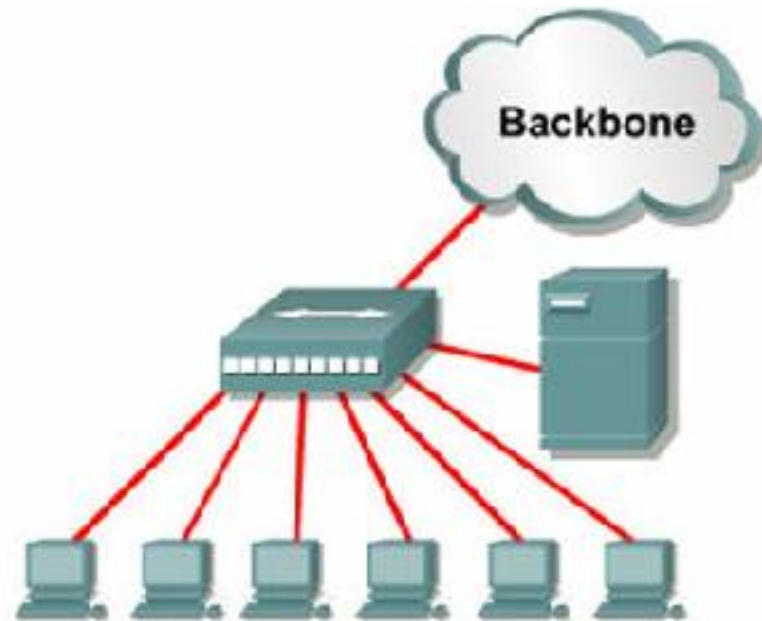
- Hub thụ động (Passive Hub): chỉ đảm bảo chức năng kết nối, không xử lý lại tín hiệu.
- Hub chủ động (Active Hub): có khả năng khuếch đại tín hiệu để chống suy hao.
- Hub thông minh (Intelligent Hub): là Hub chủ động nhưng có thêm khả năng tạo ra các gói tin thông báo hoạt động của mình giúp cho việc quản trị mạng dễ dàng hơn.



Hub (bộ tập trung)



One device sending at a time

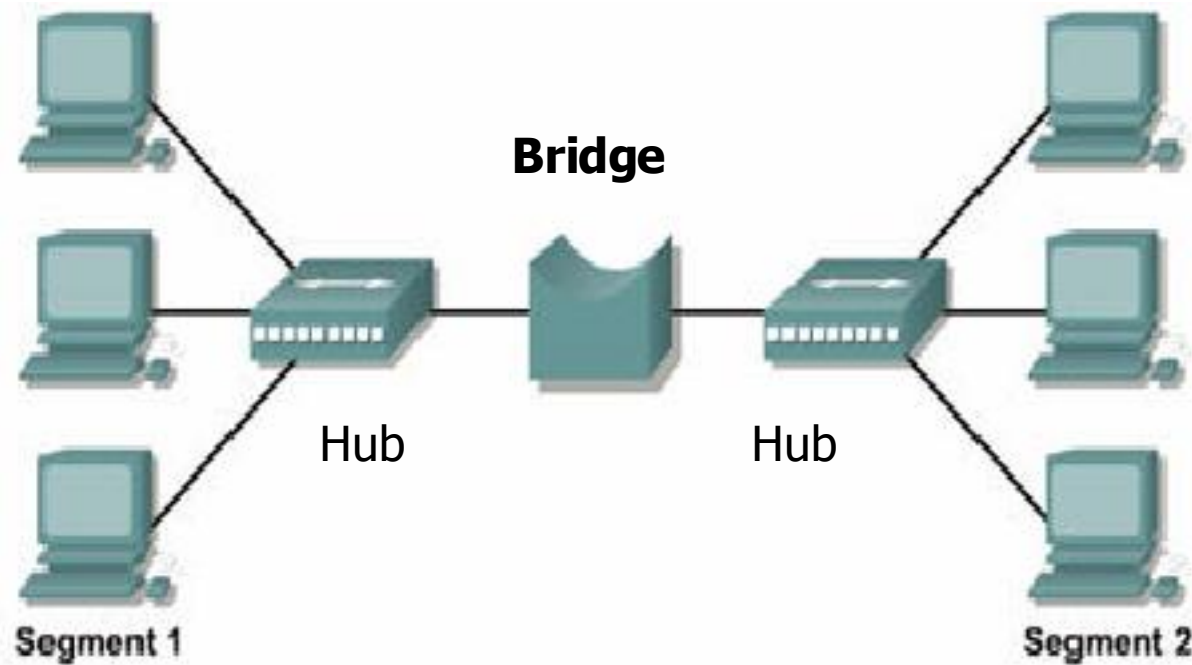


Each node shares 10 Mbps

Bridge (cầu nối)

- Dùng để nối 2 mạng có giao thức giống hoặc khác nhau.
- Chia mạng thành nhiều phân đoạn nhằm giảm lưu lượng trên mạng.
- Hoạt động ở lớp Data Link với 2 chức năng chính là lọc và chuyển vận.
- Dựa trên bảng địa chỉ MAC lưu trữ, Bridge kiểm tra các gói tin và xử lý chúng trước khi có quyết định chuyển đi hay không.

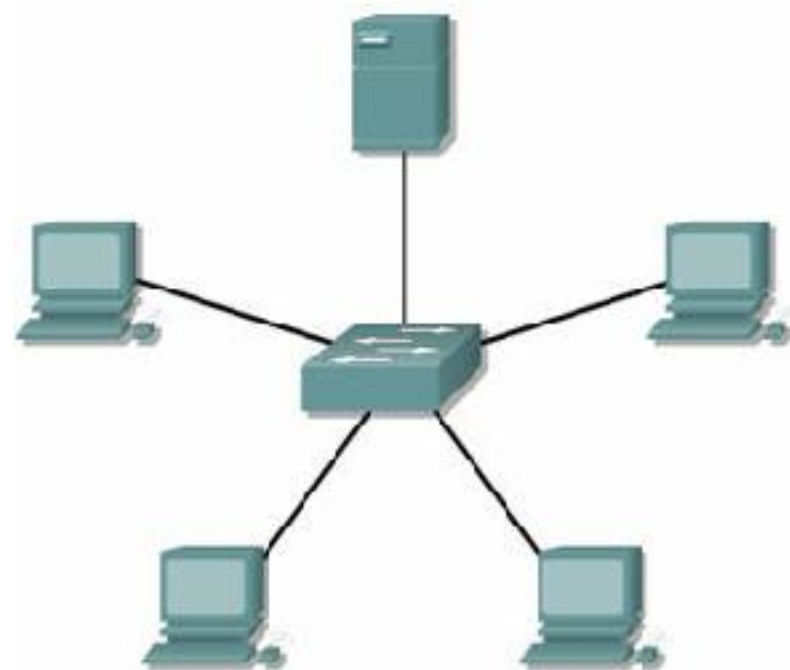
Bridge (cầu nối)



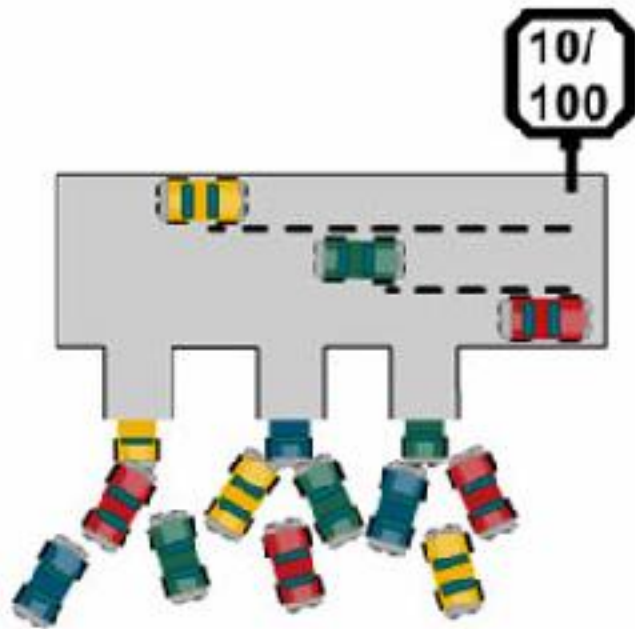
Switch (bộ chuyển mạch)

- Là thiết bị giống Bridge và Hub cộng lại nhưng thông minh hơn.
- Có khả năng chỉ chuyển dữ liệu đến đúng kết nối thực sự cần dữ liệu này làm giảm ðụng ðộ trên mạng.
- Dùng để phân ðoạn mạng trong các mạng cục bộ lớn (VLAN).
- Hoạt ðộng ở lớp Data Link.

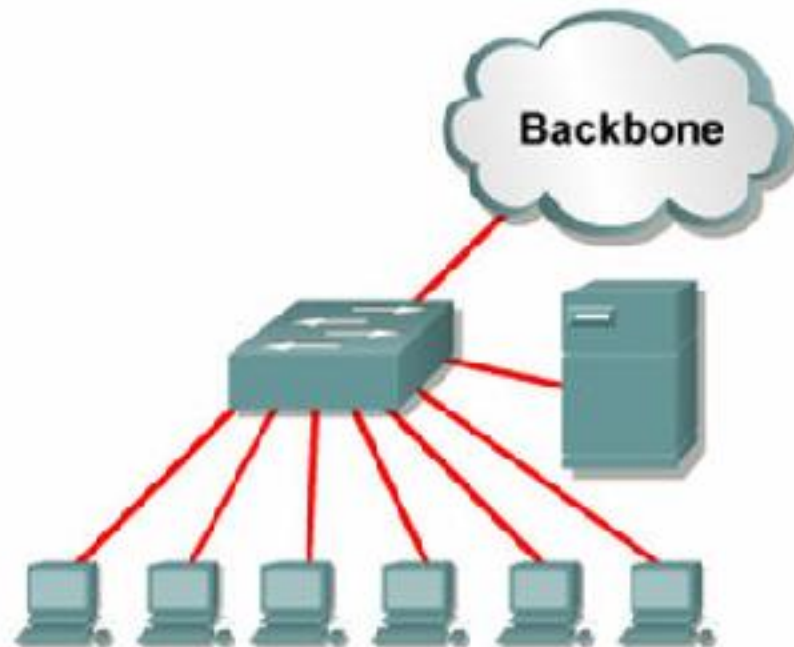
Switch (bộ chuyển mạch)



Switch (bộ chuyển mạch)



Multiple devices sending at the same time



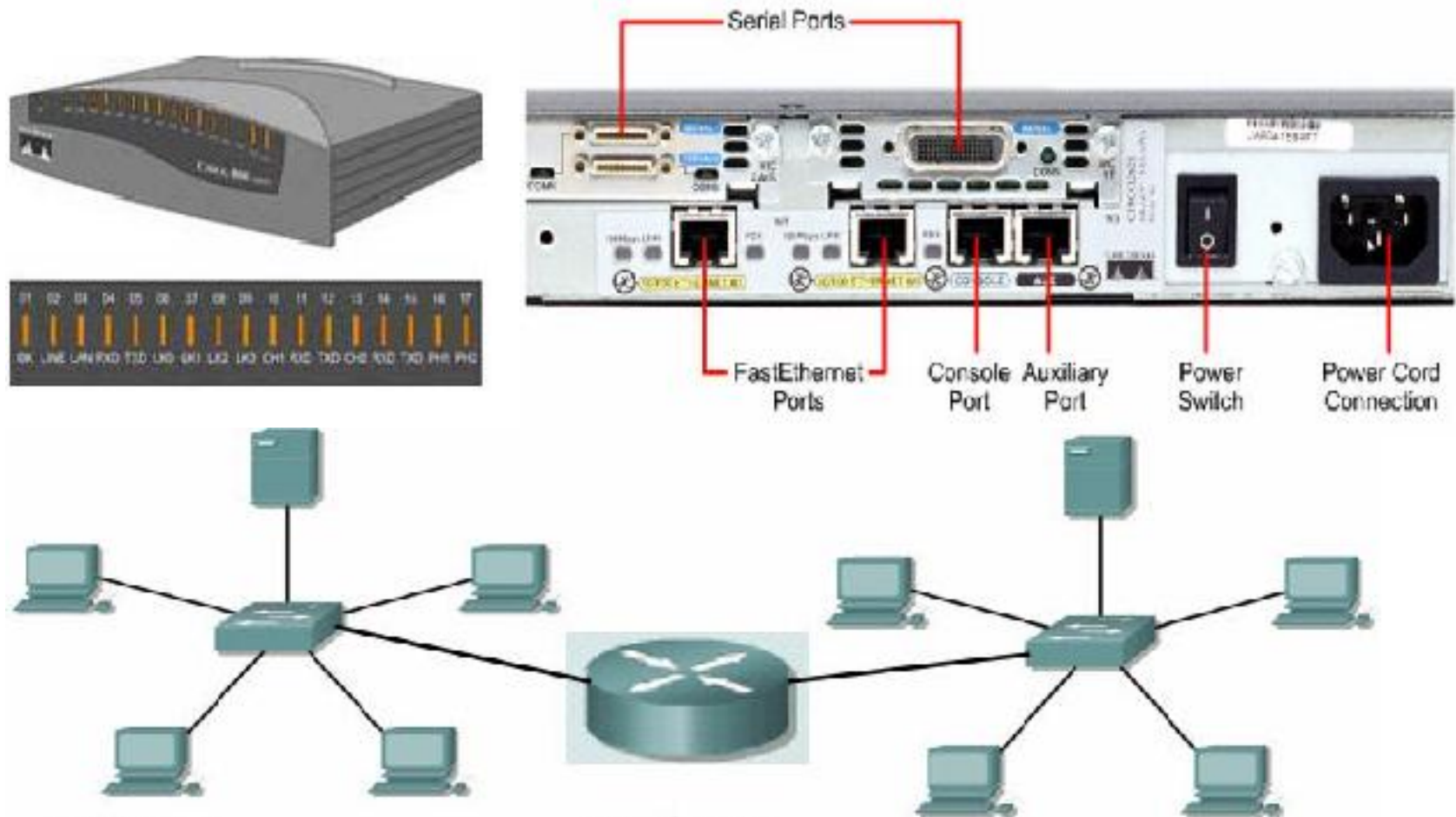
Each node has 10/100 Mbps

...

Router (Bộ định tuyến)

- Dùng để ghép nối các mạng cục bộ lại với nhau thành mạng rộng.
- Lựa chọn đường đi tốt nhất cho các gói tin hướng ra mạng bên ngoài.
- Hoạt động chủ yếu ở lớp Network.
- Có 2 phương thức định tuyến chính:
 - Định tuyến tĩnh: cấu hình các đường cố định và cài đặt các đường đi này vào bảng định tuyến.
 - Định tuyến động:
 - Vectơ khoảng cách: RIP, IGRP, EIGRP, BGP
 - Trạng thái đường liên kết: OSPF

Router (Bộ định tuyến)



Gateway (Proxy - cổng nối)

- Thường dùng để kết nối các mạng không thuần nhất, chủ yếu là mạng LAN với mạng lớn bên ngoài chứ không dùng kết nối LAN – LAN.
- Kiểm soát luồng dữ liệu ra vào mạng.
- Hoạt động phức tạp và chậm hơn Router.
- Hoạt động từ tầng thứ 4 → 7



CHƯƠNG 4: DATA LINK

- Điều khiển luồng (dòng)
- Phát hiện lỗi
- Xử lý lỗi

Điều khiển luồng

- Là kỹ thuật nhằm đảm bảo rằng bên phát không làm tràn dữ liệu bên nhận
- Hai phương pháp được sử dụng:
 - Phương pháp dừng và chờ (Stop and Wait)
 - Đơn giản nhất,
 - Kém hiệu quả, chỉ có một khung tin được truyền tại một thời điểm
 - Phương pháp cửa sổ trượt –(Sliding Window Flow Control)
 - Hiệu quả
 - Cho phép truyền nhiều khung tin cùng một lúc trên kênh truyền

Phương pháp dừng và chờ

- Truyền một gói tin và chờ báo nhận
 - Bên phát truyền một khung tin
 - Sau khi nhận được khung tin, bên nhận gửi lại xác nhận
 - Bên phát phải đợi đến khi nhận được xác nhận thì mới truyền khung tin tiếp theo
- Không hiệu quả
 - Bên nhận có thể dừng quá trình truyền bằng cách không gửi khung tin xác nhận
 - Tại một thời điểm chỉ có một khung tin trên đường truyền → chậm
 - Trường hợp độ rộng của kênh truyền lớn hơn độ rộng của khung tin thì nó tỏ ra cực kỳ kém hiệu quả.

Phương pháp cửa sổ trượt

- Cho phép nhiều khung tin được truyền tại một thời điểm ->Truyền thông hiệu quả hơn.
- A và B được kết nối trực tiếp song công (full-duplex).
- B có bộ đệm cho n khung tin -> B có thể chấp nhận n khung tin, A có thể truyền n khung tin mà không cần đợi xác nhận từ bên B
- Mỗi khung tin được gán nhãn bởi một số thứ tự.
- B xác nhận khung tin đã được nhận bằng cách gửi xác nhận cùng với số thứ tự của khung tin tiếp theo mà nó mong muốn nhận

Phương pháp cửa sổ trượt

- A duy trì danh sách các số thứ tự được phép gửi
- B duy trì danh sách số thứ tự chuẩn bị nhận
 - Gọi là cửa sổ của các khung tin
 - Điều khiển dòng cửa sổ trượt

Phương pháp cửa sổ trượt

- Đối với đường truyền 2 chiều thì mỗi bên phải sử dụng hai cửa sổ:
 - Một cho phát và một cho nhận
 - Mỗi bên đều phải gửi dữ liệu và gửi xác nhận tới bên kia
- Số thứ tự được lưu trữ trong khung tin
 - Bị giới hạn, trường k bit thì số thứ tự được đánh số theo Module của 2^k
 - Kích thước của cửa sổ không nhất thiết phải lấy là maximum (ví dụ trường 3 bit, có thể lấy độ dài cửa sổ là 4)

Phát hiện lỗi

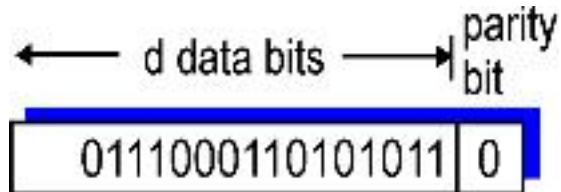
- Lý do một hay nhiều bit thay đổi trong khung tin được truyền:
 - Tín hiệu trên đường truyền bị suy yếu
 - Tốc độ truyền
 - Mất đồng bộ
- Việc phát hiện ra lỗi để khắc phục, yêu cầu phát lại là cần thiết và vô cùng quan trọng trong truyền dữ liệu.

Phát hiện lỗi: Parity Check

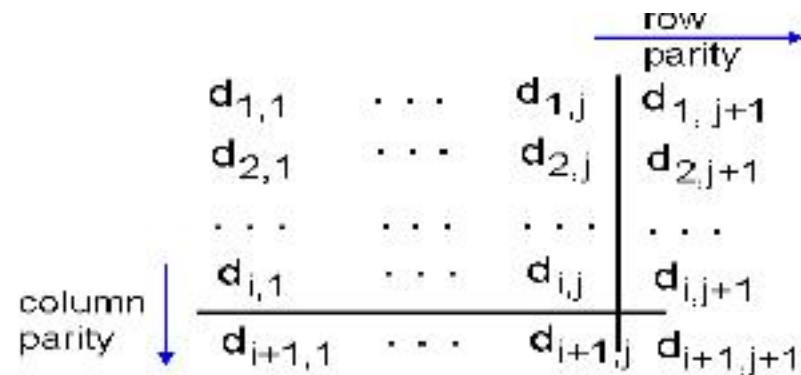
- Là kỹ thuật đơn giản nhất.
- Đưa một bit kiểm tra tính chẵn lẻ vào sau khối tin.
- Giá trị của bit này được xác định dựa trên số các số 1 là chẵn (even parity), hoặc số các số 1 là lẻ (odd parity).
- Lỗi sẽ không bị phát hiện nếu trong khung tin có 2 hoặc một số chẵn các bit bị đảo.
- Không hiệu quả khi xung nhiễu đủ mạnh.

Kiểm tra Parity

Bit Parity đơn:
phát hiện các lỗi bit



Bit Parity 2 chiều:
phát hiện & sửa các lỗi bit



| |
|--------|
| 101011 |
| 111100 |
| 011101 |
| 001010 |

no errors

| |
|-------------------|
| 101011 |
| 101100 |
| 011101 |
| 001010 |

parity error

*correctable
single bit error*

Phát hiện lỗi: Cyclic redundancy Check (CRC)

Mô tả:

- Khối dữ liệu k bit
- Mẫu $n+1$ bit ($n < k$)
- Tạo ra dãy n bit gọi là dãy kiểm tra khung tin-FCS, Frame Check Sequence
- Tạo ra một khung tin $k+n$ bit
- Bên nhận khi nhận được khung tin sẽ chia cho mẫu, nếu kết quả là chia hết, việc truyền khung tin này là không có lỗi

Phát hiện lỗi: CRC dưới dạng module của 2

M: Khối tin k bit

F: FCS n bit, n bit cuối của T

T: khung tin k+n bit

P: Mẫu n+1 bit, đây là một số chia được chọn trước.

Mục tiêu: xác định F để T chia hết cho P

$$T = 2^n M + F$$

Phát hiện lỗi: Các bước tạo và kiểm tra CRC

- Các bước tạo CRC
 - Dịch trái M đi n bit
 - Chia kết quả cho P
 - Số dư tìm được là F
- Các bước kiểm tra CRC
 - Lấy khung nhận được (n+k) bit
 - Chia cho P
 - Kiểm tra số dư, nếu số dư khác 0, khung bị lỗi, ngược lại là không lỗi

Phát hiện lỗi: CRC- Dạng đa thức nhị phân

Cách thứ 2 để biểu thị CRC là biểu diễn các giá trị như là một đa thức với các hệ số là số nhị phân, đây là các bit của số nhị phân. Gọi $T(X)$, $M(X)$, $Q(X)$, $P(X)$, $R(X)$ là các đa thức tương ứng với các số nhị phân T , M , Q , P , R đã trình bày ở trên, khi đó CRC được biểu thị:

$$\frac{X^n M(X)}{P(X)} = Q(X) + \frac{R(X)}{P(X)}$$
$$T(X) = X^n M(X) + R(X)$$

CRC- Dạng đa thức nhị phân

Một số đa thức $P(X)$ tiêu biểu:

CRC-12: $X^{12}+X^{11}+X^3+X^2+X+1$

CRC-16: $X^{16}+X^{15}+X^2+1$

CRC-CCITT: $X^{16}+X^{12}+X^5+1$

CRC32: $X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+X+1$

Ví dụ:

Tạo CRC:

1. Cho tin $M=1010001101$ (10 bit)

Mẫu $P:110101$ (6 bit)

FCS R : được tính theo phương pháp CRC và có độ dài là 5 bit

2. Nhân M với 2^5 ta được:

$M2^5=101000110100000$

3. Chia kết quả cho P :

4. Số dư là: 01110 , được đưa vào sau tin M

Ta có tin T , được truyền đi là:

101000110101110

$$\begin{array}{r}
 110101 \overline{) 101000110100000} \leftarrow 2^5 M \\
 \underline{110101} \\
 111011 \\
 \underline{110101} \\
 111010 \\
 \underline{110101} \\
 111110 \\
 \underline{110101} \\
 101100 \\
 \underline{110101} \\
 110010 \\
 \underline{110101} \\
 01110 \leftarrow R
 \end{array}$$

CRC- Dạng đa thức nhị phân

- Kiểm tra CRC:
- Giả sử bên thu nhận được T, khi đó để kiểm tra là phép truyền có lỗi không ta chia T cho P, số dư là 00000, vậy ta kết luận phép truyền tin M, không có lỗi.

$$\begin{array}{r}
 110101 \overline{) 101000110101110} \leftarrow T \\
 \underline{110101} \\
 111011 \\
 \underline{110101} \\
 111010 \\
 \underline{110101} \\
 111110 \\
 \underline{110101} \\
 101111 \\
 \underline{110101} \\
 110101 \\
 \underline{110101} \\
 00000 \leftarrow R
 \end{array}$$

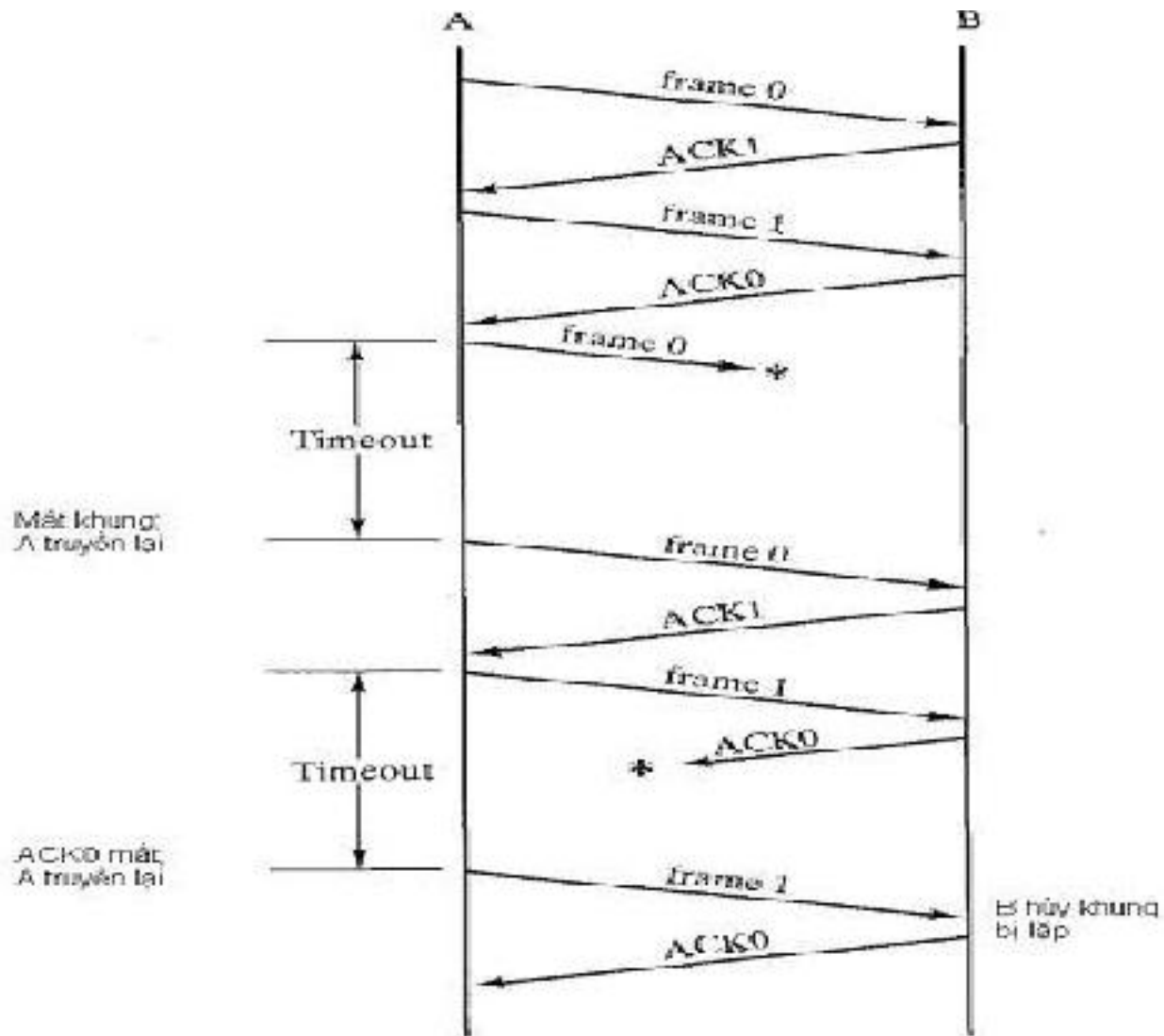
Xử lý lỗi

- Lỗi: Mất khung, hỏng khung
- Kiểm soát lỗi:
 - Phát hiện lỗi
 - Báo nhận: khung tin tốt
 - Truyền lại khi hết thời gian định trước
 - Báo nhận: khung tin lỗi và truyền lại

Xử lý lỗi: ARQ dừng và chờ

- Trên cơ sở kĩ thuật điều khiển luồng dừng-và-chờ
- Kiểm soát lỗi:
 - Khung tin tới bên nhận bị hỏng: Truyền lại, sử dụng đồng hồ đếm giờ time-out
 - Báo nhận bị hỏng: Time-out, bên phát gửi lại, sử dụng label 0/1 và ACK0/ACK1 phát hiện lỗi

Xử lý lỗi: ARQ dừng và chờ



Xử lý lỗi: ARQ Quay-lui-N

- Trên cơ sở kỹ thuật điều khiển luồng bằng Cửa sổ trượt
- Kiểm soát lỗi:
 - Khung hỏng:
 - Khung $i-1$ thành công, i lỗi, bên nhận gửi SREJ i , bên phát gửi lại
 - Khung i mất, $i+1$ được nhận không đúng trình tự, REJ i , bên gửi phát lại i và các khung sau đó
 - Chỉ khung i được truyền và bị mất, bên nhận không biết i đã được truyền đi, bên phát gửi time-out và gửi RR với $P=1$, khi bên phát nhận được RR từ bên nhận nó sẽ phát lại i

Xử lý lỗi: ARQ Quay-lui-N

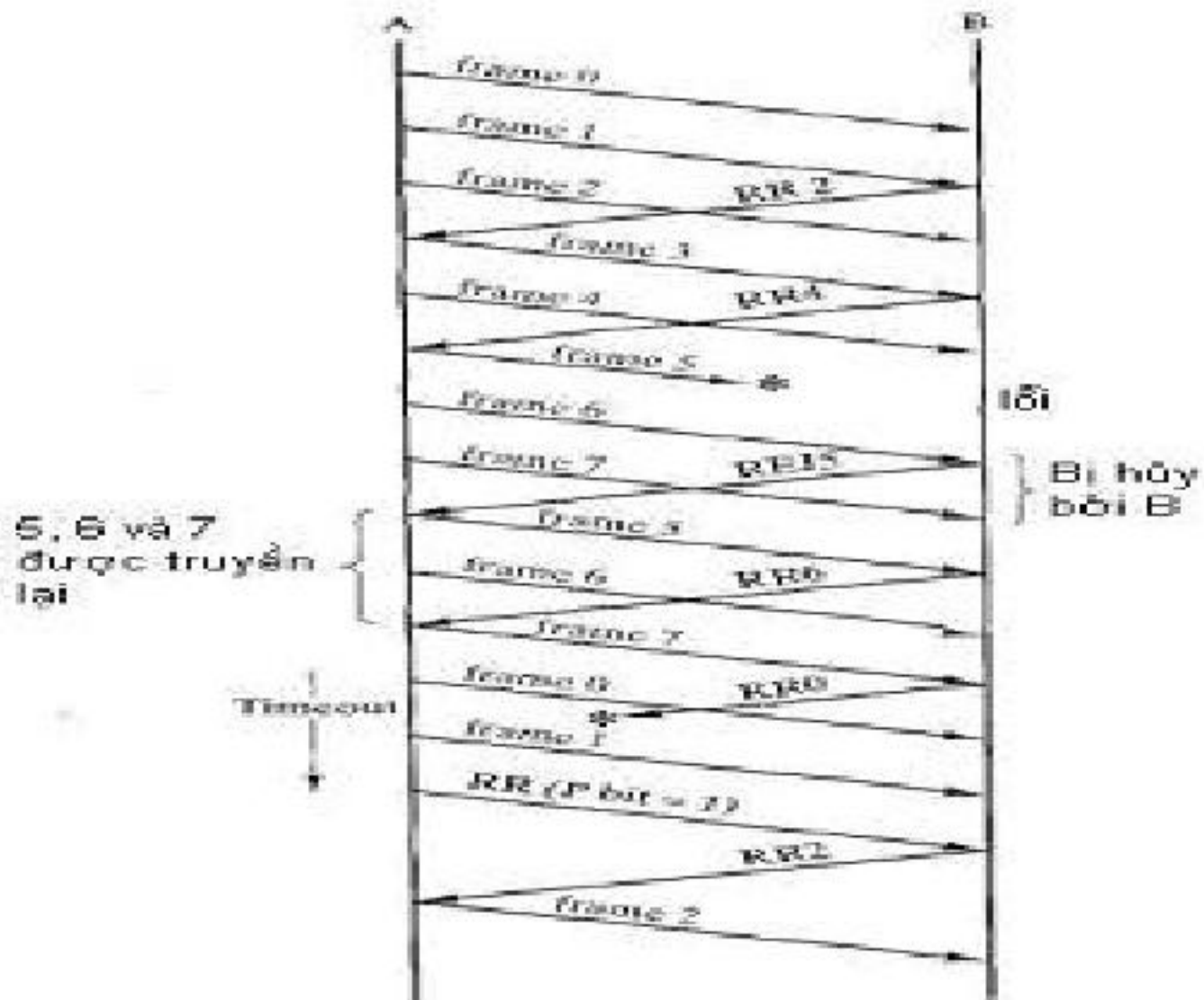
– RR hỏng:

- B nhận khung i và gửi $RR(i+1)$, $RR(i+1)$ mất, A có thể nhận $RR(>i+1)$ trước khi $RR(i+1)$ time-out, và có nghĩa là khung i đã thành công.
- $RR(i+1)$ time-out, A cố gắng gửi RR với P-bit cho đến khi nhận được RR từ B một số lần nhất định, nếu vẫn không nhận được thì Khởi động lại giao thức

– Reject hỏng:

- A time-out, A gửi RR với $P=1$ cho đến khi nhận được RR_i từ B thì A sẽ gửi lại khung i

Xử lý lỗi: ARQ Quay-lui-N



Xử lý lỗi: ARQ Chọn-Hủy (Selective-Reject)

- Chỉ truyền lại những khung có báo nhận là lỗi (SREJ)
- Phải duy trì đủ bộ đệm độ lớn
- Đảm bảo tính logic phức tạp để gửi và nhận các khung theo đúng trình tự.
- ARQ Chọn-Hủy phải giải quyết được sự chồng chéo giữa cửa sổ gửi và nhận.

Xử lý lỗi: ARQ Chọn-Hủy (Selective-Reject)

- Trạm A gửi các khung từ 0 đến 6 tới trạm B.
- Trạm B nhận tất cả 7 khung và báo nhận tích lũy với RR 7
- Vì lí do nào đó ví dụ như nhiễu làm RR 7 bị mất trên đường truyền.
- Đồng hồ ở A hết hạn và A truyền lại khung 0.
- B đã điều chỉnh trước cửa sổ nhận để có thể nhận các khung 7, 0, 1, 2, 3, 4 và 5. Do đó mà khung 7 được coi là bị mất và khung nhận được này là khung số 0 mới, và được chấp nhận bởi B.

CHƯƠNG 5: TCP/IP

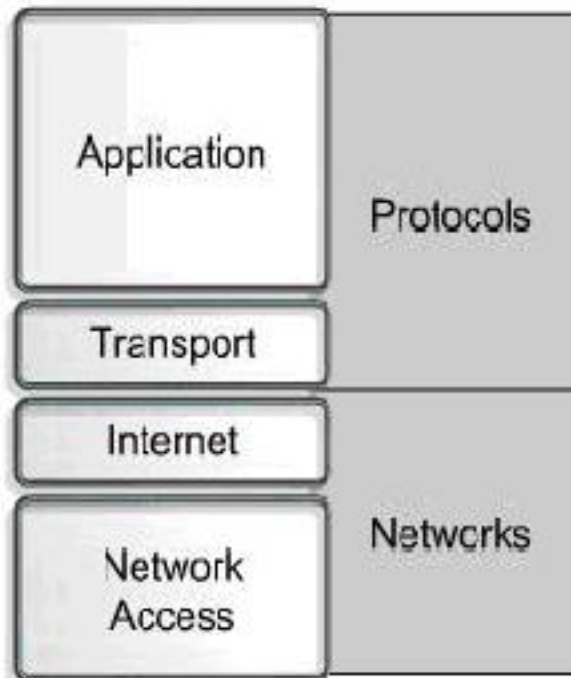
- Khái niệm về TCP và IP
- Mô hình tham chiếu TCP/IP
- So sánh OSI và TCP/IP
- Các giao thức trong mô hình TCP/IP
- Chuyển đổi giữa các hệ thống số
- Địa chỉ IP và các lớp địa chỉ
- NAT
- Mạng con và kỹ thuật chia mạng con
- Bài tập

Khái niệm về TCP và IP

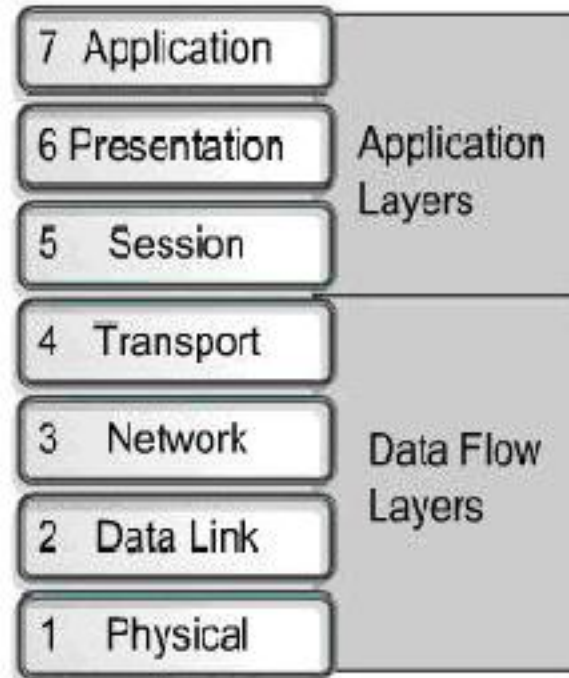
- TCP (Transmission Control Protocol) là giao thức thuộc tầng vận chuyển và là một giao thức có kết nối (connected-oriented).
- IP (Internet Protocol) là giao thức thuộc tầng mạng của mô hình OSI và là một giao thức không kết nối (connectionless).

Mô hình tham chiếu TCP/IP

TCP/IP Model

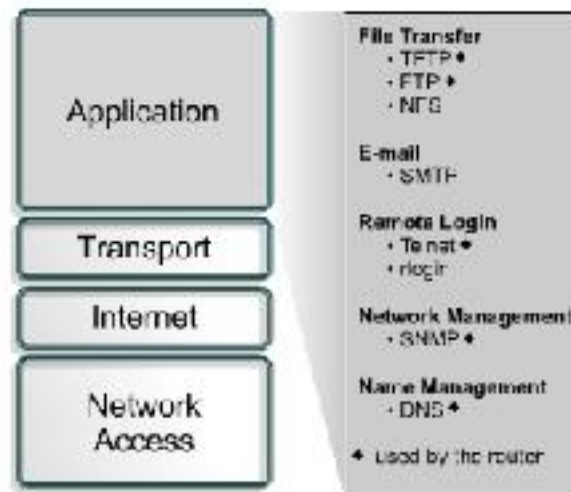


OSI Model



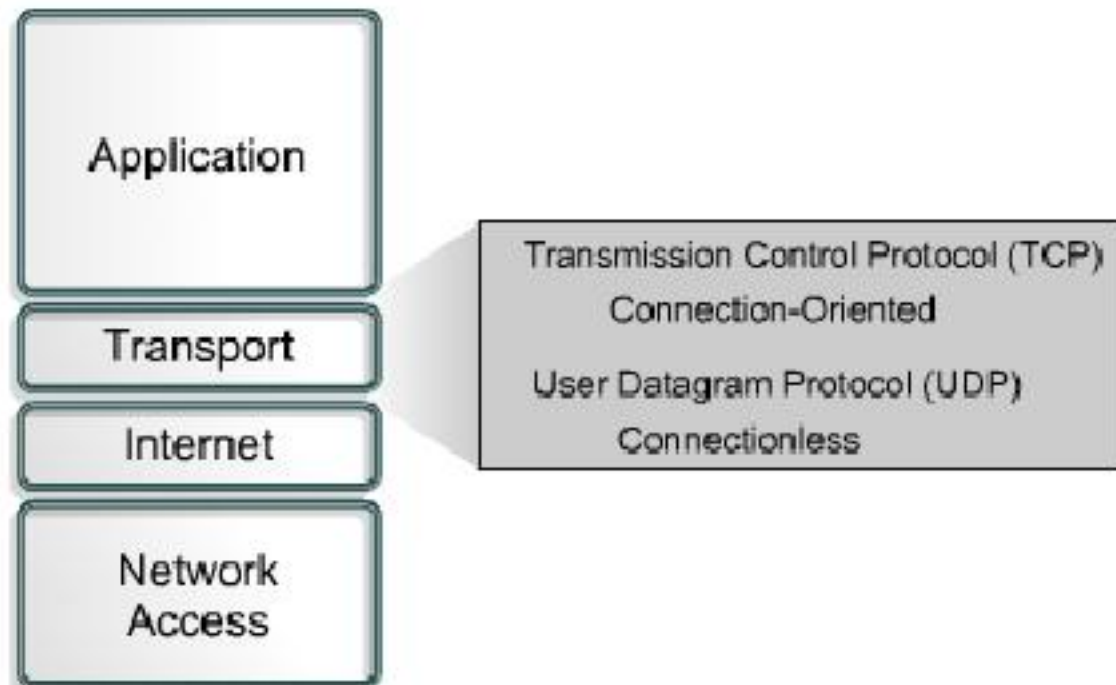
Lớp ứng dụng

Kiểm soát các giao thức lớp cao, các chủ đề về trình bày, biểu diễn thông tin, mã hóa và điều khiển hội thoại. Đặc tả cho các ứng dụng phổ biến.



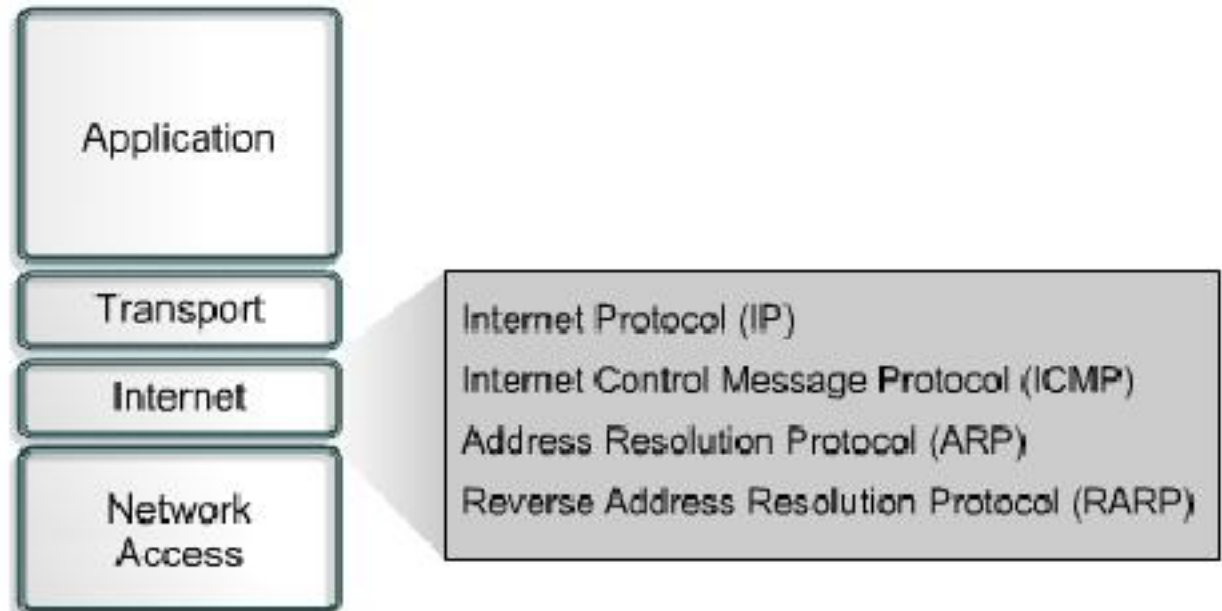
Lớp vận chuyển

Cung ứng dịch vụ vận chuyển từ host nguồn đến host đích. Thiết lập một cầu nối luận lý giữa các đầu cuối của mạng, giữa host truyền và host nhận.



Lớp Internet

Mục đích của lớp Internet là chọn đường đi tốt nhất xuyên qua mạng cho các gói dữ liệu di chuyển tới đích. Giao thức chính của lớp này là Internet Protocol (IP).



Lớp truy nhập mạng

Định ra các thủ tục để giao tiếp với phần cứng mạng và truy nhập môi trường truyền. Có nhiều giao thức hoạt động tại lớp này



- Ethernet
- Fast Ethernet
- SLIP & PPP
- FDDI
- ATM, Frame Relay & SMDS
- ARP
- Proxy ARP
- RARP

So sánh mô hình OSI và TCP/IP

- Giống nhau
 - Đều phân lớp chức năng
 - Đều có lớp vận chuyển và lớp mạng.
 - Chuyển gói là hiển nhiên.
 - Đều có mối quan hệ trên dưới, ngang hàng.
- Khác nhau
 - TCP/IP gộp lớp trình bày và lớp phiên vào lớp ứng dụng.
 - TCP/IP gộp lớp vật lý và lớp liên kết dữ liệu vào lớp truy nhập mạng.
 - TCP/IP đơn giản vì có ít lớp hơn.
 - OSI không có khái niệm chuyển phát thiếu tin cậy ở lớp 4 như UDP của TCP/IP

Các giao thức trong mô hình TCP/IP

DoD Model

| | | | | |
|-------------------------|----------|------------------|---------------|----------|
| Process/ Application | Telnet | FTP | LPD | SNMP |
| | TFTP | SMTP | NFS | X Window |
| Host-to-Host | TCP | | UDP | |
| Internet | ICMP | ARP | RARP | |
| | IP | | | |
| Network Access | Ethernet | Fast Ethernet | Token Ring | FDDI |

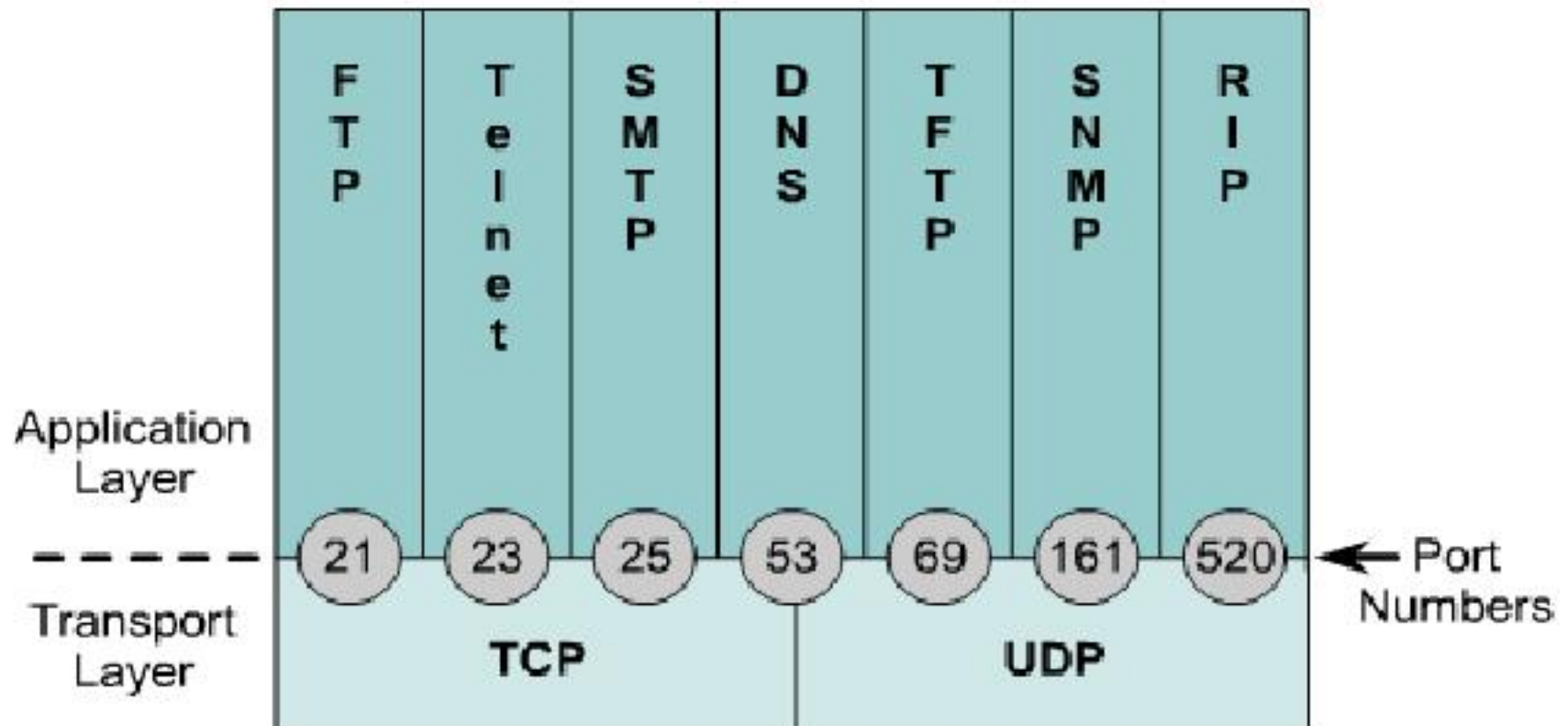
Lớp ứng dụng

- FTP (File Transfer Protocol): là dịch vụ có tạo cầu nối, sử dụng TCP để truyền các tập tin giữa các hệ thống.
- TFTP (Trivial File Transfer Protocol): là dịch vụ không tạo cầu nối, sử dụng UDP. Được dùng trên router để truyền các file cấu hình và hệ điều hành.
- NFS (Network File System): cho phép truy xuất file đến các thiết bị lưu trữ ở xa như một đĩa cứng qua mạng.
- SMTP (Simple Mail Transfer Protocol): quản lý hoạt động truyền e-mail qua mạng máy tính.

Lớp ứng dụng

- Telnet (Terminal emulation): cung cấp khả năng truy nhập từ xa vào máy tính khác. Telnet client là host cục bộ, telnet server là host ở xa.
- SNMP (Simple Network Management): cung cấp một phương pháp để giám sát và điều khiển các thiết bị mạng.
- DNS (Domain Name System): thông dịch tên của các miền (Domain) và các node mạng được công khai sang các địa chỉ IP.

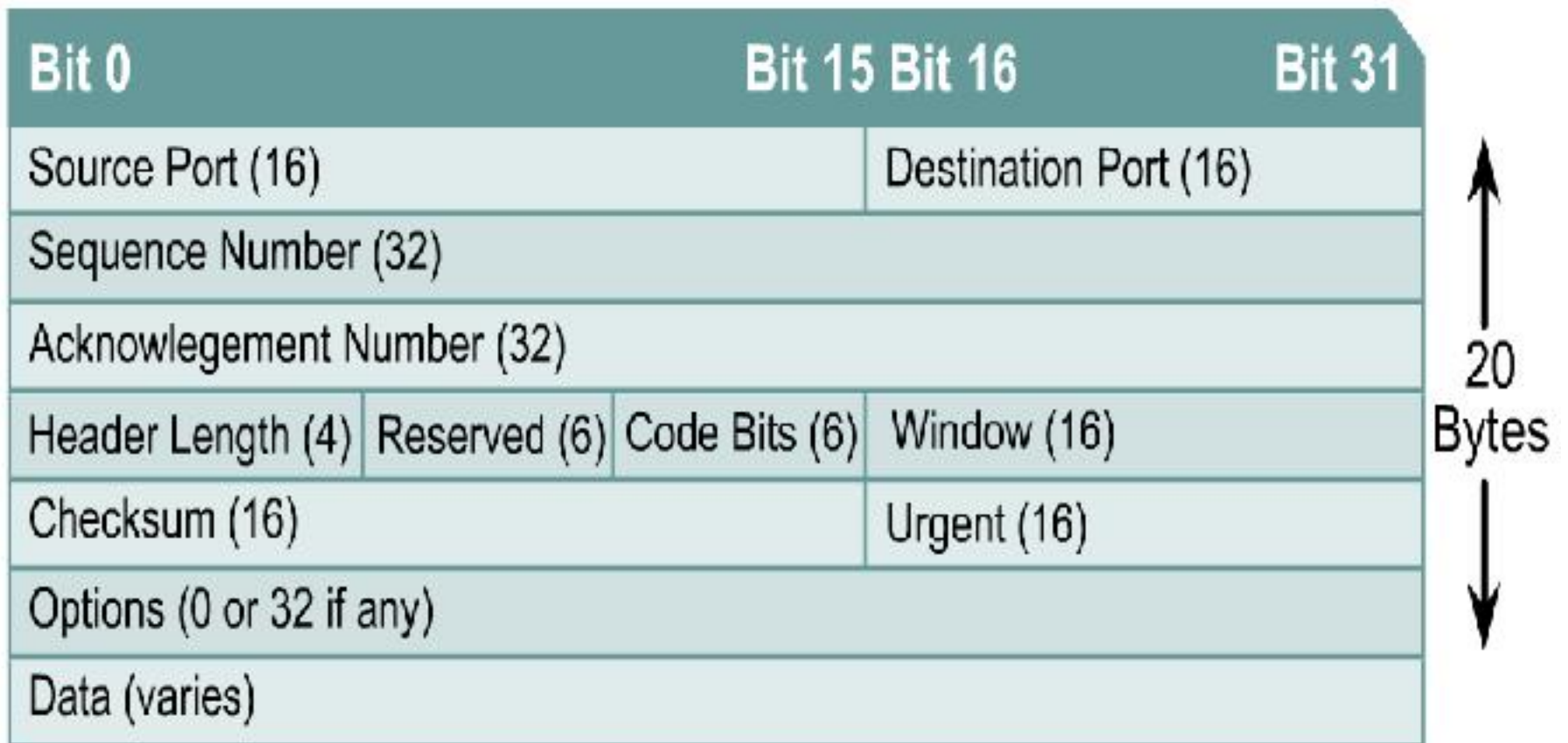
Các cổng phổ biến dùng cho các giao thức lớp ứng dụng



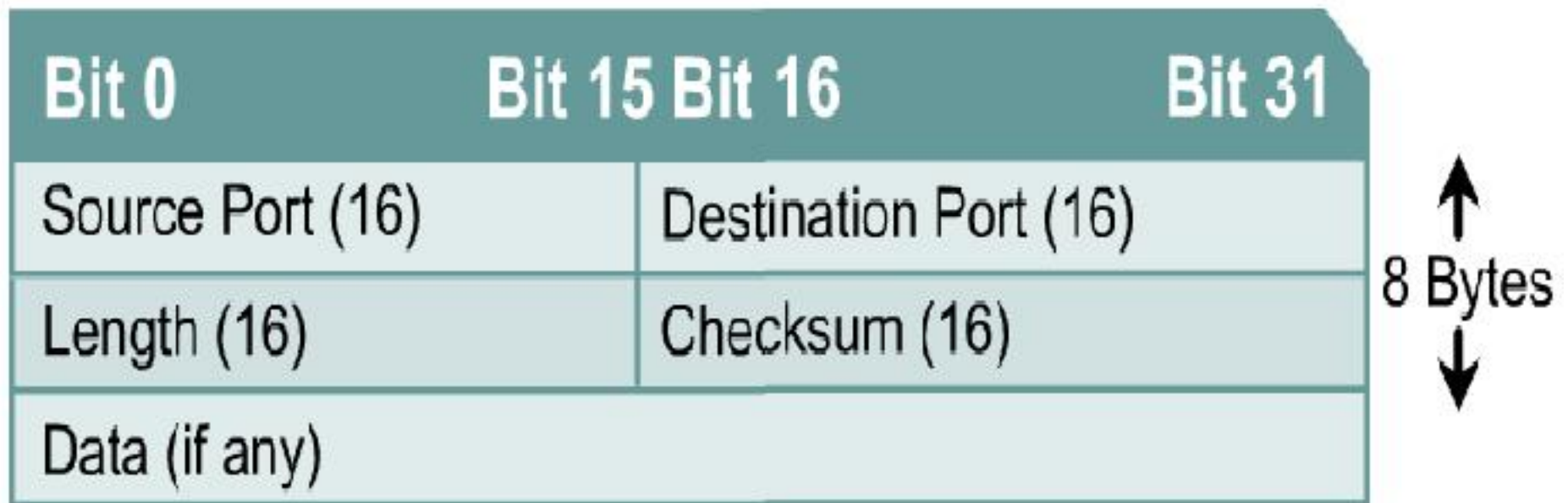
Lớp vận chuyển

- TCP và UDP (User Datagram Protocol):
 - Phân đoạn dữ liệu ứng dụng lớp trên.
 - Truyền các segment từ một thiết bị đầu cuối này đến thiết bị đầu cuối khác
- Riêng TCP còn có thêm các chức năng:
 - Thiết lập các hoạt động end-to-end.
 - Cửa sổ trượt cung cấp điều khiển luồng.
 - Chỉ số tuần tự và báo nhận cung cấp độ tin cậy cho hoạt động.

Khuôn dạng gói tin TCP



Khuôn dạng gói tin UDP



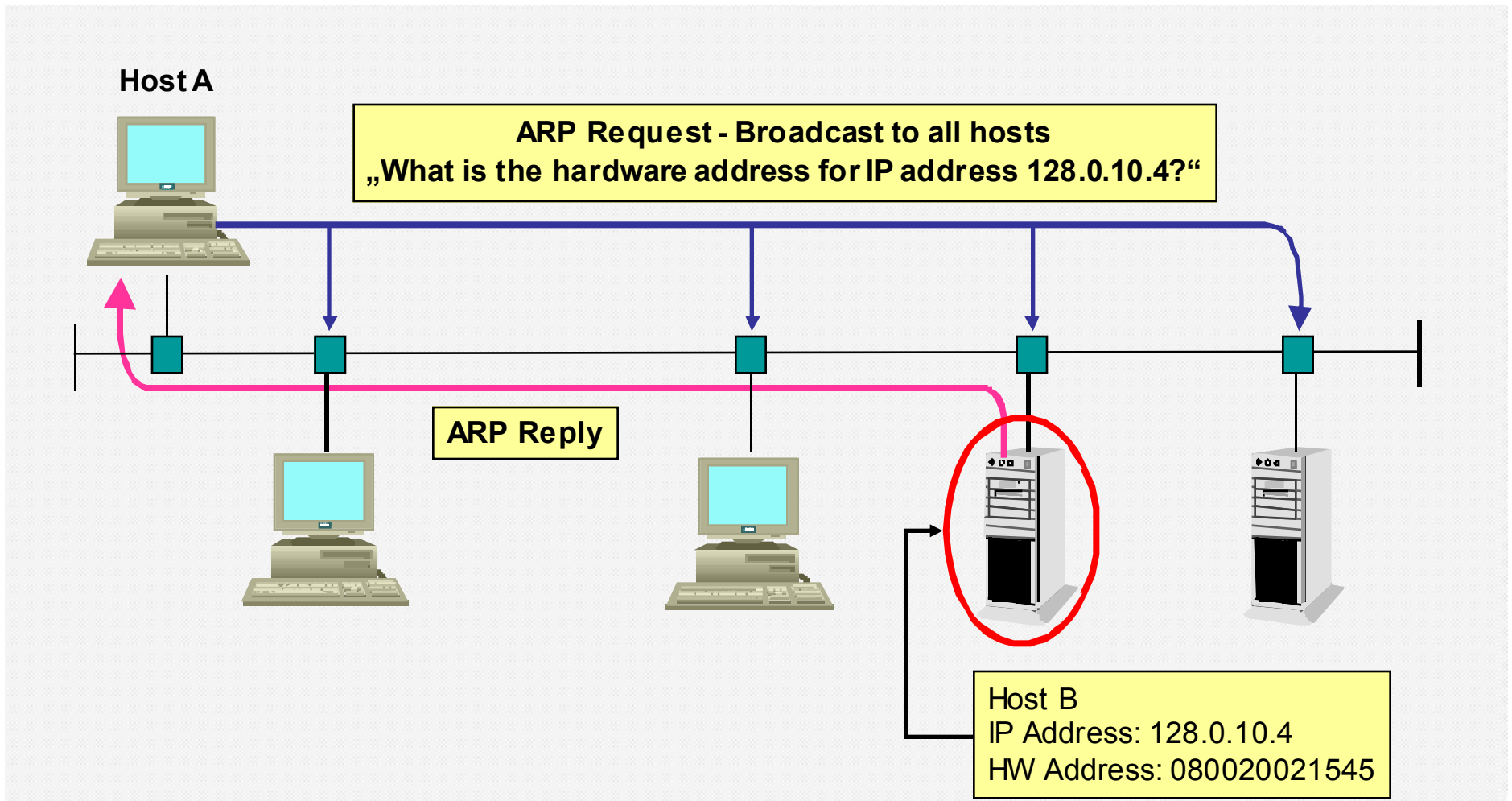
Lớp Internet

- IP: không quan tâm đến nội dung của các gói nhưng tìm kiếm đường dẫn cho gói tới đích.
- ICMP (Internet Control Message Protocol): đem đến khả năng điều khiển và chuyển thông điệp.
- ARP (Address Resolution Protocol): xác định địa chỉ lớp liên kết số liệu (MAC address) khi đã biết trước địa chỉ IP.
- RARP (Reverse Address Resolution Protocol): xác định các địa chỉ IP khi biết trước địa chỉ MAC.

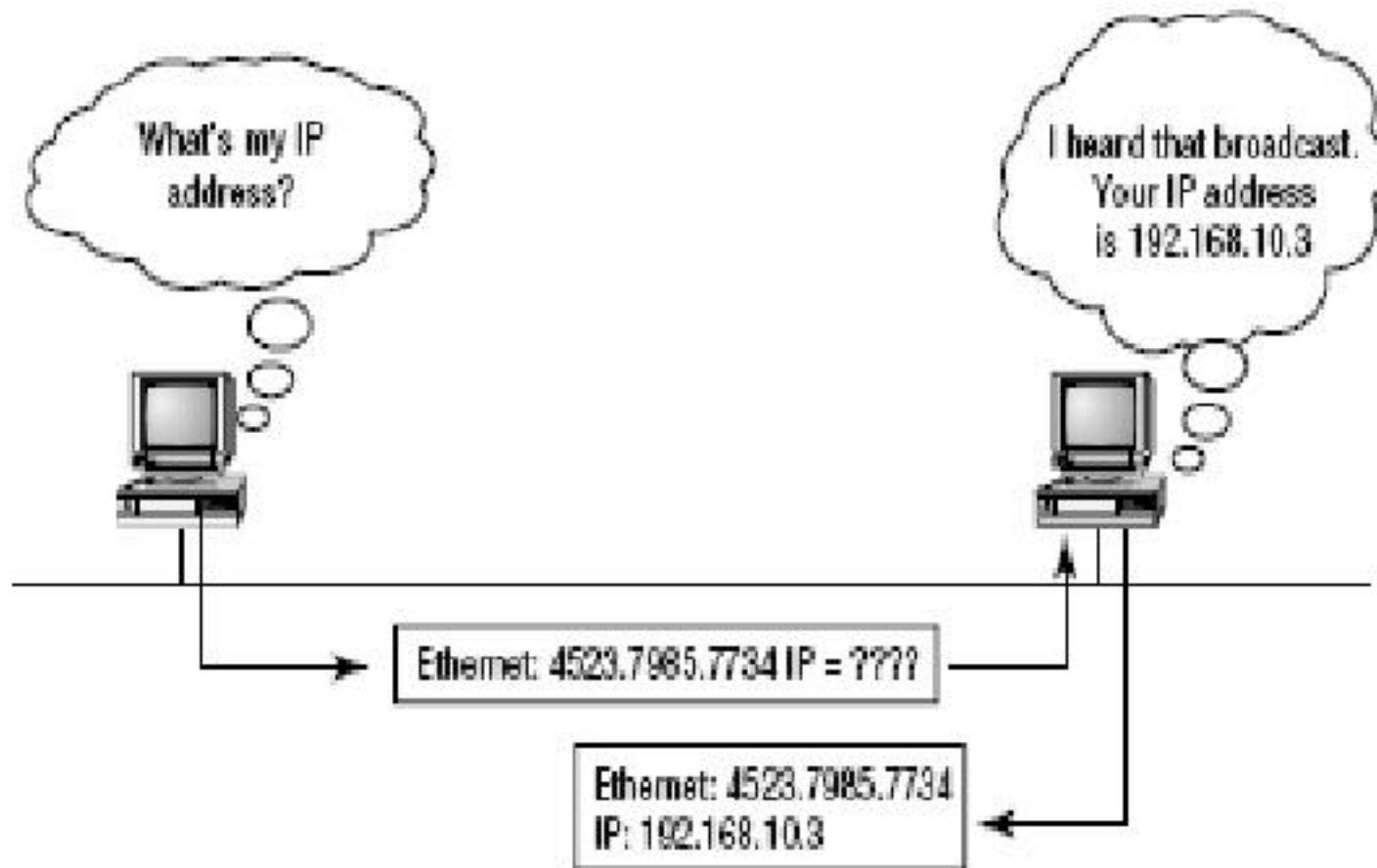
Khuôn dạng gói tin IP

| | | | | |
|---------------------|-----|------------------|-----------------|-----------------|
| VER | IHL | Type of services | Total length | |
| Identification | | | Flags | Fragment offset |
| Time to live | | Protocol | Header checksum | |
| Source address | | | | |
| Destination address | | | | |
| Options + Padding | | | | |
| Data | | | | |

ARP



RARP



Lớp truy nhập mạng

- Ethernet
 - Là giao thức truy cập LAN phổ biến nhất.
 - Được hình thành bởi định nghĩa chuẩn 802.3 của IEEE (Institute of Electrical and Electronics Engineers).
 - Tốc độ truyền 10Mbps
- Fast Ethernet
- Gigabit Ethernet

Chuyển đổi giữa các hệ thống số

- Hệ 2 (nhị phân): gồm 2 ký số 0, 1
- Hệ 8 (bát phân): gồm 8 ký số 0, 1, ..., 7
- Hệ 10 (thập phân): gồm 10 ký số 0, 1, ..., 9
- Hệ 16 (thập lục phân): gồm các ký số 0, 1, ..., 9 và các chữ cái A, B, C, D, E, F

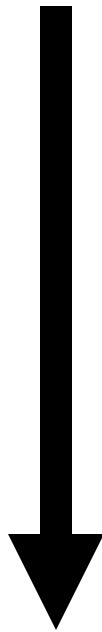

Chuyển đổi giữa hệ nhị phân sang hệ thập phân

$$10110_2 = (1 \times 2^4) + (0 \times 2^3) + (1 \times 2^2) + (1 \times 2^1) + (0 \times 2^0) = 16 + 0 + 4 + 2 + 0 = 22$$

| | |
|--------------------------|---|
| Place Value | <u>128</u> <u>64</u> <u>32</u> <u>16</u> <u>8</u> <u>4</u> <u>2</u> <u>1</u> |
| Base ^{Exponent} | $2^7 = 128$ $2^3 = 8$ $2^6 = 64$ $2^2 = 4$ $2^5 = 32$ $2^1 = 2$ $2^4 = 16$ $2^0 = 1$ |
| Number of Symbols | 2 |
| Symbols | 0, 1 |
| Rationale | Two-state (discrete binary) voltage systems made from transistors can be diverse, powerful, inexpensive, tiny and relatively immune to noise. |

Chuyển đổi giữa hệ thập phân sang hệ nhị phân

Đổi số 201_{10} sang nhị phân:

| | | | | |
|--|-----------------|----|---|--|
|  | $201 / 2 = 100$ | dư | 1 |  |
| | $100 / 2 = 50$ | dư | 0 | |
| | $50 / 2 = 25$ | dư | 0 | |
| | $25 / 2 = 12$ | dư | 1 | |
| | $12 / 2 = 6$ | dư | 0 | |
| | $6 / 2 = 3$ | dư | 0 | |
| | $3 / 2 = 1$ | dư | 1 | |
| | $1 / 2 = 0$ | dư | 1 | |

Khi thương số bằng 0, ghi các số dư theo thứ tự ngược với lúc xuất hiện, kết quả: $201_{10} = 11001001_2$

Chuyển đổi giữa hệ nhị phân sang hệ bát phân và thập lục phân

- Nhị phân sang bát phân:
 - Gom nhóm số nhị phân thành từng nhóm 3 chữ số tính từ phải sang trái. Mỗi nhóm tương ứng với một chữ số ở hệ bát phân.
 - Ví dụ: $1'101'100_{(2)} = 154_{(8)}$
- Nhị phân sang thập lục phân:
 - Tương tự như nhị phân sang bát phân nhưng mỗi nhóm có 4 chữ số.
 - Ví dụ: $110'1100_{(2)} = 6C_{(16)}$

Các phép toán làm việc trên bit

| A | B | A and B |
|----------|----------|----------------|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 0 |

Địa chỉ IP và các lớp địa chỉ

- Địa chỉ IP là địa chỉ có cấu trúc với một con số có kích thước 32 bit, chia thành 4 phần mỗi phần 8 bit gọi là octet hoặc byte.
- Ví dụ:
 - 172.16.30.56
 - 10101100 00010000 00011110 00111000.
 - AC 10 1E 38

Địa chỉ IP và các lớp địa chỉ

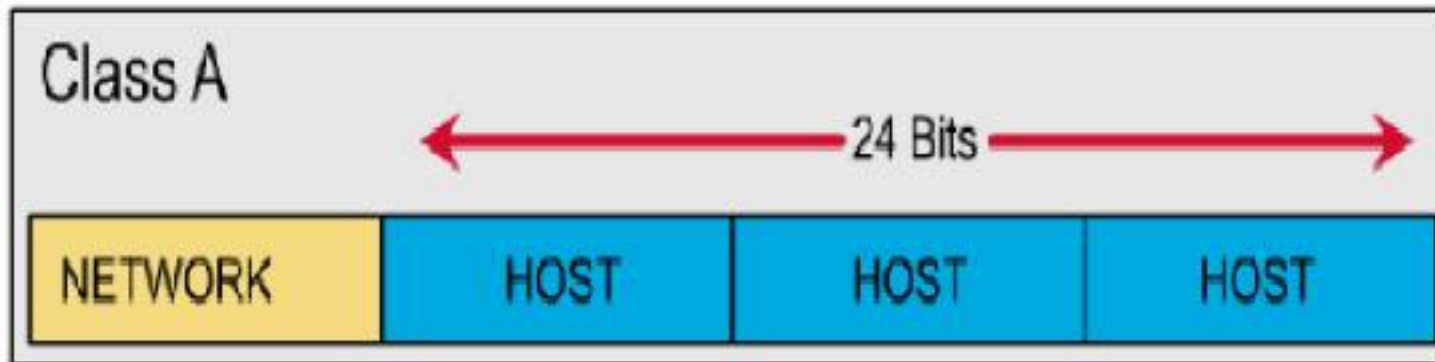
- Địa chỉ host là địa chỉ IP có thể dùng để đặt cho các interface của các host. Hai host nằm cùng một mạng sẽ có network_id giống nhau và host_id khác nhau.
- Khi cấp phát các địa chỉ host thì lưu ý **không được cho tất cả các bit trong phần host_id bằng 0 hoặc tất cả bằng 1.**
- Địa chỉ mạng (network address): là địa chỉ IP dùng để đặt cho các mạng. Phần host_id của địa chỉ chỉ chứa các bit 0. Ví dụ: 172.29.0.0
- Địa chỉ Broadcast: là địa chỉ IP được dùng để đại diện cho tất cả các host trong mạng. Phần host_id chỉ chứa các bit 1. Ví dụ: 172.29.255.255.

Các lớp địa chỉ IP

Không gian địa chỉ IP được chia thành 5 lớp (class) A, B, C, D và E. Các lớp A, B và C được triển khai để đặt cho các host trên mạng Internet, lớp D dùng cho các nhóm multicast, còn lớp E phục vụ cho mục đích nghiên cứu.

Lớp A (Class A)

Dành 1 byte cho phần network_id và 3 byte cho phần host_id.



Class A:



Lớp A (Class A)

- Bit đầu tiên của byte đầu tiên phải là bit 0. Dạng nhị phân của octet này là $0xxxxxxx$
- Những địa chỉ IP có byte đầu tiên nằm trong khoảng từ 0 ($=00000000_{(2)}$) đến 127 ($=01111111_{(2)}$) sẽ thuộc lớp A.
- Ví dụ: 50.14.32.8.

Lớp A (Class A)

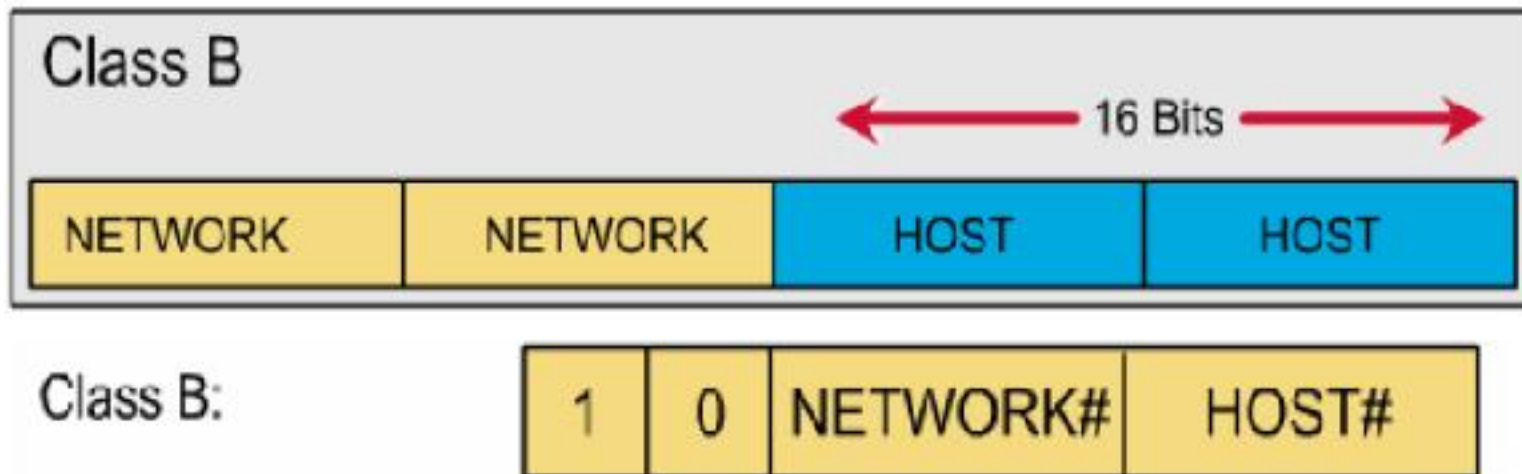
- Byte đầu tiên này cũng chính là `network_id`, trừ đi bit đầu tiên làm ID nhận dạng lớp A, còn lại 7 bit để đánh thứ tự các mạng, ta được 128 ($=2^7$) mạng lớp A khác nhau. **Bỏ đi hai trường hợp đặc biệt là 0 và 127.** Kết quả là lớp A chỉ còn 126 địa chỉ mạng, **1.0.0.0** đến **126.0.0.0**.

Lớp A (Class A)

- Phần host_id chiếm 24 bit, nghĩa là có $2^{24} = 16777216$ host khác nhau trong mỗi mạng. Bỏ đi hai trường hợp đặc biệt (phần host_id chứa toàn các bit 0 và bit 1). Còn lại: 16777214 host.
- Ví dụ đối với mạng 10.0.0.0 thì những giá trị host hợp lệ là 10.0.0.1 đến 10.255.255.254.

Lớp B (Class B)

Dành 2 byte cho phần network_id và 2 byte cho phần host_id.



Lớp B (Class B)

- Hai bit đầu tiên của byte đầu tiên phải là 10. Dạng nhị phân của octet này là **10**xxxxxx
- Những địa chỉ IP có byte đầu tiên nằm trong khoảng từ 128 (= **10**000000₍₂₎) đến 191 (= **10**111111₍₂₎) sẽ thuộc về lớp B
- Ví dụ: 172.29.10.1 .

Lớp B (Class B)

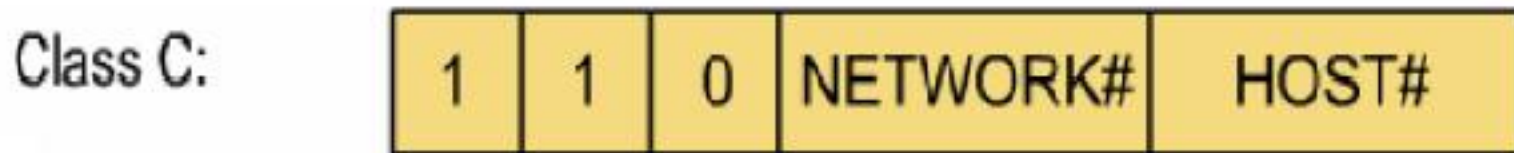
- Phần network_id chiếm 16 bit bỏ đi 2 bit làm ID cho lớp, còn lại 14 bit cho phép ta đánh thứ tự 16384 ($=2^{14}$) mạng khác nhau (128.0.0.0 đến 191.255.0.0).

Lớp B (Class B)

- Phần host_id dài 16 bit hay có 65536 ($=2^{16}$) giá trị khác nhau. Trừ đi 2 trường hợp đặc biệt còn lại 65534 host trong một mạng lớp B.
- Ví dụ đối với mạng 172.29.0.0 thì các địa chỉ host hợp lệ là từ 172.29.0.1 đến 172.29.255.254.

Lớp C (Class C)

Dành 3 byte cho phần network_id và 1 byte cho phần host_id.



Lớp C (Class C)

- Ba bit đầu tiên của byte đầu tiên phải là 110. Dạng nhị phân của octet này là **110**xxxxx
- Những địa chỉ IP có byte đầu tiên nằm trong khoảng từ 192 (= **110**00000₍₂₎) đến 223 (= **110**11111₍₂₎) sẽ thuộc về lớp C.
- Ví dụ: 203.162.41.235

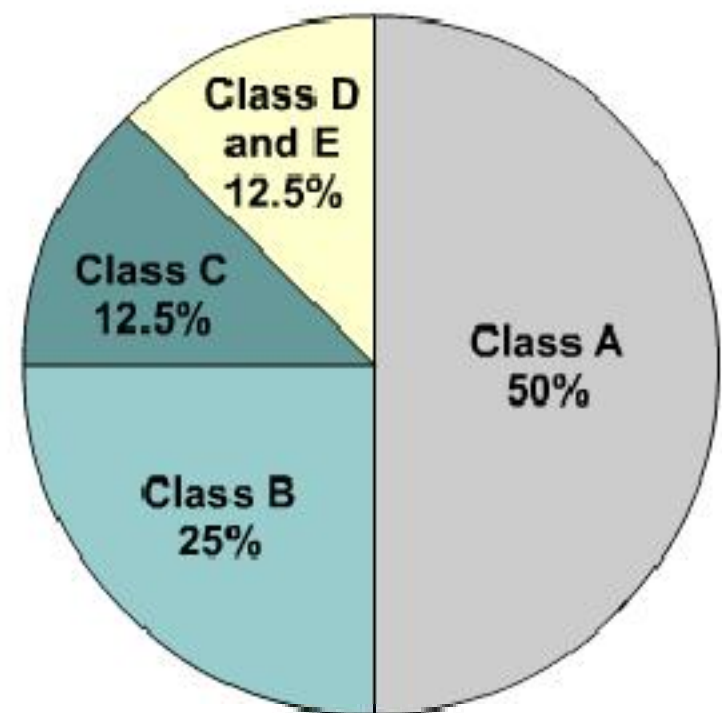
Các lớp địa chỉ IP

| Address Class | Number of Networks | Number of Host per Network |
|---------------|--------------------|----------------------------|
| A | 126 * | 16,777,216 |
| B | 16,384 | 65,535 |
| C | 2,097,152 | 254 |
| D (Multicast) | N/A | N/A |

| IP Address Class | High Order Bits | First Octet Address Range | Number of Bits in the Network Address |
|------------------|-----------------|---------------------------|---------------------------------------|
| Class A | 0 | 0 - 127 * | 8 |
| Class B | 10 | 128 - 191 | 16 |
| Class C | 110 | 192 - 223 | 24 |
| Class D | 1110 | 224 - 239 | 28 |

Các lớp địa chỉ IP

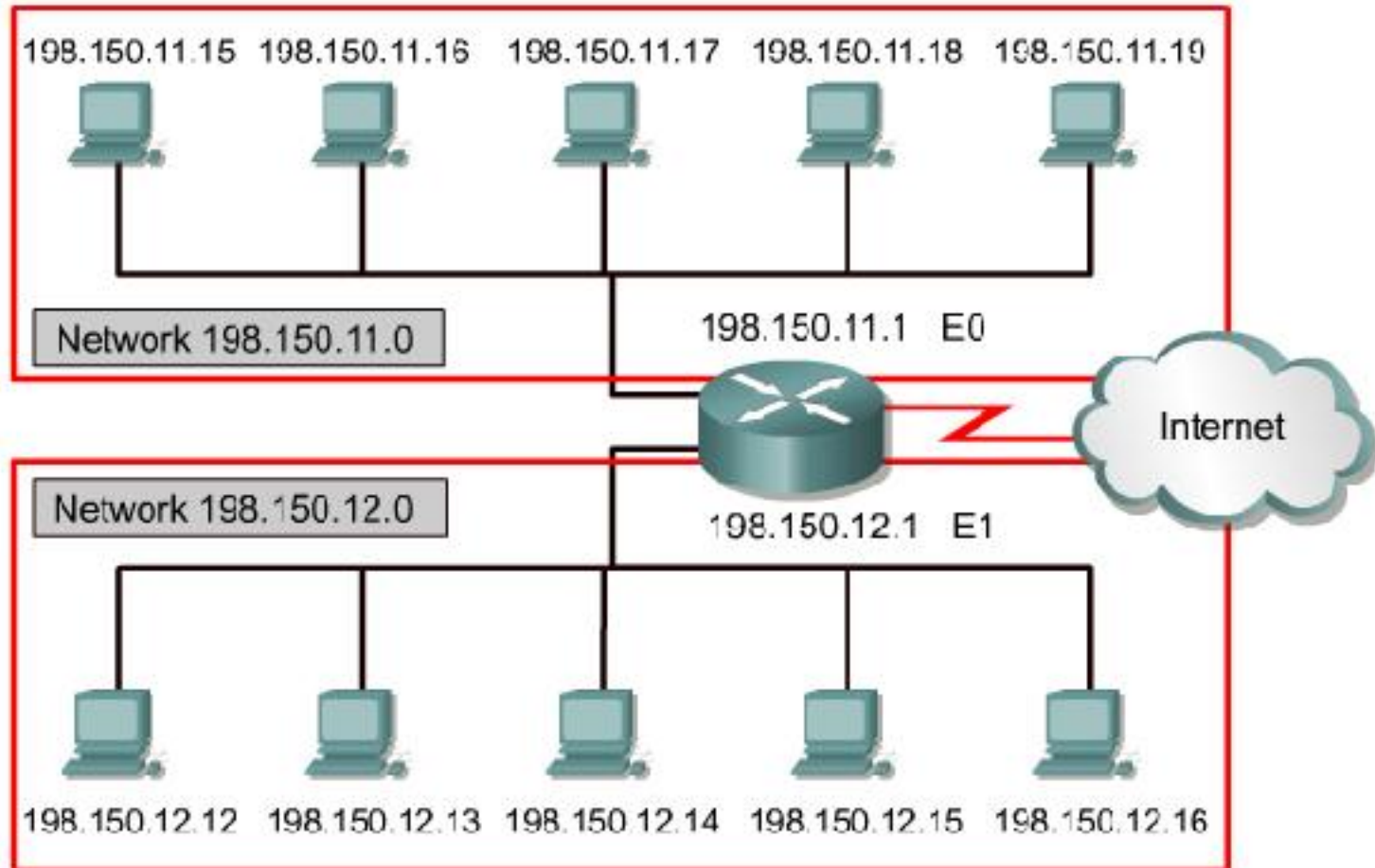
| IP address class | IP address range (First Octet Decimal Value) |
|------------------|---|
| Class A | 1-126 (00000001-01111110) * |
| Class B | 128-191 (10000000-10111111) |
| Class C | 192-223 (11000000-11011111) |
| Class D | 224-239 (11100000-11101111) |
| Class E | 240-255 (11110000-11111111) |



Địa chỉ dành riêng

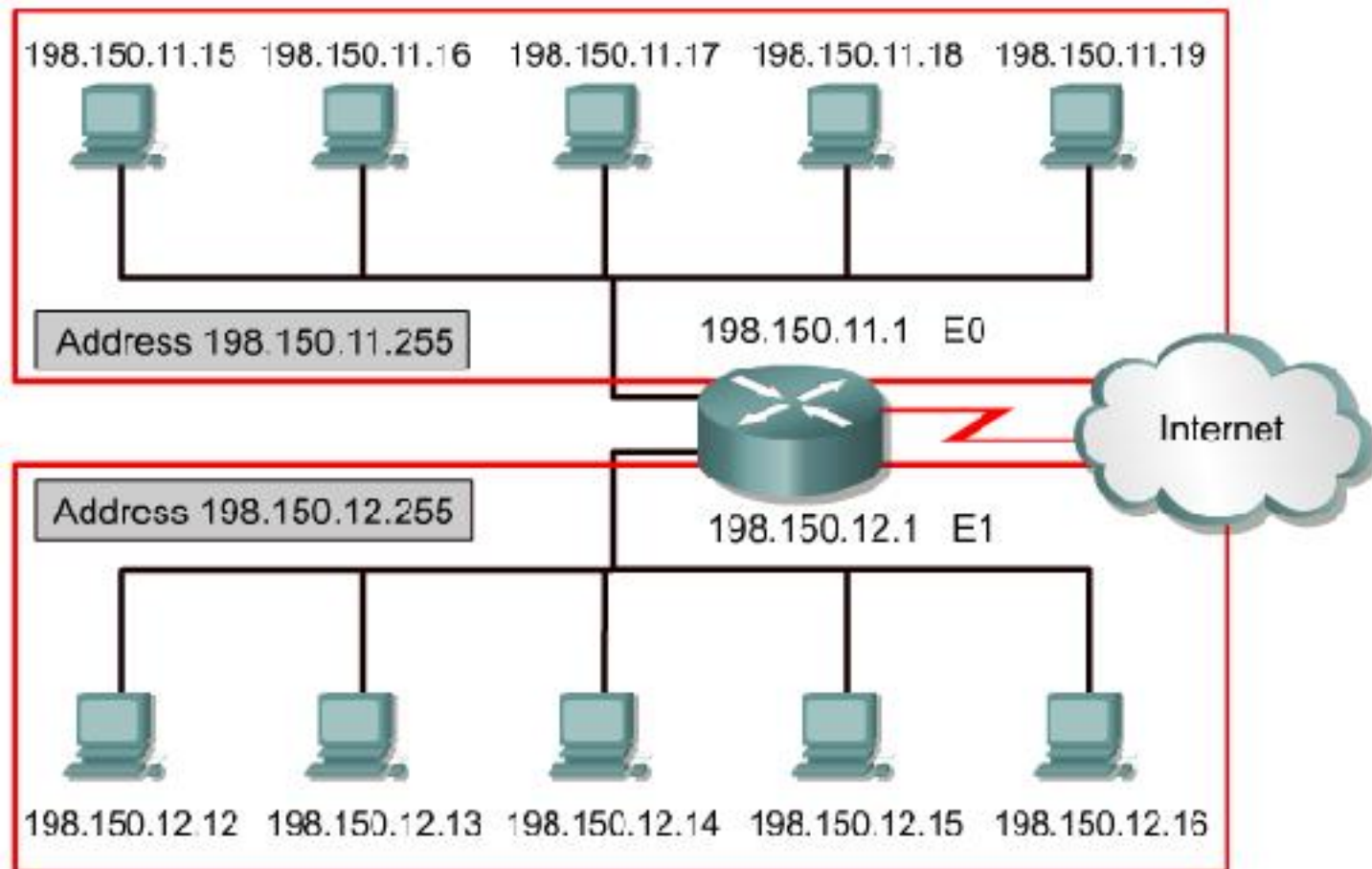
| Class | RFC 1918 internal address range |
|-------|---------------------------------|
| A | 10.0.0.0 to 10.255.255.255 |
| B | 172.16.0.0 to 172.31.255.255 |
| C | 192.168.0.0 to 192.168.255.255 |

Các lớp địa chỉ IP



Địa chỉ mạng

Các lớp địa chỉ IP



Địa chỉ broadcast

Các lớp địa chỉ IP

| Lớp | Byte đầu tiên |
|-----|---------------|
| A | 0xxxxxxx |
| B | 10xxxxxx |
| C | 110xxxxx |
| D | 1110xxxx |
| E | 11110xxx |

- **1.0.0.0 - 126.0.0.0 : Class A.**
- **127.0.0.0 : Loopback network.**
- **128.0.0.0 - 191.255.0.0 : Class B.**
- **192.0.0.0 - 223.255.255.0 : Class C.**

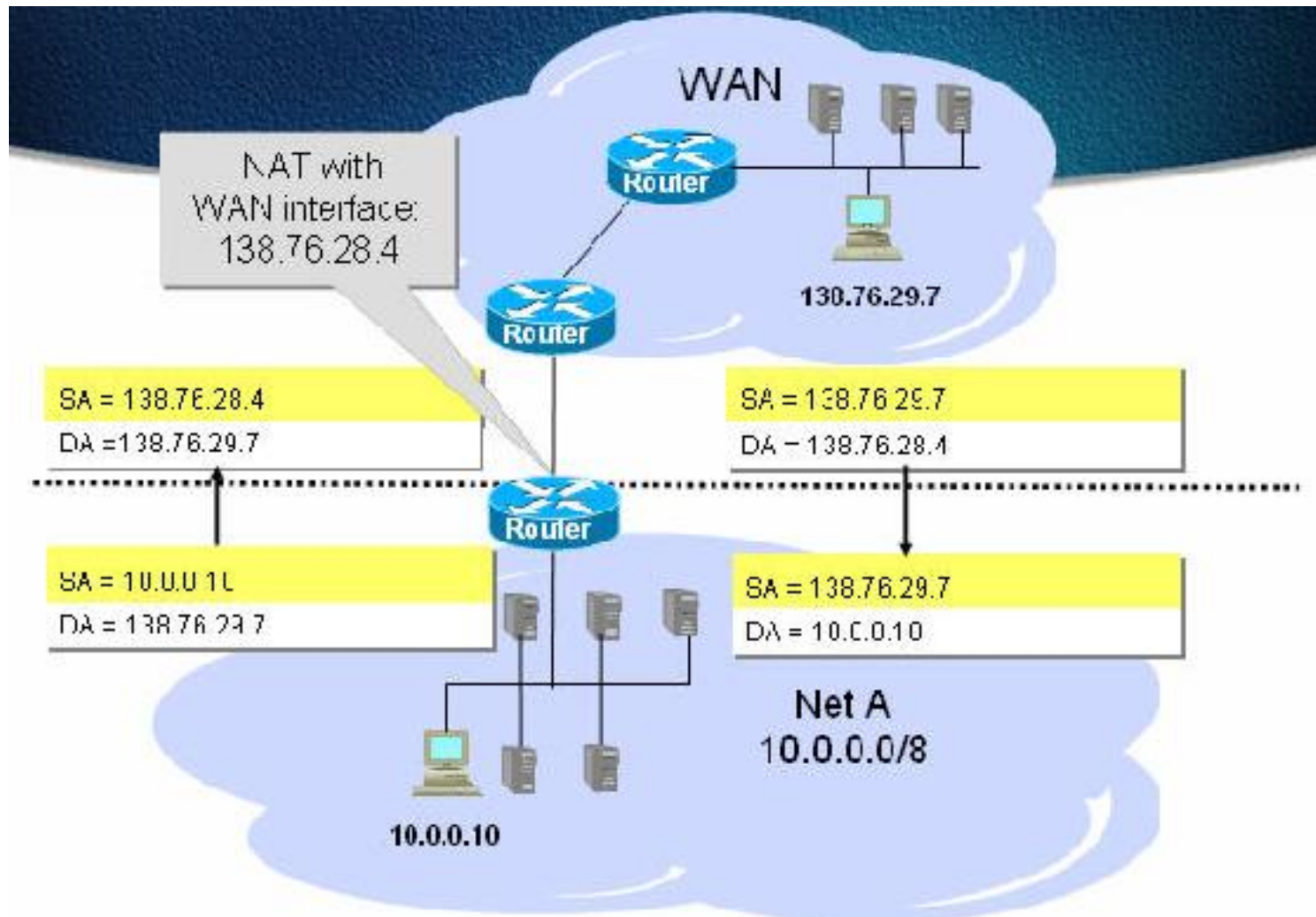
NAT: Network Address Translation

- Được thiết kế để tiết kiệm địa chỉ IP.
- Cho phép mạng nội bộ sử dụng địa chỉ IP riêng.
- Địa chỉ IP riêng sẽ được chuyển đổi sang địa chỉ công cộng định tuyến được.
- Mạng riêng được tách biệt và giấu kín IP nội bộ.
- Thường sử dụng trên router biên của mạng một cửa.

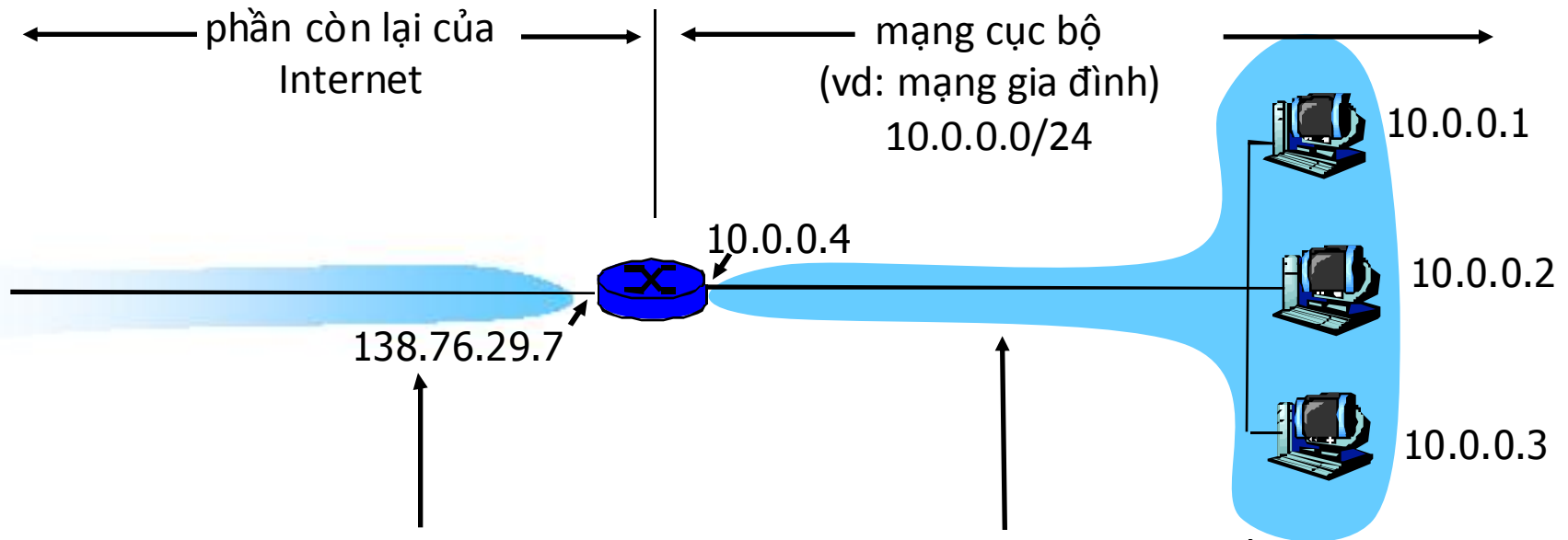
NAT

- Địa chỉ cục bộ bên trong (Inside local address): Địa chỉ được phân phối cho các host bên trong mạng nội bộ.
- Địa chỉ toàn cục bên trong (Inside global address): Địa chỉ hợp pháp được cung cấp bởi InterNIC (Internet Network Information Center) hoặc nhà cung cấp dịch vụ Internet, đại diện cho một hoặc nhiều địa chỉ nội bộ bên trong đối với thế giới bên ngoài.
- Địa chỉ cục bộ bên ngoài (Outside local address): Địa chỉ riêng của host nằm bên ngoài mạng nội bộ.
- Địa chỉ toàn cục bên ngoài (Outside global address): Địa chỉ công cộng hợp pháp của host nằm bên ngoài mạng nội bộ.

NAT



NAT



Tất cả datagram *đi ra khỏi* mạng cục bộ có **cùng** một địa chỉ IP NAT là: 138.76.29.7, với các số hiệu cổng nguồn khác nhau

các Datagram với nguồn hoặc đích trong mạng này có địa chỉ 10.0.0/24

NAT

- Mạng cục bộ chỉ dùng 1 địa chỉ IP đối với bên ngoài:
 - không cần thiết dùng 1 vùng địa chỉ từ ISP: chỉ cần 1 cho tất cả các thiết bị
 - có thể thay đổi địa chỉ các thiết bị trong mạng cục bộ mà không cần thông báo với bên ngoài
 - có thể thay đổi ISP mà không cần thay đổi địa chỉ các thiết bị trong mạng cục bộ
 - các thiết bị trong mạng cục bộ không nhìn thấy, không định địa chỉ rõ ràng từ bên ngoài (tăng cường bảo mật)

NAT

Hiện thực: NAT router phải:

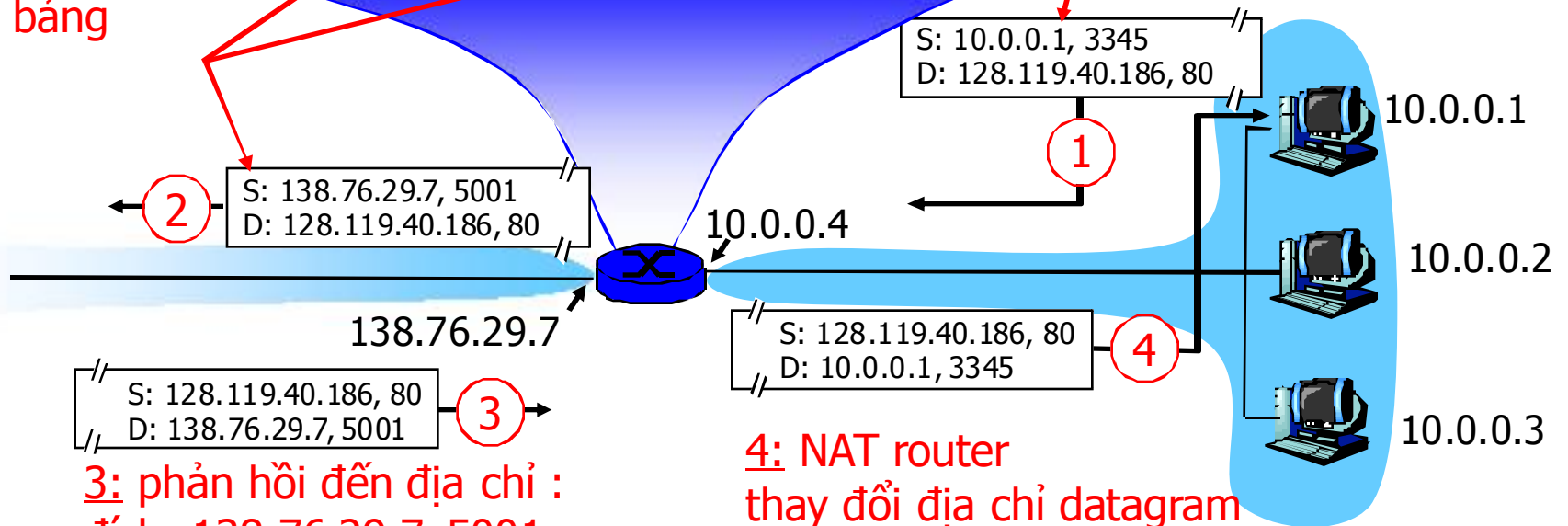
- *các datagram đi ra:* thay thế (địa chỉ IP và số hiệu cổng nguồn) mọi datagram đi ra bên ngoài bằng (địa chỉ NAT IP và số hiệu cổng nguồn mới)
 - . . . các clients/servers ở xa sẽ dùng (địa chỉ NAT IP và số hiệu cổng nguồn mới) đó như địa chỉ đích
- *ghi nhớ (trong bảng chuyển đổi NAT)* mọi cặp chuyển đổi (địa chỉ IP và số hiệu cổng nguồn) sang (địa chỉ NAT IP và số hiệu cổng nguồn mới)
- *các datagram đi đến:* thay thế (địa chỉ NAT IP và số hiệu cổng nguồn mới) trong các trường đích của mọi datagram đến với giá trị tương ứng (địa chỉ IP và số hiệu cổng nguồn) trong bảng NAT

NAT

| bảng chuyển đổi NAT | |
|---------------------|------------------|
| địa chỉ phía WAN | địa chỉ phía LAN |
| 138.76.29.7, 5001 | 10.0.0.1, 3345 |
| | |

2: NAT router thay đổi địa chỉ từ 10.0.0.1, 3345 -> 138.76.29.7, 5001 cập nhật bảng

1: host 10.0.0.1 gửi datagram đến 128.119.40.186, 80



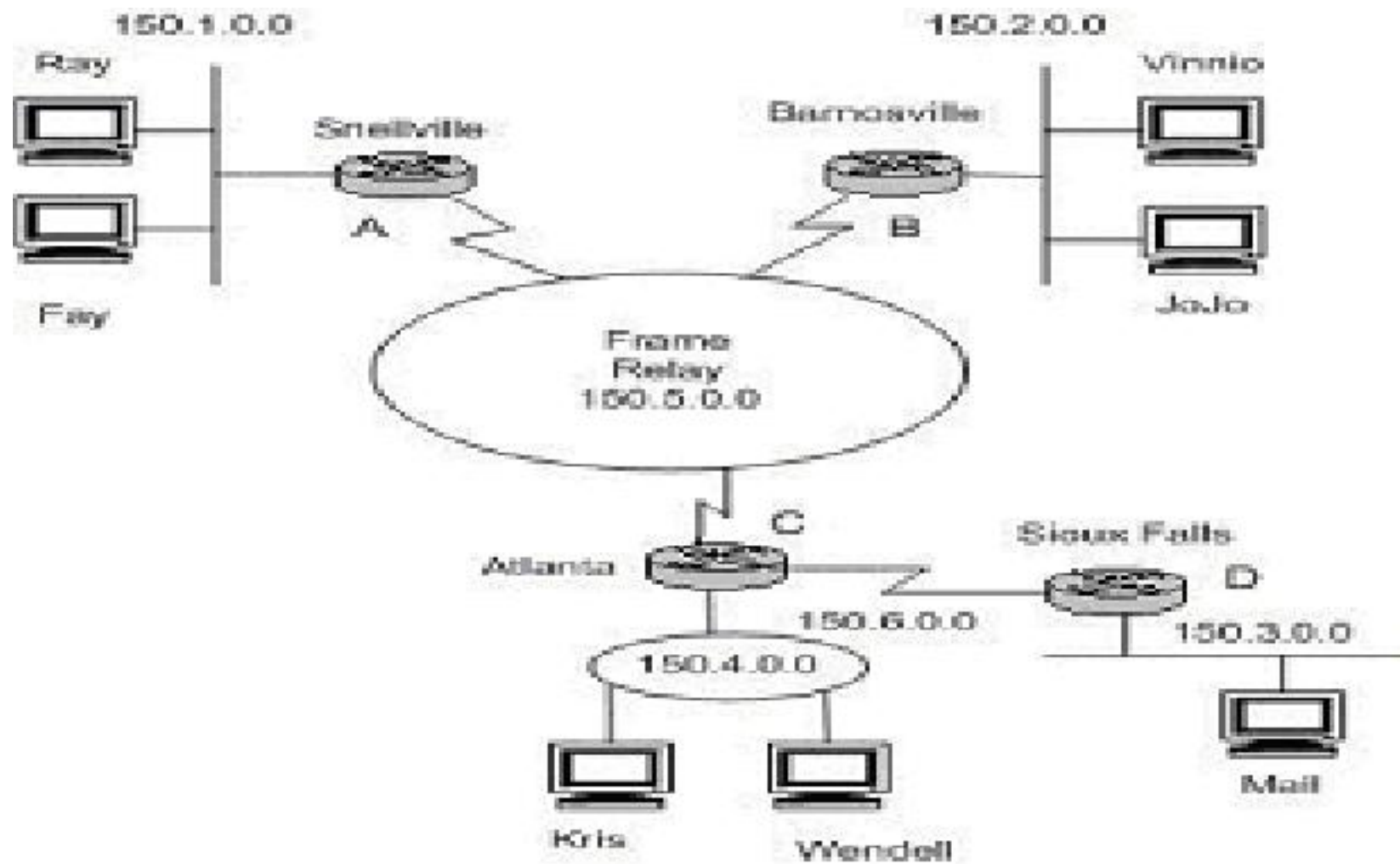
3: phản hồi đến địa chỉ : đích 138.76.29.7, 5001

4: NAT router thay đổi địa chỉ datagram đích từ 138.76.29.7, 5001 -> 10.0.0.1, 3345

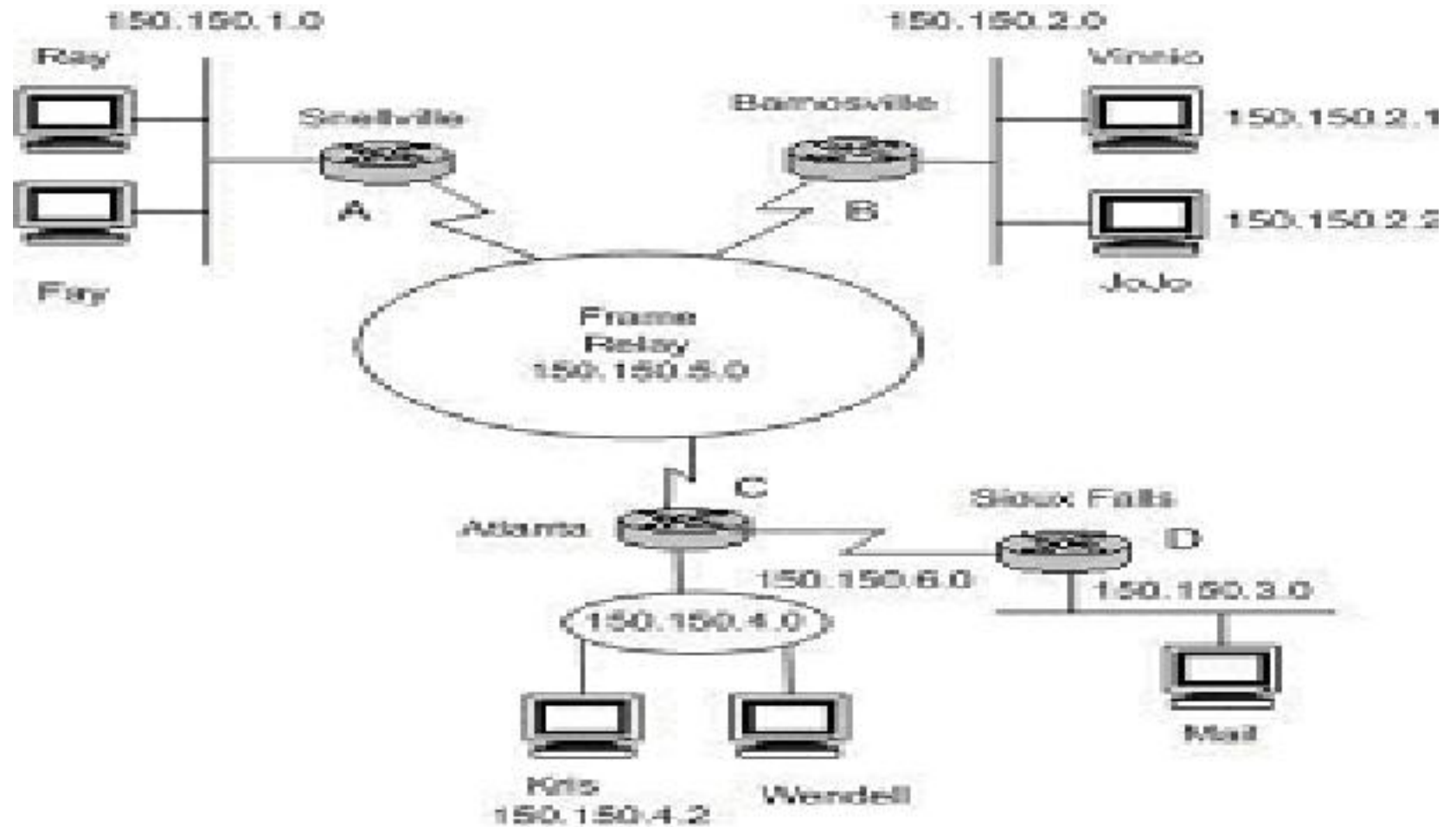
NAT

- Trường số hiệu cổng 16-bit:
 - Cho phép 60000 kết nối đồng thời chỉ với một địa chỉ phía WAN
- NAT còn có thể gây ra tranh luận:
 - các router chỉ xử lý đến lớp 3
 - vi phạm thỏa thuận end-to-end
 - những người thiết kế ứng dụng phải tính đến khả năng NAT, vd: ứng dụng P2P
 - sự thiếu thốn địa chỉ IP sẽ được giải quyết khi dùng IPv6

Mạng con

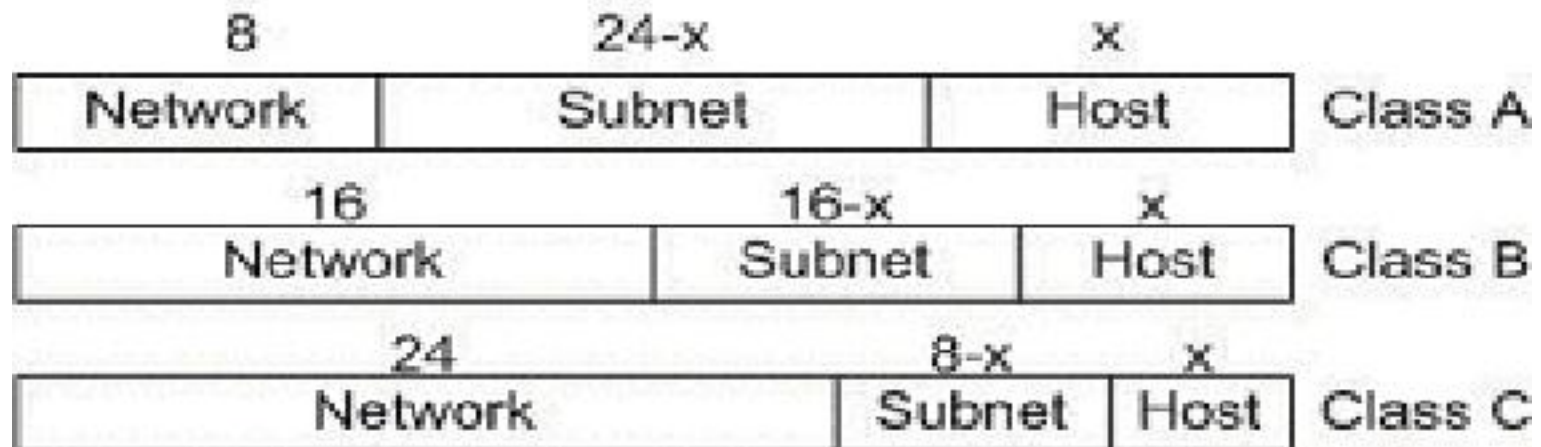


Mạng con



Kỹ thuật chia mạng con

- Mượn một số bit trong phần host_id ban đầu để đặt cho các mạng con
- Cấu trúc của địa chỉ IP lúc này sẽ gồm 3 phần: network_id, subnet_id và host_id.



Kỹ thuật chia mạng con

- Số bit dùng trong subnet_id tùy thuộc vào chiến lược chia mạng con. Tuy nhiên số bit tối đa có thể mượn phải tuân theo công thức:

$$\text{Subnet_id} \leq \text{host_id} - 2$$

- Số lượng bit tối đa có thể mượn:
 - Lớp A: **22** (= 24 – 2) bit -> chia được $2^{22} = 4194304$ mạng con
 - Lớp B: **14** (= 16 – 2) bit -> chia được $2^{14} = 16384$ mạng con
 - Lớp C: **06** (= 8 – 2) bit -> chia được $2^6 = 64$ mạng con

Kỹ thuật chia mạng con

- Số bit trong phần subnet_id xác định số lượng mạng con. Với số bit là x thì 2^x là số lượng mạng con có được.
- Ngược lại từ số lượng mạng con cần thiết theo nhu cầu, tính được phần subnet_id cần bao nhiêu bit. Nếu muốn chia 6 mạng con thì cần 3 bit ($2^3=8$), chia 12 mạng con thì cần 4 bit ($2^4 \geq 12$).

Một số khái niệm mới

- Địa chỉ mạng con (địa chỉ đường mạng): gồm cả phần `network_id` và `subnet_id`, phần `host_id` chỉ chứa các bit 0
- Địa chỉ broadcast trong một mạng con: tất cả các bit trong phần `host_id` là 1.
- Mặt nạ mạng con (subnet mask): tất cả các bit trong phần `host_id` là 0, các phần còn lại là 1.

Quy ước ghi địa chỉ IP

- Nếu có địa chỉ IP như 172.29.8.230 thì chưa thể biết được host này nằm trong mạng nào, có chia mạng con hay không và có nếu chia thì dùng bao nhiêu bit để chia. Chính vì vậy khi ghi nhận địa chỉ IP của một host, phải cho biết subnet mask của nó
- Ví dụ: 172.29.8.230/255.255.255.0 hoặc 172.29.8.230/24 (có nghĩa là dùng 24 bit đầu tiên cho NetworkID).

Kỹ thuật chia mạng con

- Thực hiện 3 bước:
 - **Bước 1:** Xác định lớp (class) và subnet mask mặc nhiên của địa chỉ.
 - **Bước 2:** Xác định số bit cần mượn và subnet mask mới, tính số lượng mạng con, số host thực sự có được.
 - **Bước 3:** Xác định các vùng địa chỉ host và chọn mạng con muốn dùng

Bài tập 1

Cho địa chỉ IP sau: 172.16.0.0/16.
Hãy chia thành 8 mạng con và có
tối thiểu 1000 host trên mỗi
mạng con đó.

Bước 1: Xác định class và subnet mask mặc nhiên

Giải:

- Địa chỉ trên viết dưới dạng nhị phân
10101100.00010000.00000000.00000000
- Xác định lớp của IP trên:
→ **Lớp B**
- Xác định Subnet mask mặc nhiên:
→ **255.255.0.0**

Bước 2: Số bit cần mượn...

➤ Cần mượn bao nhiêu bit:

→ $N = 3$, bởi vì:

→ Số mạng con có thể: $2^3 = 8$.

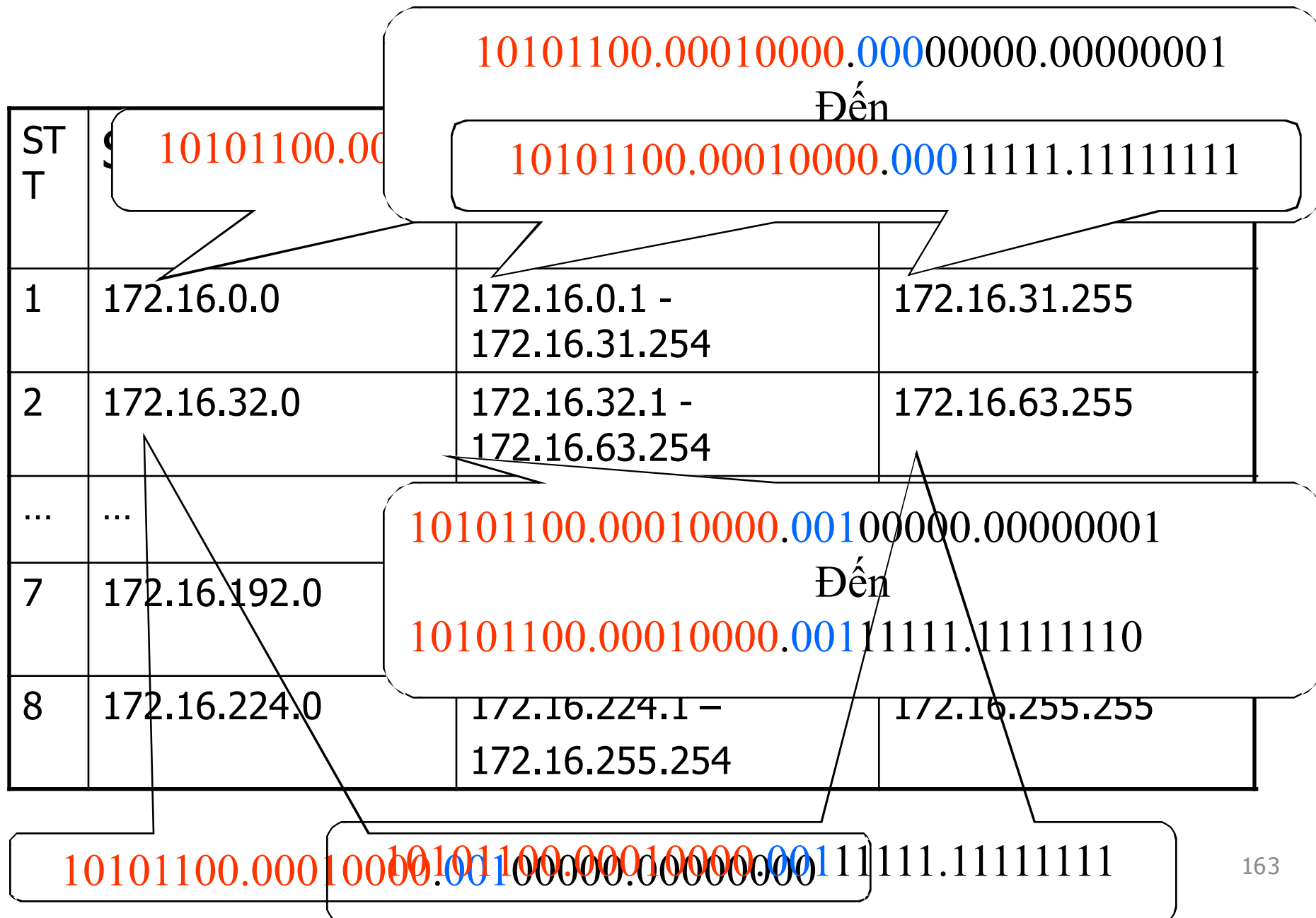
→ Số host của mỗi mạng con có thể:
 $2^{(16-3)} - 2 = 2^{13} - 2 > 1000$.

➤ Xác định Subnet mask mới:

→ 11111111.11111111.11100000.00000000

→ hay 255.255.224.0

Bước 3: Xác định vùng địa chỉ host



Bài tập 2

Cho 2 địa chỉ IP sau:

192.168.5.9/28

192.168.5.39/28

- Hãy cho biết các địa chỉ network, host của từng IP trên?
- Các máy trên có cùng mạng hay không ?
- Hãy liệt kê tất cả các địa chỉ IP thuộc các mạng vừa tìm được?

Địa chỉ IP thứ nhất: 192.168.5.9/28

- Chú ý: 28 là số bit dành cho NetworkID
- Đây là IP thuộc lớp C
- Subnet mask mặc nhiên: 255.255.255.0

| | | | | |
|----------------------|----------|----------|----------|----------|
| IP (thập phân) | 192 | 168 | 5 | 9 |
| | ↓ | ↓ | ↓ | ↓ |
| IP (nhị phân) | 11000000 | 10101000 | 00000101 | 00001001 |

Thực hiện AND địa chỉ IP với Subnet mask

| | | | | |
|-------------|----------|----------|----------|----------|
| IP | 11000000 | 10101000 | 00000101 | 00001001 |
| | ↓ | ↓ | ↓ | ↓ |
| Subnet mask | 11111111 | 11111111 | 11111111 | 11110000 |
| | ↓ | ↓ | ↓ | ↓ |
| Kết quả AND | 11000000 | 10101000 | 00000101 | 00000000 |

Chuyển IP sang dạng thập phân

| | | | | |
|-------------|----------|----------|-----------------|----------|
| Kết quả AND | 11000000 | 10101000 | 00000101 | 00000000 |
| Net ID | 192 | 168 | 5 | 0 |
| Host ID | | | <u>00001001</u> | 9 |

Địa chỉ IP thứ hai: 192.168.5.39/28

| IP | 192 | 168 | 5 | 39 |
|---------------|----------|----------|----------|----------|
| IP (nhị phân) | 11000000 | 10101000 | 00000101 | 00100111 |
| Subnet Mask | 11111111 | 11111111 | 11111111 | 11110000 |
| AND | 11000000 | 10101000 | 00000101 | 00100000 |
| Network ID | 192 | 168 | 5 | 32 |
| HostID | | | | 7 |

Hai địa chỉ trên có cùng mạng?

- 192.168.5.9/28
- 192.168.5.39/28

Kết luận: Hai địa chỉ trên không cùng mạng

| | | | | |
|--------------------------|-----|-----|---|----|
| Net ID của địa chỉ thứ 1 | 192 | 168 | 5 | 0 |
| Net ID của địa chỉ thứ 2 | 192 | 168 | 5 | 32 |

Liệt kê tất cả các địa chỉ IP

| Mạng tương ứng với IP | Vùng địa chỉ HostID với dạng nhị phân | Vùng địa chỉ HostID với dạng thập phân |
|-----------------------|--|--|
| 1 | 11000000.10101000.00000101.00000001 | 192.168.5.1/28 |
| | Đến 11000000.10101000.00000101.00001110 | Đến 192.168.5.14/28 |
| 2 | 11000000.10101000.00000101.00100001 | 192.168.5.33/28 |
| | Đến 11000000.10101000.00000101.00101110 | Đến 192.168.5.46/28 |

Bài tập 3

Hãy xét đến một địa chỉ IP class B, **139.12.0.0**, với subnet mask là **255.255.0.0**. Một Network với địa chỉ thể này có thể chứa 65534 nodes hay computers. Đây là một con số quá lớn, trên mạng sẽ có đầy broadcast traffic. Hãy chia network thành 5 mạng con.

Bước 1: Xác định Subnet mask

- Để chia thành 5 mạng con thì cần thêm 3 bit (vì $2^3 > 5$).
- Do đó Subnet mask sẽ cần: 16 (bits trước đây) + 3 (bits mới) = 19 bits
- Địa chỉ IP mới sẽ là **139.12.0.0/19** (để ý con số **19** thay vì **16** như trước đây).

Bước 2: Liệt kê ID của các Subnet mới

| Subnet mask với dạng nhị phân | Subnet mask với dạng thập phân |
|-------------------------------------|--------------------------------|
| 11111111.11111111.11100000.00000000 | 255.255.224.0 |

NetworkID của bốn Subnets mới

| TT | Subnet ID với dạng nhị phân | Subnet ID với dạng thập phân |
|----|-------------------------------------|------------------------------|
| 1 | 10001011.00001100.00000000.00000000 | 139.12.0.0/19 |
| 2 | 10001011.00001100.00100000.00000000 | 139.12.32.0/19 |
| 3 | 10001011.00001100.01000000.00000000 | 139.12.64.0/19 |
| 4 | 10001011.00001100.01100000.00000000 | 139.12.96.0/19 |
| 5 | 10001011.00001100.10000000.00000000 | 139.12.128.0/19 |

Bước 3: Cho biết vùng địa chỉ IP của các HostID

| TT | Dạng nhị phân | Dạng thập phân |
|----|--|--|
| 1 | 10001011.00001100.00000000.00000001 10001011.00001100.00011111.11111110 | 139.12.0.1/19 - 139.12.31.254/19 |
| 2 | 10001011.00001100.00100000.00000001 10001011.00001100.00111111.11111110 | 139.12.32.1/19 - 139.12.63.254/19 |
| 3 | 10001011.00001100.01000000.00000001 10001011.00001100.01011111.11111110 | 139.12.64.1/19 - 139.12.95.254/19 |
| 4 | 10001011.00001100.01100000.00000001 10001011.00001100.01111111.11111110 | 139.12.96.1/19 - 139.12.127.254/19 |
| 5 | 10001011.00001100.10000000.00000001 10001011.00001100.10011111.11111110 | 139.12.128.1/19 - 139.12.159.254/19 |

Tính nhanh vùng địa chỉ IP

- n – số bit làm subnet
- Số mạng con: $S = 2^n$
- Số gia địa chỉ mạng con: $M = 2^{8-n}$ ($n \leq 8$)
- Byte cuối của IP địa chỉ mạng, ví dụ lớp C: $(k-1)*M$ (với $k=1,2,\dots$)
- Byte cuối của IP host đầu tiên, ví dụ lớp C: $(k-1)*M + 1$ (với $k=1,2,\dots$)
- Byte cuối của IP host cuối cùng, ví dụ lớp C: $k*M - 2$ (với $k=1,2,\dots$)
- Byte cuối của IP broadcast, ví dụ lớp C: $k*M - 1$ (với $k=1,2,\dots$)

Ví dụ tính nhanh vùng địa chỉ IP

- Cho địa chỉ: 192.168.0.0/24
- Với $n=4 \rightarrow M=16 (= 2^{8-4}) \rightarrow$
 - Network 1: 192.168.0.0. Host range: 192.168.0.1–192.168.0.14. Broadcast: 192.168.0.15
 - Network 2: 192.168.0.16. Host range: 192.168.0.17–192.168.0.30. Broadcast: 192.168.0.31
 - Network 3: 192.168.0.32. Host range: 192.168.0.33–192.168.0.46. Broadcast: 192.168.0.47
 - Network 4: 192.168.0.48. Host range: 192.168.0.49–192.168.0.62. Broadcast: 192.168.0.63

Bài tập 4

- Cho địa chỉ IP: 102.16.10.107/12
 - Tìm địa chỉ mạng con? Địa chỉ host
 - Dải địa chỉ host có cùng mạng với IP trên?
 - Broadcast của mạng mà IP trên thuộc vào?

Bước: Tính subnet mask

- 102.16.10.107/12 →
- Subnet mask:
11111111.11110000.00000000.00000000
- Byte đầu tiên chắc chắn khi dùng phép toán AND ra kết quả bằng 102 → không cần đổi 102 sang nhị phân

Trả lời câu hỏi 1: Địa chỉ mạng con?

- Xét byte kế tiếp là: 16 (10) → 00010000 (2)
- Khi AND byte này với Subnet mask, ta được kết quả là: 00010000 (2)
- Như vậy địa chỉ mạng con sẽ là:

102.16.0.0/12

- Như vậy địa chỉ host sẽ là:

0.10.107

Trả lời câu hỏi 2: Dải địa chỉ host? Broadcast?

- Dải địa chỉ host sẽ từ:

01100110 00010000 00000000 00000001

(hay 102.16.0.1/12)

Đến:

01100110 00011111 11111111 11111110

(hay 102.31.255.254/12)

- Broadcast:

102.31.255.255/12

Bài tập 5: Cho IP 172.19.160.0/21

- Chia làm 4 mạng con
- Liệt kê các thông số gồm địa chỉ mạng, dãy địa chỉ host, địa chỉ broadcast của các mạng con đó

Giải BT 5

- Chia làm 4 mạng con nên phải mượn 2 bit
- Do /21 nên 2 byte đầu tiên của IP đã cho không thay đổi. Xét byte thứ 3
- $160 = 10100\underline{000}_{(2)}$
- Phần 2 bit 00 là nơi ta mượn làm subnet

Giải BT 5 (tt)

- Xét byte thứ 3
- Mạng con thứ 1: $10100000_{(2)}$
- Mạng con thứ 2: $10100010_{(2)}$
- Mạng con thứ 3: $10100100_{(2)}$
- Mạng con thứ 4: $10100110_{(2)}$

Giải BT 5 (tt)

| Địa chỉ mạng | Dải địa chỉ host | Địa chỉ broadcast |
|--------------|------------------------------------|-------------------|
| 172.19.160.0 | 172.19.160.1 đến 172.19.161.254 | 172.19.161.255 |
| 172.19.162.0 | 172.19.162.1 đến 172.19.163.254 | 172.19.163.255 |
| 172.19.164.0 | 172.19.164.1 đến 172.19.165.254 | 172.19.165.255 |
| 172.19.166.0 | 172.19.166.1 đến 172.19.167.254 | 172.19.167.255 |

Bài tập 6: Cho IP 172.16.192.0/18

- Chia làm 4 mạng con
- Liệt kê các thông số gồm địa chỉ mạng, dãy địa chỉ host, địa chỉ broadcast của các mạng con đó

Giải BT 6

- Chia làm 4 mạng con nên phải mượn 2 bit
- Do /18 nên 2 byte đầu tiên của IP đã cho không thay đổi. Xét byte thứ 3
- $192 = 11\underline{00}0000_{(2)}$
- Phần 2 bit 00 là nơi ta mượn làm subnet

Giải BT 6 (tt)

- Xét byte thứ 3
- Mạng con thứ 1: $11000000_{(2)}$
- Mạng con thứ 2: $11010000_{(2)}$
- Mạng con thứ 3: $11100000_{(2)}$
- Mạng con thứ 4: $11110000_{(2)}$

Giải BT 6 (tt)

| Địa chỉ mạng | Dải địa chỉ host | Địa chỉ broadcast |
|--------------|------------------------------------|-------------------|
| 172.16.192.0 | 172.16.192.1 đến 172.16.207.254 | 172.16.207.255 |
| 172.16.208.0 | 172.16.208.1 đến 172.16.223.254 | 172.16.223.255 |
| 172.16.224.0 | 172.16.224.1 đến 172.16.239.254 | 172.16.239.255 |
| 172.16.240.0 | 172.16.240.1 đến 172.16.255.254 | 172.16.255.255 |

CHƯƠNG 6: BẢO MẬT MẠNG

- Hiểu các nguyên lý của bảo mật mạng:
 - mật mã
 - chứng thực
 - tính toàn vẹn
 - khóa phân bố
- Bảo mật trong thực tế:
 - các firewall
 - bảo mật trong các lớp application, transport, network, data-link

Bảo mật mạng là gì?

Sự bảo mật: chỉ có người gửi, người nhận mới “hiểu” được nội dung thông điệp

- người gửi mã hóa thông điệp
- người nhận giải mã thông điệp

Chứng thực: người gửi, người nhận xác định là nhận ra nhau

Sự toàn vẹn thông điệp: người gửi, người nhận muốn bảo đảm thông điệp không bị thay đổi (trên đường truyền hoặc sau khi nhận)

Truy cập & tính sẵn sàng: các dịch vụ phải có khả năng truy cập và sẵn sàng đối với các user

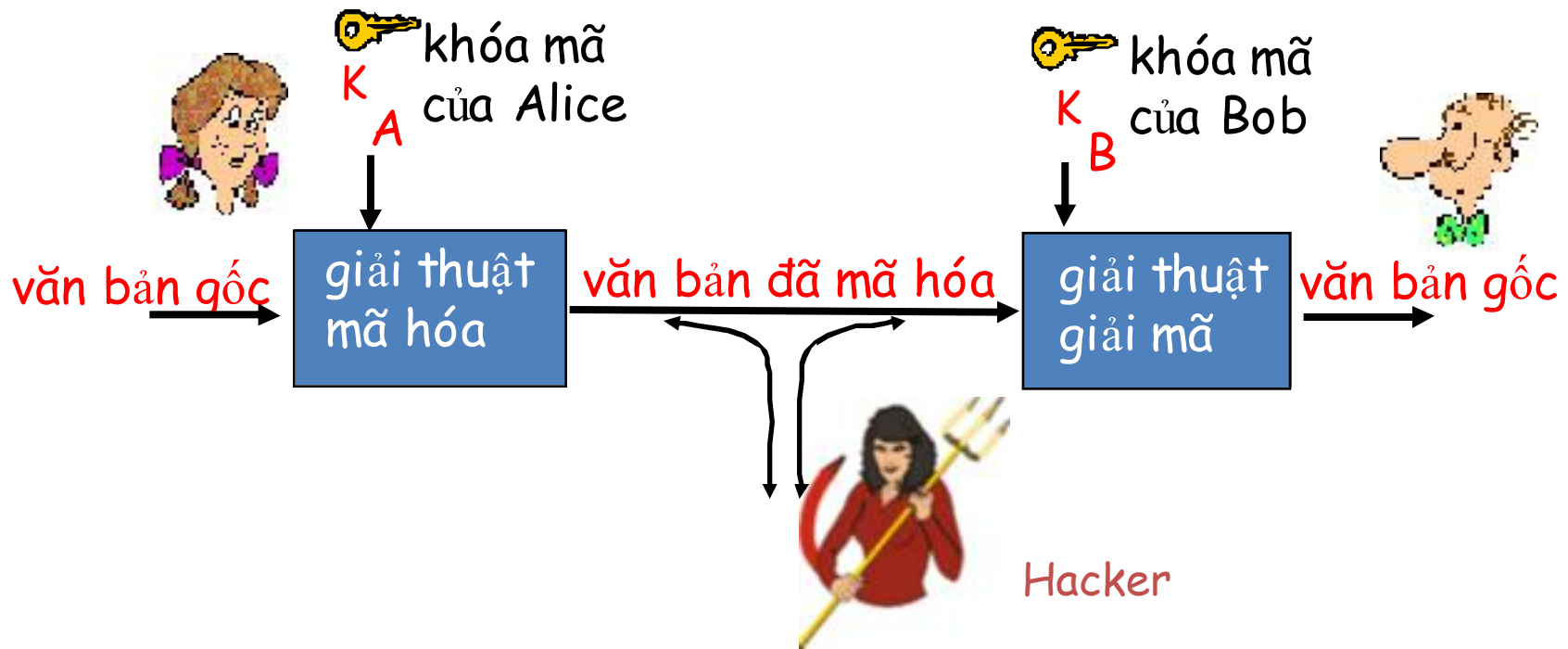
Các đối tượng cần bảo mật

- Trình duyệt Web/server cho các giao dịch điện tử
- Client/Server ngân hàng trực tuyến
- DNS servers
- Các router trao đổi thông tin cập nhật bảng routing
- .v.v.

Kẻ xấu có thể làm những việc gì?

- *nghe lén*: ngăn chặn các thông điệp
- kích hoạt *chèn* các thông điệp vào trong kết nối
- *giả danh*: có thể giả mạo địa chỉ nguồn trong gói (hoặc bất kỳ trường nào trong đó)
- *cướp*: “tiếp tục” kết nối hiện hành nhưng thay người gửi hoặc người nhận bằng chính họ
- *từ chối dịch vụ*: dịch vụ hiện tại bị người khác dùng (đồng nghĩa quá tải)
- .v.v.

Các nguyên lý mã hóa



khóa đối xứng: khóa bên gửi và bên nhận giống nhau

khóa công cộng: khóa mã chung, khóa giải mã bí mật (riêng)

Mã hóa khóa đối xứng

mật mã thay thế: thay thứ này thành thứ khác

– mã hóa ký tự đơn: thay thế từng ký tự một

văn bản gốc: abcdefghijklmnopqrstuvwxyz



văn bản đã mã hóa: mnbvcxzasdfghjklpoiuytrewq

ví dụ: văn bản gốc: Bob. i love you. Alice
 mã hóa thành: nko. s gktc wky. mgsbc

• Bẻ khóa kiểu mã hóa đơn giản này dễ không?

- brute force (khó như thế nào?)
- khác?

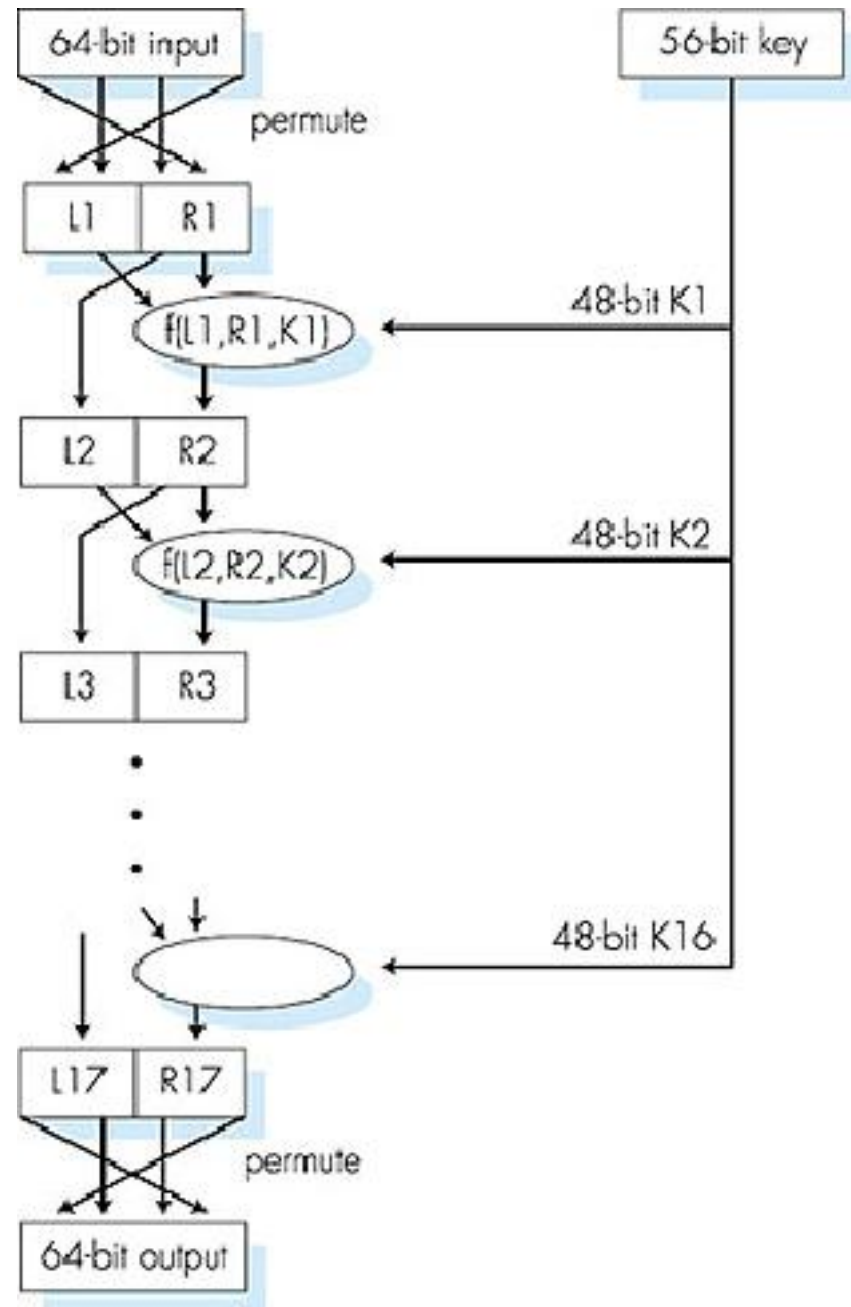
Mã hóa khóa đối xứng: DES

DES: Data Encryption Standard

- Chuẩn mã hóa của Hoa Kỳ [NIST 1993]
- Khóa đối xứng 56-bit, văn bản gốc vào 64-bit
- Bảo mật trong DES như thế nào?
 - chưa có cách tiếp cận “backdoor-cửa sau” để giải mã
- làm cho DES bảo mật hơn:
 - dùng 3 khóa tuần tự (3-DES) trong mỗi datum
 - dùng cơ chế liên kết khối mã

Mã hóa khóa đối xứng: DES

DES hoạt động



AES: Advanced Encryption Standard

- Chuẩn NIST khóa đối xứng mới (tháng 11-2001) thay thế cho DES
- Dữ liệu xử lý từng khối 128 bit
- Các khóa 128, 192 hoặc 256 bit
- Giải mã brute force (thử sai) tốn 1s với DES, tốn 149 tỷ tỷ năm với AES

Mã hóa khóa công cộng

khóa đối xứng

- yêu cầu người gửi, người nhận phải biết khóa công cộng
- Làm sao biết khóa công cộng đó trong lần đầu tiên (đặc biệt với những người chưa bao giờ gặp trước)?

Mã hóa khóa công cộng

- tiếp cận khác hoàn toàn
- người gửi, người nhận không chia sẻ khóa công cộng
- khóa công cộng cho mọi người đều biết
- khóa giải mã riêng chỉ có người nhận biết

Giải thuật mã hóa khóa công cộng

Yêu cầu:

① cần K_B^+ và K_B^- như sau:

$$K_B^-(K_B^+(m)) = m$$

② cho khóa công cộng K_B^+ , phải không thể tính toán ra được khóa riêng K_B^-

giải thuật RSA: Rivest, Shamir, Adelson

Sự chứng thực

Mục tiêu: Bob muốn Alice “chứng thực” nhân dạng của cô đối với anh ta

Mô tả cách thức hiện thực: Alice nói “Tôi là Alice”



“Tôi là Alice”



Thất bại sẽ xảy ra??



Sự toàn vẹn

- Chữ ký số: **Kỹ thuật mã hóa tương tự như các chữ ký bằng tay.**
 - người gửi (Bob) đánh dấu (số hóa) tài liệu, thiết lập thuộc tính là người sở hữu/tạo lập tài liệu.
 - **có thể kiểm tra, không thể làm giả:** người nhận (Alice) có thể chứng thực với người khác là chỉ có Bob chứ ngoài ra không có ai (kể cả Alice) đã ký trên tài liệu đó.

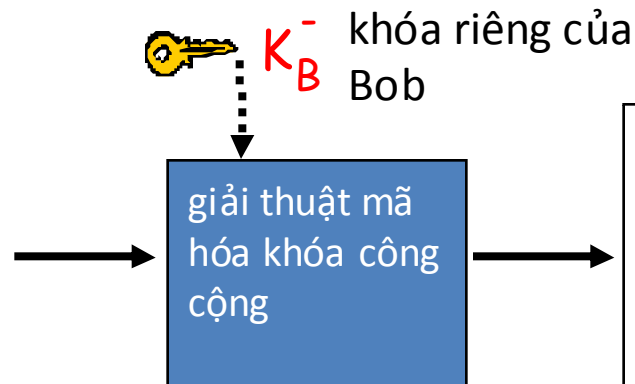
Chữ ký số

Chữ ký số đơn giản cho thông điệp m :

- Bob ký m bằng cách mã hóa với khóa riêng của anh ấy K_B^- , tạo thông điệp “đã được ký”, $K_B^-(m)$

thông điệp của Bob, m

Dear Alice
Oh, how I have missed
you. I think of you all the
time! ... (blah blah blah)
Bob



$K_B^-(m)$

thông điệp của
Bob là m , đã ký
(mã hóa) với khóa
riêng của anh ấy

Chữ ký số (tt)

- Giả sử Alice nhận được m , với chữ ký số hóa là $K_B(m)$
- Alice kiểm tra m đã được ký bởi Bob bằng cách áp dụng khóa công cộng của Bob là K_B cho $K_B(m)$ sau đó kiểm tra $K_B(K_B(m)) = m$.
- Nếu $K_B(K_B(m)) = m$, bất cứ ai đã ký m phải dùng khóa riêng của Bob

Alice kiểm tra:

- ✓ Bob đã ký m .
- ✓ Không có ai khác đã ký m .
- ✓ Bob đã ký m và không ký m' .

Không thể phủ nhận:

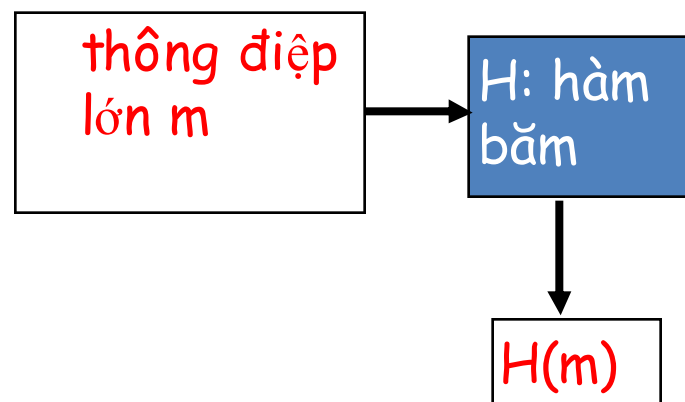
- ✓ Alice có thể giữ m và chữ ký $K_B(m)$ để chứng thực rằng Bob đã ký m .

Phân loại thông điệp

Tính toán các thông điệp dài
có chi phí đắt

Mục tiêu: “dấu tay” số hóa có
kích thước cố định, dễ tính
toán được

- áp dụng hàm băm H vào
m, tính được phân loại
thông điệp kích thước cố
định, $H(m)$.



Các đặc tính hàm băm:

- nhiều-một
- sinh ra phân loại thông điệp
kích thước cố định (“dấu
tay”)
- cho phân loại thông điệp x,
không thể tính toán để tìm
m dùng $x = H(m)$

Khóa phân bố và chứng chỉ

Vấn đề khóa đối xứng:

- Làm thế nào 2 thực thể cùng thiết lập khóa bí mật trên mạng?

Giải pháp:

- Trung tâm phân bố khóa (key distribution center-KDC) được tin cậy – hoạt động trung gian giữa các thực thể

Vấn đề khóa công cộng:

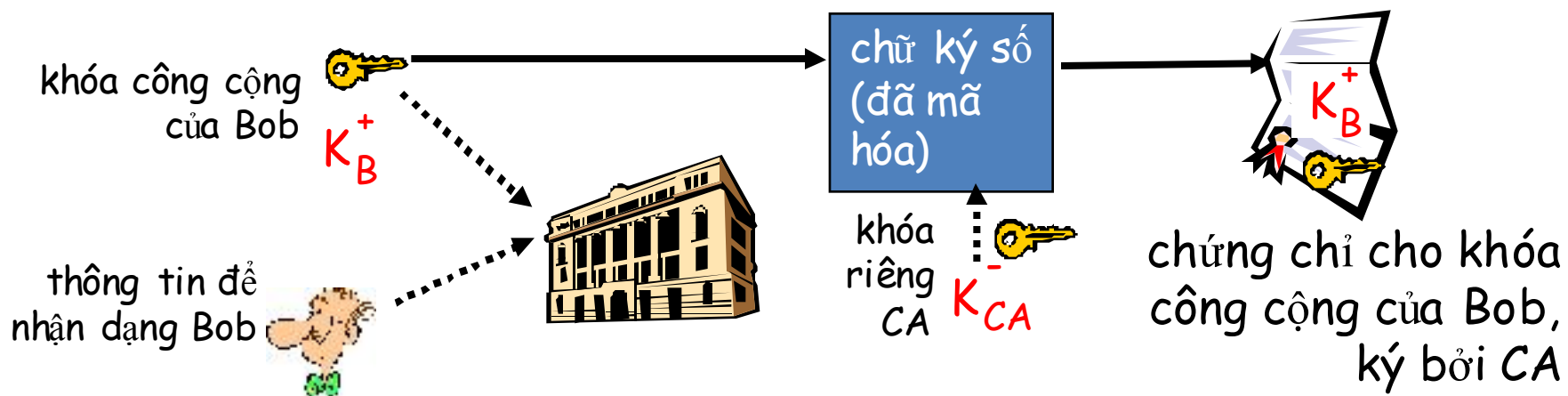
- Khi Alice lấy được khóa công cộng của Bob (từ web site, email, đĩa) làm sao biết khóa công cộng của Bob chứ không phải của Hacker?

Giải pháp:

- nơi cấp chứng chỉ (certification authority-CA) được tin cậy

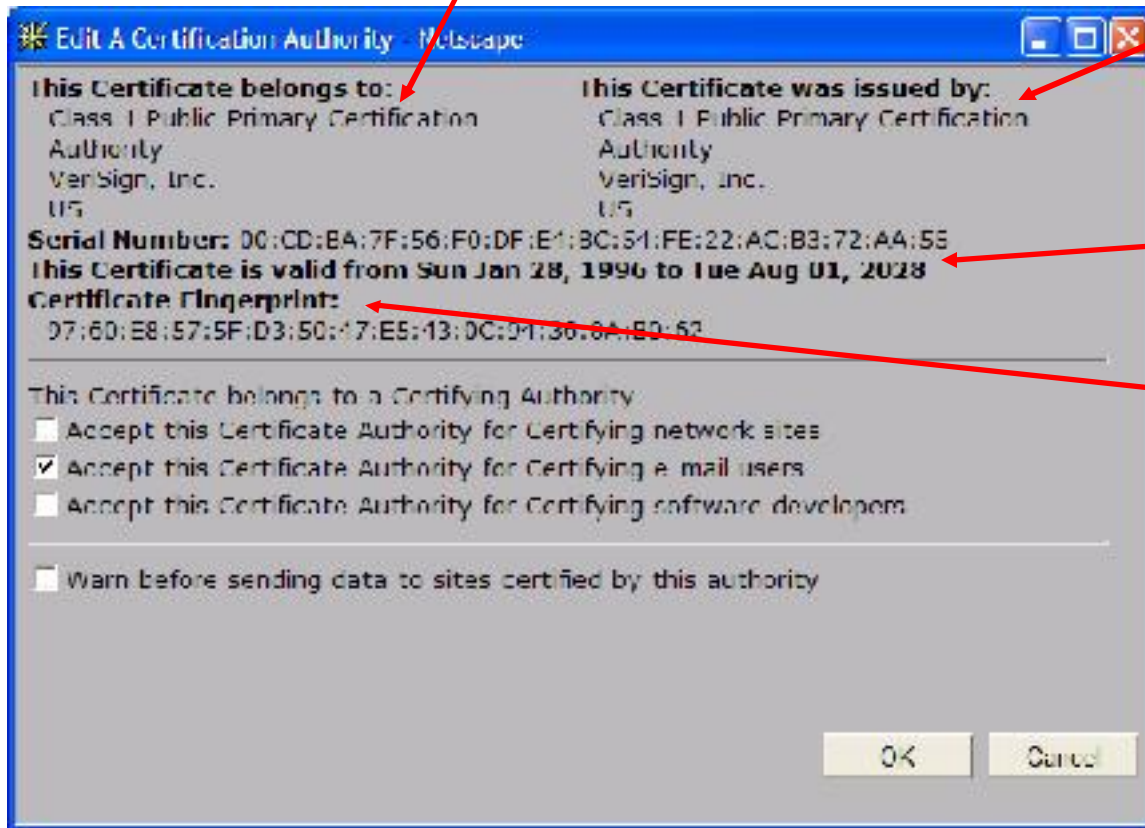
Cấp chứng chỉ

- **Certification authority (CA):** gắn kết khóa công cộng với thực thể E nào đó.
- E (người, router) đăng ký khóa công cộng của họ với CA.
 - E cung cấp “bằng chứng để nhận dạng” cho CA.
 - CA tạo ra chứng chỉ ràng buộc E với khóa công cộng của nó.
 - chứng chỉ chứa khóa công cộng của E được ký số bởi CA – CA nói “đây là khóa công cộng của E”



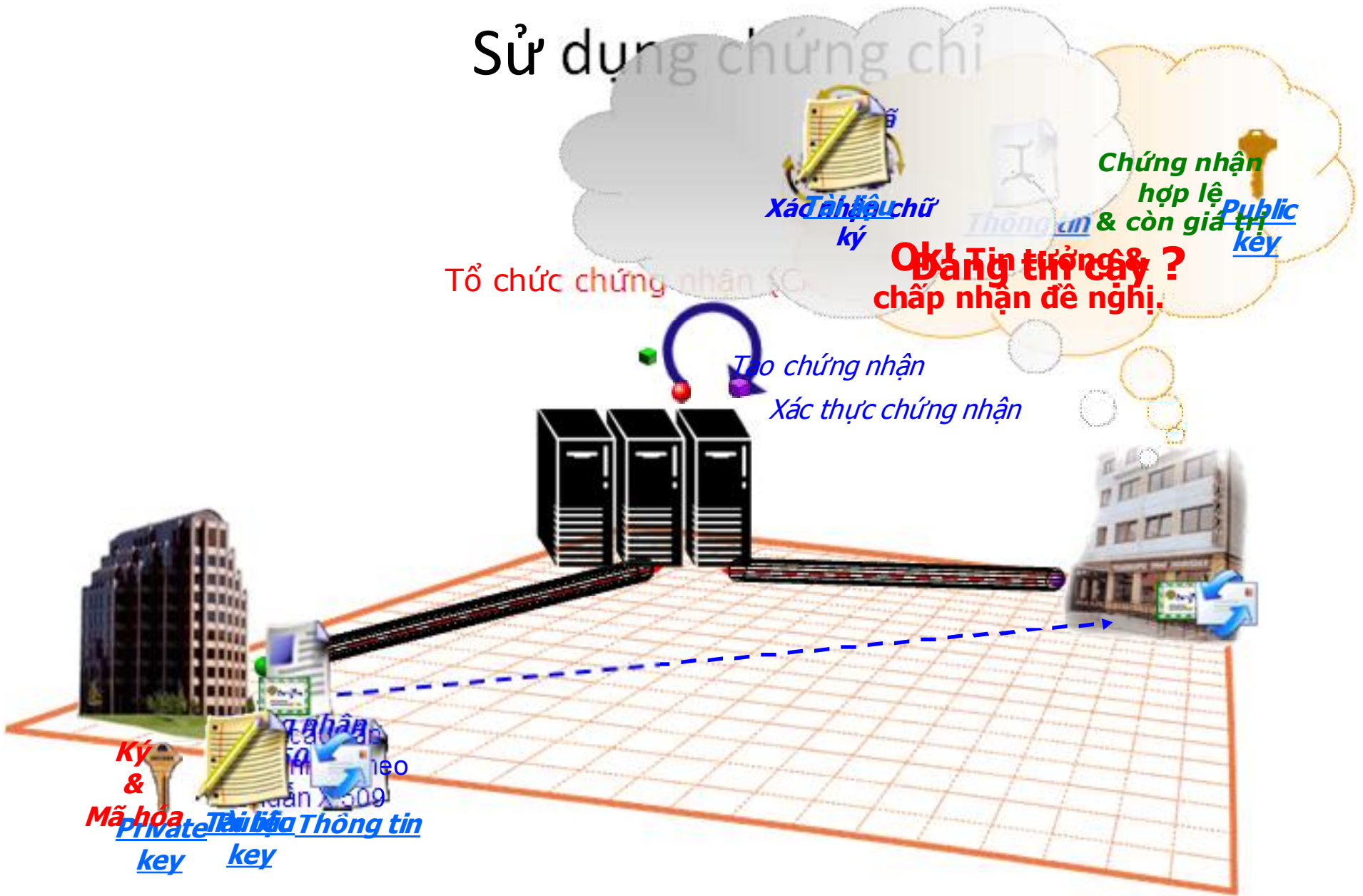
Mô tả chứng chỉ

- Số thứ tự (duy nhất)
- thông tin về người sở hữu chứng chỉ, bao gồm giải thuật và chính giá trị khóa (không hiển thị ra)

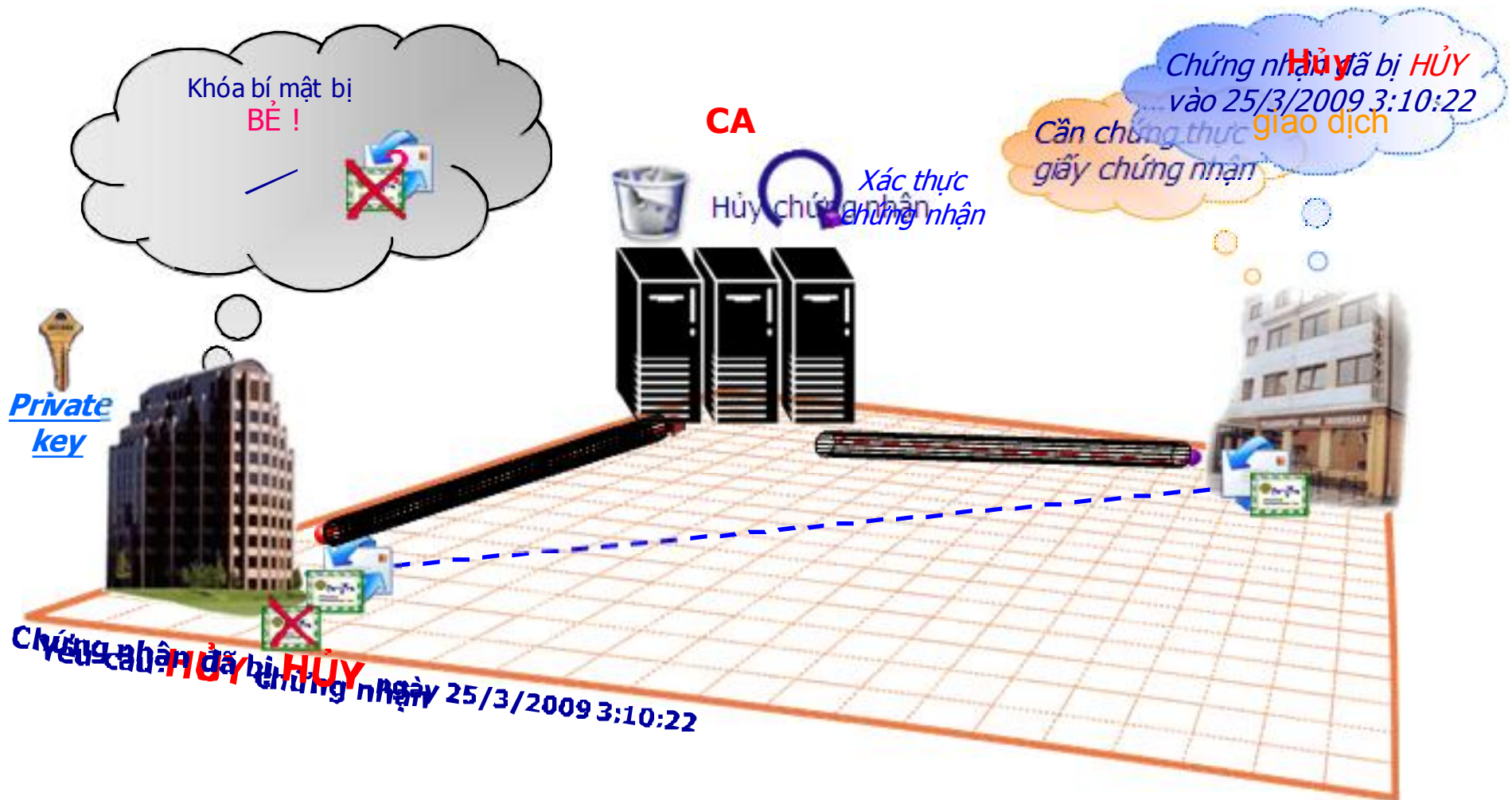


- thông tin về người phát hành chứng chỉ
- ngày kiểm tra tính hợp lệ
- chữ ký số bởi người phát hành chứng chỉ

Sử dụng chứng chỉ



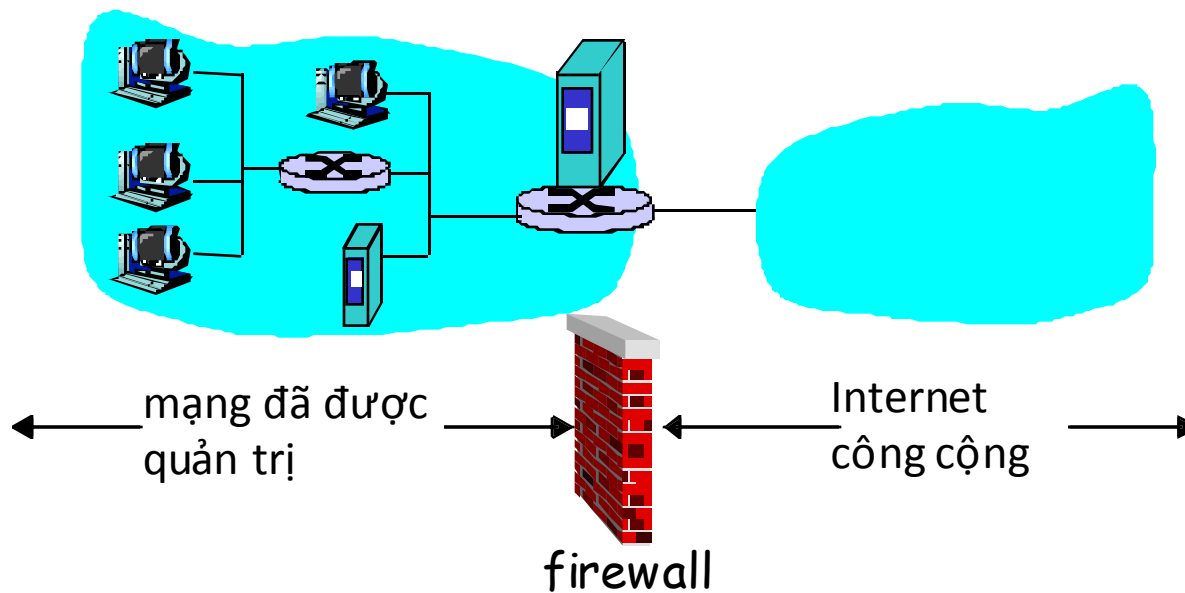
Sử dụng chứng chỉ



Các Firewall-Tường lửa

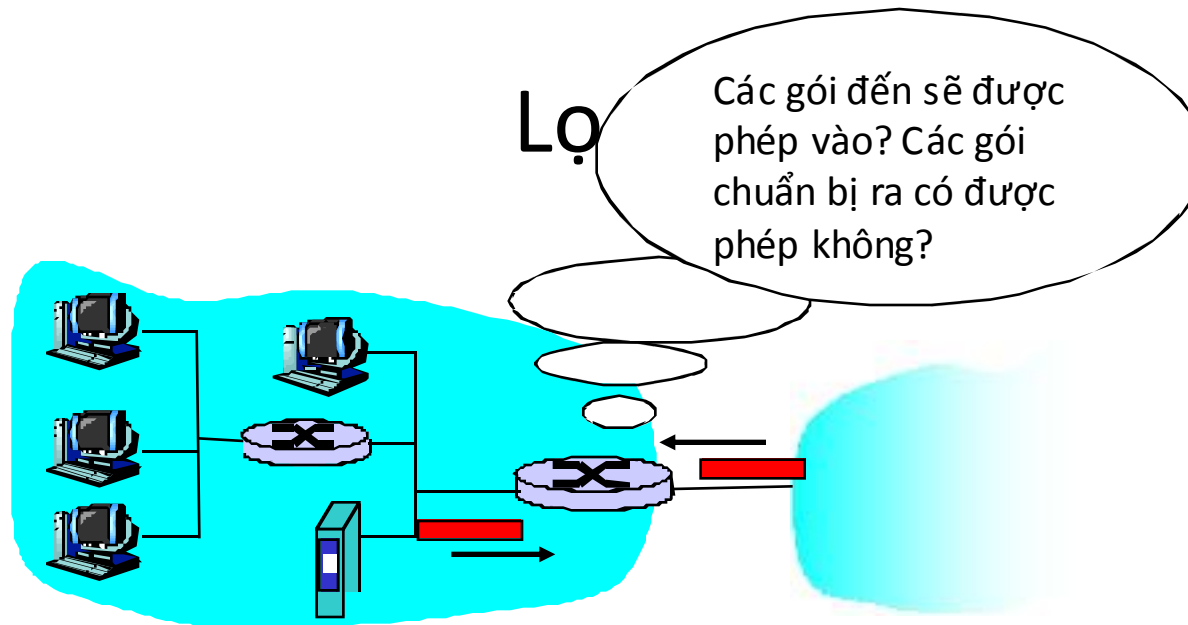
firewall

cô lập mạng nội bộ của tổ chức với Internet, cho phép một số gói được truyền qua, ngăn chặn các gói khác



Firewall: Tại sao phải dùng?

- **Ngăn chặn các cuộc tấn công từ chối dịch vụ Denial Of Service (DoS):**
 - SYN flooding: kẻ tấn công thiết lập nhiều kết nối TCP “ảo”, không còn tài nguyên cho các kết nối “thật”
- **Ngăn chặn việc sửa đổi/truy cập bất hợp pháp các dữ liệu nội bộ.**
 - Ví dụ: kẻ tấn công thay thế trang chủ của CIA bằng trang nào đó
- **Chỉ cho phép các truy cập hợp pháp vào bên trong mạng** (tập hợp các host/user được chứng thực)
- **2 kiểu firewall:**
 - mức ứng dụng
 - lọc gói tin



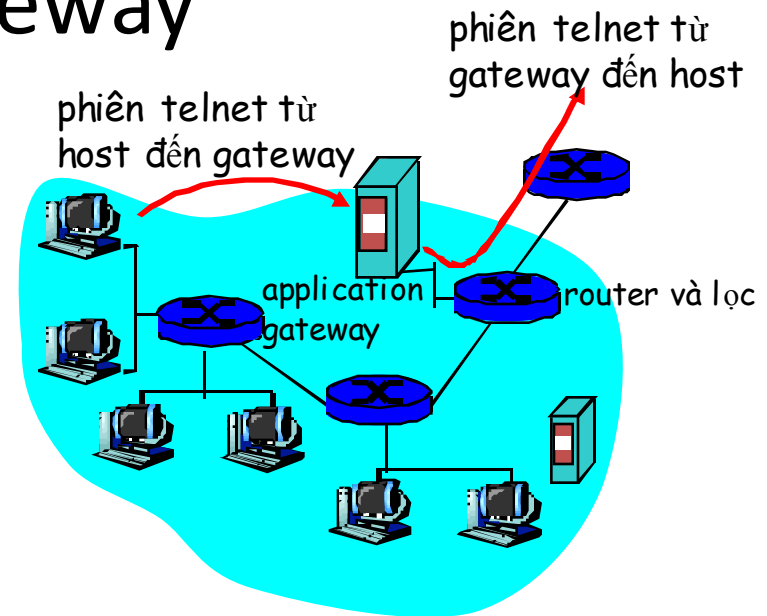
- mạng nội bộ kết nối với Internet thông qua **router firewall**
- router **lọc từng gói một**, xác định chuyển tiếp hoặc bỏ các gói dựa trên:
 - địa chỉ IP nguồn, địa chỉ IP đích
 - các số hiệu port TCP/UDP nguồn và đích
 - kiểu thông điệp ICMP
 - các bit TCP SYN và ACK

Lọc gói tin

- Ví dụ 1: chặn các datagram đến và đi với trường giao thức IP = 17 và port nguồn hoặc đích = 23.
 - Tất cả các dòng UDP đến/đi và các kết nối telnet đều bị chặn lại.
- Ví dụ 2: chặn các đoạn Block TCP với ACK=0.
 - Ngăn chặn các client bên ngoài tạo các kết nối TCP với các client bên trong, nhưng cho phép các client bên trong kết nối ra ngoài.

Các ứng dụng gateway

- Lọc các gói trên dữ liệu ứng dụng cũng như các trường IP/TCP/UDP.
- Ví dụ: cho phép chọn các user bên trong được telnet ra ngoài.



1. yêu cầu tất cả các user phải telnet thông qua gateway
2. với các user đã được cấp phép, gateway thiết lập kết nối với host đích. gateway tiếp vận dữ liệu giữa 2 kết nối.
3. Router lọc và chặn tất cả các kết nối telnet không xuất phát từ gateway.

Các hạn chế của các firewall và gateway

- giả mạo IP: router không thể biết dữ liệu có thực sự đến từ nguồn tin cậy hay không
- nếu nhiều ứng dụng cần đối xử đặc biệt, mỗi cái sở hữu gateway riêng...
- phần mềm client phải biết cách tiếp xúc với gateway.
 - ví dụ: phải thiết lập địa chỉ IP của proxy trong trình duyệt Web
- các lọc thường dùng tất cả hoặc không có chính sách nào dành cho UDP
- sự cân bằng: **mức độ truyền thông với bên ngoài và sự an toàn**
- nhiều site bảo vệ mức cao vẫn phải chịu đựng sự tấn công

Các loại tấn công và cách phòng chống

Phương thức:

- Trước khi tấn công: hacker tìm hiểu các dịch vụ đã hiện thực/hoạt động trên mạng
- Dùng ping để xác định các host nào có địa chỉ trên mạng
- Quét port: liên tục thử thiết lập các kết nối TCP với mỗi port (xem thử chuyện gì xảy ra)

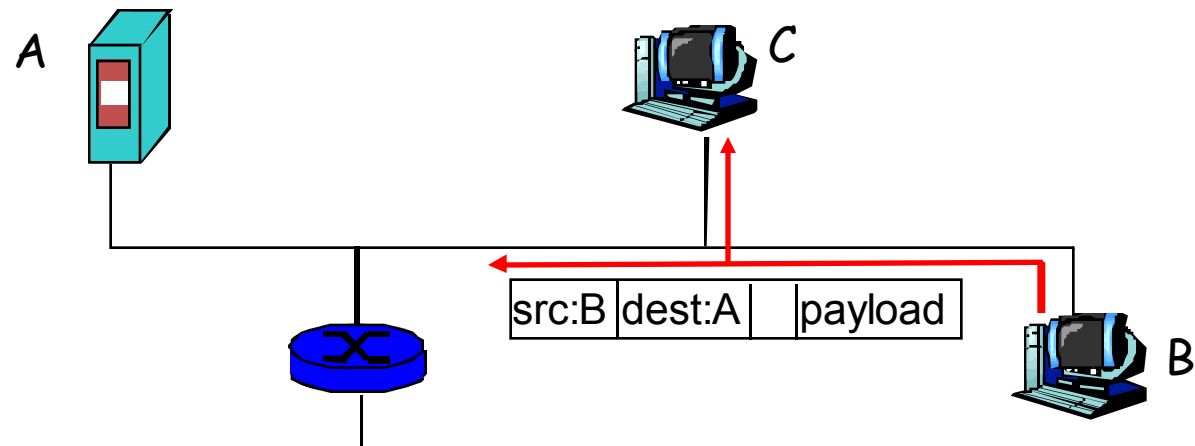
Biện pháp đối phó?

- Ghi nhận lưu thông vào mạng
- Quan tâm các hành vi nghi ngờ (các địa chỉ IP, port bị quét liên tục)

Các mối đe dọa bảo mật Internet

Packet sniffing: Nghe ngóng gói

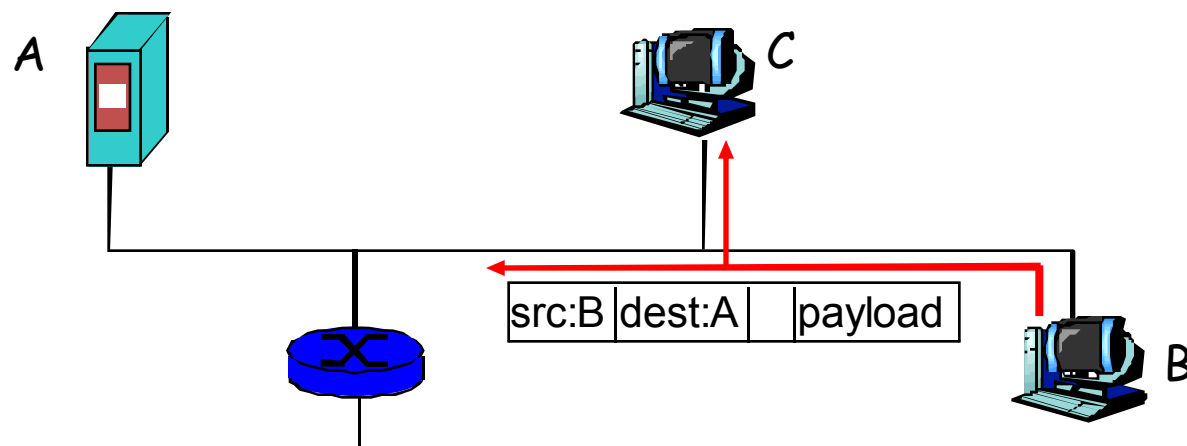
- NIC promiscuous (hỗn tạp) đọc tất cả các gói chuyển qua nó
- Có thể đọc tất cả các dữ liệu được mã hóa (như mật khẩu)
- Ví dụ: C nghe ngóng các gói của B



Các mối đe dọa bảo mật Internet

Packet sniffing: Biện pháp đối phó

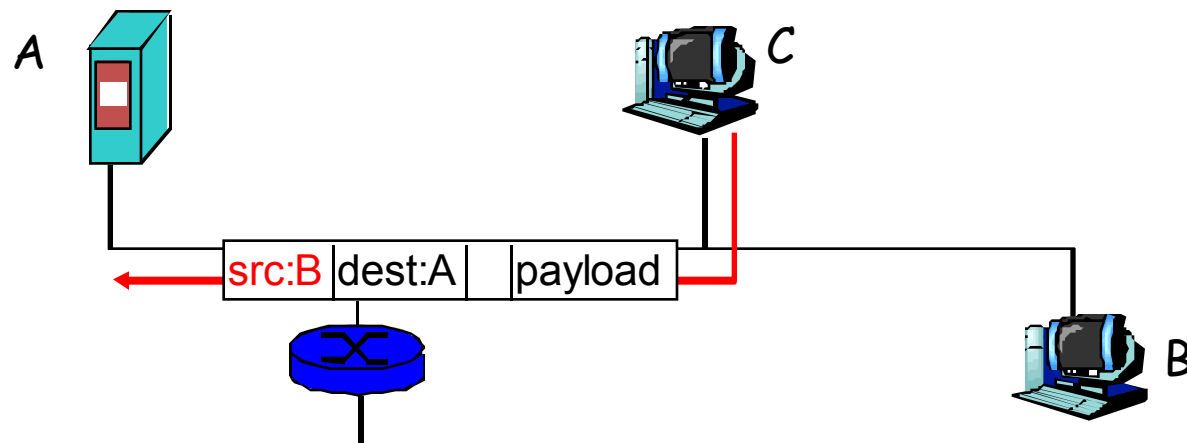
- Tất cả các host trong tổ chức chạy phần mềm kiểm tra định kỳ xem host có ở chế độ promiscuous
- 1 host mỗi đoạn của phương tiện truyền thông



Các mối đe dọa bảo mật Internet

IP Spoofing (giả mạo IP):

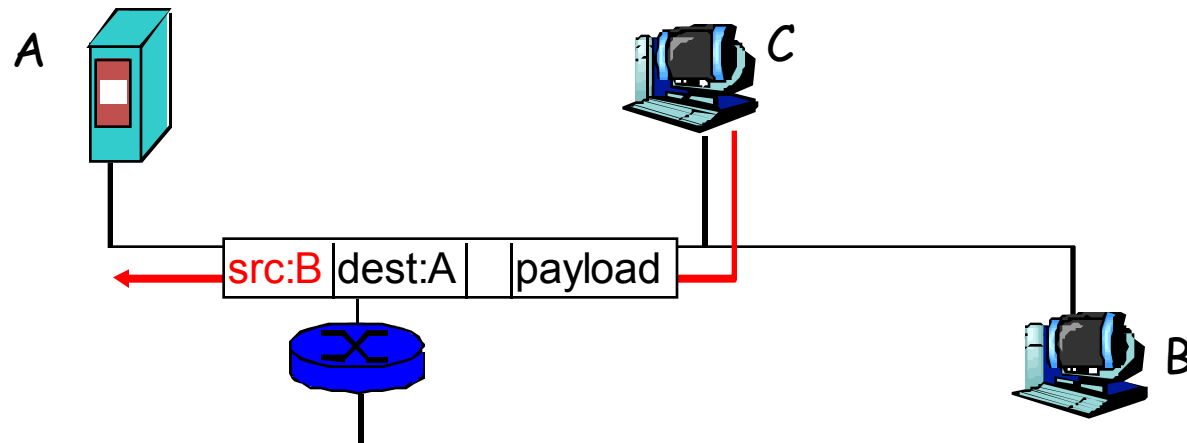
- Có thể sinh ra các gói IP “thô” trực tiếp từ ứng dụng, gán giá trị bất kỳ vào trường địa chỉ IP nguồn
- Bên nhận không thể xác định nguồn bị giả mạo
- Ví dụ: C giả mạo là B



Các mối đe dọa bảo mật Internet

IP Spoofing: lọc quyền vào

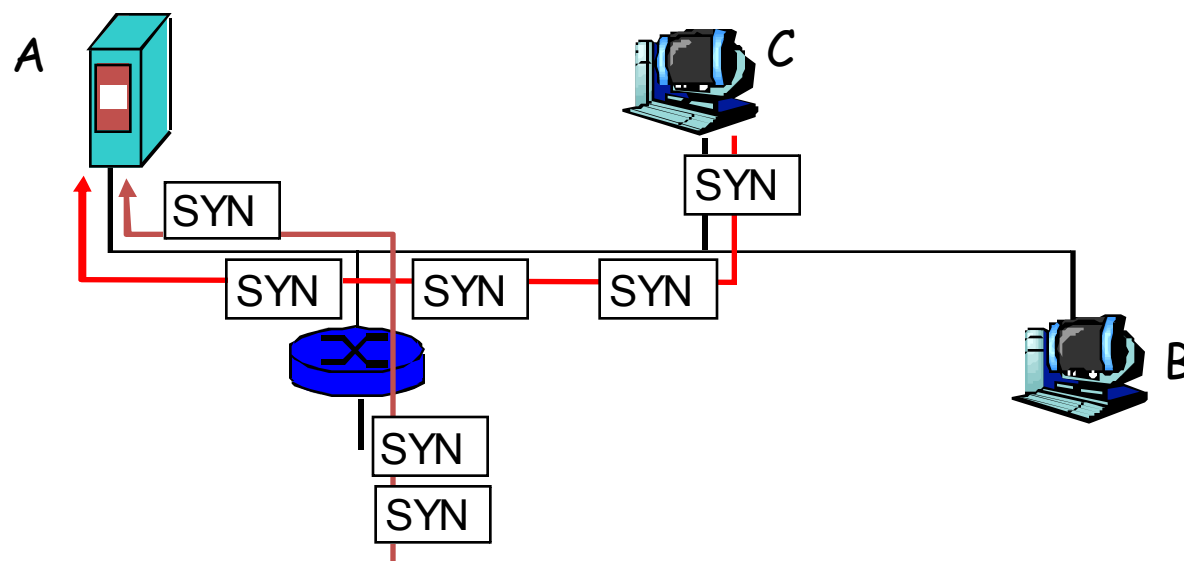
- Router sẽ không chuyển tiếp các gói đi với trường hợp các địa chỉ nguồn không hợp lệ
- Tuyệt vời, nhưng lọc như thế không thể áp dụng cho tất cả các mạng



Các mối đe dọa bảo mật Internet

Denial of Service (DoS):

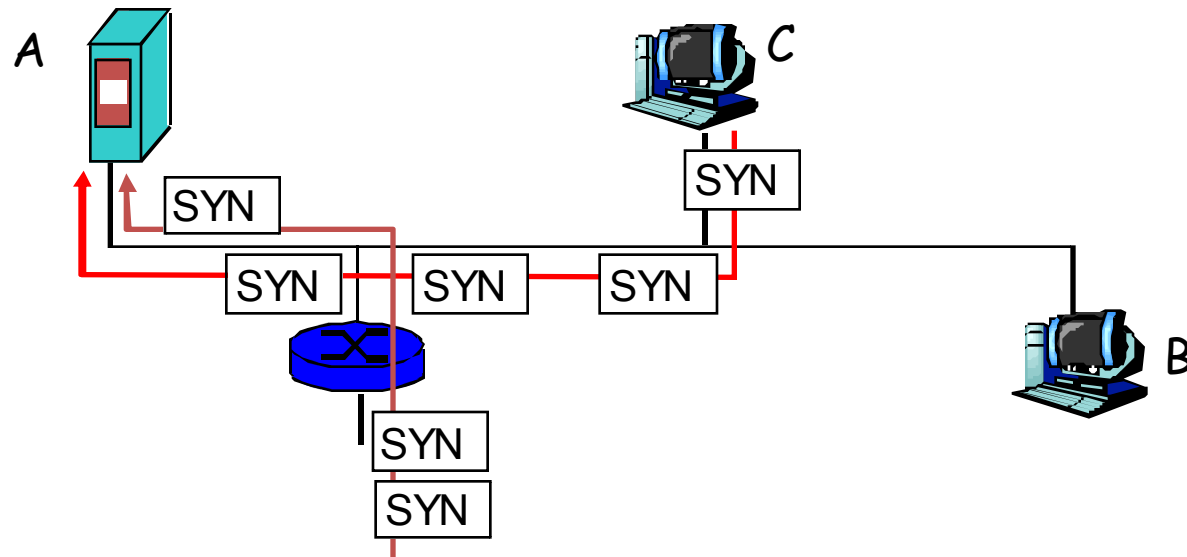
- Gây ra “ngập lụt” bằng các gói sinh ra bởi ý đồ xấu cho bên nhận
- Distributed DOS (DDoS): nhiều nguồn phối hợp làm “ngập lụt” bên nhận
- Ví dụ: C và các host ở xa tấn công SYN A



Các mối đe dọa bảo mật Internet

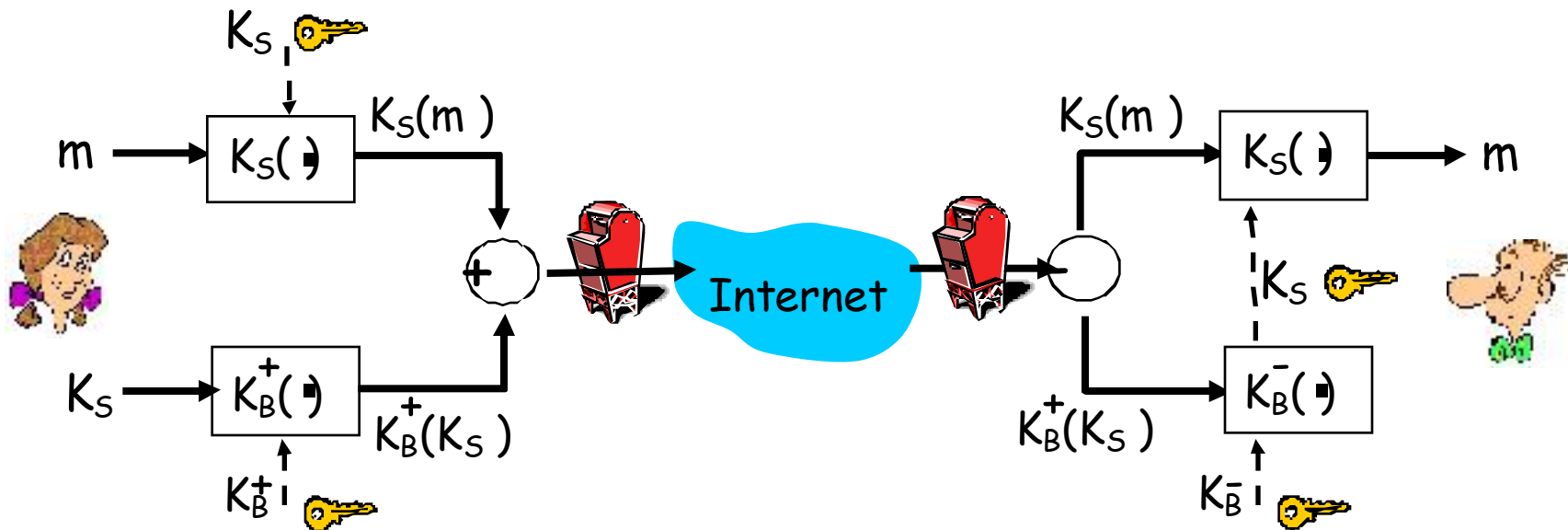
Denial of Service (DoS): Biện pháp đối phó?

- **Lọc ra trước** các gói dùng làm “ngập lụt” (ví dụ: SYN)
- **Theo dõi ngược lại** nguồn gây ra “ngập lụt” (cơ chế giống máy phát hiện nói dối của Mỹ)



Bảo mật e-mail

- ❑ Alice muốn gửi 1 e-mail bí mật, m , đến Bob.



Alice:

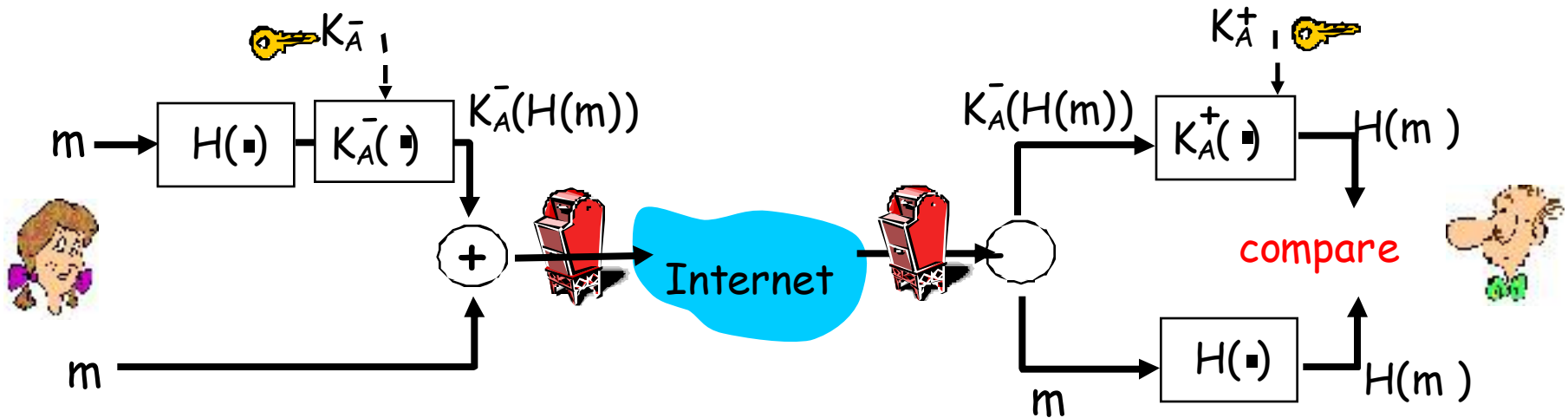
- ❑ sinh ra khóa riêng đối xứng ngẫu nhiên, K_S .
- ❑ mã hóa thông điệp với K_S
- ❑ cũng mã hóa K_S với khóa công cộng của Bob.
- ❑ gửi cả $K_S(m)$ và $K_B(K_S)$ cho Bob.

Bob:

- ❑ dùng khóa riêng của anh ấy để giải mã và phục hồi K_S
- ❑ dùng K_S để giải mã $K_S(m)$ và phục hồi m

Bảo mật e-mail

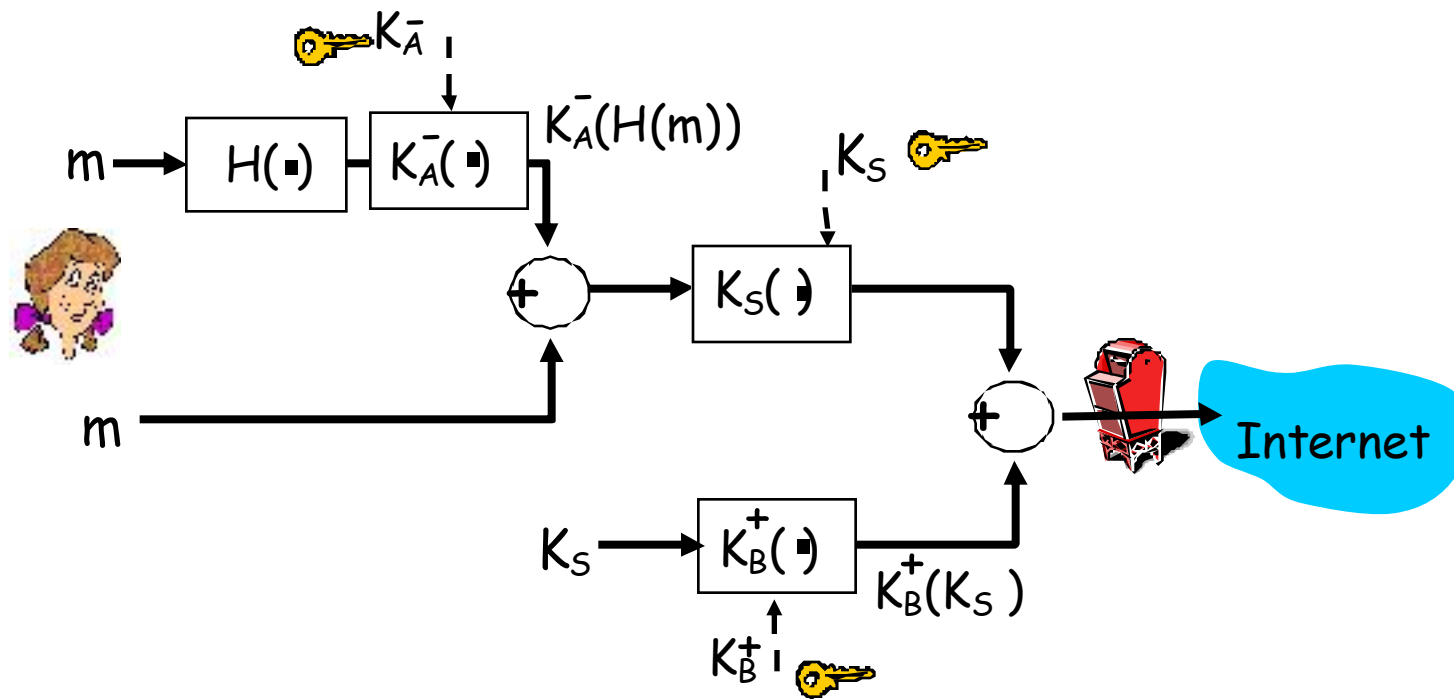
- Alice muốn cung cấp sự toàn vẹn thông điệp chứng thực người gửi.



- Alice ký số trên thông điệp.
- gửi cả thông điệp (dạng rõ ràng) và chữ ký số.

Bảo mật e-mail

- Alice muốn cung cấp sự toàn vẹn thông điệp chứng thực người gửi → sự bí mật



Alice dùng 3 khóa: khóa riêng của cô ấy, khóa công cộng của Bob, khóa đối xứng vừa mới tạo

Pretty good privacy (PGP)

- Chuẩn trên thực tế để mã hóa email Internet. Một thông điệp đã được ký bằng PGP
- Dùng mã hóa khóa đối xứng, khóa công cộng, hàm băm và chữ ký số như đã trình bày ở trước.
- Hỗ trợ đồng nhất, chứng thực người gửi, bí mật
- Người phát minh: Phil Zimmerman.

```
---BEGIN PGP SIGNED MESSAGE---  
Hash: SHA1  
  
Bob:My husband is out of town  
    tonight.Passionately yours, A  
  
---BEGIN PGP SIGNATURE---  
Version: PGP 5.0  
Charset: noconv  
yhHJRHhGJGhgg/12EpJ+1o8gE4vB3mqJ  
    hFEvZP9t6n7G6m5Gw2  
---END PGP SIGNATURE---
```

Secure sockets layer (SSL)

- Bảo mật lớp transport với bất kỳ ứng dụng nào dựa trên TCP dùng các dịch vụ SSL
- Dùng giữa trình duyệt Web, các server trong thương mại điện tử
- Các dịch vụ bảo mật:
 - Chứng thực server
 - Mã hóa dữ liệu
 - Chứng thực client (tùy chọn)
- Chứng thực server:
 - Trình duyệt cho phép SSL chứa các khóa công cộng cho các CA được tin cậy
 - Trình duyệt yêu cầu chứng chỉ server, phát ra bởi CA được tin cậy
 - Trình duyệt dùng khóa công cộng của CA để trích ra khóa công cộng của server từ chứng chỉ
- Kiểm tra trong trình duyệt của bạn để thấy các CA được tin cậy

SSL (tt)

Mã hóa phiên làm việc SSL :

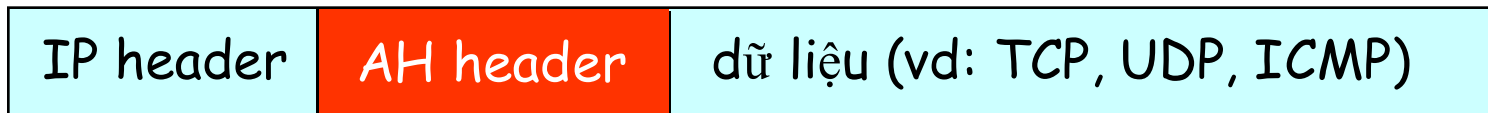
- Trình duyệt sinh ra *khóa phiên đối xứng*, mã hóa nó với khóa công cộng của server, gửi khóa (đã mã hóa) cho server.
- Dùng khóa riêng, server giải mã khóa phiên
- Trình duyệt, server biết khóa phiên
 - Tất cả dữ liệu gửi vào trong TCP socket (do client hoặc server) được mã hóa bởi khóa phiên.
- SSL: cơ sở của IETF Transport Layer Security (TLS).
- SSL có thể dùng cho các ứng dụng không Web, như IMAP.
- Chứng thực client có thể hoàn thành với các chứng chỉ client

IPSec: bảo mật lớp Network

- **Bảo mật lớp Network:**
 - host gửi mã hóa dữ liệu trong IP datagram
 - các đoạn TCP & UDP; các thông điệp ICMP & SNMP.
- **Chứng thực lớp Network:**
 - host đích có thể chứng thực địa chỉ IP nguồn
- **2 giao thức cơ bản:**
 - authentication header (AH)
 - encapsulation security payload (ESP)
- **Với cả AH và ESP, nguồn – đích bắt tay nhau:**
 - tạo kênh logic lớp network gọi là một security association (SA)
- **Mỗi SA theo 1 chiều duy nhất**
- **duy nhất xác định bởi:**
 - giao thức bảo mật (AH hoặc ESP)
 - địa chỉ IP nguồn
 - ID của kết nối 32-bit

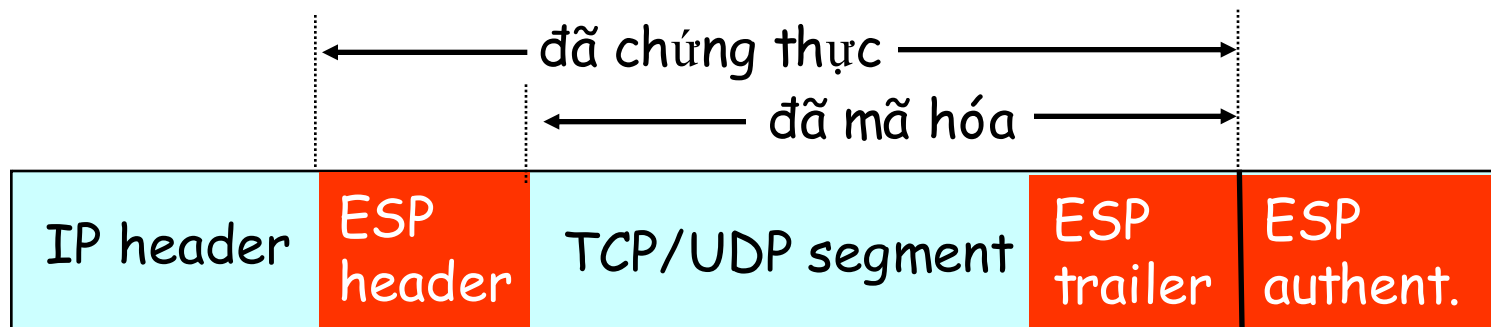
Giao thức AH

- Hỗ trợ chứng thực nguồn, toàn vẹn dữ liệu, không tin cậy
 - AH header được chèn vào giữa IP header, trường dữ liệu.
 - Trường giao thức: 51
 - Trung gian xử lý các datagram như bình thường
- AH header chứa:**
- Nhân dạng kết nối
 - Dữ liệu chứng thực: thông điệp đã được ký từ nguồn được tính toán dựa trên IP datagram gốc
 - Trường header kế tiếp: xác định kiểu của dữ liệu (vd: TCP, UDP, ICMP)



Giao thức ESP

- Hỗ trợ toàn vẹn dữ liệu, chứng thực host, tính bí mật
- Mã hóa dữ liệu, ESP trailer
- Trường header kế tiếp nằm trong ESP trailer.
- Trường chứng thực ESP tương tự như của AH
- Protocol = 50.



Bảo mật IEEE 802.11

- *Khảo sát:*
 - 85% việc sử dụng mà không có mã hóa/chứng thực
 - Dễ dàng bị phát hiện/nghe ngóng và nhiều loại tấn công khác!
- **Bảo mật 802.11**
 - Mã hóa, chứng thực
 - Thử nghiệm bảo mật 802.11 đầu tiên là Wired Equivalent Privacy (WEP): có thiếu sót
 - Thử nghiệm hiện tại: 802.11i

Wired Equivalent Privacy (WEP):

- Chứng thực như trong giao thức *ap4.0*
 - host yêu cầu chứng thực từ access point
 - access point gửi 128 bit
 - host mã hóa dùng khóa đối xứng chia sẻ
 - access point giải mã, chứng thực host
- Không có cơ chế phân bố khóa
- Chứng thực: chỉ cần biết khóa chia sẻ

Wi-Fi Protected Access (WPA)

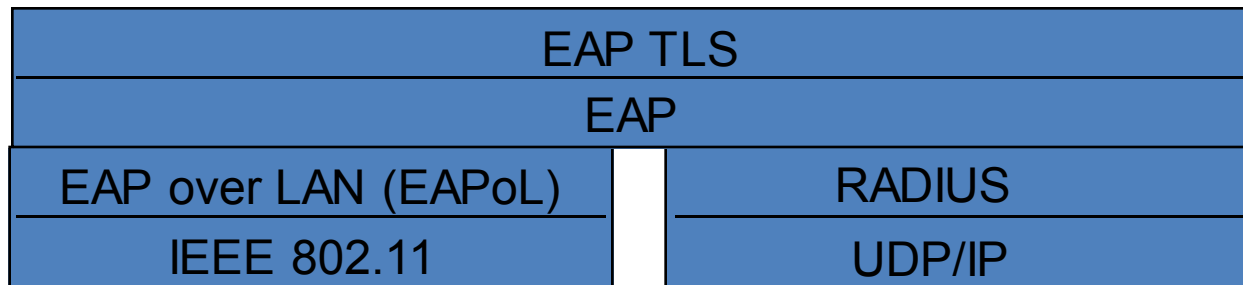
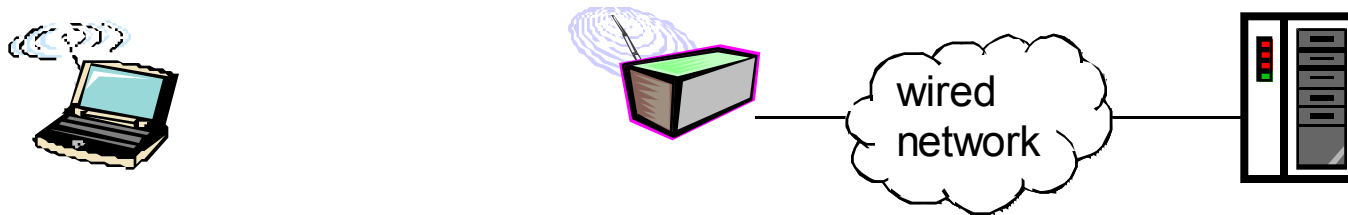
- Hai sự cải tiến chính so với WEP:
 - Mã hóa dữ liệu cải tiến thông qua giao thức Temporal Key Integrity Protocol (TKIP). TKIP scrambles key sử dụng thuật toán hashing và bảng đặc tính kiểm tra số nguyên, đảm bảo rằng Key sẽ không bị giả mạo.
 - Chứng thực người dùng, thông qua EAP.
- WPA là tiêu chuẩn tạm thời mà sẽ được thay thế với chuẩn IEEE 802.11i

802.11i: cải tiến sự bảo mật

- Rất nhiều (và chắc chắn hơn) dạng mã hóa có thể
- Hỗ trợ phân bố khóa
- Dùng chứng thực server tách riêng khỏi AP

EAP: Extensible Authentication Protocol

- EAP được gửi trên các “link” riêng biệt
 - mobile-đến-AP (EAP trên LAN)
 - AP đến server chứng thực (RADIUS trên UDP)



TÀI LIỆU THAM KHẢO, ĐỊA CHỈ LIÊN LẠC

- Giáo trình Mạng máy tính, KS. Nguyễn Bình Dương, TS. Đàm Quang Hồng Hải
- Giáo trình hệ thống Mạng máy tính CCNA, Nguyễn Hồng Sơn
- CCNA: Cisco Certified Network Associate – Study Guide, Todde Lammle - 2007
- Computer Networking: A Top Down Approach Featuring the Internet, 3rd edition. Jim Kurose, Keith Ross. 2004.
- Computer Networks, 4th edition. Andrew S. Tanenbaum. 2003
- Địa chỉ liên lạc: Trần Bá Nhiệm – Khoa Mạng máy tính & Truyền thông – ĐH CNTT – 34 Trương Định, Q3, Tp.HCM. Email: tranbanhiem@yahoo.com