Mạng cục bộ - LAN

- **Mạng cục bộ (LAN) là hệ truyền thông tốc độ cao được thiết kế để kết nối các máy tính và các thiết bị xử lý dữ liệu khác cùng hoạt động với nhau trong một khu vực địa lý nhỏ như ở một tầng của toà nhà, hoặc trong một toà nhà.... Một số mạng LAN có thể kết nối lại với nhau trong một khu làm việc.**
- **Các mạng LAN trở nên thông dụng vì nó cho phép những người sử dụng (users) dùng chung những tài nguyên quan trọng như máy in mầu, ổ đĩa CD-ROM, các phần mềm ứng dụng và những thông tin cần thiết khác. …**

- **…Trước khi phát triển công nghệ LAN các máy tính là độc lập với nhau, bị hạn chế bởi số lượng các chương trình tiện ích, sau khi kết nối mạng rõ ràng hiệu quả của chúng tăng lên gấp bội. Để tận dụng hết những ưu điểm của mạng LAN người ta đã kết nối các LAN riêng biệt vào mạng chính yếu diện rộng (WAN).**
- **Các thiết bị gắn với mạng LAN đều dùng chung một phương tiện truyền tin đó là dây cáp, cáp thường dùng hiện nay là: Cáp đồng trục (Coaxial cable), Cáp dây xoắn (shielded twisted pair), cáp quang (Fiber optic),....**

Băng thông: phương tiện LAN

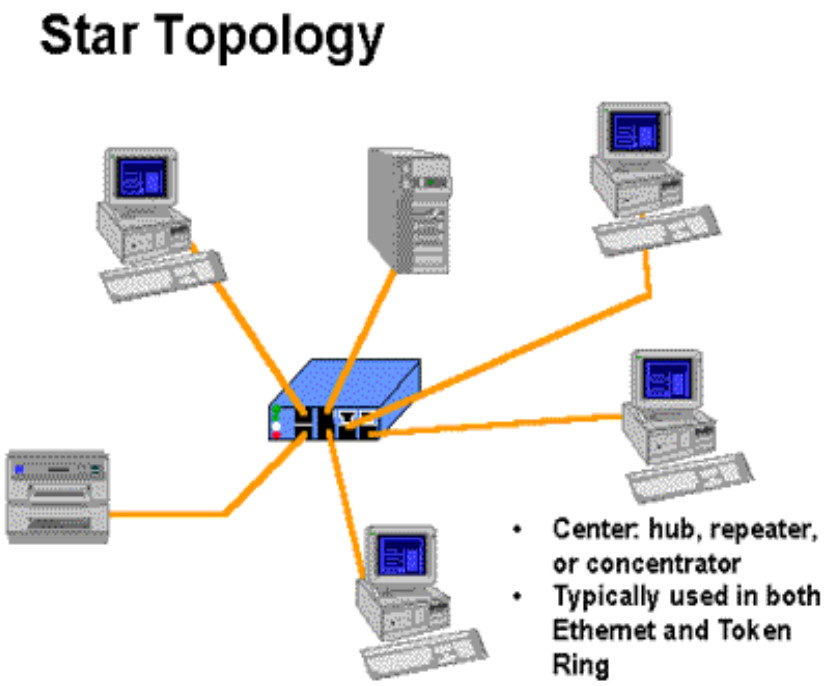
Some Typical Media	Bandwidth	Max. Physical Distance
50-Ohm Coaxial Cable (Ethernet 10BASE2, ThinNet)	10-100 Mbps	185m
50-Ohm Coaxial Cable (Ethernet 10BASE5, ThickNet)	10-100 Mbps	500m
Category 5 Unshielded Twisted Pair (UTP) (Ethernet 10BASE-T)	10 Mbps	100m
Category 5 Unshielded Twisted Pair (UTP) (Ethernet 100BASE-TX)(Fast Ethernet)	100 Mbps	100m
Multimode (62.5/125μm) Optical Fiber 100BASE-FX	100 Mbps	2000m
Singlemode (9/125μm core) Optical Fiber 1000BASE-LX	1000 Mbps (1.000 Gbps)	3000m
Wireless	11 Mbps	a few 100meters

Sơ đồ mạng LAN (Topologies)

- **Topology của mạng là cấu trúc hình học không gian mà thực chất là cách bố trí phần tử của mạng cũng như cách nối giữa chúng với nhau. Thông thường mạng có 3 dạng cấu trúc là:**
  - **Mạng dạng hình sao (Star Topology),**
  - **mạng dạng vòng (Ring Topology) và**
  - **mạng dạng tuyến (Linear Bus Topology).**
  - **Ngoài 3 dạng cấu hình kể trên còn có một số dạng khác kết hợp từ 3 dạng này như mạng dạng cây, mạng dạng hình sao - vòng, mạng hỗn hợp,v.v....**

Mạng dạng hình sao (Star topology)

- **Mạng dạng hình sao bao gồm một trung tâm và các nút thông tin. Các nút thông tin là các trạm đầu cuối, các máy tính và các thiết bị khác của mạng. Trung tâm của mạng điều phối mọi hoạt động trong mạng với các chức năng cơ bản là:**
  - **Xác định cặp địa chỉ gửi và nhận được phép chiếm tuyến thông tin và liên lạc với nhau.**
  - **Cho phép theo dõi và xử lý sai trong quá trình trao đổi thông tin.**
  - **Thông báo các trạng thái của mạng...**

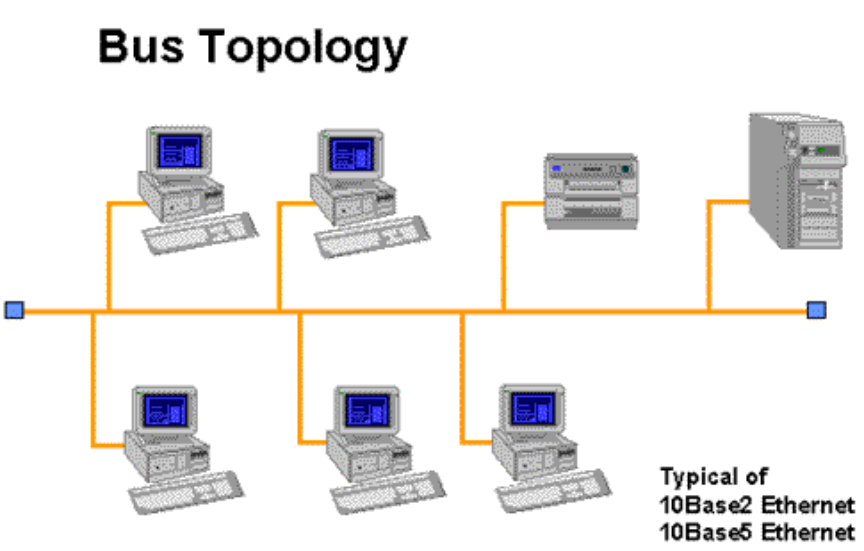


Mạng dạng hình sao (Star topology)

- **Các ưu điểm của mạng hình sao:**
  - **Hoạt động theo nguyên lý nối song song nên nếu có một thiết bị nào đó ở một nút thông tin bị hỏng thì mạng vẫn hoạt động bình thường.**
  - **Cấu trúc mạng đơn giản và các thuật toán điều khiển ổn định.**
  - **Mạng có thể mở rộng hoặc thu hẹp tuỳ theo yêu cầu của người sử dụng.**
- **Nhược điểm của mạng hình sao:**
  - **Khả năng mở rộng mạng hoàn toàn phụ thuộc vào khả năng của trung tâm . Khi trung tâm có sự cố thì toàn mạng ngừng hoạt động.**
    Mạng yêu cầu nối độc lập riêng rẽ từng thiết bị ở các nút thông tin đến trung tâm. Khoảng cách từ máy đến trung tâm rất hạn chế (100 m).
- **Nhìn chung, mạng dạng hình sao cho phép nối các máy tính vào một bộ tập trung (HUB) bằng cáp xoắn, giải pháp này cho phép nối trực tiếp máy tính với HUB không cần thông qua trục BUS, tránh được các yếu tố gây ngưng trệ mạng. Gần đây, cùng với sự phát triển switching hub, mô hình này ngày càng trở nên phổ biến và chiếm đa số các mạng mới lắp.**

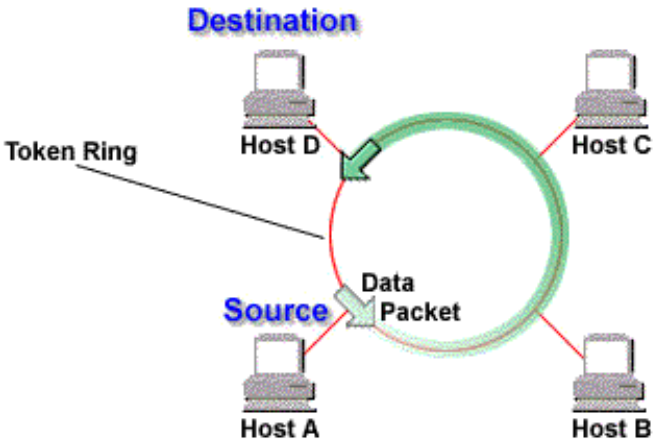
Bus topology

- Máy chủ (host) cũng như tất cả các máy tính khác (workstation) hoặc các nút (node) đều được nối về với nhau trên một trục đường dây cáp chính để chuyển tải tín hiệu.
- Tất cả các nút đều sử dụng chung đường dây cáp chính này. Phía hai đầu dây cáp được chặn bởi một thiết bị gọi là terminator. Các tín hiệu và gói dữ liệu (packet) khi di chuyển lên hoặc xuống trong dây cáp đều mang theo địa chỉ của nơi đến.
- Loại hình mạng này dùng dây cáp ít nhất, dễ lắp đặt. Tuy vậy cũng có những bất lợi đó là sẽ có sự tắc nghẽn khi chuyển dữ liệu với lưu lượng lớn và khi có sự hỏng hóc ở đoạn nào đó thì rất khó phát hiện, một sự ngừng trên đường dây để sửa chữa sẽ ngừng toàn bộ hệ thống.



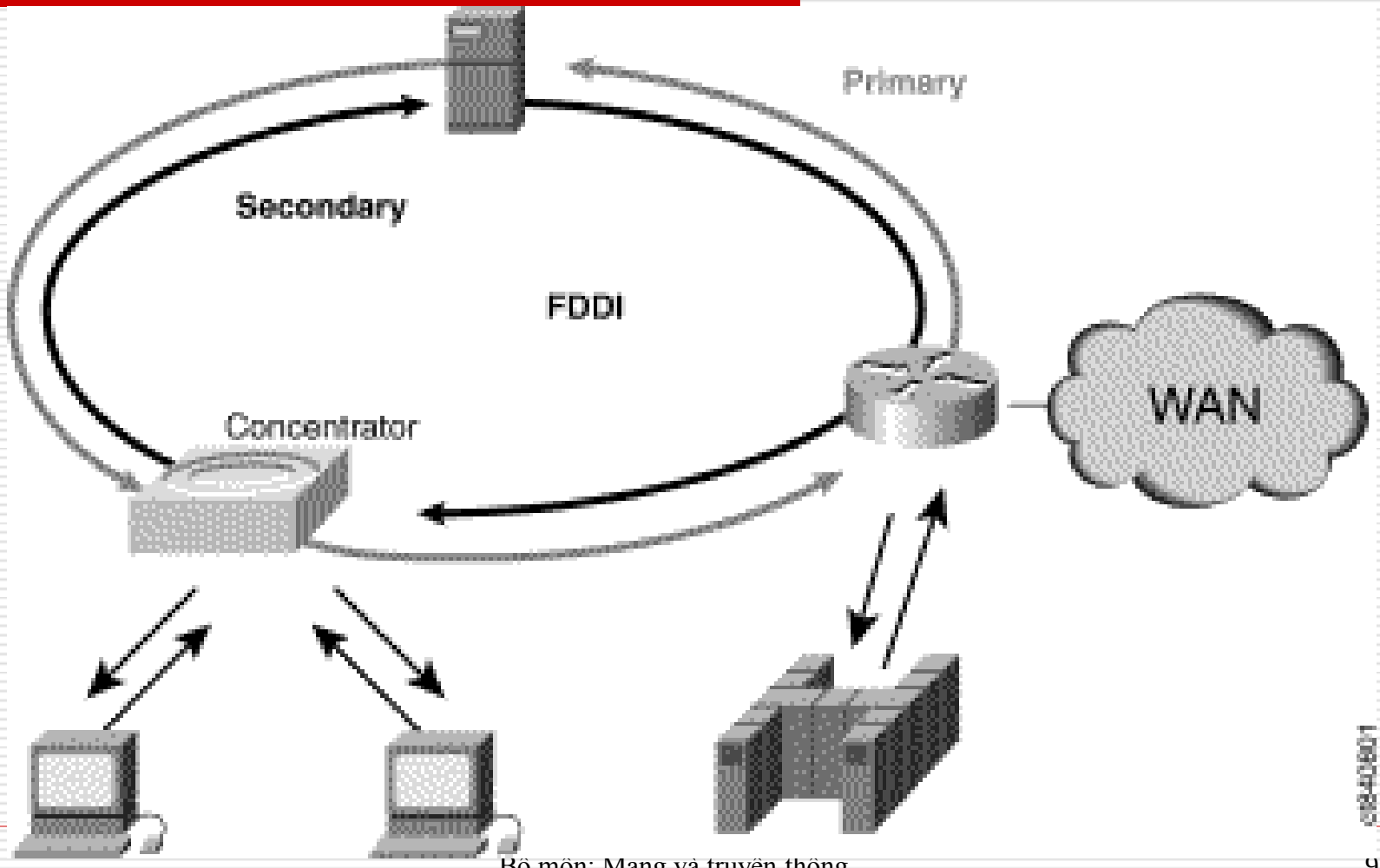
Ring topology

- Mạng dạng này, bố trí theo dạng xoay vòng, đường dây cáp được thiết kế làm thành một vòng khép kín, tín hiệu chạy quanh theo một chiều nào đó. Các nút truyền tín hiệu cho nhau, mỗi thời điểm chỉ được một nút mà thôi. Dữ liệu truyền đi phải có kèm theo địa chỉ cụ thể của mỗi trạm tiếp nhận.
- Mạng dạng vòng có thuận lợi là có thể nới rộng ra xa, tổng đường dây cần thiết ít hơn so với hai kiểu trên. Nhược điểm là đường dây phải khép kín, nếu bị ngắt ở một nơi nào đó thì toàn bộ hệ thống cũng bị ngừng.



Token Ring Token Passing
A free token is routed around the ring. As it passes around the ring devices on the network to see if they want to transmit data.

Mạng FDDI (Fiber Distributed Data Interface).



Mạng dạng kết hợp

Kết hợp hình sao và tuyến (star/Bus Topology)

- **Cấu hình mạng dạng này có bộ phận tách tín hiệu (splitter) giữ vai trò thiết bị trung tâm, hệ thống dây cáp mạng có thể chọn hoặc Ring Topology hoặc Linear Bus Topology.**
- **Lợi điểm của cấu hình này là mạng có thể gồm nhiều nhóm làm việc ở cách xa nhau, ARCNET là mạng dạng kết hợp Star/Bus Topology. Cấu hình dạng này đưa lại sự uyển chuyển trong việc bố trí đường dây tương thích dễ dàng đối với bất cứ toà nhà nào.**

Kết hợp hình sao và vòng (Star/Ring Topology)

- **Cấu hình dạng kết hợp Star/Ring Topology, có một "thẻ bài" liên lạc (Token) được chuyển vòng quanh một HUB trung tâm. Mỗi trạm làm việc (workstation) được nối với HUB - là cầu nối giữa các trạm làm việc và để tăng khoảng cách cần thiết.**

Các giao thức (protocol)

- Một tập các tiêu chuẩn để trao đổi thông tin giữa hai hệ thống máy tính hoặc hai thiết bị máy tính với nhau được gọi là giao thức (Protocol).
- Các giao thức (Protocol) còn được gọi là nghi thức hoặc định ước của mạng máy tính.
- Để đánh giá khả năng của một mạng được phân chia bởi các trạm như thế nào. Hệ số này được quyết định chủ yếu bởi hiệu quả sử dụng môi trường truy xuất (medium access) của giao thức, môi trường này ở dạng tuyến tính hoặc vòng.... Một trong các giao thức được sử dụng nhiều trong các LAN là:
  - Giao thức tranh chấp CSMA/CD
  - Giao thức truyền token (token passing protocol)

Giao thức tranh chấp (Contention Protocol) CSMA/CD trong Ethernet và IEEE 803.3

- CSMA/CD: Carrier Sense Multiple Access /Conllision Detect -Phương pháp đa truy nhập sử dụng sóng mang có phát hiện xung đột.
- Sử dụng giao thức này các trạm hoàn toàn có quyền truyền dữ liệu trên mạng với số lượng nhiều hay ít và một cách ngẫu nhiên hoặc bất kỳ khi nào có nhu cầu truyền dữ liệu ở mỗi trạm. Mối trạm sẽ kiểm tra tuyến và chỉ khi nào tuyến không bận mới bắt đầu truyền các gói dữ liệu.
- Phương pháp này sử dụng cho topo dạng bus, trong đó tất cả các trạm của mạng đều được nối trực tiếp vào bus. Mọi trạm đều có thể truy nhập vào bus chung (đa truy nhập) một cách ngẫu nhiên và do vậy rất có thể dẫn đến xung đột (hai hoặc nhiều trạm đồng thời truyền dữ liệu). Dữ liệu được truyền trên mạng theo một khuôn dạng đã định sẵn trong đó có một vùng thông tin điều khiển chứa địa chỉ trạm đích.
- CSMA/CD có nguồn gốc từ hệ thống radio đã phát triển ở trường đại học Hawaii vào khoảng năm 1970, gọi là ALOHANET.

CSMA/CD

- Với phương pháp CSMA, thỉnh thoảng sẽ có hơn một trạm đồng thời truyền dữ liệu và tạo ra sự xung đột (collision) làm cho dữ liệu thu được ở các trạm bị sai lệch.
- Để tránh sự tranh chấp này mỗi trạm đều phải phát hiện được sự xung đột dữ liệu. Trạm phát phải kiểm tra Bus trong khi gửi dữ liệu để xác nhận rằng tín hiệu trên Bus thật sự đúng, như vậy mới có thể phát hiện được bất kỳ xung đột nào có thể xẩy ra. Khi phát hiện có một sự xung đột, lập tức trạm phát sẽ gửi đi một mẫu làm nhiễu (Jamming) đã định trước để báo cho tất cả các trạm là có sự xung đột xẩy ra và chúng sẽ bỏ qua gói dữ liệu này. Sau đó trạm phát sẽ trì hoãn một khoảng thời gian ngẫu nhiên trước khi phát lại dữ liệu.
- Ưu điểm của CSMA/CD là đơn giản, mềm dẻo, hiệu quả truyền thông tin cao khi lưu lượng thông tin của mạng thấp và có tính đột biến. Việc thêm vào hay dịch chuyển các trạm trên tuyến không ảnh hưởng đến các thủ tục của giao thức. Điểm bất lợi của CSMA/CD là hiệu suất của tuyến giảm xuống nhanh chóng khi phải tải quá nhiều thông tin.

Giao thức truyền token (Token passing protocol)

Phương pháp Token Ring (Vòng với thẻ bài)

- Đây là giao thức thông dụng sau CSMA/CD được dùng trong các LAN có cấu trúc vòng (Ring) hay Token Ring và IEEE 802.5. Trong phương pháp này, khối điều khiển mạng hoặc token được truyền lần lượt từ trạm này đến trạm khác. Token là một khối dữ liệu đặc biệt. Khi một trạm đang chiếm token thì nó có thể phát đi một gói dữ liệu. Khi đã phát hết gói dữ liệu cho phép hoặc không còn gì để phát nữa thì trạm đó lại gửi token sang trạm kế tiếp.
- Trong token có chứa một địa chỉ đích và được luân chuyển tới các trạm theo một trật tự đã định trước. Đối với cấu hình mạng dạng xoay vòng thì trật tự của sự truyền token tương đương với trật tự vật lý của các trạm xung quanh vòng.

Giao thức truyền token (Token passing protocol)

Phương pháp Token Ring (Vòng với thẻ bài)

- **Giao thức truyền token có trật tự hơn nhưng cũng phức tạp hơn CSMA/CD, có ưu điểm là vẫn hoạt động tốt khi lưu lượng truyền thông lớn. Giao thức truyền token tuân thủ đúng sự phân chia của môi trường mạng, hoạt động dựa vào sự xoay vòng tới các trạm. Việc truyền token sẽ không thực hiện được nếu việc xoay vòng bị đứt đoạn. Giao thức phải chứa các thủ tục kiểm tra token để cho phép khôi phục lại token bị mất hoặc thay thế trạng thái của token và cung cấp các phương tiện để sửa đổi logic (thêm vào, bớt đi hoặc định lại trật tự của các trạm).**

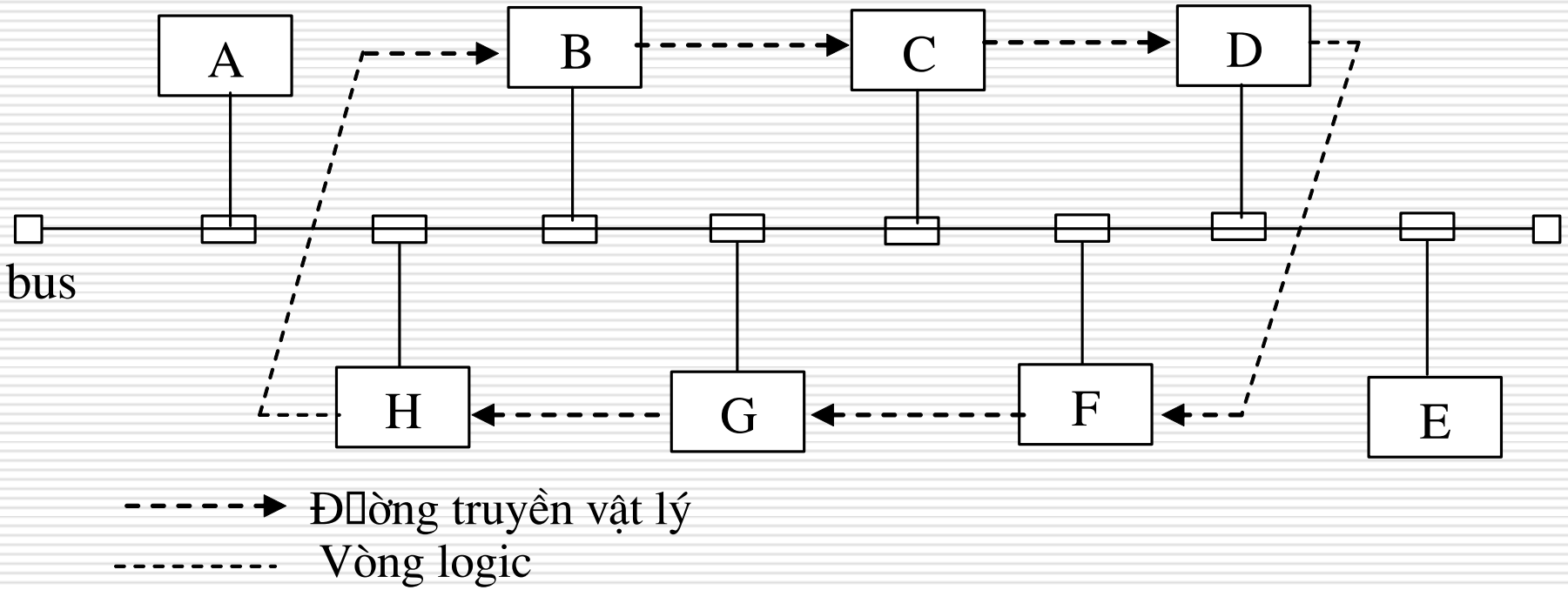
Giao thức truyền token (Token passing protocol)

Phương pháp Token BUS (BUS với thẻ bài)

- Phương pháp truy nhập có điều khiển dùng kỹ thuật "chuyển thẻ bài" để cấp phát quyền truy nhập đường truyền.
- Để cấp phát quyền truy nhập đường truyền cho các trạm đang có nhu cầu truyền dữ liệu,một thẻ bài được lưu chuyển trên một vòng logic thiết lập bởi các trạm đó. Khi một trạm nhận được thẻ bài thì nó có quyền sử dụng đường truyền trong một thời gian định trước. Trong thời gian đó nó có thể truyền một hoặc nhiều đơn vị dữ liệu. Khi đã hết dữ liệu hay hết thời đoạn cho phép, trạm phải chuyển thẻ bài đến trạm tiếp theo trong vòng logic.
- Thiết lập vòng logic (hay còn gọi là vòng ảo) bao gồm các trạm đang có nhu cầu truyền dữ liệu được xác định vị trí theo một chuỗi thứ tự mà trạm cuối cùng của chuỗi sẽ tiếp liền sau bởi trạm đầu tiên. Mỗi trạm được biết địa chỉ của các trạm kề trước và sau nó. Thứ tự của các trạm trên vòng logic có thể độc lập với thứ tự vật lý. Các trạm không hoặc chưa có nhu cầu truyền dữ liệu thì không được đưa vào vòng logic và chúng chỉ có thể tiếp nhận dữ liệu.

Giao thức truyền token (Token passing protocol)

Phương pháp Token BUS (BUS với thẻ bài)



Giao thức truyền token (Token passing protocol)

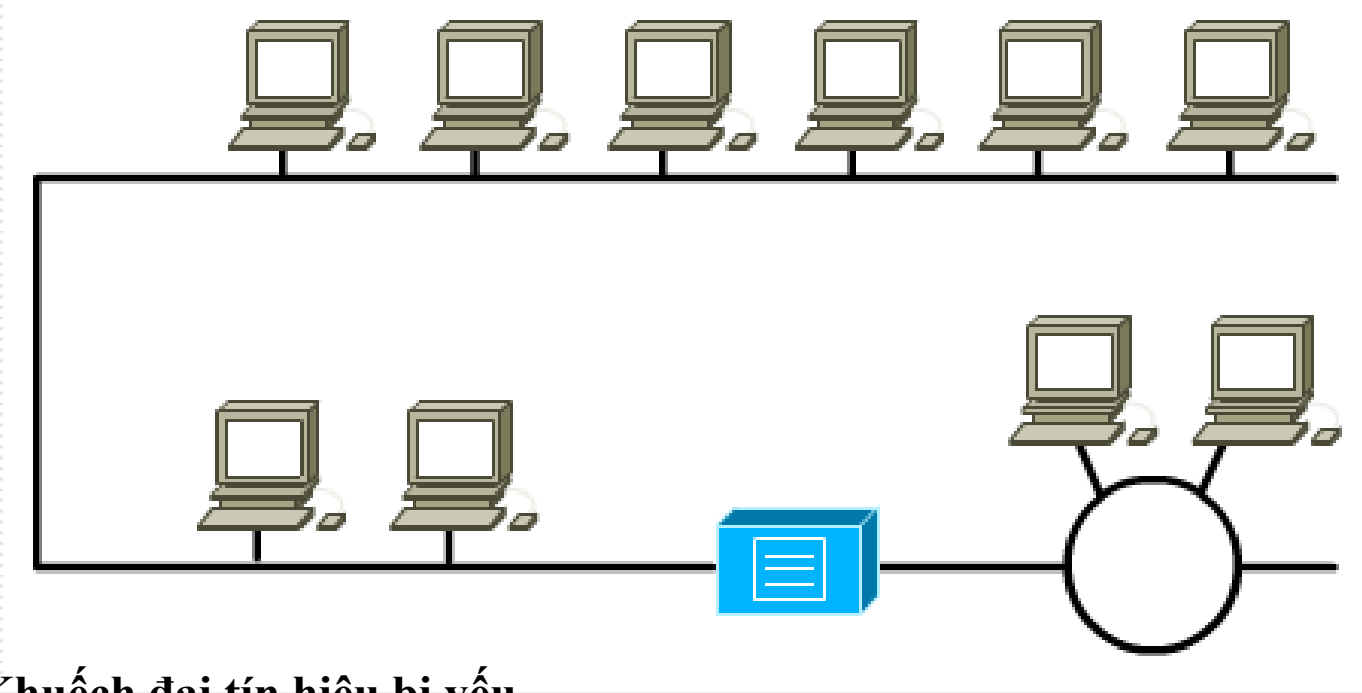
Phương pháp Token BUS (BUS với thẻ bài)

- Vấn đề quan trọng là phải duy trì được vòng logic tuỳ theo trạng thái thực tế của mạng tại thời điểm nào đó. Cụ thể cần phải thực hiện các chức năng sau:
- Bổ sung một trạm vào vòng logic: các trạm nằm ngoài vòng logic cần được xem xét định kỳ để nếu có nhu cầu truyền dữ liệu thì bổ sung vào vòng logic.
- Loại bỏ một trạm khỏi vòng logic: Khi một trạm không còn nhu cầu truyền dữ liệu cần loại nó ra khỏi vòng logic để tối ưu hoá việc điều khiển truy nhập bằng thẻ bài
- Quản lý lỗi: một số lỗi có thể xảy ra, chẳng hạn trùng địa chỉ (hai trạm đều nghĩ rằng đến lượt mình) hoặc "đứt vòng" (không trạm nào nghĩ đến lượt mình)
- Khởi tạo vòng logic: Khi cài đặt mạng hoặc sau khi "đứt vòng", cần phải khởi tạo lại vòng.

Thiết bị LAN: Bộ thu phát (Transceiver)

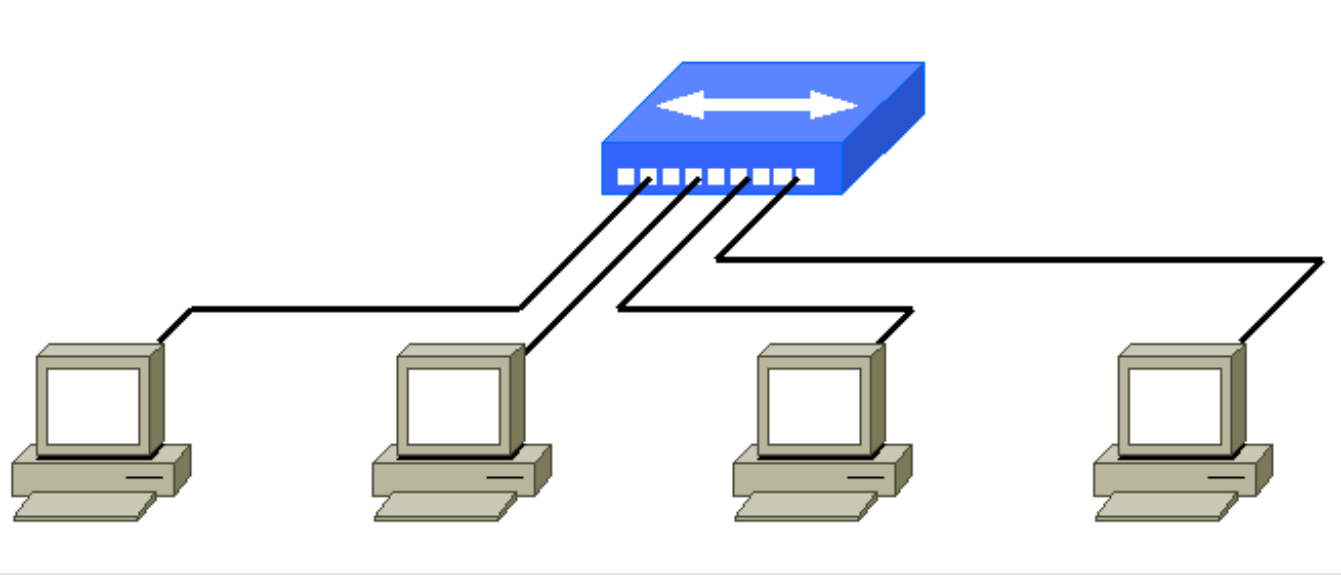
- Kết nối các phương tiện khác nhau
- Thiết bị lớp 1

Thiết bị LAN: Bộ lặp (Repeater)



- Khuếch đại tín hiệu bị yếu
- Thiết bị lớp 1

Thiết bị LAN: Bộ tập trung dây (hub)



- Bộ lặp đa cổng
- Thiết bị lớp 1

Các thiết bị LAN - Hub

- Hub là một trong những yếu tố quan trọng nhất của LAN, đây là điểm kết nối dây trung tâm của mạng, tất cả các trạm trên mạng LAN được kết nối thông qua HUB.
- Một hub thông thường có nhiều cổng nối với người sử dụng để gắn máy tính và các thiết bị ngoại vi. Mỗi cổng hỗ trợ một bộ kết nối dùng cặp dây xoắn 10BASET từ mỗi trạm của mạng. Khi bó tín hiệu Ethernet được truyền từ một trạm tới hub, nó được lặp lại trên khắp các cổng khác của hub.
- Các hub thông minh có thể định dạng, kiểm tra, cho phép hoặc không cho phép bởi người điều hành mạng từ trung tâm quản lý hub.

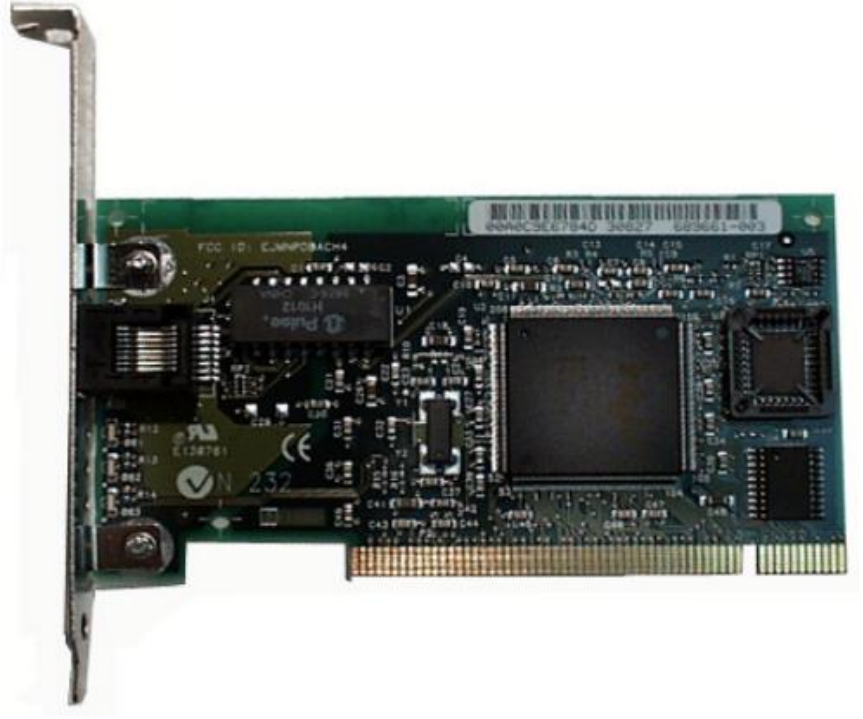
HUB - Phân loại

Có ba loại hub:

- **Hub đơn (stand alone hub)**
- **Hub phân tầng (stackable hub)**
- **Hub -môdun (modular hub)**
- **Modular hub rất phổ biến cho các hệ thống mạng vì nó có thể dễ dàng mở rộng và luôn có chức năng quản lý, modular có từ 4 đến 14 khe cắm, có thể lắp thêm các modun Ethernet 10BASET.**
- **Stackable hub là lý tưởng cho những cơ quan muốn đầu tư tối thiểu ban đầu nhưng lại có kế hoạch phát triển LAN sau này.**

Thiết bị LAN: NIC Network Interface Card

- Giao diện mạng của máy tính
- Có địa chỉ vật lý
- Thiết bị lớp 2



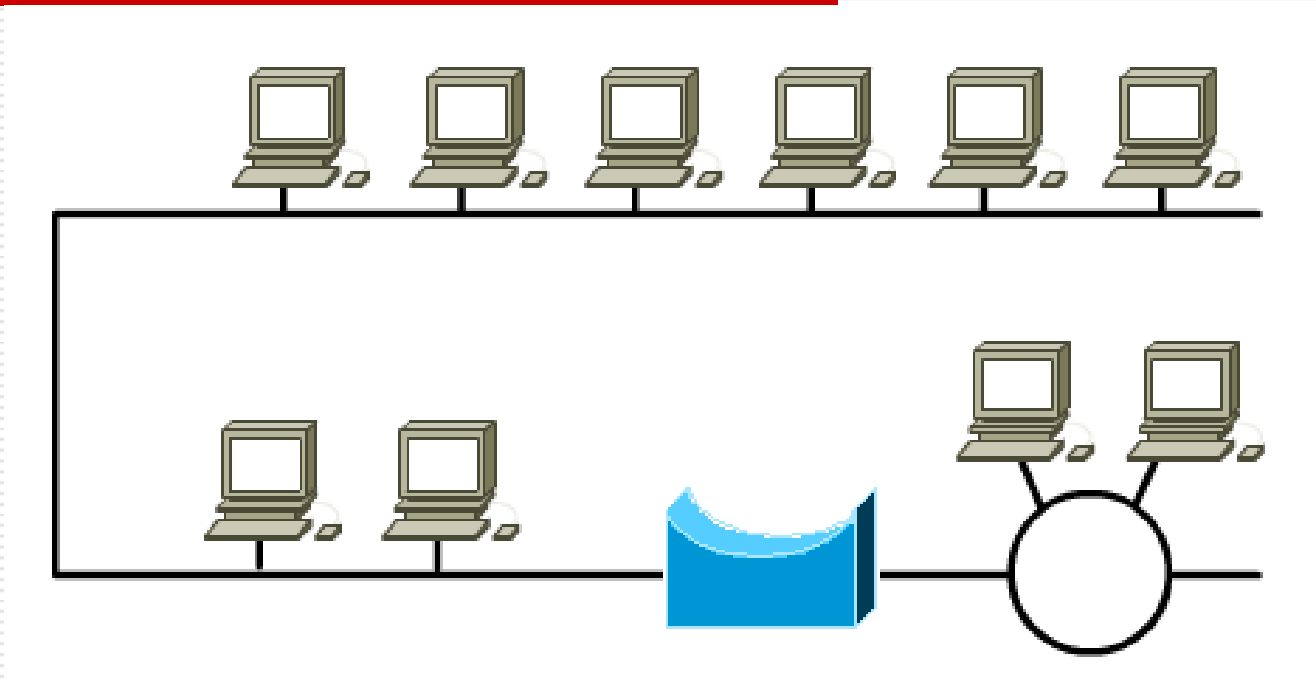
NIC

- Cung cấp cổng kết nối mạng
- Chọn lựa card mạng
  - Kiểu mạng
    - Ethernet
    - Token Ring
    - FDDI
  - Kiểu phương tiện truyền dẫn
    - Cáp xoắn
    - Cáp đồng trục
    - Cáp quang
  - Kiểu bus hệ thống trên máy tính
    - PCI
    - ISA

NIC: Chức năng lớp 2

- Điều khiển kết nối luận lý (LLC): giao tiếp với lớp trên trong máy tính
- Đặt tên: cung cấp xác định bằng địa chỉ MAC
- Định khung: một phần của quá trình đóng gói để truyền dữ liệu
- Điều khiển truy xuất phương tiện (MAC): cung cấp cách thức truy xuất phương tiện truyền dẫn
- Phát tín hiệu: tạo tín hiệu và giao tiếp với phương tiện truyền dẫn

Thiết bị LAN: Cầu nối (bridge)



- Chuyển các gói tin có đích ở phần mạng bên kia dựa vào địa chỉ vật lý
- Thiết bị lớp 2

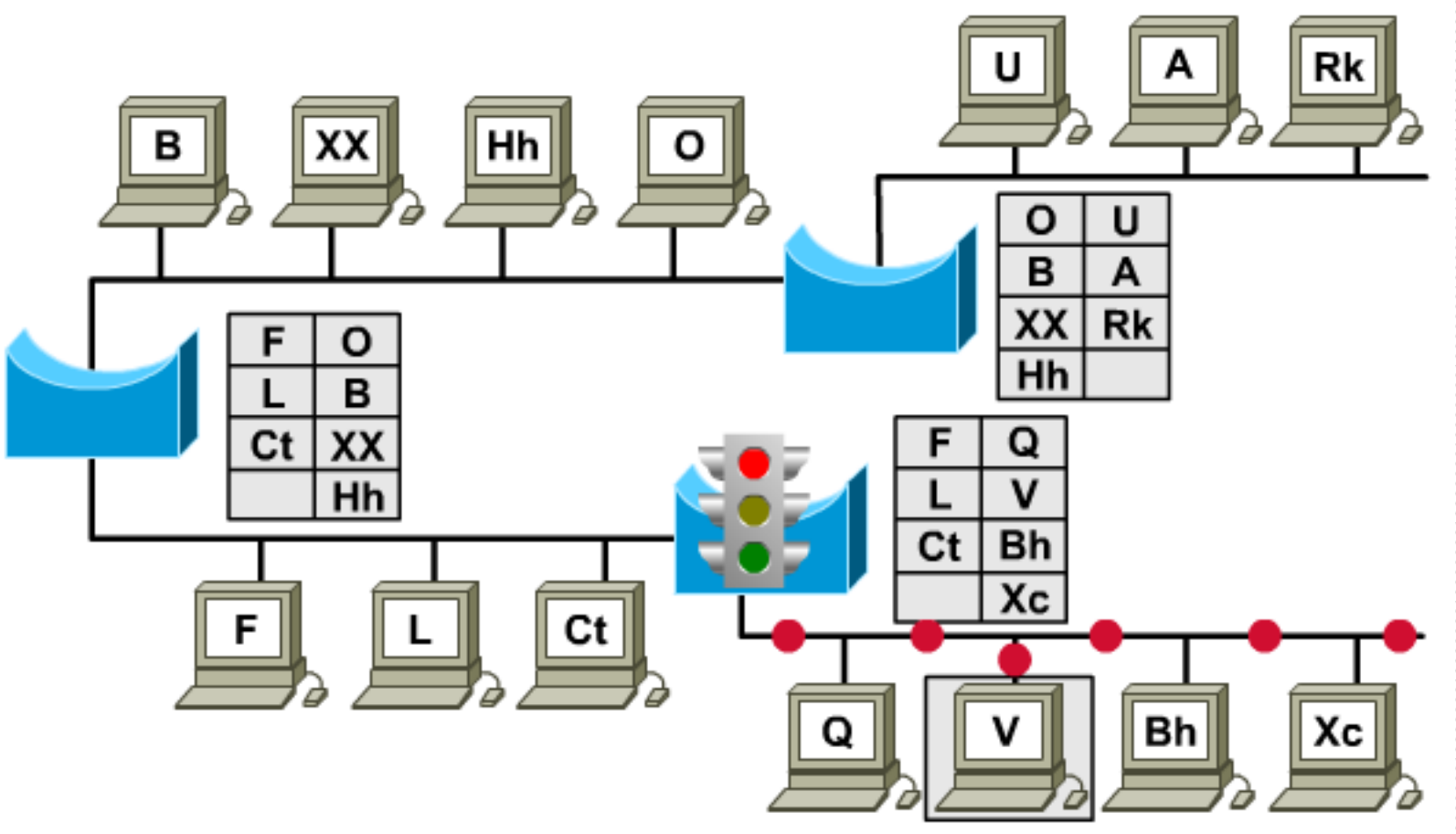
Thiết bị LAN: Cầu nối (bridge)

- Là cầu nối hai hoặc nhiều đoạn (segment) của một mạng.
- Theo mô hình OSI thì bridge thuộc mức 2.
- Bridge sẽ lọc những gói dữ liệu để gửi đi (hay không gửi) cho đoạn nối, hoặc gửi trả lại nơi xuất phát.
- Các bridge cũng thường được dùng để phân chia một mạng lớn thành hai mạng nhỏ nhằm làm tăng tốc độ.
- Mặc dầu ít chức năng hơn router, nhưng bridge cũng được dùng phổ biến.

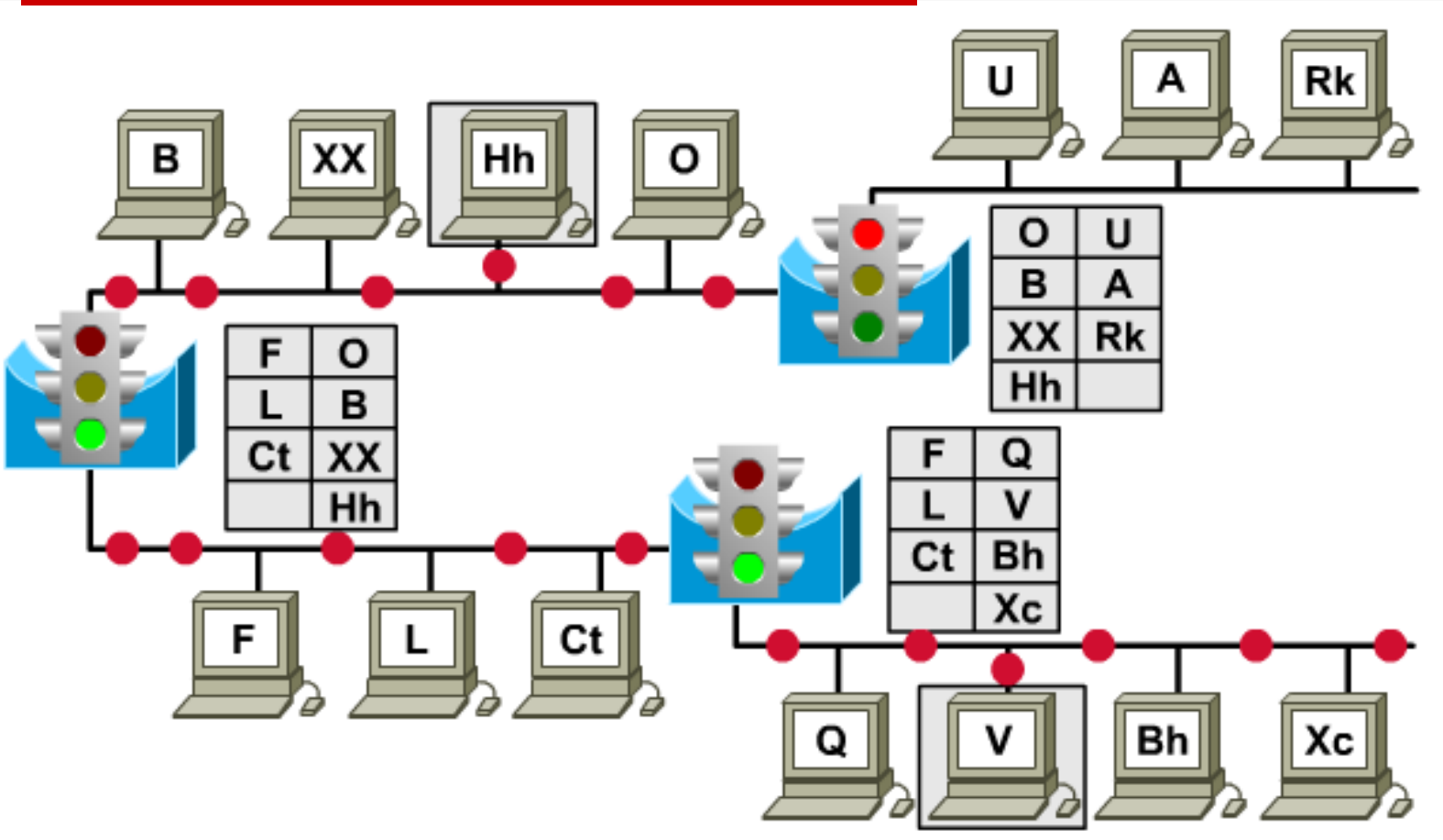
Bridge

- Kết nối các đoạn mạng
- Thông minh hơn trong việc quyết định có chuyển tín hiệu qua đoạn mạng kia hay không
- Tăng hiệu suất mạng bởi loại trừ lưu lượng mạng không cần thiết và giảm sự đụng độ
- Chia mạng thành các đoạn mạng và lọc lưu lượng dựa trên địa chỉ MAC
- Chuyển frame giữa các đoạn mạng có giao thức lớp 2 khác nhau

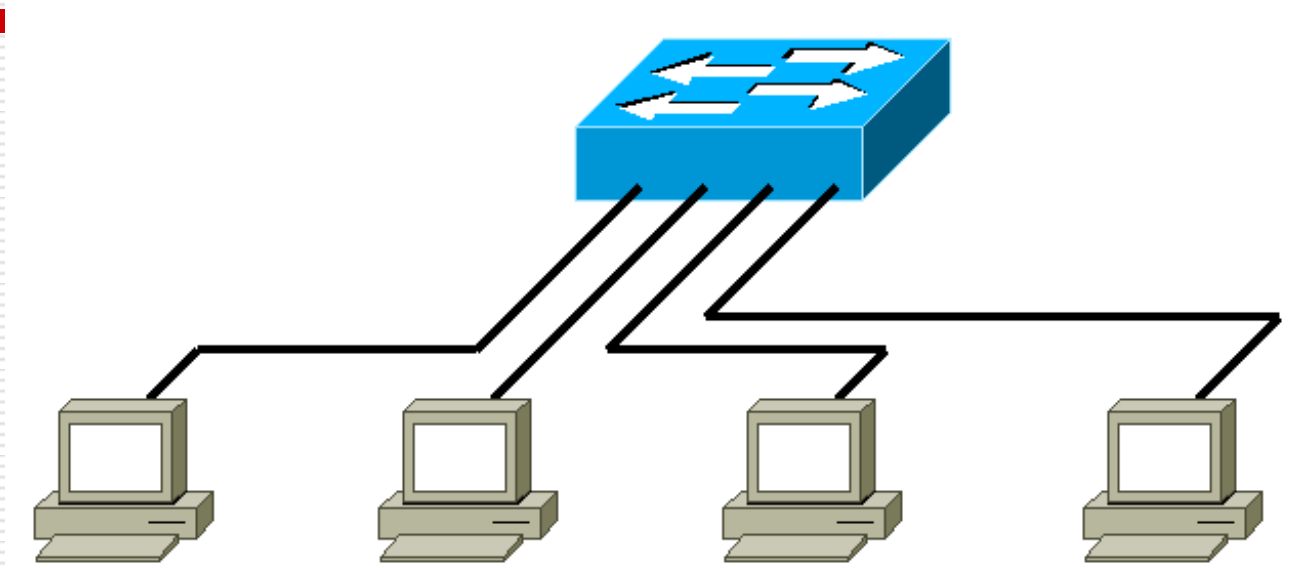
Bridge : lọc


B
XX
Hh
O
U
A
Rk
O U
B A
XX Rk
Hh
F O
L B
Ct XX
Hh
F Q
L V
Ct Bh
Xc
F
L
Ct
Q
V
Bh
Xc

Bridge : chuyển



Thiết bị LAN: Bộ chuyển mạch (Switch)



- Cầu nối đa cổng
- Thiết bị lớp 2

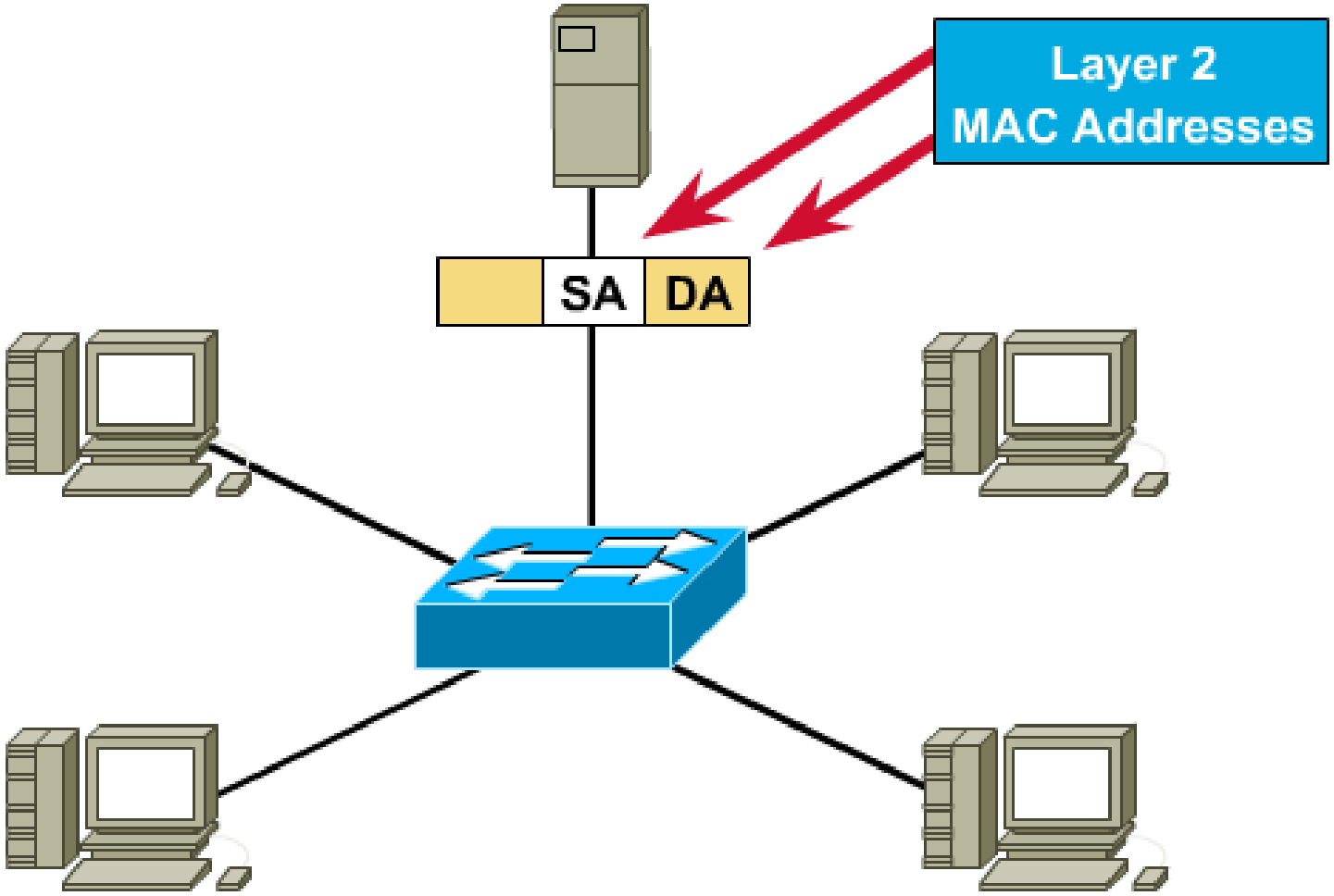
Bộ chuyển mạch (switch)

- Chức năng chính của switch là cùng một lúc duy trì nhiều cầu nối giữa các thiết bị mạng bằng cách dựa vào một loại đường truyền xương sống (backbone) nội tại tốc độ cao.
- Switch có nhiều cổng, mỗi cổng có thể hỗ trợ toàn bộ Ethernet LAN hoặc Token Ring.
- Bộ chuyển mạch kết nối một số LAN riêng biệt và cung cấp khả năng lọc gói dữ liệu giữa chúng.
- Các switch là loại thiết bị mạng mới, nhiều người cho rằng, nó sẽ trở nên phổ biến nhất vì nó là bước đầu tiên trên con đường chuyển sang chế độ truyền không đồng bộ ATM.

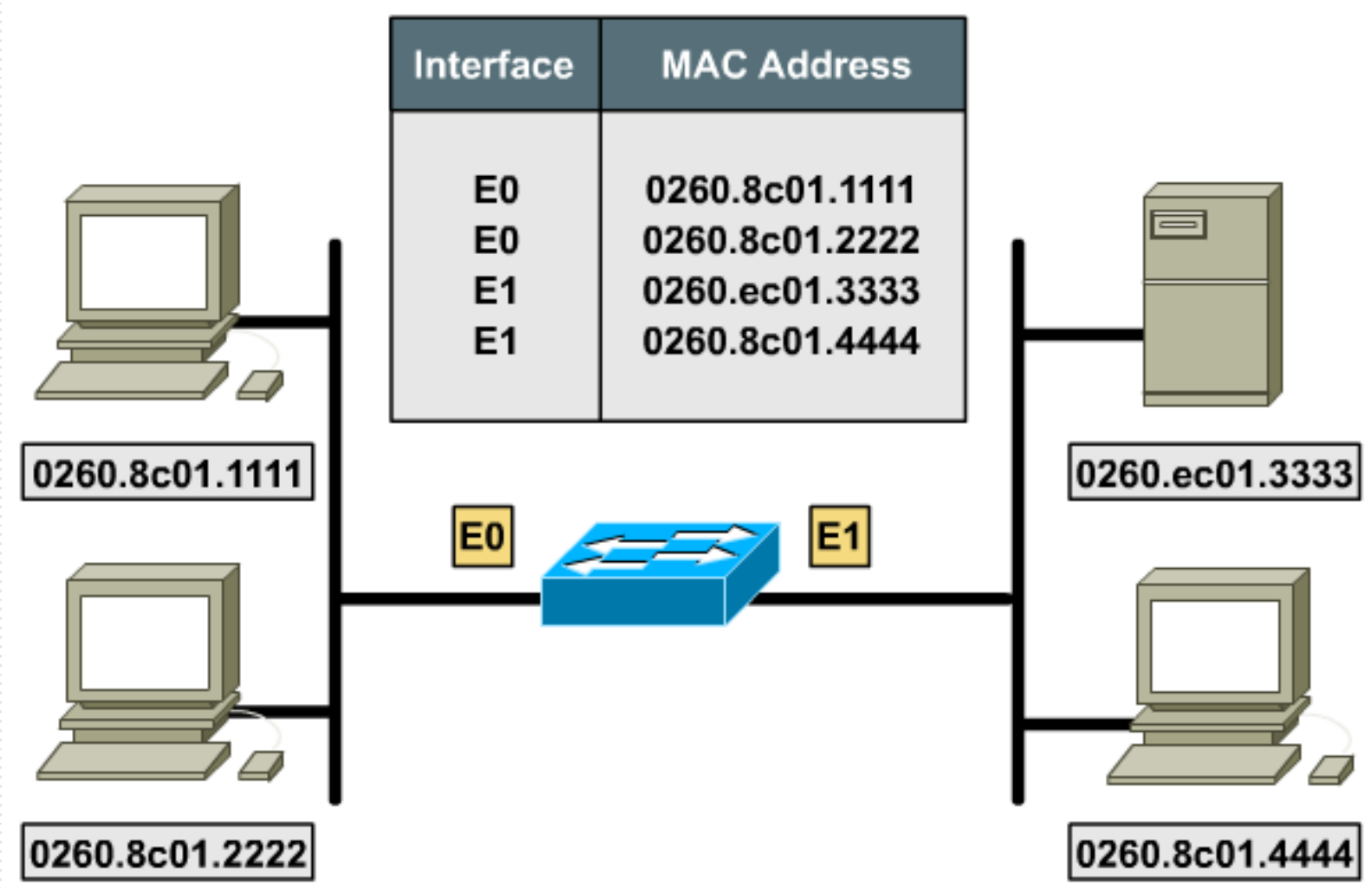
LAN Switch

- Switch kết nối các đoạn mạng LAN
- Switch được xem như là bridge đa cổng
- Sử dụng bảng địa chỉ MAC để xác định đoạn mạng frame cần truyền
- Switch thay thế hub với hệ thống dây giữ nguyên
- Tốc độ cao hơn bridge
- Hỗ trợ các tính năng mới như VLAN (LAN ảo)

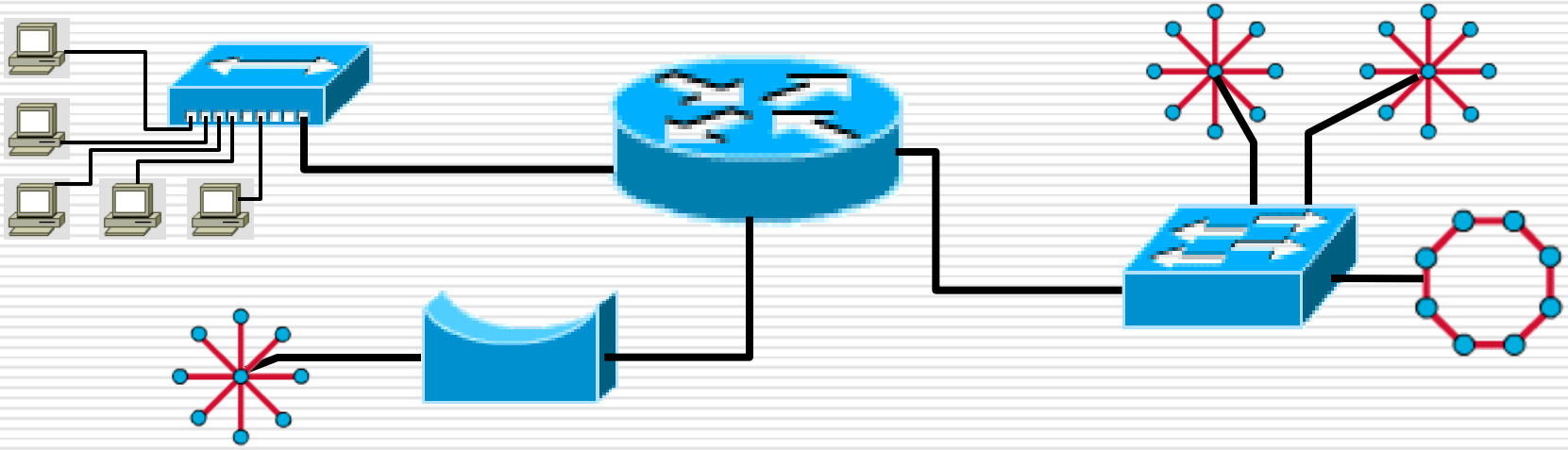
LAN Switch



LAN Switch: bảng MAC



Thiết bị LAN: Bộ định tuyến (Router)



- Hoạt động dựa trên địa chỉ lớp 3 (địa chỉ luận lý)
- Thiết bị lớp 3

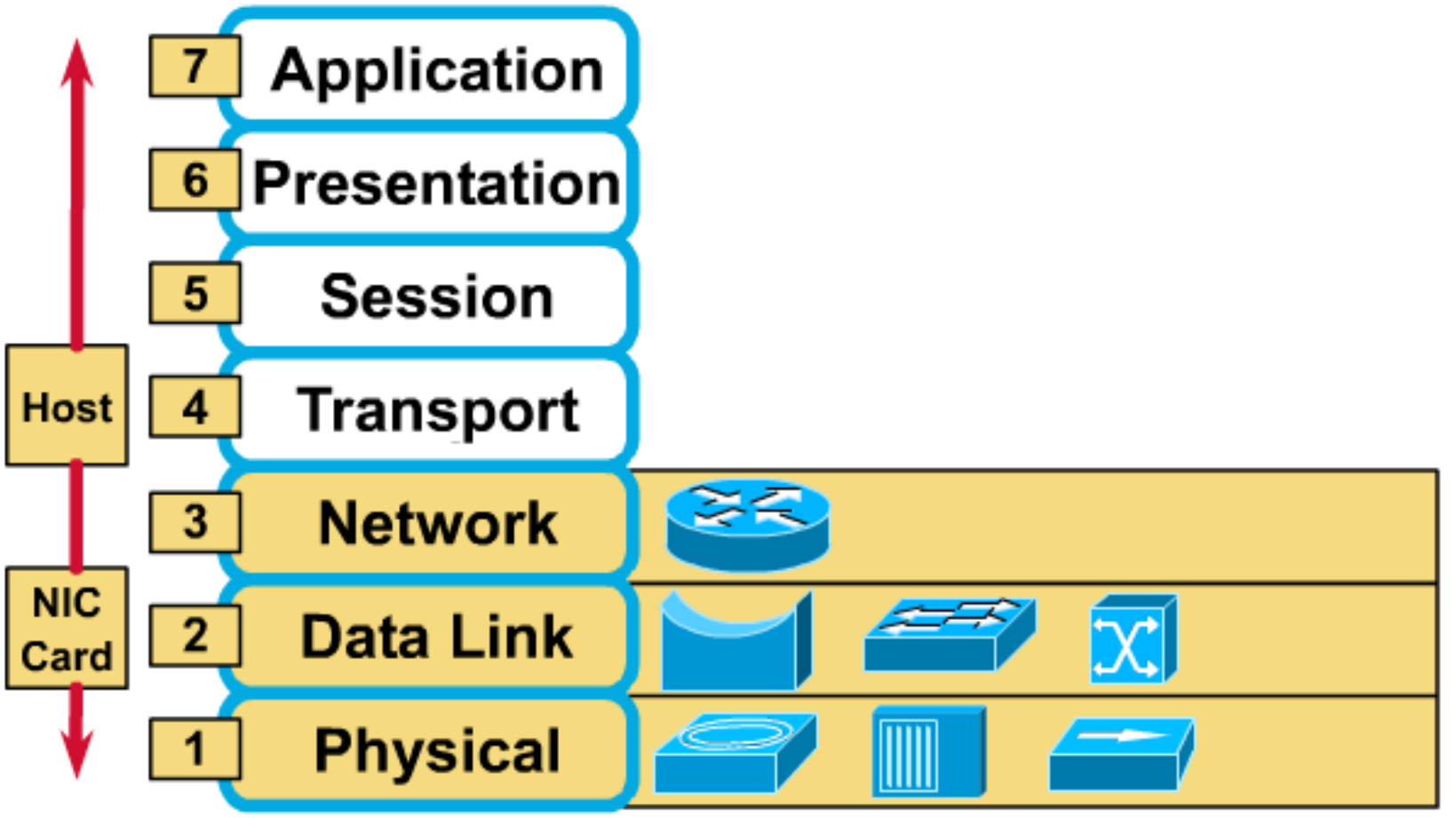
Bộ dẫn đường (router)

- Chức năng cơ bản của router là gửi đi các gói dữ liệu dựa trên địa chỉ phân lớp của mạng và cung cấp các dịch vụ như bảo mật, quản lý lưu thông...
- Giống như bridge, router là một thiết bị thông minh đối với các mạng thực sự lớn. Router biết địa chỉ của tất cả các máy tính ở từng phía và có thể chuyển các thông điệp cho phù hợp. Chúng còn phân đường-định truyền để gửi từng thông điệp có hiệu quả.
- Theo mô hình OSI thì chức năng của router thuộc mức 3, cung cấp thiết bị với thông tin chứa trong các header của giao thức, giúp cho việc xử lý các gói dữ liệu thông minh.
- Dựa trên những giao thức, router cung cấp dịch vụ mà trong đó mỗi packet dữ liệu được đọc và chuyển đến đích một cách độc lập.
- Khi số kết nối tăng thêm, mạng theo dạng router trở nên kém hiệu quả và cần suy nghĩ đến sự thay đổi.

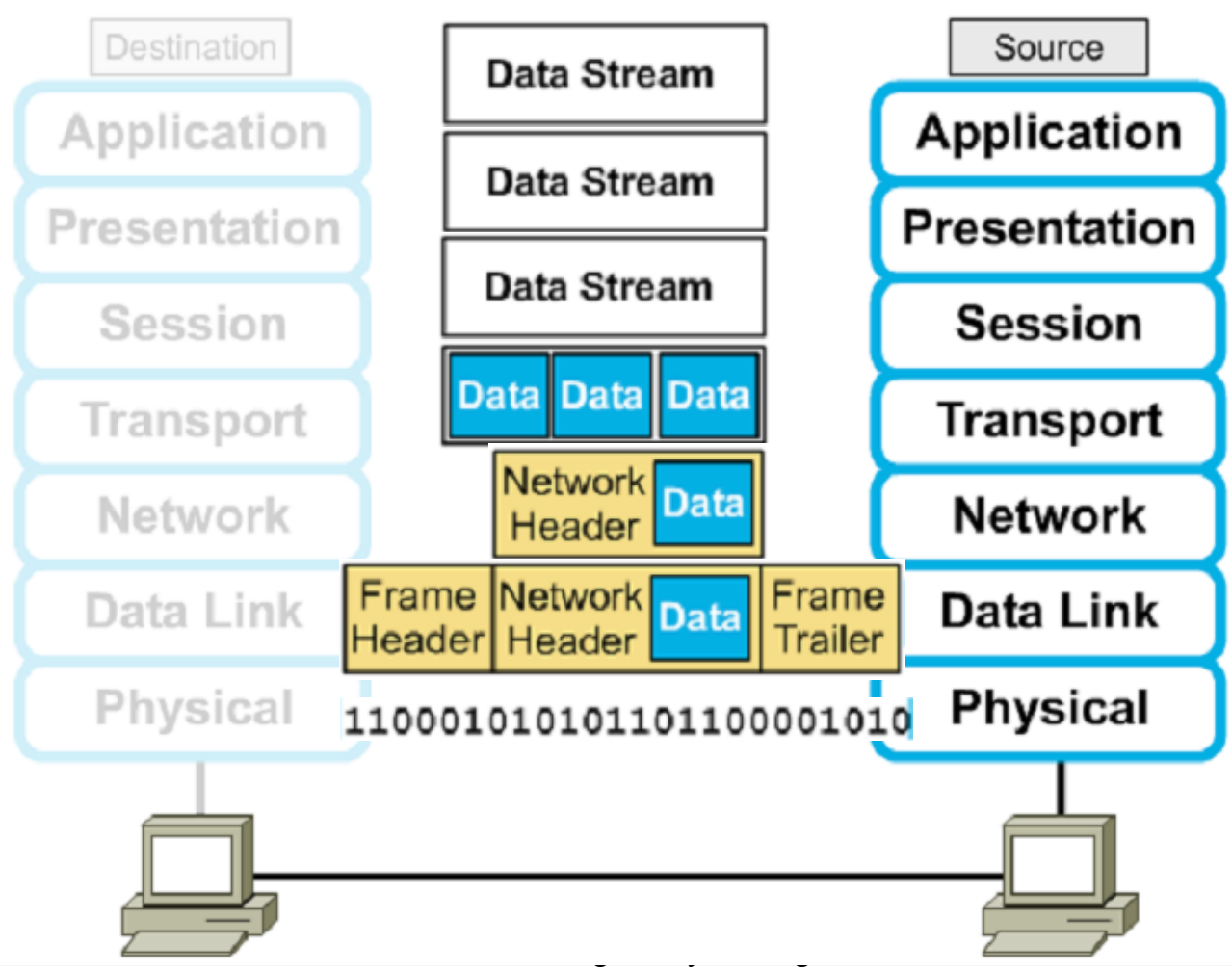
Chức năng bộ định tuyến

- **Tìm đường**
  - **Quá trình tính toán dựa trên địa chỉ IP đích để quyết định sẽ gửi gói tin ra cổng nào**
- **Chuyển gói tin**
  - **Đóng gói gói tin lại theo giao thức ở cổng ra và chuyển gói tin ra cổng đó**

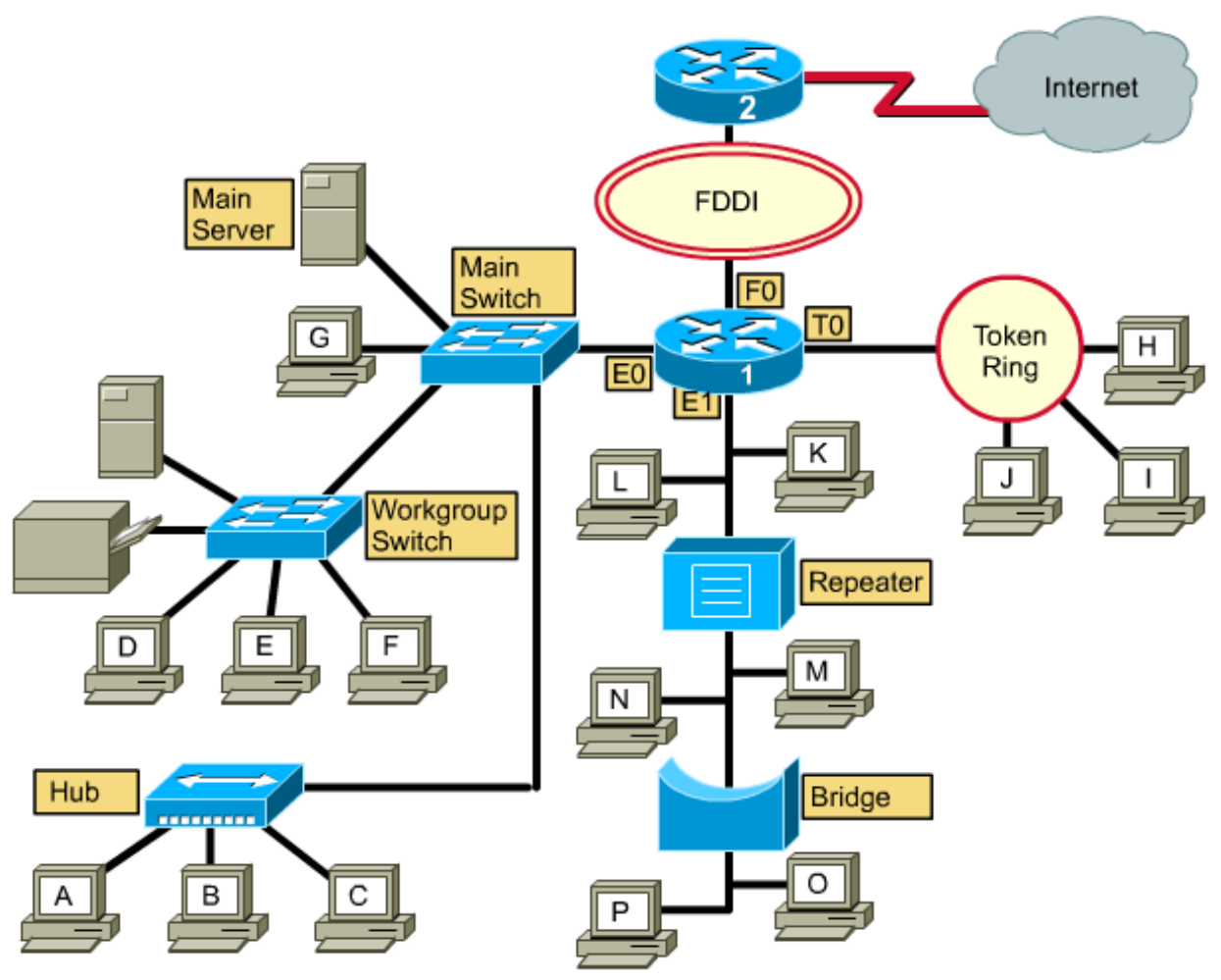
Các thiết bị hoạt động ở từng lớp



Sự đóng gói


Destination
Application
Presentation
Session
Transport
Network
Data Link
Physical
Data Stream
Data Stream
Data Stream
Data
Data
Data
Network Header
Data
Frame Header
Network Header
Data
Frame Trailer
1100010101011011000010 10
Source
Application
Presentation
Session
Transport
Network
Data Link
Physical

Ví dụ minh họa



Hệ điều hành mạng (NOS Network Operating System)

- **Cùng với sự nghiên cứu và phát triển mạng máy tính, hệ điều hành mạng đã được nhiều công ty đầu tư nghiên cứu và đã công bố nhiều phần mềm quản lý và điều hành mạng có hiệu quả như: *NetWare* của công ty NOVELL, *LAN Manager* của Microsoft dùng cho các máy server chạy hệ điều hành OS/2, *LAN server* của IBM (gần như đồng nhất với LAN Manager), *Vines* của Banyan Systems là hệ điều hành mạng dùng cho server chạy hệ điều hành UNIX, *Promise LAN* của Mises Computer chạy trên card điều hợp mạng độc quyền, *Windows for Workgroups* của Microsoft, *LANtastic* của Artisoft, *NetWare Lite* của Novell,....**
- **Chọn hệ điều hành mạng nào sẽ làm nền tảng cho mạng sẽ được phát triển tuỳ thuộc vào kích cỡ của mạng hiện tại và sự phát triển trong tương lai, còn tuỳ thuộc vào những ưu điểm và nhược điểm của từng hệ điều hành.**

Hệ Điều Hành Mạng

- **Hệ điều hành mạng UNIX: Đây là hệ điều hành do các nhà khoa học xây dựng và được dùng rất phổ biến trong giới khoa học, giáo dục. Hệ điều hành mạng UNIX là hệ điều hành đa nhiệm, đa người sử dụng, phục vụ cho truyền thông tốt. Nhược điểm của nó là hiện nay có nhiều *Version* khác nhau, không thống nhất gây khó khăn cho người sử dụng. Ngoài ra hệ điều hành này khá phức tạp lại đòi hỏi cấu hình máy mạnh (trước đây chạy trên máy mini, gần đây có SCO UNIX chạy trên máy vi tính với cấu hình mạnh).**
- **BSD, Linux là các HĐH tựa UNIX và có thể cài chạy trên các máy tính có cấu hình thấp hơn.**

Hệ Điều Hành Mạng

- **Hệ điều hành mạng *Windows NT*: Đây là hệ điều hành của hãng Microsoft, cũng là hệ điều hành đa nhiệm, đa người sử dụng. Đặc điểm của nó là tương đối dễ sử dụng, hỗ trợ mạnh cho phần mềm WINDOWS. Ngoài ra, *Windows NT* có thể liên kết tốt với máy chủ Novell Netware. Tuy nhiên, để chạy có hiệu quả, *Windows NT* cũng đòi hỏi cấu hình máy tương đối mạnh.**
- **Hệ điều hành mạng *Windows for Worrkgroup*: Đây là hệ điều hành mạng ngang hàng nhỏ, cho phép một nhóm người làm việc (khoảng 3-4 người) dùng chung ổ đĩa trên máy của nhau, dùng chung máy in nhưng không cho phép chạy chung một ứng dụng. Hiện nay rất ít sử dụng.**
- **Hiện nay có *Windows 2000*.**

Hệ Điều Hành Mạng

- **Hệ điều hành mạng *NetWare* của Novell: Đây là hệ điều hành phổ biến, nó có thể dùng cho các mạng nhỏ (khoảng từ 5-25 máy tính) và cũng có thể dùng cho các mạng lớn gồm hàng trăm máy tính. Có nhiều phiên bản của *Netware*. *Netware* là một hệ điều hành mạng cục bộ dùng cho các máy vi tính theo chuẩn của IBM hay các máy tính Apple Macintosh, chạy hệ điều hành MS-DOS hoặc OS/2.**

AN TOÀN MẠNG

An toàn mạng

Mật mã và chứng thực

Các hình thức tấn công trên mạng

TCP có thực sự an toàn không?

An ninh mạng máy tính

An toàn mạng máy tính

- **1. Giữ bí mật**
  - **"Nếu chúng ta không nói cho ai biết các số điện thoại truy cập thì sẽ không có các xâm nhập qua các số điện thoại này"**
  - **nhân viên trong cơ quan đều biết các số điện thoại này.**
  - **các hacker có thể thử tất cả các số có thể.**

- **2. Thiết lập cơ cấu kiểm tra và lọc tin**
  - **"Chúng tôi thiết lập các cơ chế lọc gói tin ngay tại các gateway, không cho phép các truy cập telnet hay ftp"**

- **nếu có một modem trong cơ quan cho phép kết nối từ bên ngoài thì sao?**
- **cơ chế lọc tin có đảm bảo cho tất cả các trường hợp không?**

3. Mã hóa

- **“Chúng tôi mã hoá mọi thông tin”**
- **Nếu thông tin là có giá trị thì việc sử dụng hệ thống máy tính mạnh, đắt tiền để bẻ khóa là hoàn toàn có thể xảy ra.**
- **nếu khoá mật mã bị mất ở đâu đó thì sao?**
- **giải mã sẽ mất nhiều thời gian và công sức, gây khó khăn nhất định cho công việc chung.**

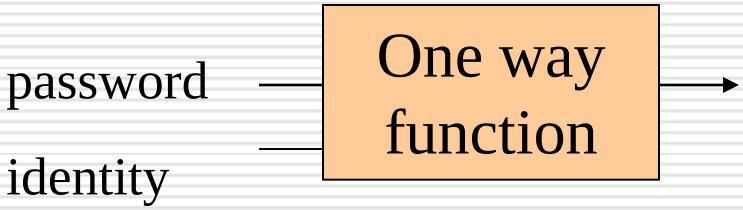
- **4. Giải pháp chung**
  - **giải pháp hiệu quả nhất thường đơn giản và có thể để người ngoài đánh giá.**
  - **các giải pháp đòi hỏi một chi phí nhất định.**
  - **đòi hỏi sự đóng góp nỗ lực của nhiều người.**

Chứng nhận (Authentication)

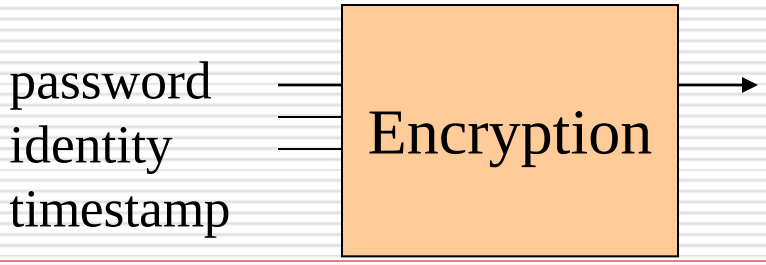
password

Level 0

Level 1



Level 2



Level 3

One way functions

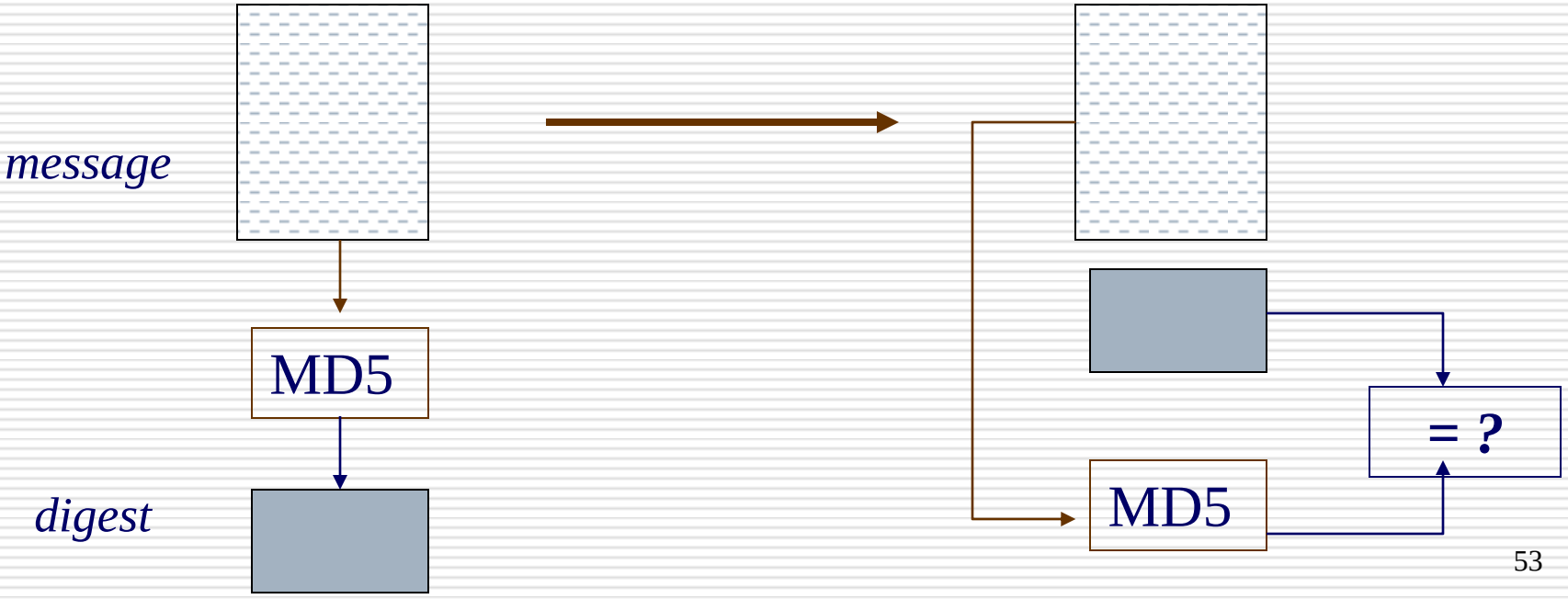
- **Các hàm này được đưa ra nhằm mục đích "xáo trộn" thông tin đầu vào sao cho thông tin đầu ra không thể được phục hồi thành thông tin ban đầu.**
- **Hàm exclusive-OR (XOR):**

  $$C = b_1\ b_2\ b_3\ \ldots\ldots\ b_n$$

- **tuy nhiên hàm XOR có thể bị bẻ khóa dễ dàng.**

Thuật toán "Tiêu hoá" MD5

- dùng cho chứng nhận thông tin đòi hỏi tính bảo mật cao.
- làm thế nào chúng ta biết được thông tin gửi đến không bị thay đổi?



Thuật toán “Tiêu hoá” MD5

- thông điệp được gửi cùng với bản bị “tiêu hóa”. Tại nơi nhận, thông điệp bị “tiêu hoá” một lần nữa và sau đó, được so sánh với bản “tiêu hóa” nhận được. Nếu hai bản không trùng nhau, nghĩa là thông điệp nhận được đã bị thay đổi.
- MD5 lấy các khối tin 128bit và chia khối này thành 3 từ 32bit
- các từ 32bit được xử lý tiếp như sau:
  F(X,Y,Z) = X · Y + X’ · Z
  G(X,Y,Z) = X · Z + Y · Z’
  H(X,Y,Z) = X Å Y Å Z
  I(X,Y,Z) = Y Å (X + Z’)
- với các phép toán logic AND (·) OR (+) NOT (’) và XOR (Å)
- kết quả sau đó được đưa qua bảng chân trị 64bit. Bảng này được tạo từ hàm sin.

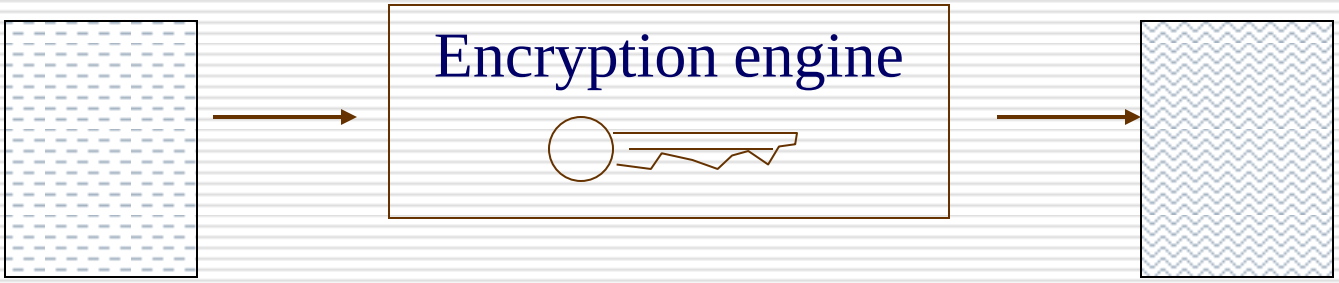
Trao đổi khoá

- giả sử George muốn liên lạc với Fred: hai người tạo ra các số ngẫu nhiên riêng A và B, cùng quy định sử dụng một hàm modulo β và số α.
- sau đó George tính và gửi kết quả sau
  $\alpha^A \pmod{\beta}$
- tương tự, Fred cũng tính và gửi kết quả
  $\alpha^B \pmod{\beta}$
- George biết được A và $\alpha^B \pmod{\beta}$ nên có thể tính
  $\alpha^{AB} \pmod{\beta}$

  và Fred cũng thực hiện tương tự với B và $\alpha^A \pmod{\beta}$. Kết quả nhận được sẽ được dùng như là chìa khóa mật mã chung giữa George và Fred.

Mã hóa (encryption)

- **thông tin ban đầu (*plaintext*) cần được thay đổi (*mật mã hoá - encryption*) thành thông tin được mã hoá (*cyphertext*).**
- **một cơ chế mật mã bằng khóa mật mã được sử dụng để mật mã hoá thông tin.**



plaintext

cyphertext

Mã hóa (encryption)

- sau đó, cơ chế giải mã (*decryption*) bằng khóa giải mã sẽ giải mã thông tin mã hoá thành thông tin ban đầu.
- nếu khóa mật mã và khoá giải mã giống nhau thì đây là hệ thống mật mã dùng khoá đối xứng (*symmetric key*). Ngoài ra còn có hệ thống mật mã dùng khóa không đối xứng (*asymmetric key*)
- Mã hoá DES – *Data Encryption System* là hệ thống mật mã dùng khoá đối xứng. Hệ thống mật mã PGP – *Pretty Good Privacy* dùng khóa không đối xứng.
- bài toán an toàn cho hệ thống mật mã dùng khóa đối xứng là làm thế nào để gửi khoá giải mã cho người nhận thông tin (bằng đường bưu điện? email hoặc điện thoại thì không an toàn).

DES và các thuật toán cùng loại

- **DES là mã hoá theo khối, đọc vào các khối thông tin nguồn có chiều dài 64bit. DES dùng khóa có chiều dài 64bit (trong đó có 8bit kiểm tra chẵn lẻ - parity bit)**
- **DES được xây dựng theo yêu cầu của Văn phòng quốc gia về chuẩn của Mỹ (National Bureau of Standards, sau này được gọi là NIST), được đưa vào sử dụng năm 1978 và được duyệt lại mỗi 5 năm một lần (lần cuối cùng là vào năm 1993).**
- **IDEA mã hoá giống như của DES, sử dụng các phép toán XOR, cộng và nhân giá trị tuyệt đối, khóa 128bit.**
- **Skipjack:**

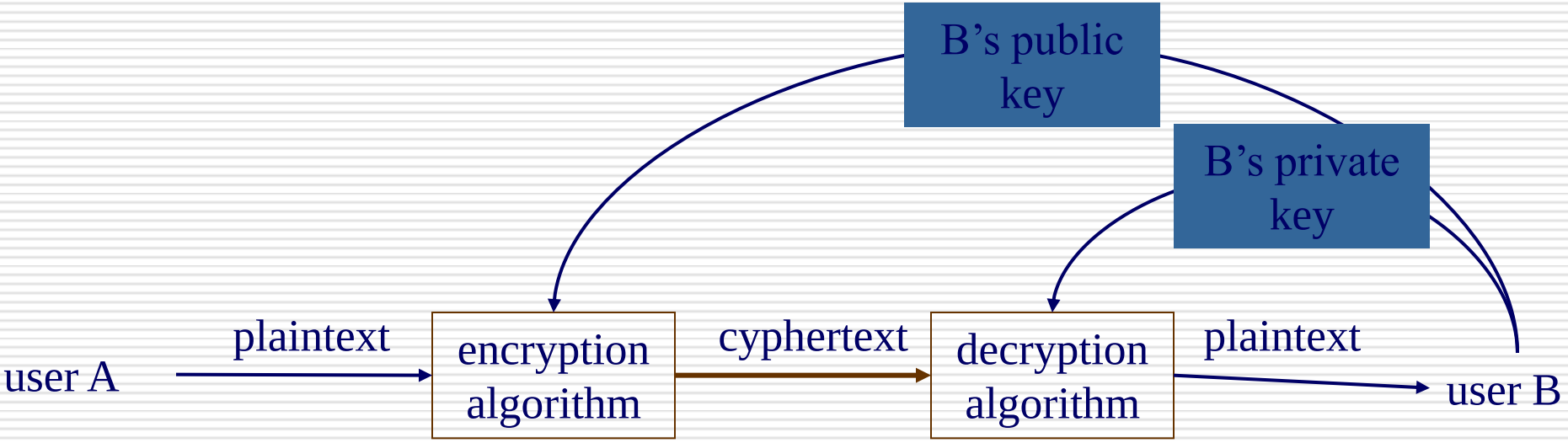
Mức độ an toàn của DES

- **Wiener[1994] đưa ra một ước lượng cho thấy một hệ thống bẻ khóa DES có giá 1M có thể tìm được khóa DES trong vòng 7 giờ, và hệ thống được xây dựng với giá thành thấp hơn (100K) có thể tìm được khóa DES trong 70 giờ.**

Mã hoá khóa công khai

- hệ thống mật mã hoá khóa đối xứng đòi hỏi hai bên gửi và nhận thông tin phải thực hiện trao đổi khoá chung trước khi liên lạc.
- số lượng khoá cần phát sinh cho mỗi cặp như thế sẽ rất nhiều (n2).
- hệ thống mật mã hóa khóa công khai (public key encryption) là mô hình mật mã hoá trong đó khóa mật mã (encryption key) được công khai, nhưng khóa giải mã (decryption key) lại được giữ kín.

- **thuật toán mã hoá khoá công khai RSA lấy tên viết tắt của những người phát minh ra nó: Rivest, Shamir và Adleman.**
- **tính an toàn của RSA có được là do sự khó khăn khi thực hiện phép phân tích thừa số các số lớn.**



RSA

- **chọn hai số nguyên tố *p* và *q*. Tính *n = pq, f(n) = (p-1)(q-1)*.**
- **chọn một số nguyên *d* ngẫu nhiên, *1<d<f(n)*, nguyên tố cùng nhau với *f(n)*, và tính số *e* thỏa mãn:**

  ed = kf(n) + 1

  hay: ***ed º 1 mod f(n)***
- **Public key: *(e,n)* và private key: *(d,n)*.**
- **Mật mã hóa: với khối tin nguồn P <*n*, thông tin được mã hoá (C) theo công thức: $C = P^e \pmod{n}$.**
- **Giải mã: $P = C^d \pmod{n}$**

Tấn công vào hệ thống mã hoá

- Sử dụng các thông điệp đã biết nội dung và bản mã hoá của chúng, từ đó suy ra khoá mật mã.
- Đánh lừa hệ thống và thu nhận những thông tin phản hồi có chọn lựa.
- Tìm kiếm vét cạn: thử tất cả các trường hợp. Đòi hỏi hệ thống máy tính rất mạnh.
- …

Đánh giá hệ thống mã hoá

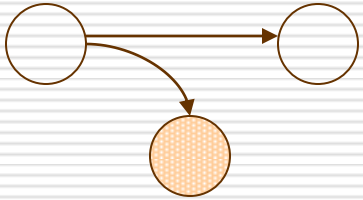
- **Một số hệ thống mã hoá không đủ mạnh:**
  - **các phương pháp mã hóa văn bản trong các chương trình soạn thảo văn bản (vd: MSWord) đã bị phá vỡ. Thậm chí còn có các công ty nhận bẻ khóa các tài liệu như vậy (với mục đích phục hồi tài liệu).**
- **Hệ thống mã hoá an toàn được đánh giá trên các yếu tố sau:**
  - **dựa vào mức độ bí mật và an toàn của khóa chứ không phải là giữ bí mật thuật toán mã hoá. Các hệ thống mã hóa tốt nhất đều được quảng bá rộng rãi.**
  - **miền tồn tại của khóa lớn. Ví dụ: DES có khóa với kích thước 256, hệ thống mã hoá Dolphin có khóa 10109.**

- **tạo ra được các bản mã hoá có tính ngẫu nhiên, loại trừ được các phép thử thống kê cũng như không làm xuất hiện các dấu vết cho phép dò được khoá.**

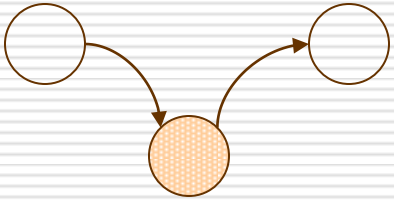
Tấn công và bảo vệ mạng

- **Một số hình thức tấn công vào mạng**

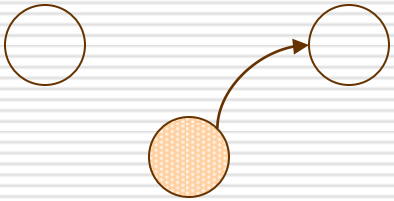
Interruption



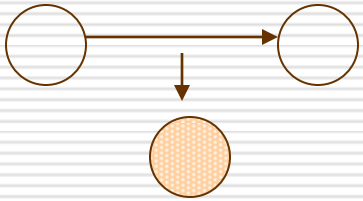
Interception



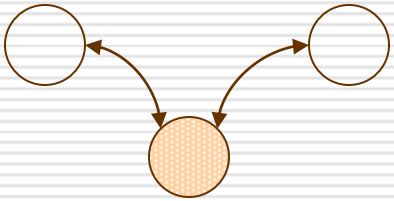
Modification



Masquerade



Eavesdropping



Double Masquerade

- ***interruption*** **có thể được thực hiện bằng các làm hỏng thiết bị mạng. Cách này có thể thực hiện "hiệu quả" hơn nếu chỉ làm thiết bị bị chập chờn vào những thời điểm quan trọng nhất.**
- ***interception*** **là phương pháp thu thập thông tin, đặc biệt hiệu quả cho việc bẻ khóa thông tin.**
- ***modification*** **thường được dùng nhằm mục đích nắm được quyền truy cập hệ thống. Người ta có thể dùng phương pháp truyền lại (replay) ghi lại một thông tin chọn trước (login script) rồi sau đó phát lại thông tin đến hệ thống.**
- ***masquerade*** **rất hiệu quả khi muốn truy nhập hệ thống, ví dụ: ngươi xâm nhập giả làm một hệ thống phân phối qua đó xâm nhập vào hệ thống của nơi nhận.**

- ***double masquerade*: người xâm nhập giả làm đối tác của cả hai bên.**
- ***passive monitoring* (theo dõi thụ động) kết hợp với phân tích tình hình và hoạt động của đối phương. Ví dụ: nếu giữa bộ phận nghiên cứu, sản xuất và bán hàng đột nhiên tăng tần suất liên lạc, có thể suy ra rằng một sản phẩm mới sắp được đưa ra.**

Bảo vệ mạng

- Trong khi có rất nhiều hình thức tấn công vào mạng máy tính, thì các biện pháp phòng chống lại khá tập trung.
- cơ chế bảo vệ dựa trên địa chỉ mạng cung cấp giải pháp hạn chế và không đủ mạnh vì các máy tính có thể được thay đổi địa chỉ và giả địa chỉ của máy tính khác.
- dùng các gateway cho hệ thống nhằm tập trung các mối kết nối mạng và kiểm soát hạn chế được các truy cập từ bên ngoài.
- sử dụng "bức tường lửa" (firewall), kết hợp với các phương pháp phát hiện xâm nhập

TCP/IP có an toàn không?

- **Giả địa chỉ IP:**
  - **một kết nối TCP được thiết lập dựa vào các địa chỉ IP. Các địa chỉ IP có thể bị thay đổi.**
- **Thay đổi định tuyến**
  - **người xâm nhập có thể gửi các thông điệp ICMP (Internet Control Message Protocol) thông báo rằng một host nào đó không thể liên lạc được (unreachable) mặc dù host này vẫn hoạt động bình thường, kết quả là định tuyến liên lạc sẽ bị thay đổi.**
  - **có thể gửi các thông điệp chuyển hướng (redirect), hướng các luồng thông tin về máy của người xâm nhập thay vì về một máy tính định trước.**

- **các thông điệp RIP giả có thể được dùng để thay đổi thông tin định tuyến.**
- **các máy tính có thể xác định đường đi trên mạng.**

TCP/IP có an toàn không?

- Tấn công bằng mail.
- Khai thác yếu điểm của hệ thống.
- Tạo các cuộc tấn công từ chối dịch vụ (DOS)→ làm tê liệt hoạt động mạng.
- Virus lây lan qua mạng.

Mobile IP

Mobile IP là gì?

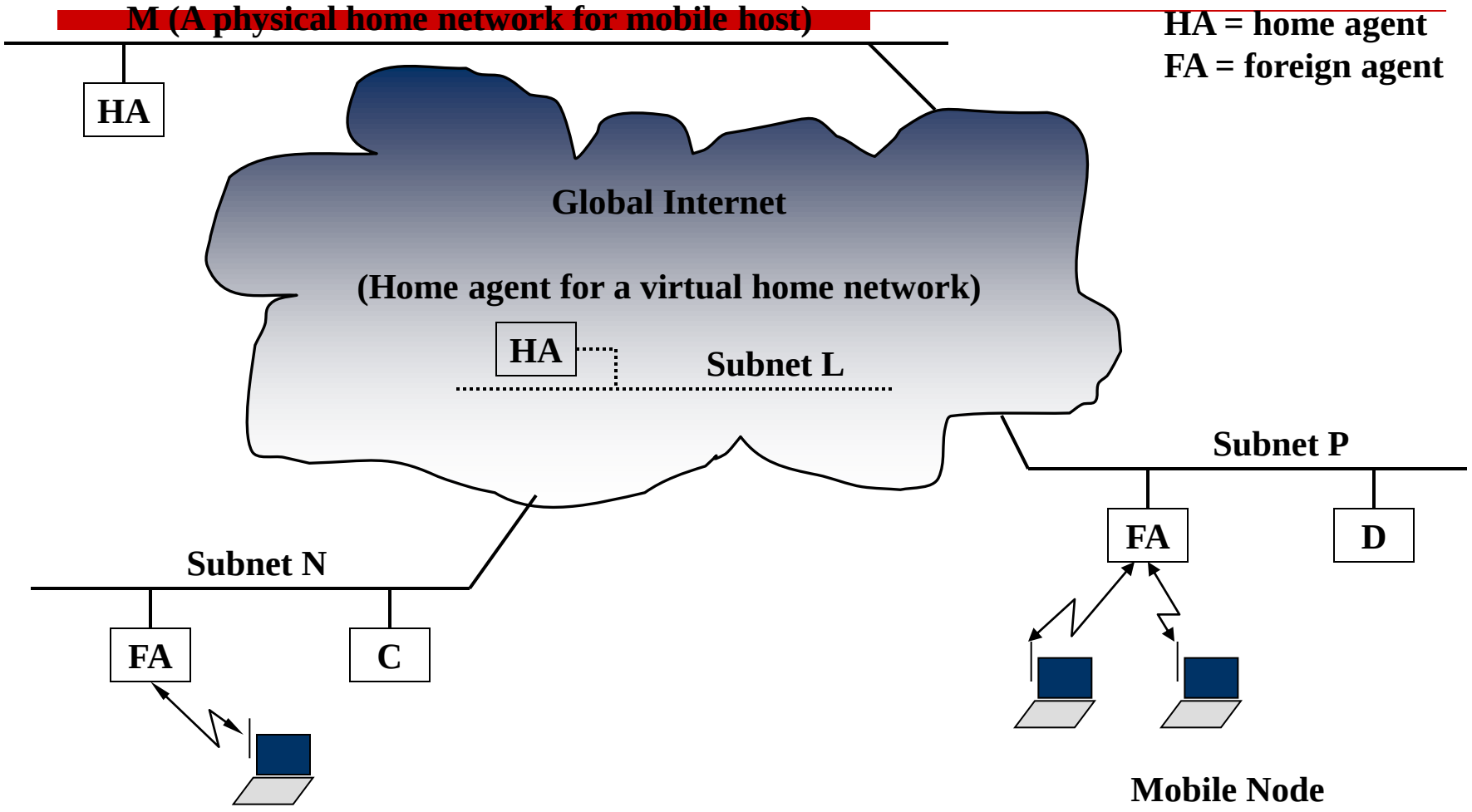
Hoạt động của mô hình Mobile IP

Mobile IP

- **Cho phép các máy tính di chuyển trong khi vẫn kết nối đến mạng**
- **ứng dụng: cho các máy tính xách tay, máy tính cầm tay, các thiết bị thông tin di động có thể truy cập internet…**
- **một máy tính muốn tồn tại trên mạng và liên lạc được với các máy tính khác trên mạng (TCP/IP), máy tính đó buộc phải có một địa chỉ IP không thay đổi it nhất là trong một phiên kết nối.**
- **Khi di chuyển sang mạng khác, máy tính buộc phải đăng ký một địa chỉ IP mới do mạng nơi đến quản lý.**
- **Dữ liệu truyền đến cho máy ở địa chỉ IP cố định (địa chỉ thường trú) không chuyển tiếp đến cho máy ở địa chỉ tạm trú.**

- **mobile IP cho phép các máy tính di động được trong mạng mà vẫn giữ được liên lạc bằng cách đưa ra mô hình liên lạc qua 2 địa chỉ cho mỗi máy: địa chỉ IP của máy ở mạng thường trú (home address) và địa chỉ IP ở mạng tạm trú (care-of-address)**
- **Khi máy tính di chuyển đến một mạng khác, nó phải thực hiện đăng ký với mạng nơi đến để có địa chỉ tạm trú và báo địa chỉ này với mạng ở nhà qua một máy trung gian (home agent).**
- **nếu có một gói tin gửi đến máy di động theo địa chỉ ở mạng thường trú, các máy trung gian (home agent và foreign agent) sẽ nhận gói tin này rồi chuyển đến máy theo địa chỉ tạm trú đã được đăng ký. Ngược lại, máy trung gian tại mạng tạm trú chịu trách nhiệm chuyển gói tin từ máy di động lên mạng.**

Mobile IP



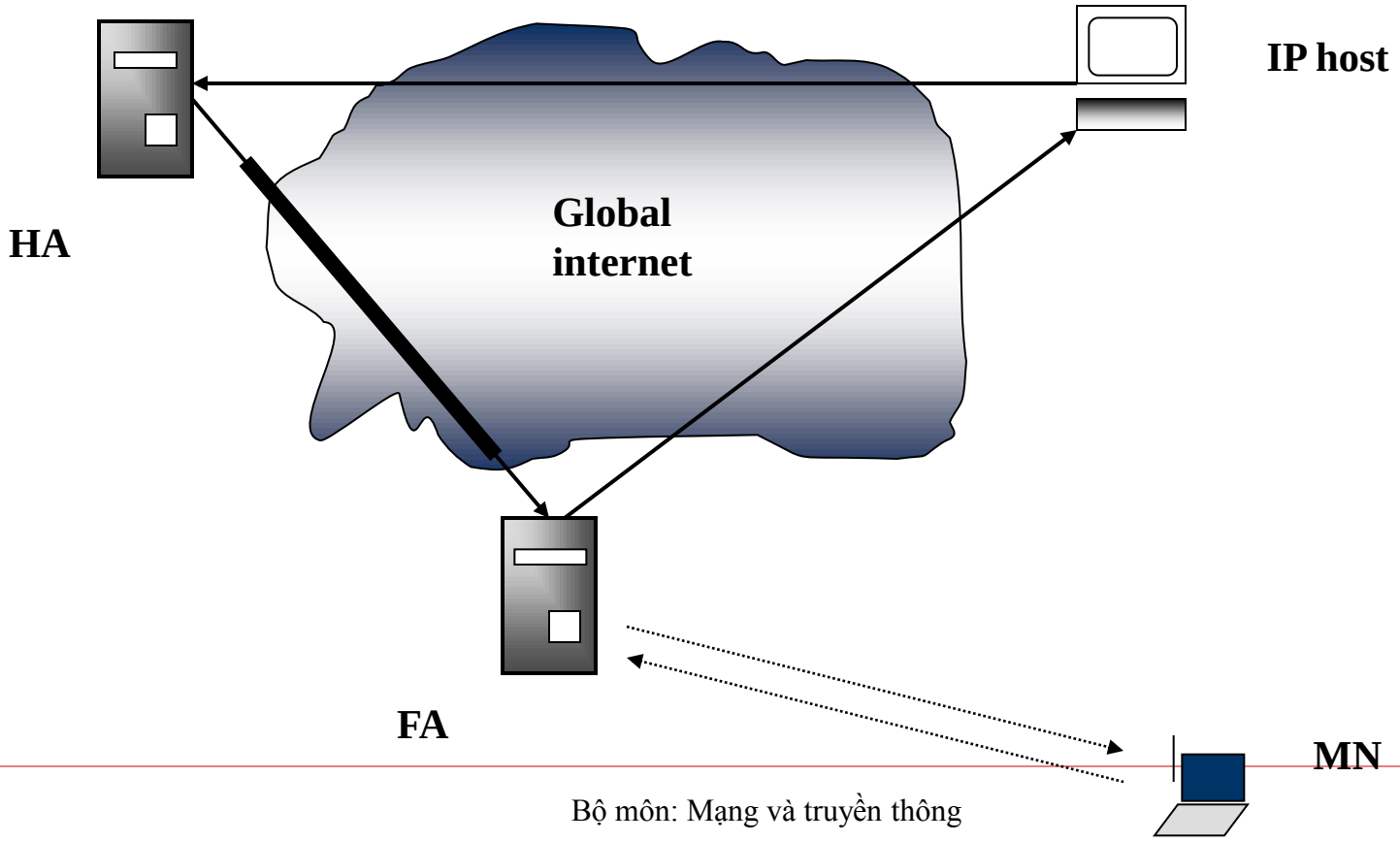
Source: *Mobile IP: Design principles and practices*. Charles E.Perkins

- **để tránh việc phải thay đổi giao thức TCP sẵn có, người ta dùng cơ chế đường ống IP (*IP tunneling*) thiết lập giữa *home agent* - HA và *care-of-address* (COA): HA chuyển các gói tin gửi cho MH qua đường hầm IP đến COA. Tại đầu kia, các gói tin sẽ được chuyển tiếp đến MH.**
- **Cơ chế IP lồng nhau (*IP within IP*) được sử dụng trong *IP tunneling*. (RFC2003)**

HA	COM	4 or 55	X	MH	?	payload
Src	Dest	Proto	Src	Dest	Proto	

Triangle routing

- **Triangle routing causes long delays in signaling and traffic.**



- **cần phải có cơ chế chứng nhận xác thực MH với HA**
  - **dùng cơ chế đánh dấu thời gian đăng ký (timestamp)**
  - **dùng các bộ phát sinh số giả ngẫu nhiên đồng bộ ở MH và HA.**

- **Tài liệu tham khảo**
  - **C. Perkins. "IP Mobility Support". IETF RFC 2002, Oct 1996.**