



# **MẠNG MÁY TÍNH**

---

## **BÀI 06: KHẢO SÁT CHI TIẾT CÁC LỚP TRONG MÔ HÌNH OSI**

**GV: Ths TRẦN VĂN THÀNH**



# Nội dung

---

- Khảo sát chi tiết lớp Datalink.
- Khảo sát chi tiết lớp Network.
- Khảo sát chi tiết lớp Transport.
- Giới thiệu mô hình Firewall.



# Khảo sát chi tiết lớp Datalink

---

- Chia làm hai tầng con: LLC, và MAC.
- Lớp 2 hỗ trợ lớp 1:
  - Lớp 1 không thể giao tiếp được với các lớp trên -> lớp 2 sử dụng tầng LLC để giao tiếp
  - Lớp 1 không thể xác định các máy tính -> lớp 2 xác định máy tính dựa vào địa chỉ MAC
  - Lớp 1 chỉ có thể mô tả 1 chuỗi bit liên tục -> lớp 2 tổ chức, phân chia thành từng nhóm bit có ý nghĩa
  - Lớp 1 không thể nào quyết định máy tính nào được quyền gửi thông tin lên môi trường nếu cùng một lúc có nhiều máy tính muốn gửi thông tin -> Lớp 2 sử dụng hệ thống hỗ trợ Media Access Control (MAC).



## Các phương pháp truy cập trên môi trường truyền dẫn

---

- Cảm sóng đa truy có phát hiện đụng độ (CSMA/CD)
- Chuyển thẻ bài (Token-passing)

# Các phương pháp truy cập

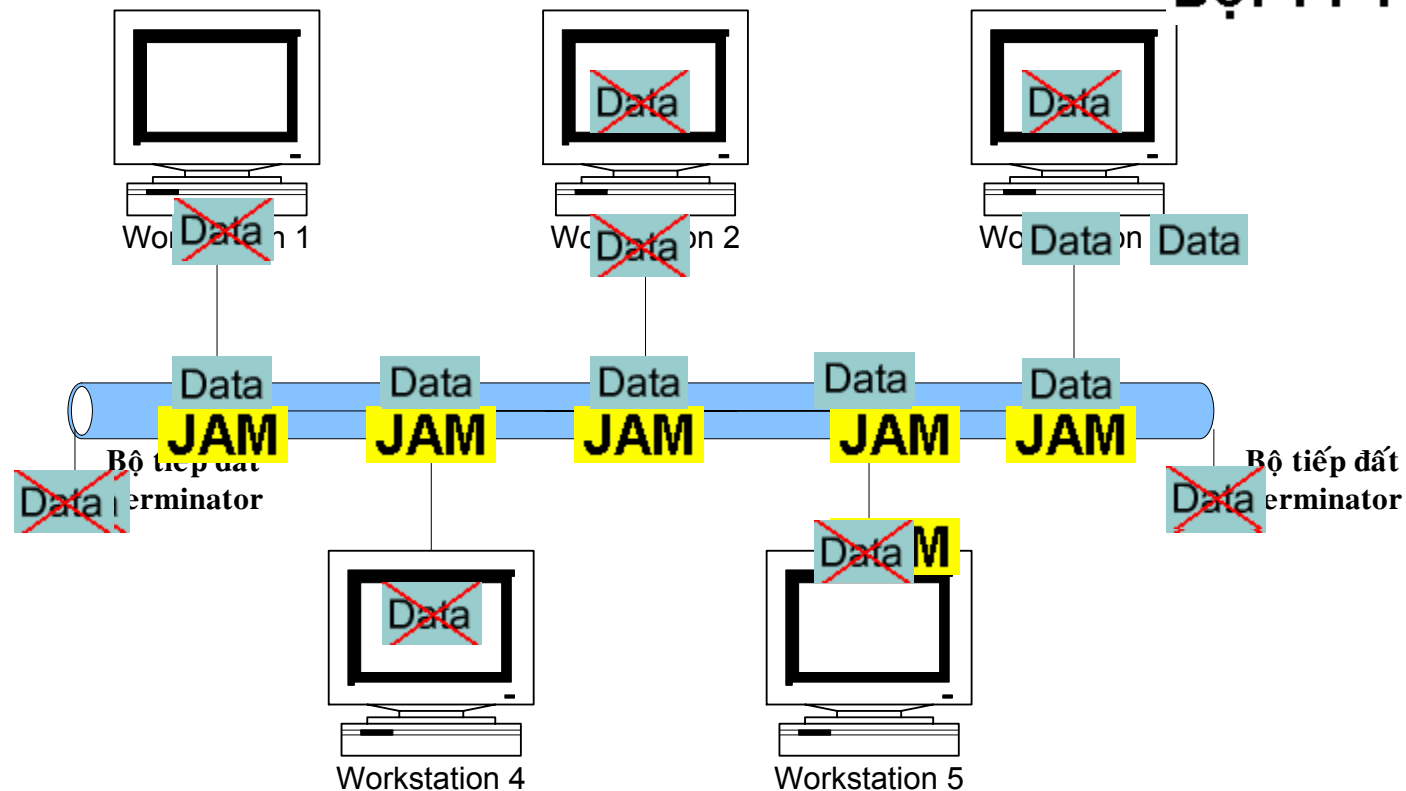
## ■ Kỹ thuật CSMA/CD

- Workstation 1 gửi đến workstation 5

- Workstation 3 gửi đến workstation 4

Đợi T ms

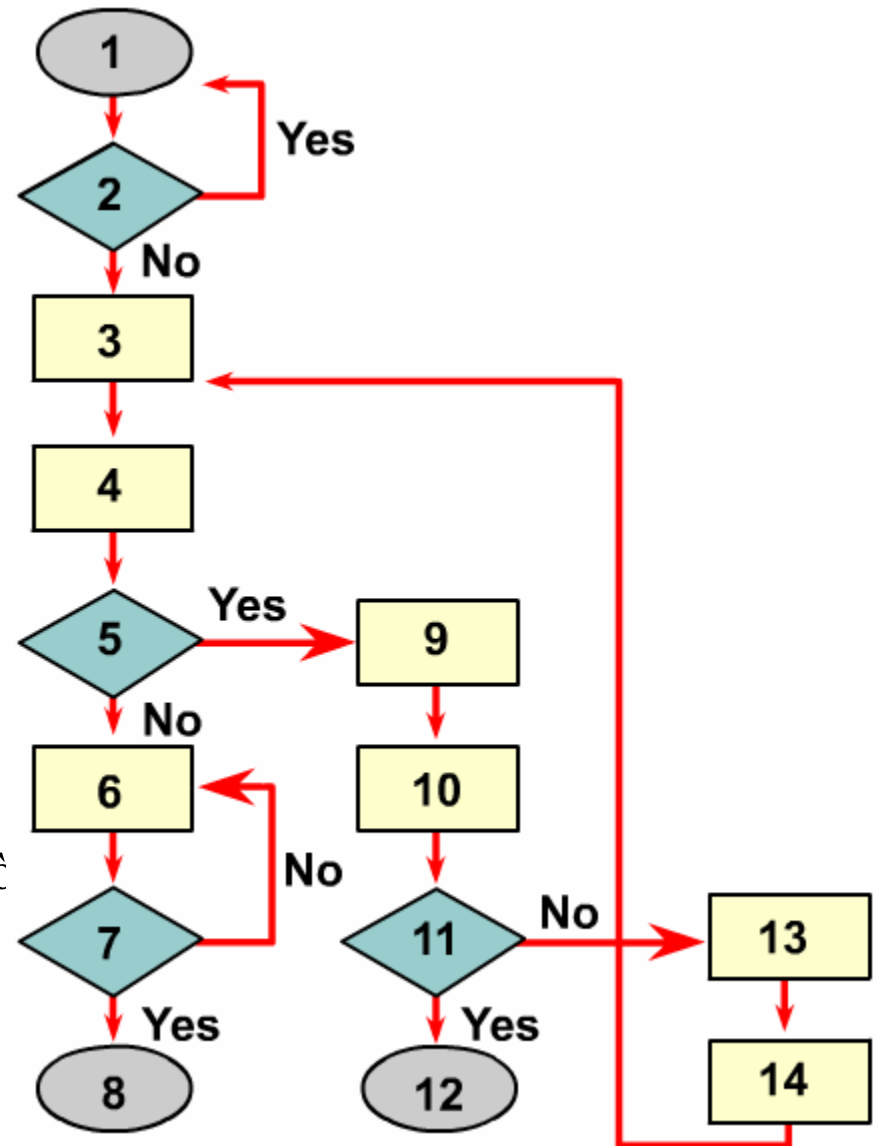
Đợi T1-T ms



# Các phương pháp truy cập

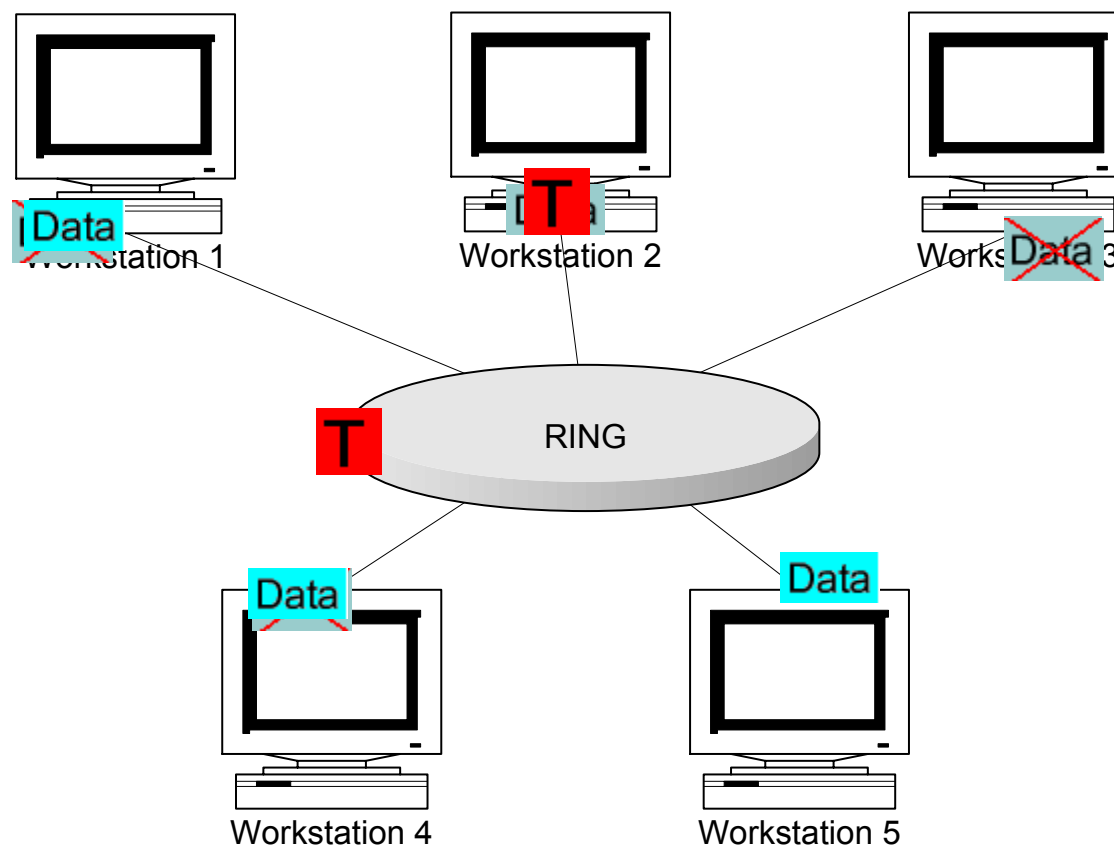
## ■ Kỹ thuật CSMA/CD

- Host muốn gửi dữ liệu.
- Tín hiệu trên đường truyền ?
- Chuẩn bị frame để gửi.
- Gửi Frame đi.
- Kiểm tra collision ?
- Tiếp tục gửi frame.
- Đã gửi xong dữ liệu ?
- Kết thúc gửi dữ liệu.
- Phát sinh tín hiệu tắt nghẽn (JAM)
- Số lần đã gửi tăng lên 1
- Số lần đã gửi quá lớn ?
- Hủy bỏ việc truyền dữ liệu
- Dùng thuật toán backoff để tính toán thời chờ (t ms)
- Chờ t ms, sau đó gửi lại



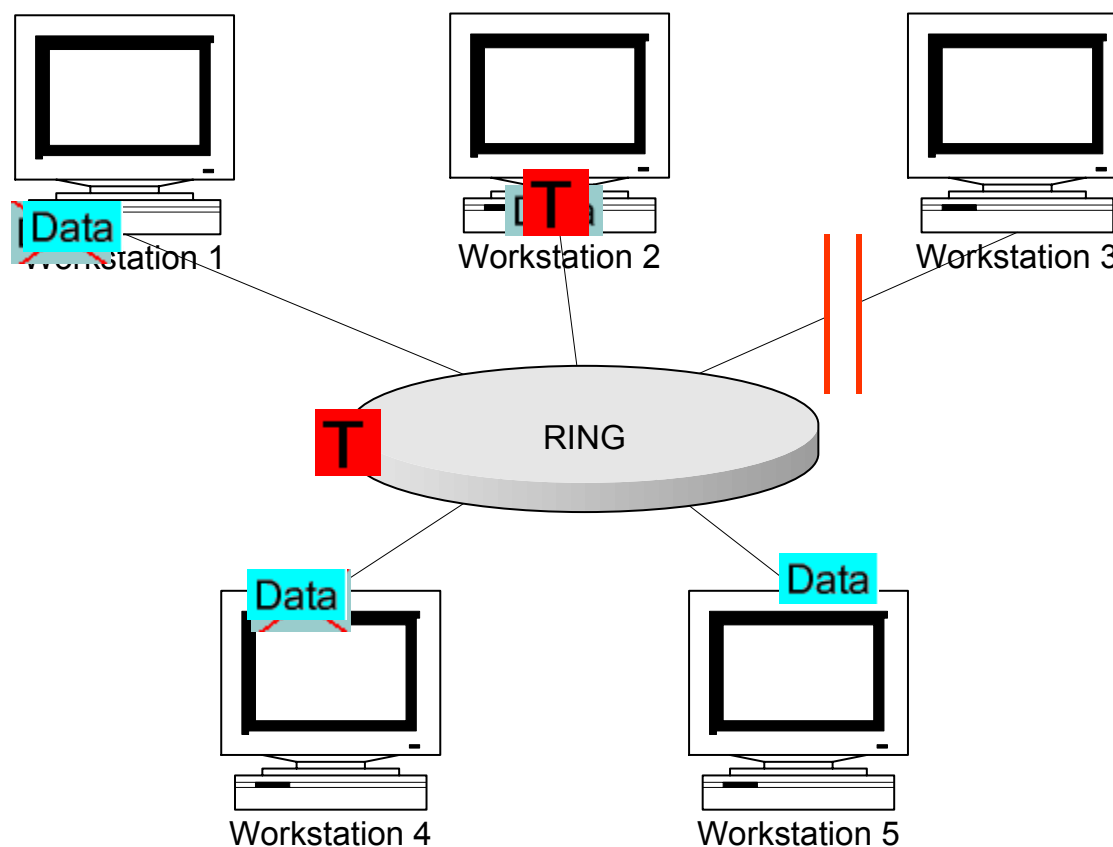
# Các phương pháp truy cập

- Kỹ thuật Token-Ring
  - Đi từ Workstation 2 đến Workstation 5



# Các phương pháp truy cập

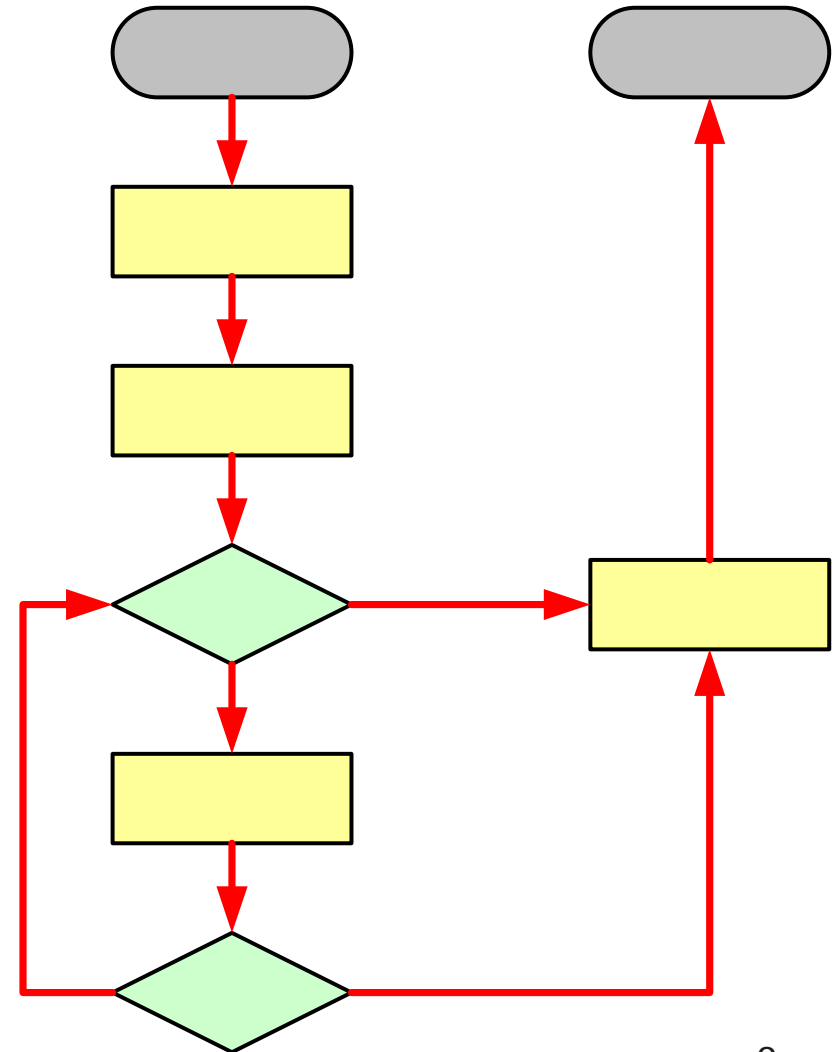
- Kỹ thuật Token-Ring (khi có sự cố)





# Các phương pháp truy cập

- Kỹ thuật Token Ring
  - Bắt đầu
  - Chờ thẻ bài (Token)
  - Giữ thẻ bài
  - Có muốn gửi dữ liệu ?
  - Gửi dữ liệu đi
  - Đã hết thời gian cho phép ?
  - Giải phóng thẻ bài
  - Kết thúc





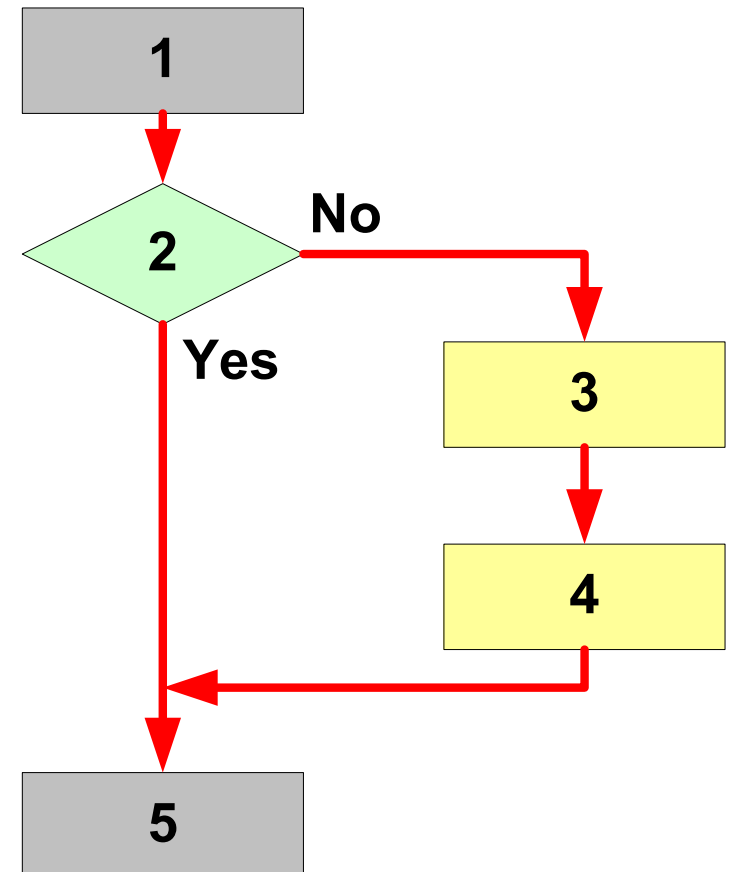
# Khảo sát chi tiết lớp Network

---

- Định tuyến (Routing) là quá trình chuyển thông tin qua mạng từ nơi gửi tới nơi nhận. Định tuyến có hai thành phần là chuyển mạch (switching) và chọn đường (path determination).
- Dựa vào bảng định tuyến (routing table), thiết bị sẽ quyết định địa chỉ kế tiếp cần đi qua để dữ liệu có thể đến được đích.
- Cung cấp địa chỉ logical address (IP address)
- Cung cấp các giao thức IP, IPX,...

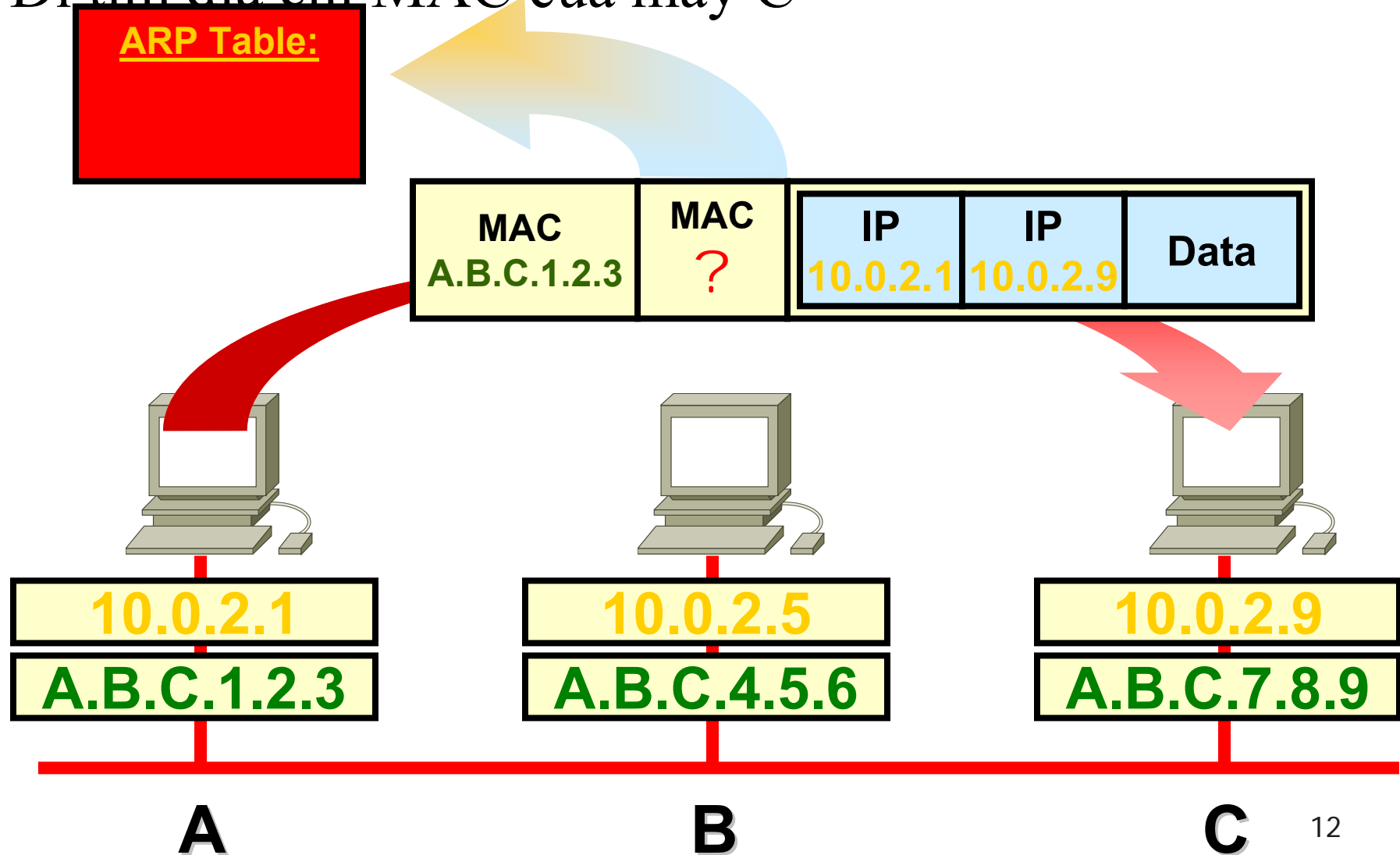
# Khảo sát chi tiết lớp Network

- Quá trình xử lý ARP
  - Chuẩn bị gói dữ liệu
  - Kiểm tra địa chỉ MAC có trong ARP table ?
  - Gửi gói tin ARP request
  - Nhận gói tin ARP reply
  - Lấy thông tin địa chỉ MAC để gửi gói tin.



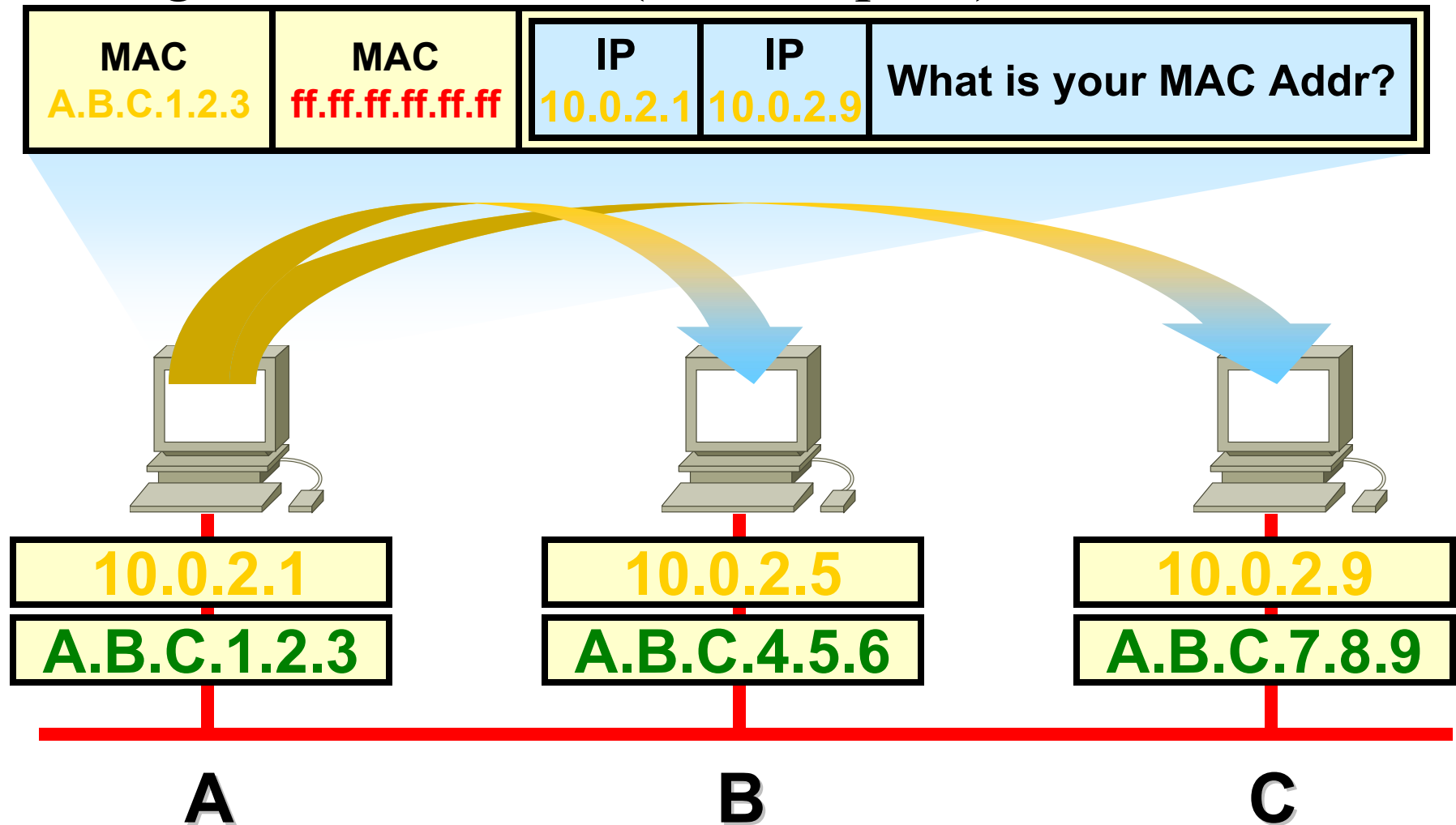
# Khảo sát chi tiết lớp Network

- Đi tìm địa chỉ MAC của máy C



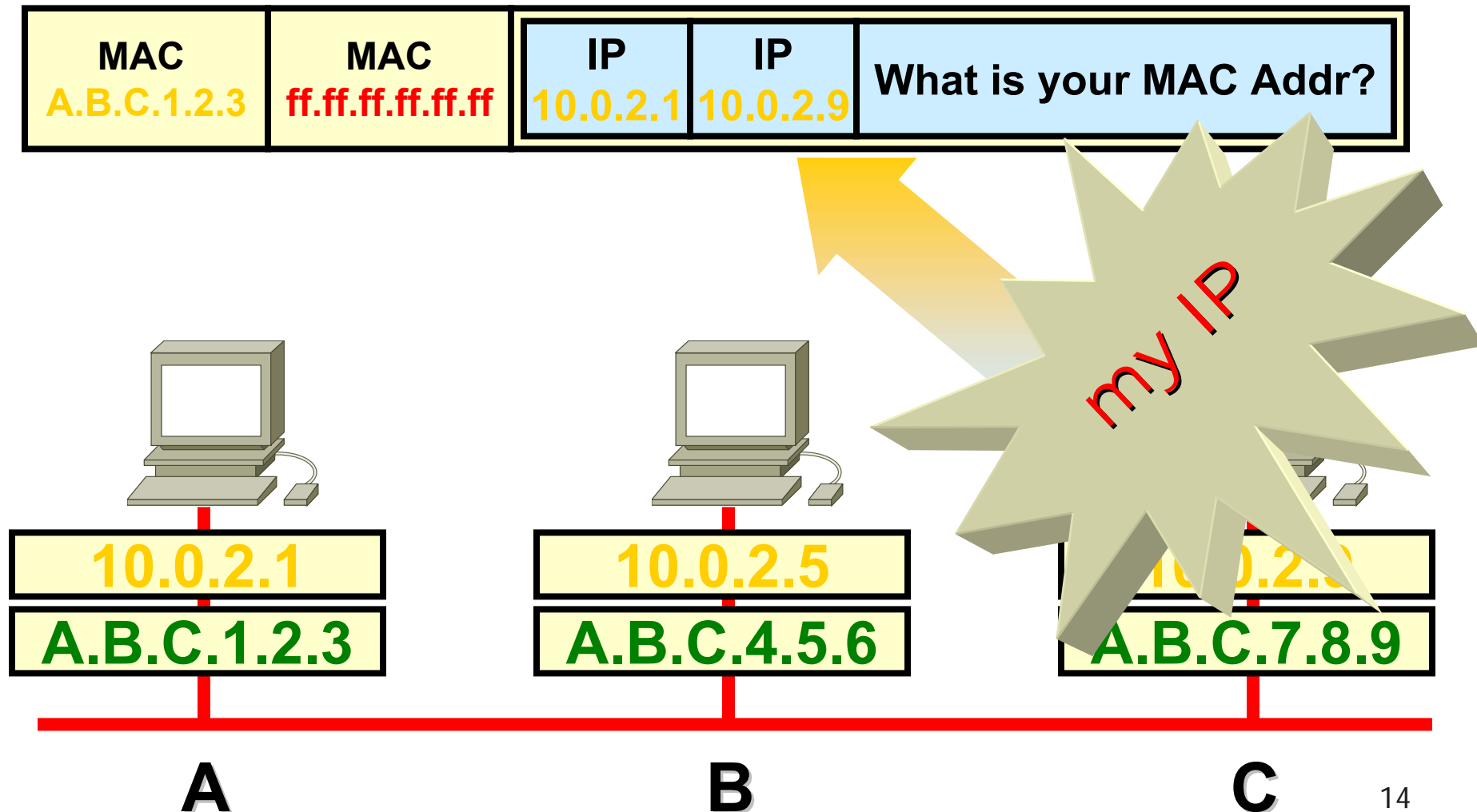
# Khảo sát chi tiết lớp Network

- Gửi gói tin Broadcast (ARP request) đi



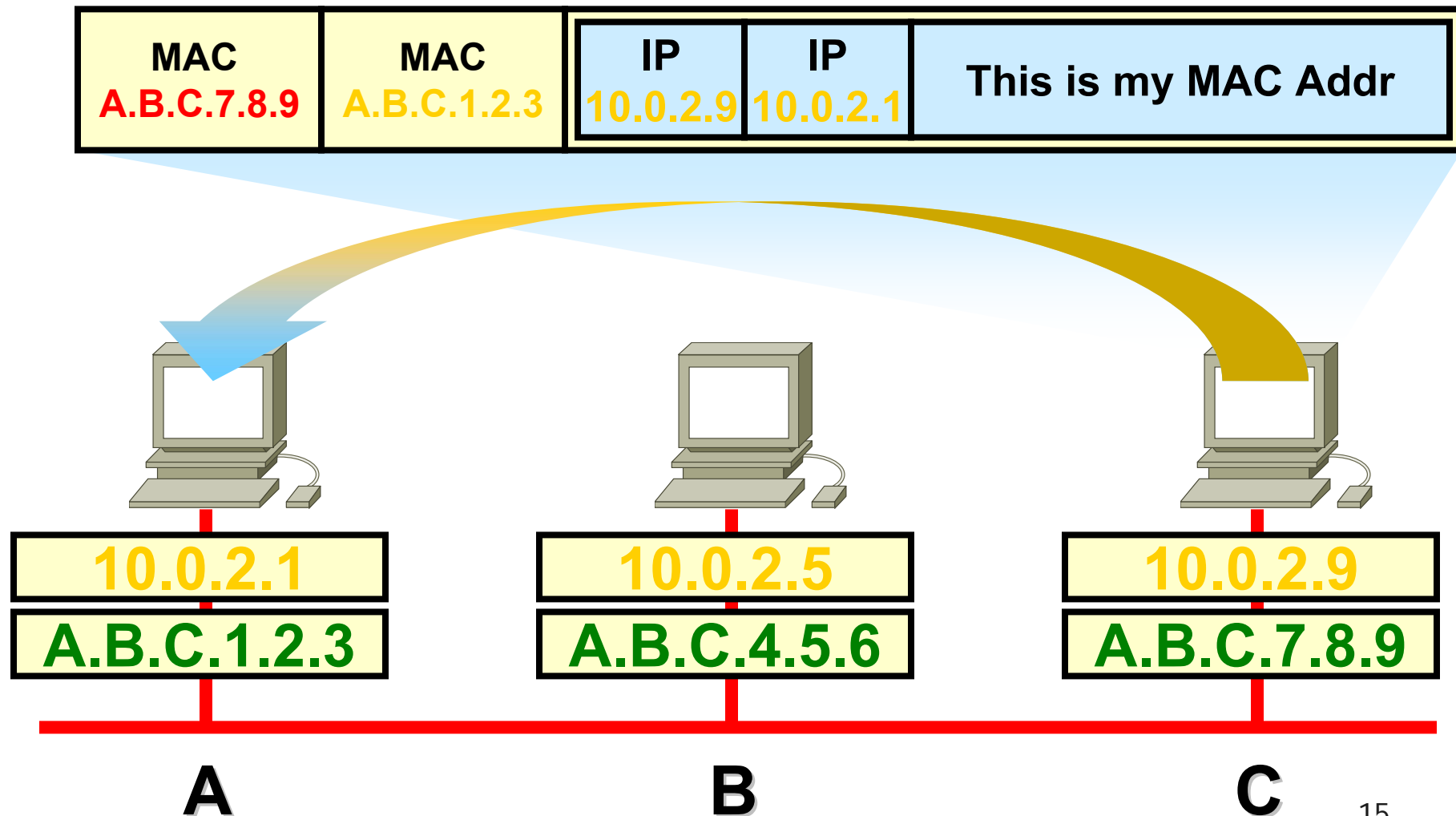
# Khảo sát chi tiết lớp Network

- Máy C nhận được gói tin Broadcast



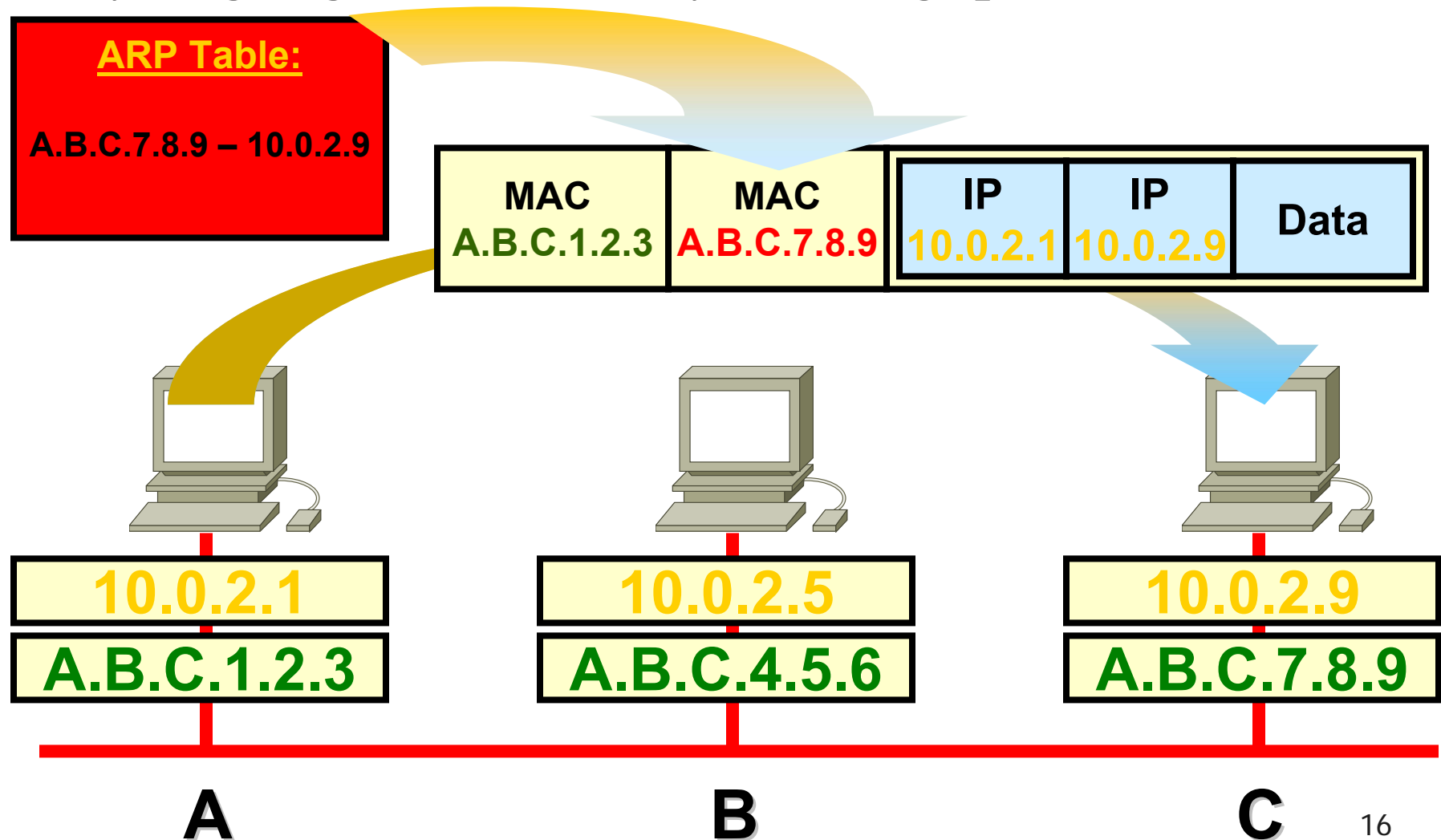
# Khảo sát chi tiết lớp Network

- Máy C trả lời bằng gói tin ARP reply



# Khảo sát chi tiết lớp Network

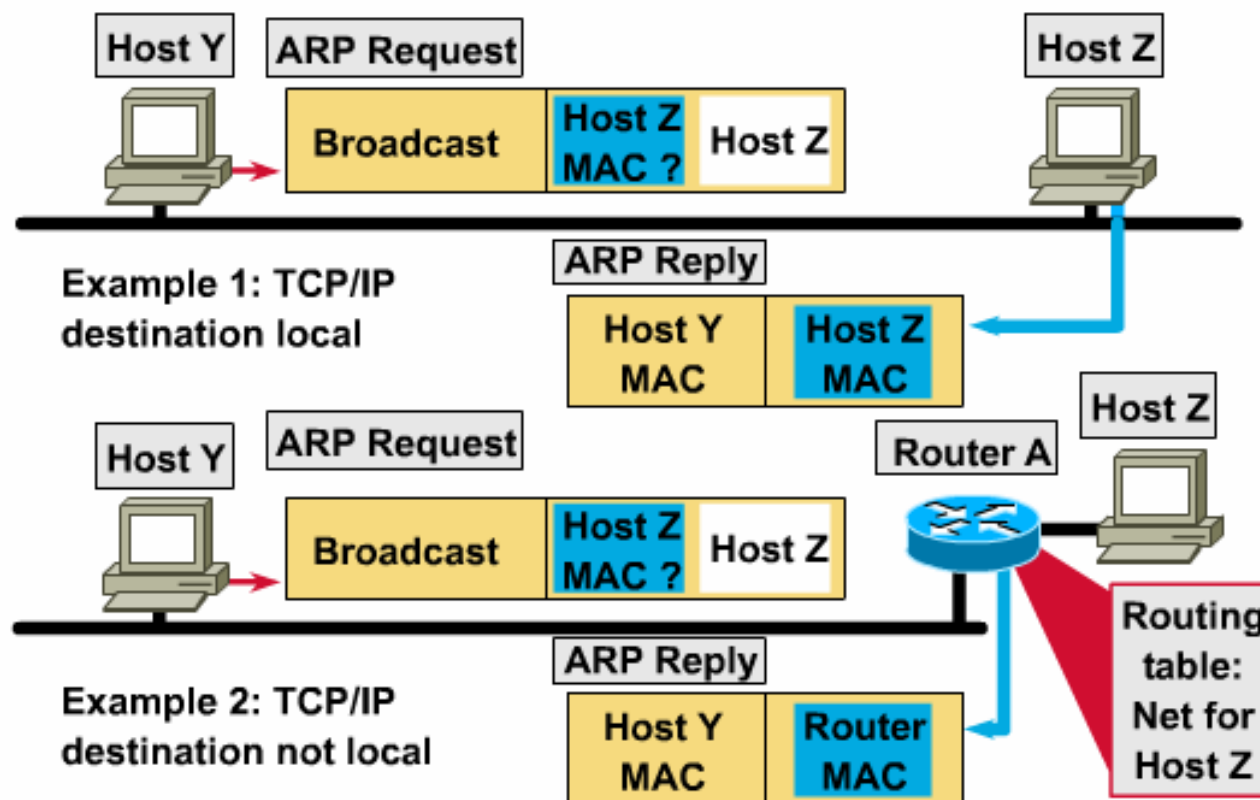
- Máy A gửi gói tin đến máy C thông qua địa chỉ MAC





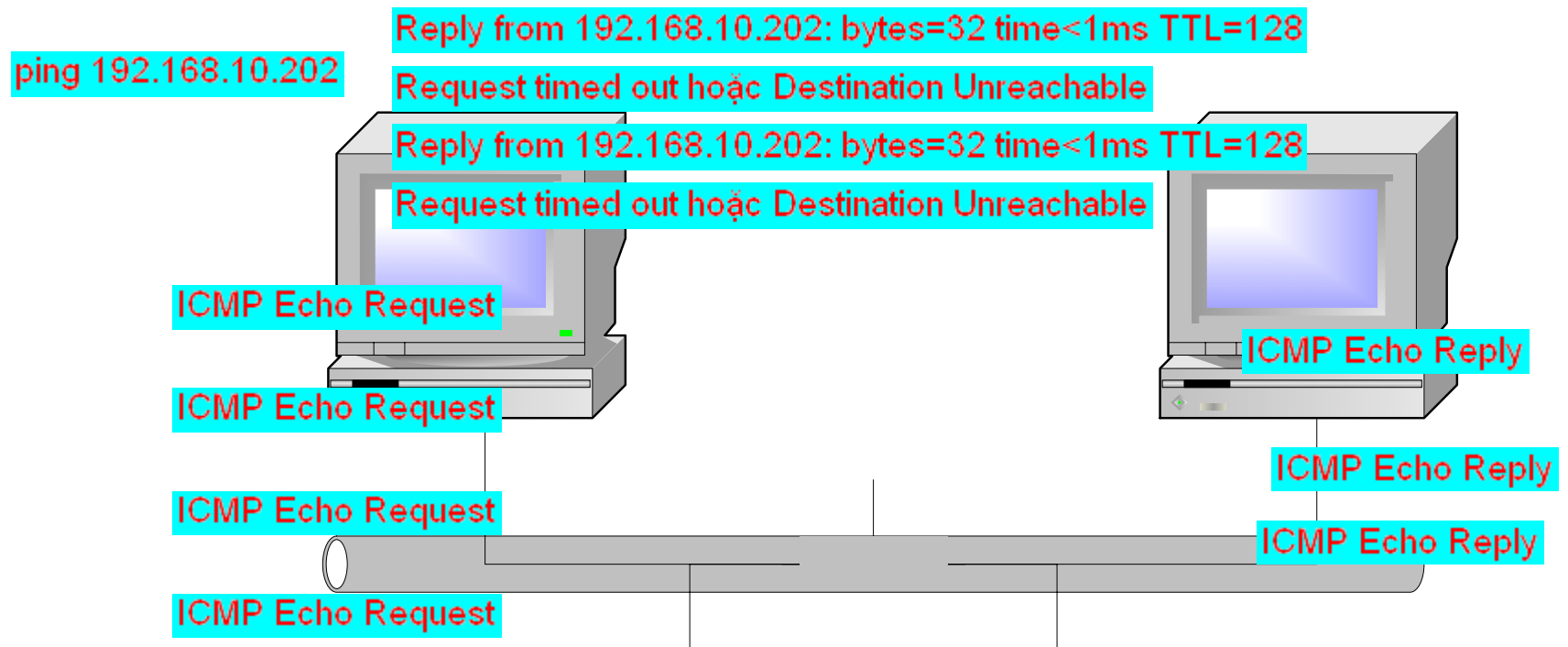
# Khảo sát chi tiết lớp Network

- Quá trình địa chỉ MAC trong 2 trường hợp
  - Cùng đường mạng
  - Khác đường mạng



# Khảo sát chi tiết lớp Network

- Quá trình thực hiện lệnh Ping





# Khảo sát chi tiết lớp Transport

---

- Hỗ trợ cho việc phân mảnh và tập hợp dữ liệu thành các data stream.
  - Reliability (tin cậy)
  - Flow Control
- Hai protocol ở lớp transport layer là TCP và UDP:
- Với TCP thì quá trình thực hiện qua ba bước sau:
  - Thiết lập kết nối (connection establishment).
  - Truyền dữ liệu (data transfer).
  - Kết thúc kết nối (connection termination).
- UDP là nghi thức không tin cậy, nó không đảm bảo dữ liệu đến đích có bị mất hay không, đúng thứ tự hay không. UDP nhờ các nghi thức ở lớp trên đảm nhận chức năng này.



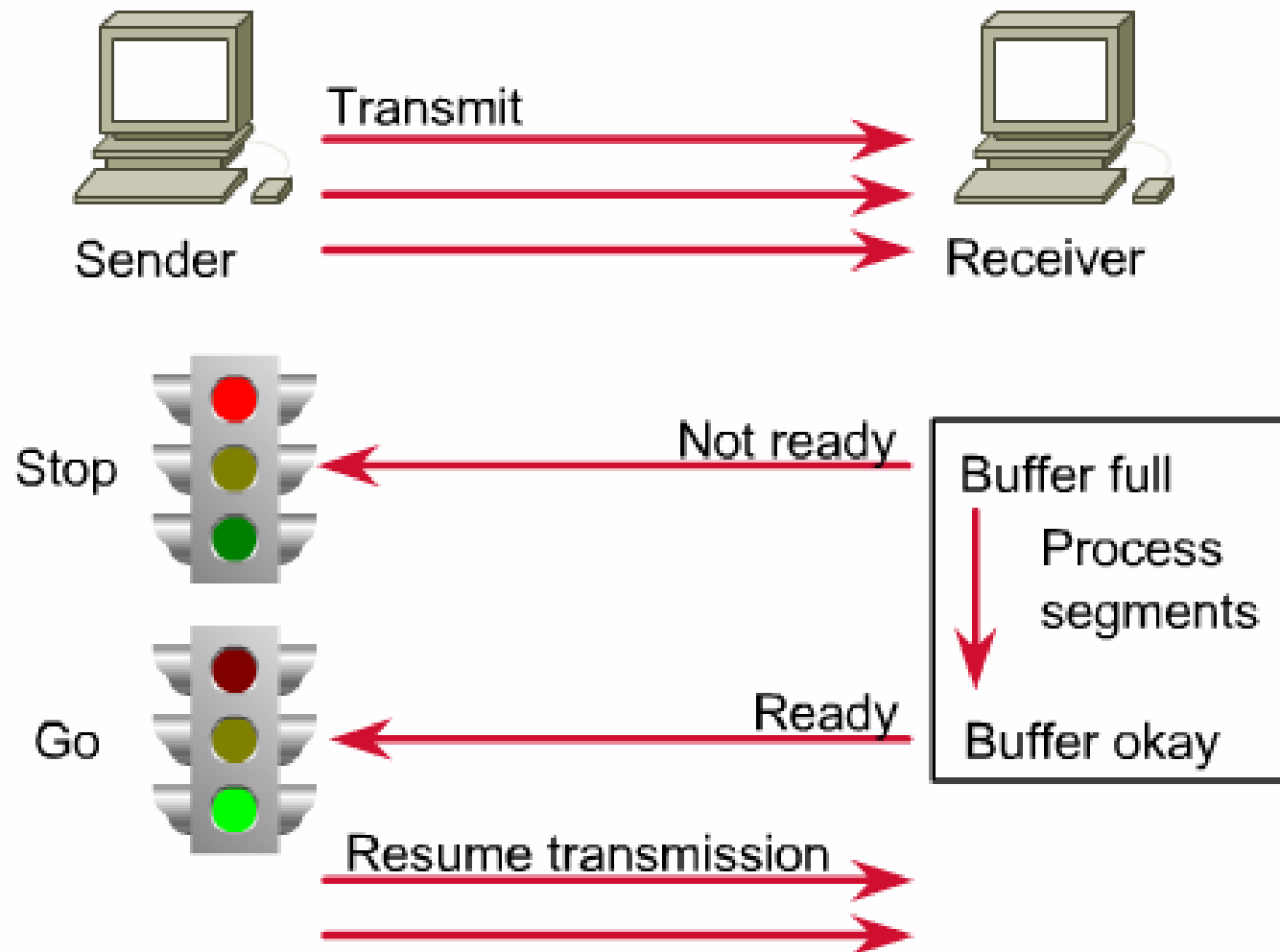
# Khảo sát chi tiết lớp Transport

---

- TCP hoặc UDP dùng port hoặc socket, nó là con số mà thông qua đó thông tin được truyền lên các lớp cao hơn. Các port có giá trị nhỏ hơn 1024 được dùng làm các port chuẩn. Các ứng dụng riêng nên dùng port có giá trị lớn hơn 1024.
- Giá trị port được chứa trong phần địa chỉ nguồn và đích của mỗi segment TCP.

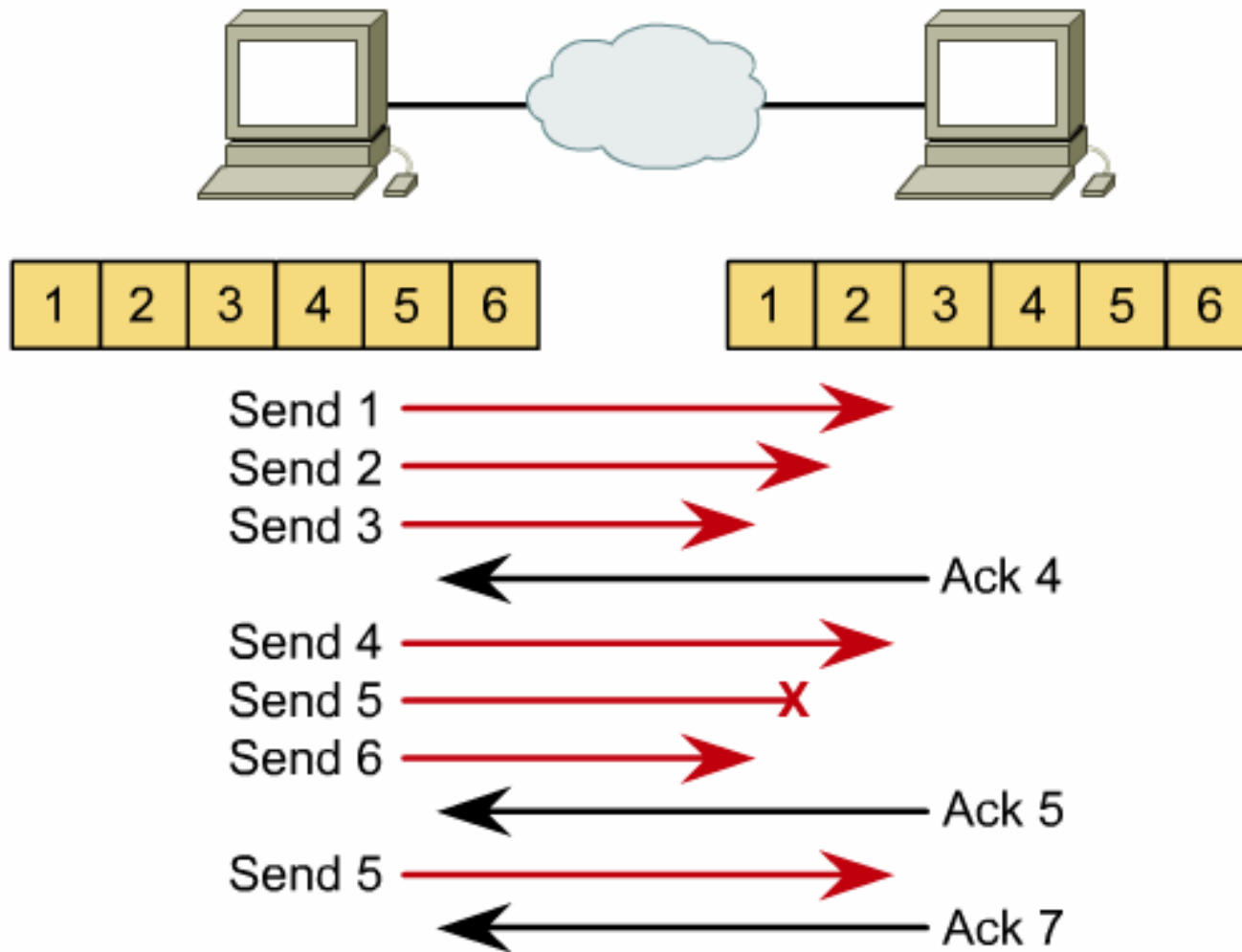
# Khảo sát chi tiết lớp Transport

## Flow Control



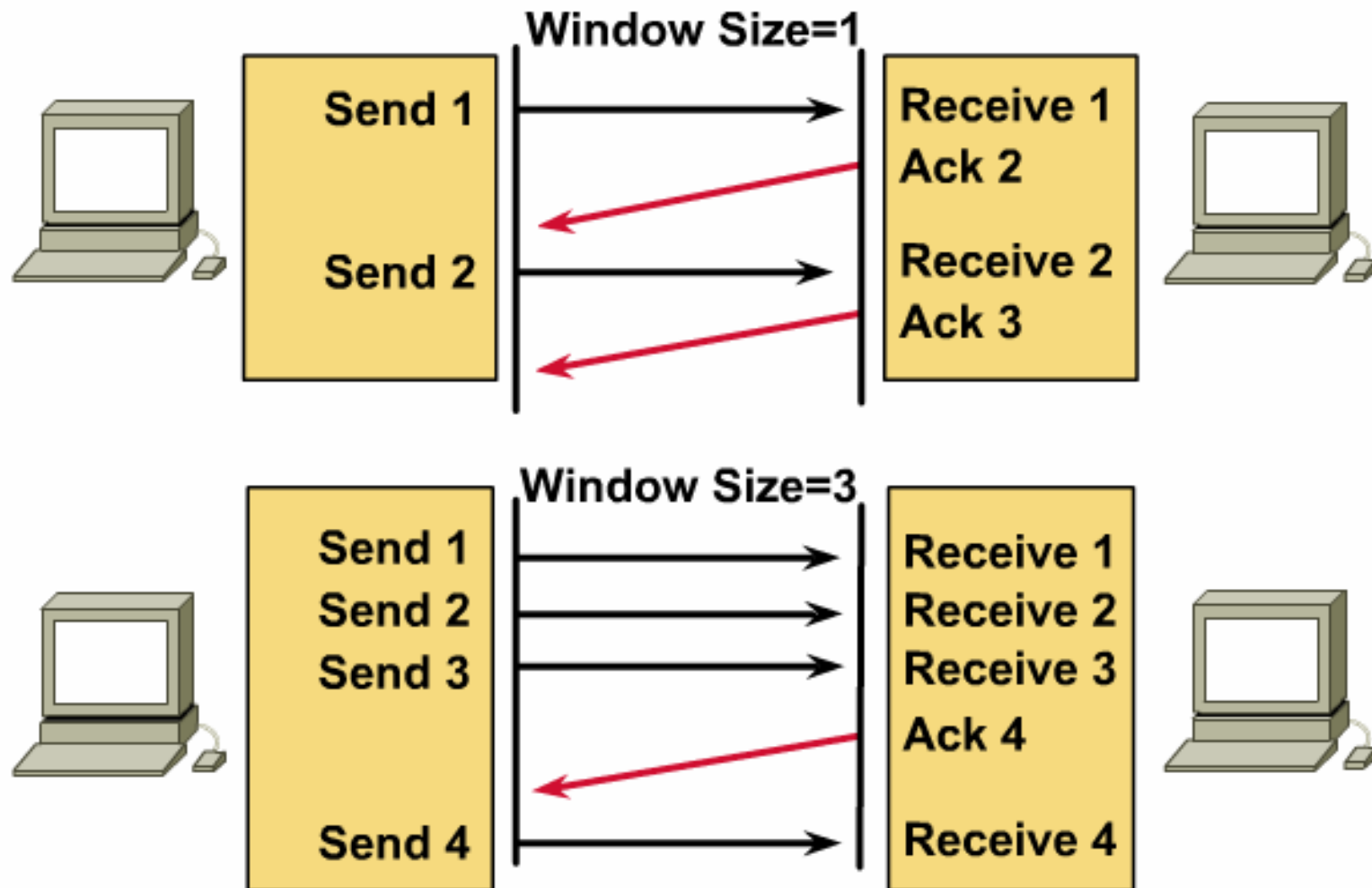
# Khảo sát chi tiết lớp Transport

## Acknowledgment

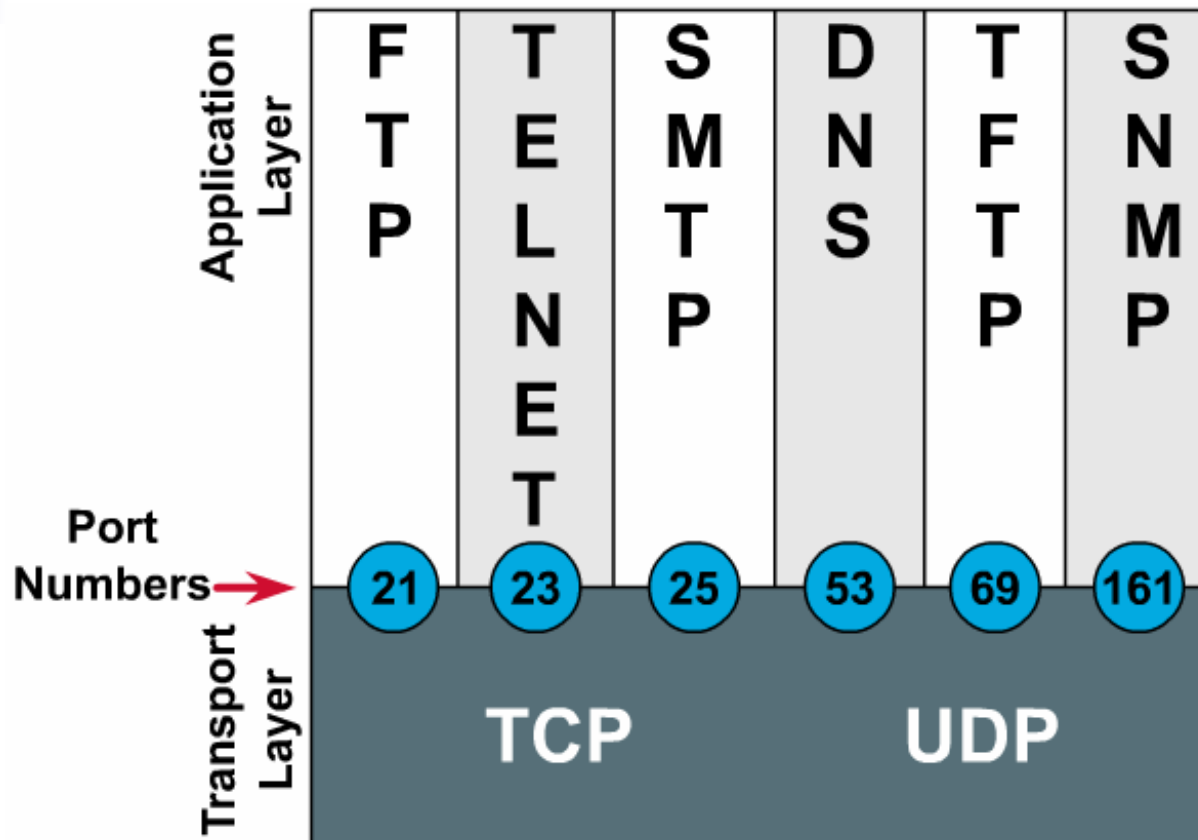


# Khảo sát chi tiết lớp Transport

## Windowing



# Khảo sát chi tiết lớp Transport



- Cả TCP và UDP đều sử dụng Port (hoặc socket) để gửi thông tin đến các tầng trên





# Khảo sát chi tiết lớp Transport

---

- Port có giá trị từ: **0 – 65535**.
  - Port dưới **1023**: dành cho các ứng dụng phổ biến, gọi là các Port chuẩn.
  - Port từ **1024** : các Port chưa sử dụng.
- Mỗi ứng dụng có Port riêng. Ví dụ dịch vụ FTP có Port mặc định là 20 và 21, trong khi dịch vụ Web lại có Port mặc định là 80. Khi máy tính khác muốn sử dụng dịch vụ Web thì phải kết nối vào Port 80.



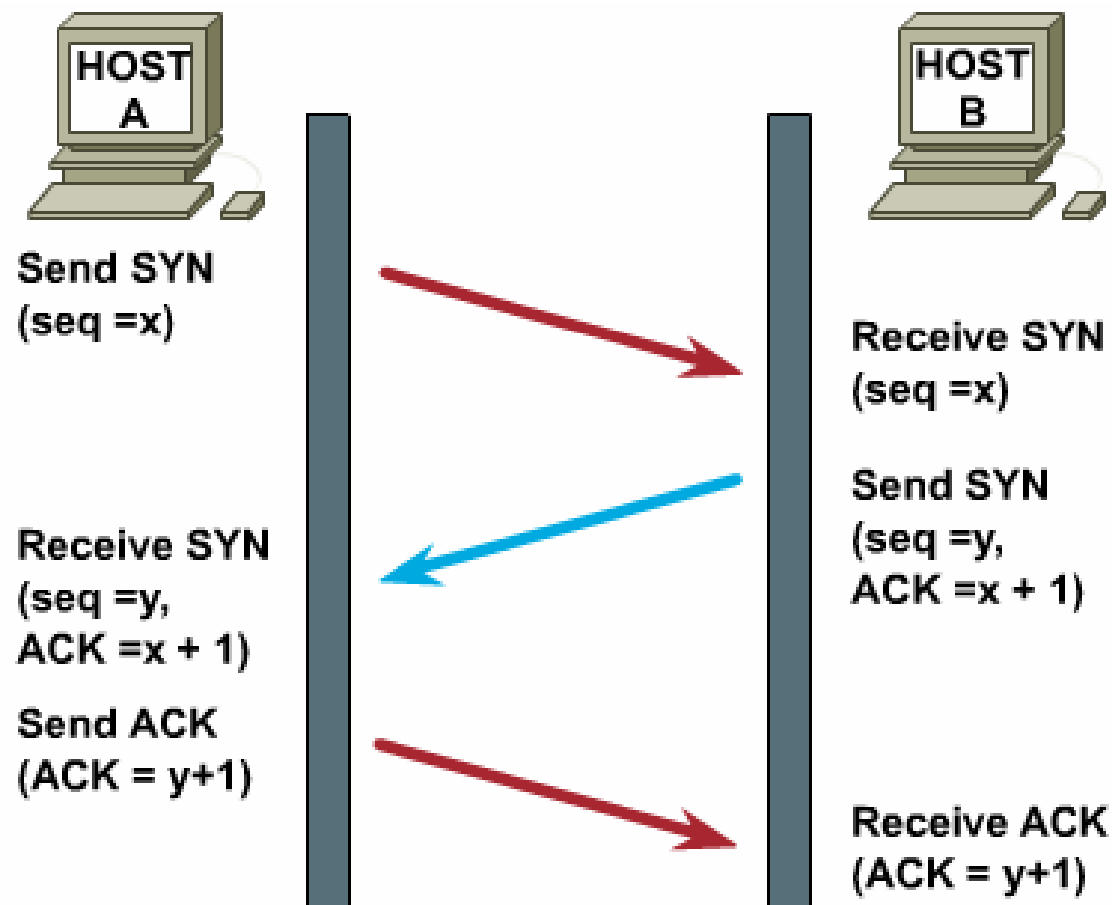
# Khảo sát chi tiết lớp Transport

---

- Đặc điểm của giao thức TCP:
  - Connection-oriented (hướng kết nối)
  - Reliable (tin cậy)
  - Có thể gửi lại các thông tin đã gửi nhưng máy nhận chưa nhận được.
  - Sắp xếp lại các gói tin nhận được theo đúng trật tự như bên gửi.

# Khảo sát chi tiết lớp Transport

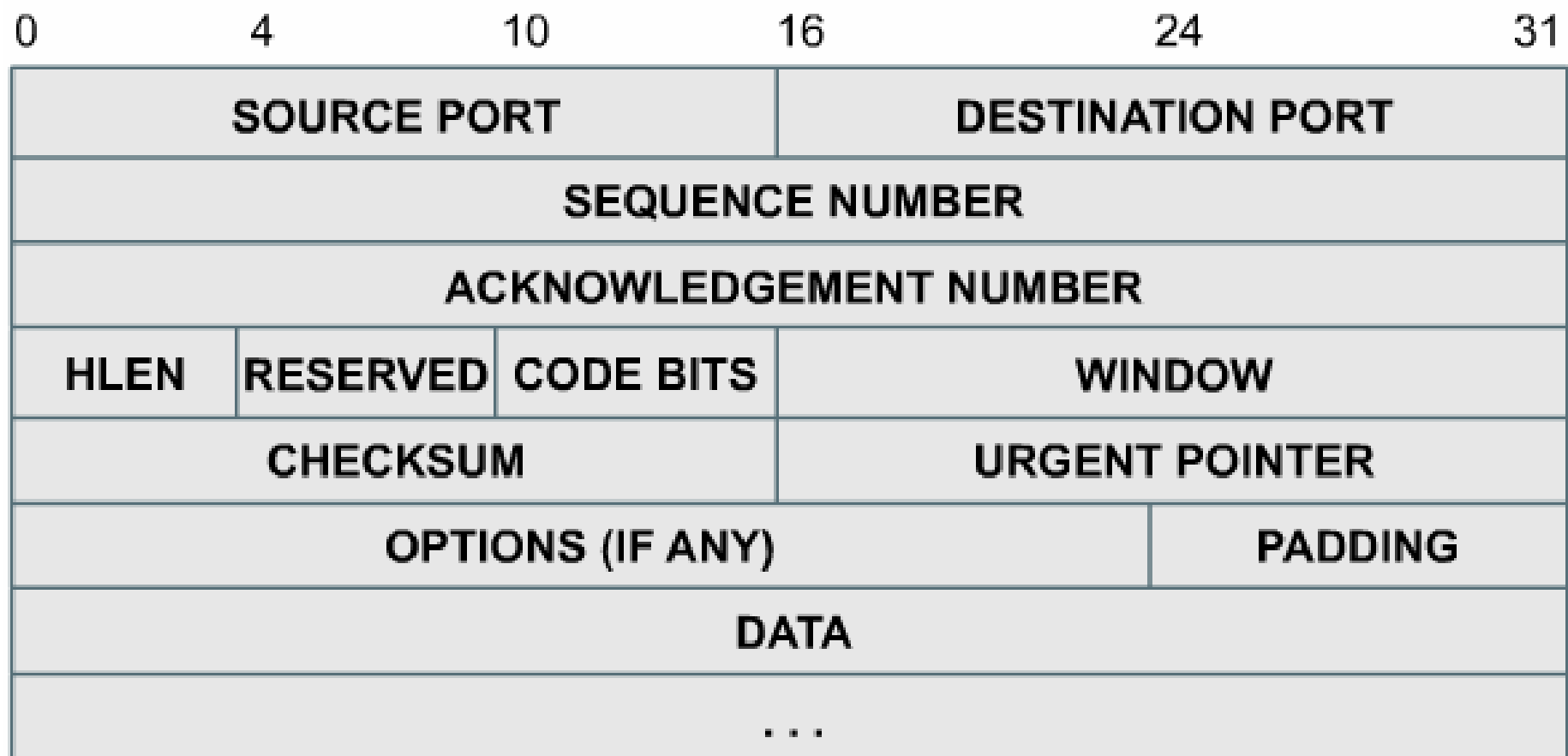
- Giao thức TCP - Cách thức bắt tay 3 lần





# Khảo sát chi tiết lớp Transport

- Định dạng của gói tin TCP





# Khảo sát chi tiết lớp Transport

---

- Một số trường cần quan tâm trong cấu trúc gói tin TCP:
  - Source Port: Port nguồn (Port trên máy gửi)
  - Destination Port: Port đích (Port trên máy nhận)
  - Sequence Number: Là số tuần tự của octet dữ liệu đầu tiên trong segment (trừ khi cờ SYN được bật)
  - Acknowledgment number: Chứa giá trị của gói tin kế tiếp mà bên nhận đang chờ.
  - Window: Chỉ ra số lượng gói tin tối đa mà bên nhận có thể nhận cùng một thời điểm



# Khảo sát chi tiết lớp Transport

---

- Một số trường cần quan tâm trong cấu trúc gói tin TCP (tt):
  - Control bits: (8 bit)
    - **URG**: Urgent Pointer field significant
    - **ACK**: Acknowledgment field significant
    - **EOL**: End of Letter
    - **RST**: Reset the connection
    - **SYN**: Synchronize sequence numbers
    - **FIN** : No more data from sender
  - Checksum: Dùng để kiểm lỗi ở phần header và phần dữ liệu
  - Data: dữ liệu được chứa trong phần này



# Khảo sát chi tiết lớp Transport

---

- UDP chuyển dữ liệu theo hình thức không tin cậy.  
Đặc điểm của UDP:
  - Connectionless (phi kết nối).
  - Unreliable (không tin cậy)
  - Không đảm bảo việc phân phát các gói tin đến đúng đích (unreliable).
  - Không sắp xếp thứ tự của các gói tin sau khi nhận được.



# Khảo sát chi tiết lớp Transport

---

- Một số giao thức (protocols) sử dụng UDP là:
  - TFTP (Trivial File Transfer Protocol)
  - SNMP (Simple Network Management Protocol)
  - DHCP (Dynamic Host Control Protocol)
  - DNS (Domain Name System)





# Khảo sát chi tiết lớp Transport

- Định dạng gói tin UDP

# of Bits	16	16	16	16	
	<b>Source Port</b>	<b>Destination Port</b>	<b>Length</b>	<b>Check Sum</b>	<b>Data...</b>

- UDP là giao thức đơn giản để chuyển dữ liệu, mà không cần xác nhận và đảm bảo việc phân phối.



# Giới thiệu mô hình Firewall

---

- Giới thiệu về Firewall
- Dual-homed host
- Screened Host
- Screened Subnet



# Giới thiệu về Firewall

---

- Firewall hay còn gọi là bức tường lửa được hiểu như là một hệ thống máy tính và thiết bị mạng giúp ta có thể bảo mật, giám sát các truy xuất từ bên trong ra ngoài và ngược lại. Từ đó ta có thể phòng chống các truy cập bất hợp pháp.



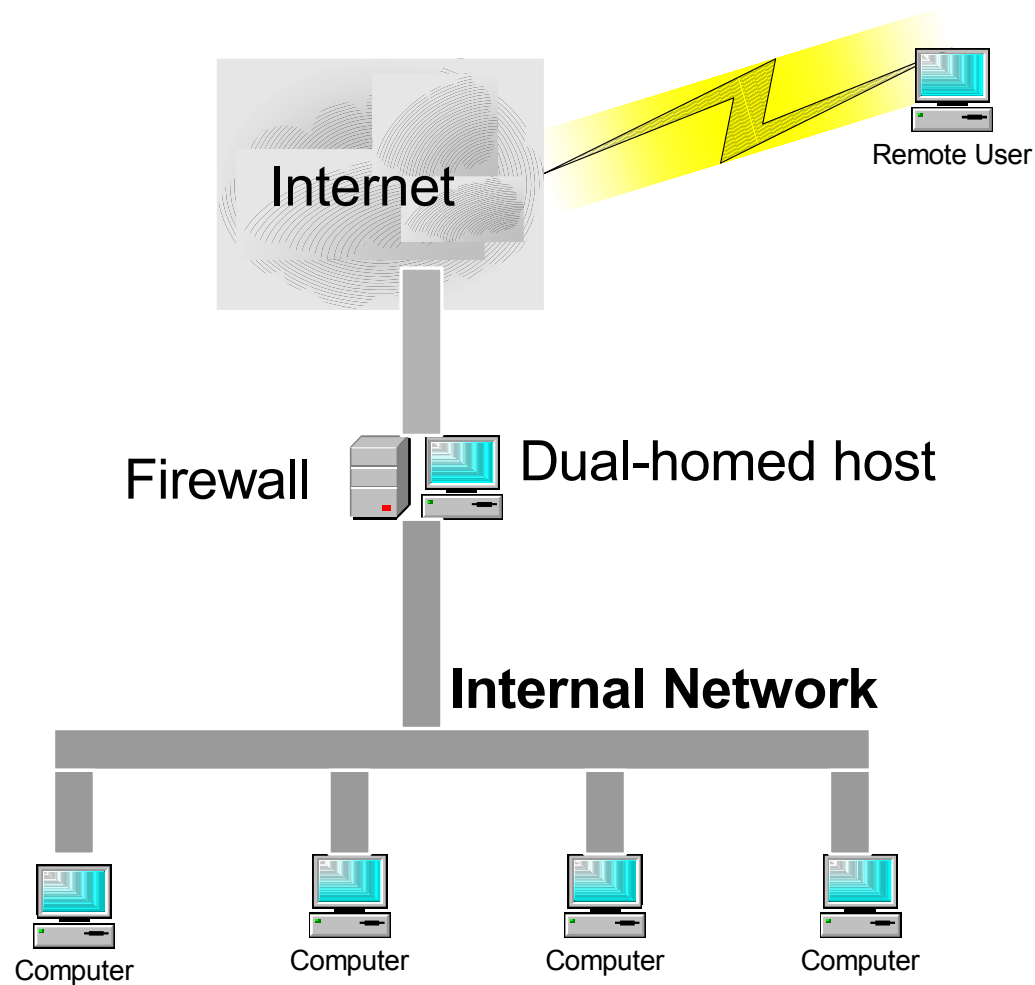
## Mô hình Dual-homed host

---

- Firewall theo kiến trúc Dual-homed host được xây dựng dựa trên máy tính dual-homed host.
- Một máy tính được gọi là dual-homed host nếu nó có ít nhất hai network interfaces. Một interface giao tiếp với bên trong (LAN), một interface giao tiếp với bên ngoài (WAN).
- Dual-homed host chỉ có thể cung cấp các dịch vụ bằng cách ủy quyền (proxy) hoặc cho phép users đăng nhập trực tiếp vào dual-homed host. Mọi giao tiếp trực tiếp giữa một host trong mạng nội bộ và một host bên ngoài đều bị cấm.

# Mô hình Dual-homed host

- Mô hình





## Mô hình Screened Host

---

- Screened Host có cấu trúc gần giống với cấu trúc Dual-homed host. Kiến trúc này cung cấp các dịch vụ từ một host bên trong mạng nội bộ, dùng một Router tách rời với mạng bên ngoài. Trong kiểu kiến trúc này, bảo mật chính là phương pháp Packet Filtering (lọc gói tin).
- Bastion host được đặt bên trong mạng nội bộ. Packet Filtering được cài trên router. Theo cách này, Bastion host là hệ thống duy nhất trong mạng nội bộ mà những host trên Internet có thể kết nối tới.



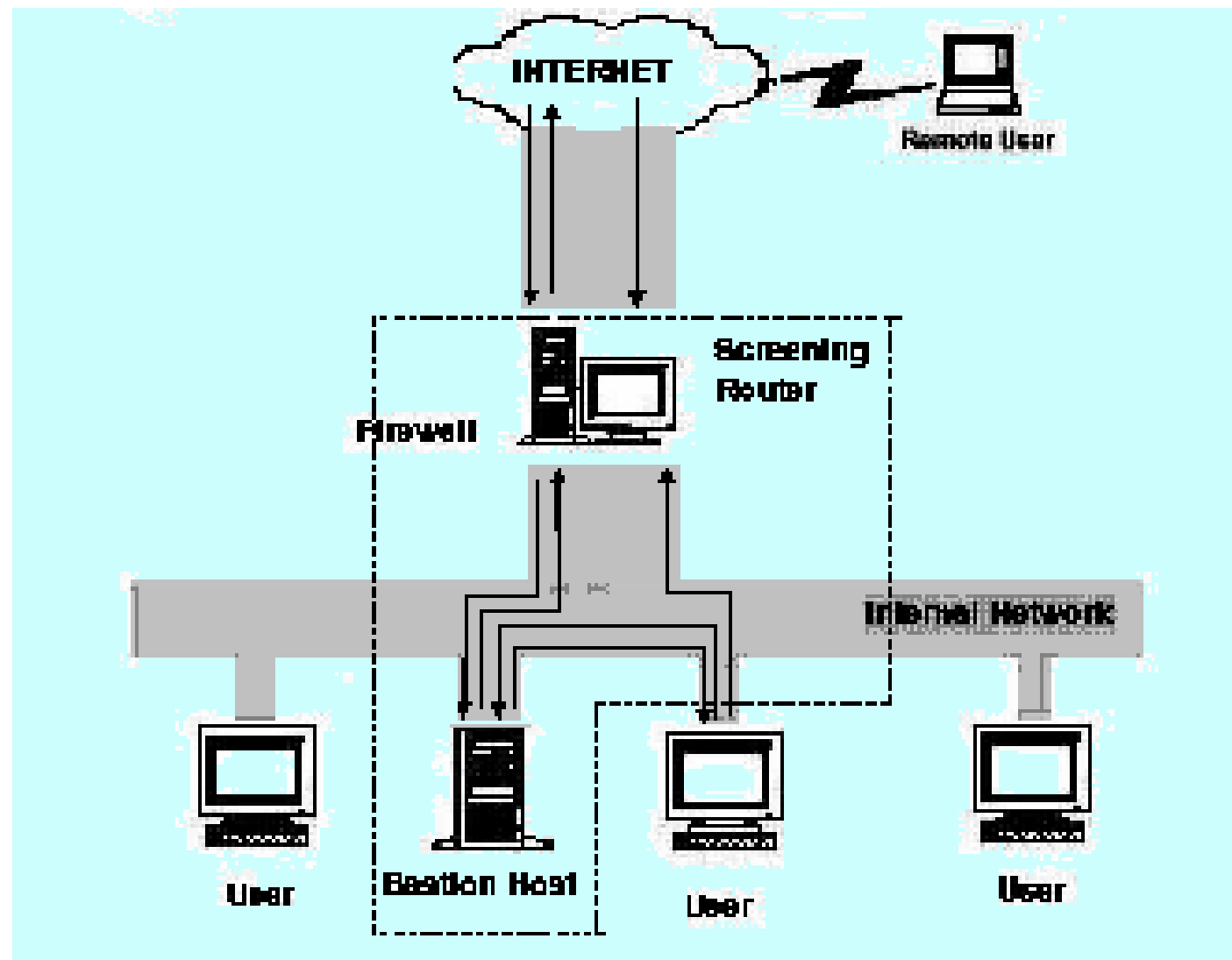
## Mô hình Screened Host

---

- Packet filtering cũng cho phép bastion host có thể mở kết nối ra bên ngoài. Cấu hình của packet filtering trên screening router như sau:
  - Cho phép tất cả các host bên trong mở kết nối tới host bên ngoài thông qua một số dịch vụ cố định.
  - Không cho phép tất cả các kết nối từ các host bên trong (cấm những host này sử dụng dịch proxy thông qua bastion host).
  - Một số dịch vụ được phép đi vào trực tiếp qua packet filtering.
  - Một số dịch vụ khác thì chỉ được phép đi vào gián tiếp qua proxy.

# Mô hình Screened Host

- Mô hình







## Screened Subnet

---

- Nhằm tăng cường khả năng bảo vệ mạng nội bộ, thực hiện chiến lược phòng thủ theo chiều sâu, tăng cường sự an toàn cho *bastion host*, *tách bastion host khỏi các host khác, phần nào tránh lây lan* một khi bastion host bị tổn thương
- Kiến trúc Screened subnet dẫn xuất từ kiến trúc screened host bằng cách thêm vào phần an toàn: mạng ngoại vi (perimeter network) nhằm cô lập mạng nội bộ ra khỏi mạng bên ngoài, tách bastion host ra khỏi các host thông thường khác.



## Screened Subnet

---

- Router ngoài (External router còn gọi là access router): nằm giữa mạng ngoại vi và mạng ngoài có chức năng bảo vệ cho mạng ngoại vi (bastion host, interior router). Nó cho phép hầu hết những gì outbound từ mạng ngoại vi.
- Interior Router (còn gọi là choke router): nằm giữa mạng ngoại vi và mạng nội bộ, nhằm bảo vệ mạng nội bộ trước khi ra ngoài và mạng ngoại vi. Nó không thực hiện hết các qui tắc packet filtering của toàn bộ firewall.

# Screened Subnet

- Mô hình

