



TRƯỜNG ĐẠI HỌC THỦY LỢI

KHOA CÔNG NGHỆ THÔNG TIN
Bộ môn: Kỹ thuật máy tính và mạng

QUẢN TRỊ MẠNG

Giảng viên: Trần Văn Hội

Email: hoitv@tlu.edu.vn

Điện thoại: 0944.736.007

GIỚI THIỆU MÔN HỌC

- ▶ **Số tín chỉ: 3 (LT: 2, TH:1)**
- ▶ **Đánh giá:** *Điểm quá trình: 40%*
(Chuyên cần, tham gia bài giảng, thực hành, kiểm tra)
Điểm thi kết thúc: 60%
- ▶ **Hình thức thi:** *Thi viết, thời gian 60-90 phút*
- ▶ **Giáo trình:**
 - Huỳnh Nguyên Chính, **Mạng máy tính nâng cao**, Nhà xuất bản Đại học Quốc gia TPHCM, 2013.
 - Chris Carthern, Will Wilson, Noel Rivera, Richard Bedwell, **Cisco Network Management Fundamentals**, Cisco Press, 2015.
 - Bài giảng Quản trị mạng

YÊU CẦU

- ❖ In bài giảng, đọc bài giảng và tài liệu trước khi lên lớp.
- ❖ Tham gia đầy đủ các buổi học.
- ❖ Chuẩn bị bút, vở, tham gia trao đổi bài trên lớp.
- ❖ Làm bài tập về nhà, bài tập lớn theo quy định.
- ❖ Chuẩn bị máy tính cài đặt phần mềm Cisco Packet Tracer 7, tìm hiểu thêm GNS3 ...

NỘI DUNG MÔN HỌC



Chương 1: Tổng quan về mạng



Chương 2: Các kỹ thuật định tuyến



Chương 3: Chuyển mạch trong mạng LAN



Chương 4: Công nghệ mạng WAN



Chương 5: Bảo mật mạng

CHƯƠNG 1: TỔNG QUAN VỀ MẠNG

1

- Giới thiệu về quản trị mạng

2

- Mô hình OSI và TCP/IP

3

- Địa chỉ IPv4

4

- Địa chỉ IPv6

5

- Chuyển đổi IPv4-IPv6

6

- Cấu hình cơ bản thiết bị mạng

GIỚI THIỆU VỀ QUẢN TRỊ MẠNG

- ❖ **Quản trị mạng** được định nghĩa là các công việc quản trị mạng lưới bao gồm cung cấp các dịch vụ hỗ trợ, đảm bảo mạng lưới hoạt động hiệu quả, đảm bảo mạng lưới cung cấp đúng chỉ tiêu định ra.
- ❖ **Quản trị mạng có thể chia làm 2 mảng chính:**
 - Quản trị hạ tầng mạng: Thiết lập, cấu hình các thiết bị mạng, vận hành hệ thống mạng, giải quyết sự cố, bảo vệ mạng trước sự tấn công.
 - Quản trị hệ thống: Quản trị hệ điều hành mạng (Win Server, Unix, Linux) để cung cấp các dịch vụ mạng, quản lý Data Center ...

GIỚI THIỆU VỀ QUẢN TRỊ MẠNG

- ❖ Công việc quản trị mạng bao gồm:
- ❖ Quản trị cấu hình, tài nguyên mạng: Bao gồm các công tác quản lý, kiểm soát cấu hình, quản lý tài nguyên cấp phát cho các đối tượng sử dụng khác nhau.
- ❖ Quản trị người dùng, dịch vụ mạng: bao gồm các công tác quản lý người sử dụng trên hệ thống và đảm bảo dịch vụ cung cấp có độ tin cậy cao, chất lượng đảm bảo theo đúng các chỉ tiêu đã đề ra.

GIỚI THIỆU VỀ QUẢN TRỊ MẠNG

- ❖ Công việc quản trị mạng bao gồm:
- ❖ Quản trị hiệu năng, hoạt động mạng: bao gồm các công tác quản lý, giám sát hoạt động mạng lưới, đảm bảo các hoạt động của thiết bị hệ thống ổn định.
- ❖ Quản trị an ninh, an toàn mạng: Quản lý, giám sát mạng lưới, các hệ thống để đảm bảo phòng tránh các truy nhập trái phép. Việc phòng chống, ngăn chặn sự lây lan của các loại virus máy tính, các phương thức tấn công như DoS làm tê liệt hoạt động của mạng cũng là một phần rất quan trọng trong công tác quản trị, an ninh, an toàn mạng.

CHƯƠNG 1: TỔNG QUAN VỀ MẠNG

1

- Giới thiệu về quản trị mạng

2

- Mô hình OSI và TCP/IP

3

- Địa chỉ IPv4

4

- Địa chỉ IPv6

5

- Chuyển đổi IPv4-IPv6

6

- Cấu hình cơ bản thiết bị mạng

MÔ HÌNH OSI VÀ TCP/IP

❖ Khái niệm về TCP và IP

- TCP (Transmission Control Protocol) là giao thức thuộc tầng vận chuyển (Transport Layer) và là một giao thức hướng 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 gồm ? lớp tương ứng với mô hình OSI ? lớp.**

Câu 1: Thứ tự các tầng (layer) của mô hình OSI theo thứ tự từ trên xuống là:

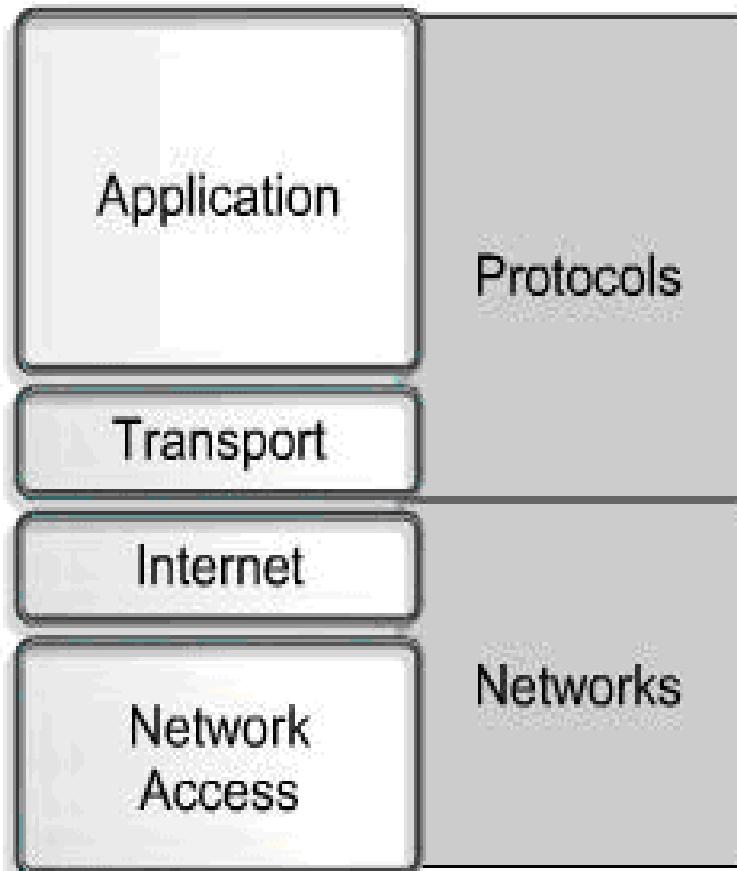
- a. Application, Presentation, Session, Transport, Data Link, Network, Physical
- b. Application, Presentation, Session, Network, Transport, Data Link, Physical
- c. Application, Presentation, Session, Transport, Network, Data Link, Physical
- d. Application, Presentation, Transport, Session, Data Link, Network, Physical

Câu 2: Thứ tự các tầng (layer) của mô hình TCP/IP theo thứ tự từ trên xuống là:

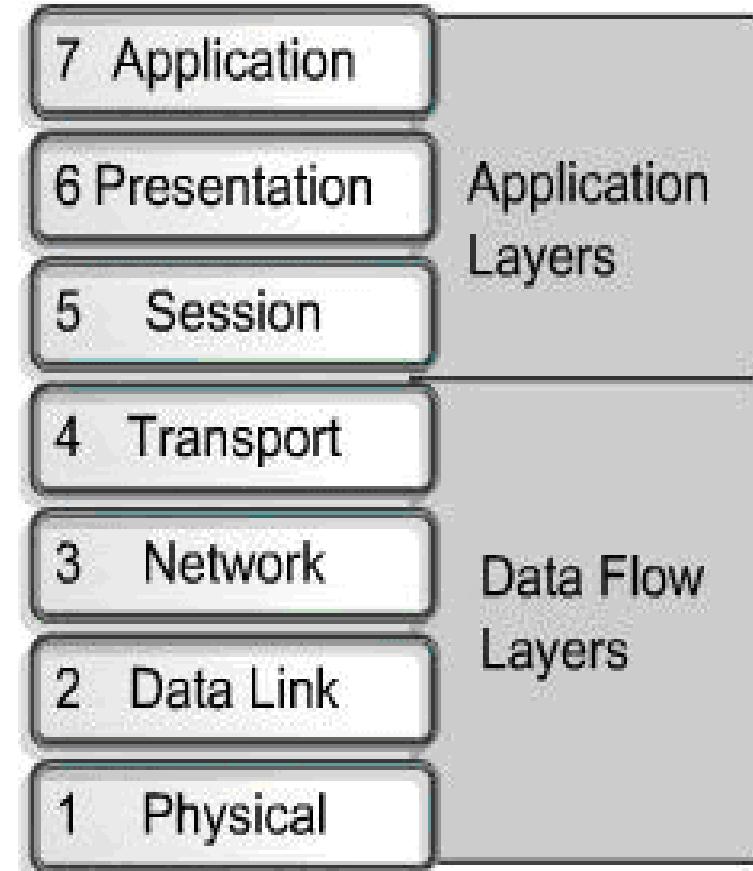
- a. Application, Transport, Network, Data Link, Physical.
- b. Application, Transport, Network, Network Access.
- c. Application, Transport, Internet, Physical.
- d. Application, Transport, Internet, Network Access.

MÔ HÌNH OSI VÀ TCP/IP

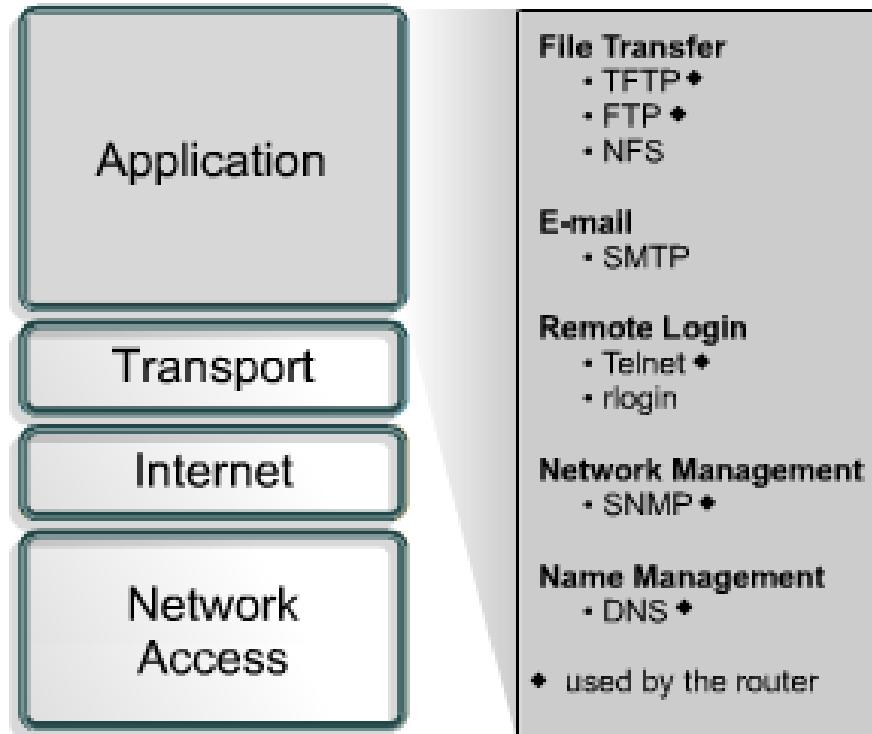
TCP/IP Model



OSI Model



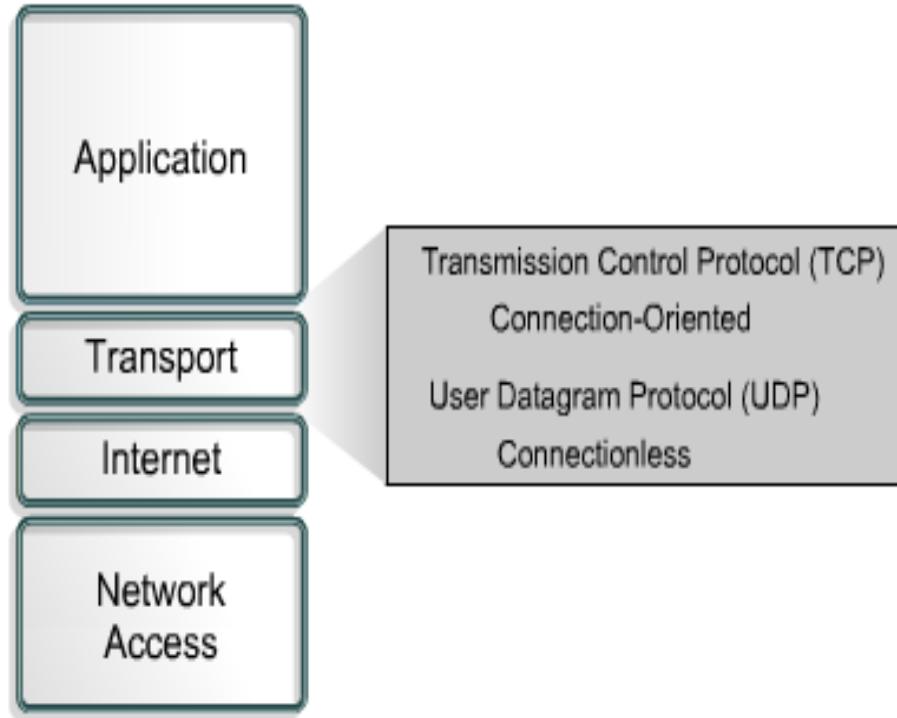
Lớp ứng dụng



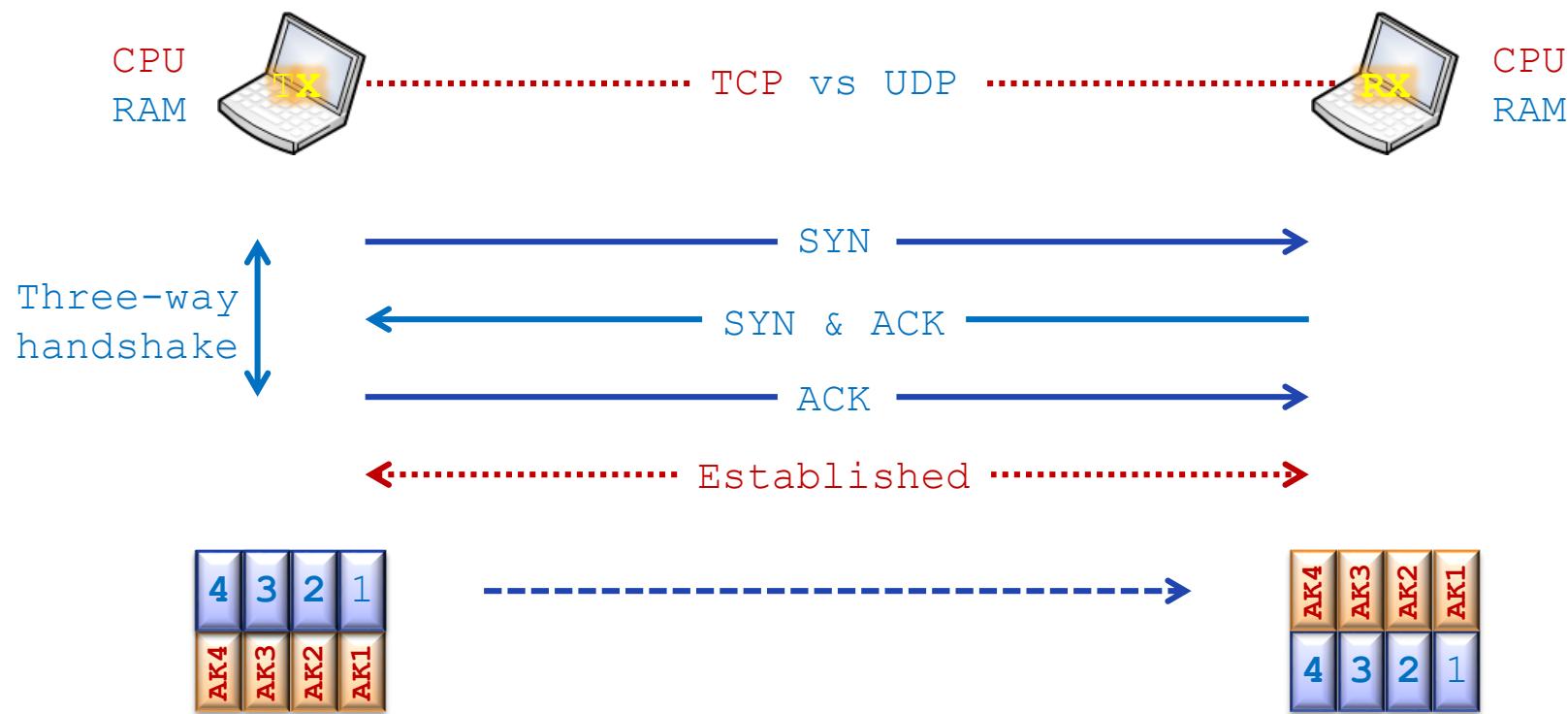
- ❖ Kiểm soát các giao thức lớp cao, các chủ đề về định dạng dữ liệu, biểu diễn thông tin, mã hóa và điều khiển hội thoại.
- ❖ Lớp ứng dụng liên quan đến các chương trình ứng dụng.

Lớp vận chuyển

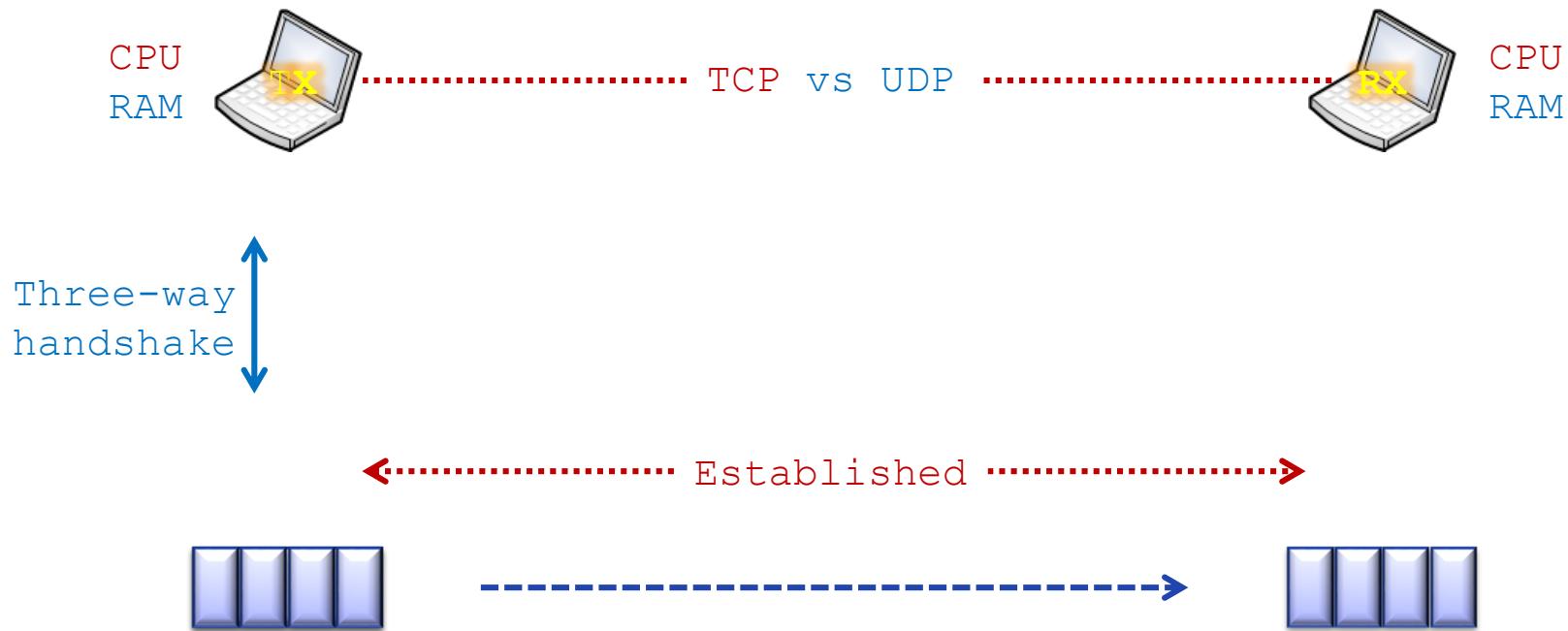
- ❖ Thực hiện chức năng đảm bảo việc vận chuyển dữ liệu từ host nguồn đến host đích.
- ❖ Thiết lập một cầu nối luận lý giữa các đầu cuối của mạng, giữa host truyền và host nhận.



GIAO THÚC TCP



GIAO THỨC UDP



S.Port vs D.Port

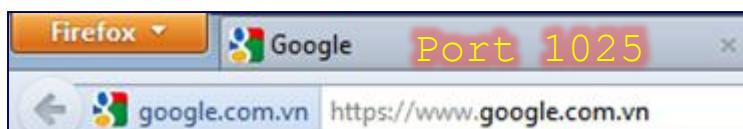


Established

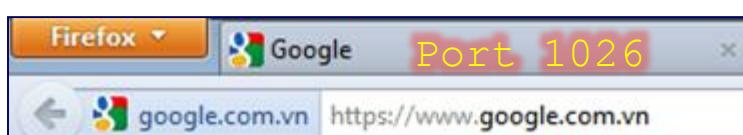


Segment	S.Port 1025	D.Port 443
Segment	S.Port 443	D.Port 1025

Segment	S.Port 1025	D.Port 443
Segment	S.Port 443	D.Port 1025



Established



Established

Port 1025

Lớp Internet

Application

Transport

Internet

Network
Access

Mục đích của lớp Internet là chọn đường đi tốt nhất xuyên qua mạng cho các gói dữ liệu di chuyển tới đích, liên quan đến địa chỉ IP. Thiết bị hoạt động ở lớp này là Router

Internet Protocol (IP)

Internet Control Message Protocol (ICMP)

Address Resolution Protocol (ARP)

Reverse Address Resolution Protocol (RARP)

Giao thức lớp Internet

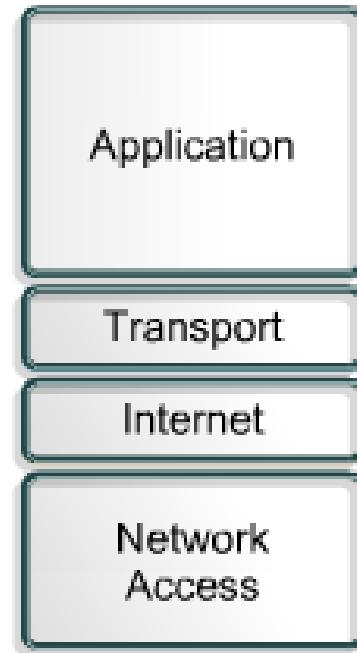
- ❖ IP: Không quan tâm đến nội dung của các gói nhưng tìm kiếm đường dẫn cho gói tới đích.
- ❖ ICMP (Internet Control Message Protocol): Đem đến khả năng điều khiển và chuyển thông điệp trong lớp Internet.
- ❖ ARP (Address Resolution Protocol): Xác định địa chỉ lớp liên kết số liệu (MAC address) khi 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 IPv4

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

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

Thiết bị hoạt động ở lớp này là HUB, SWITCH

Lớp truy nhập mạng

❖ Ethernet

- Là giao thức truy cập LAN định nghĩa chuẩn 802.3 của IEEE (Institute of Electrical and Electronics Engineers).
- Tốc độ truyỀn 10Mbps

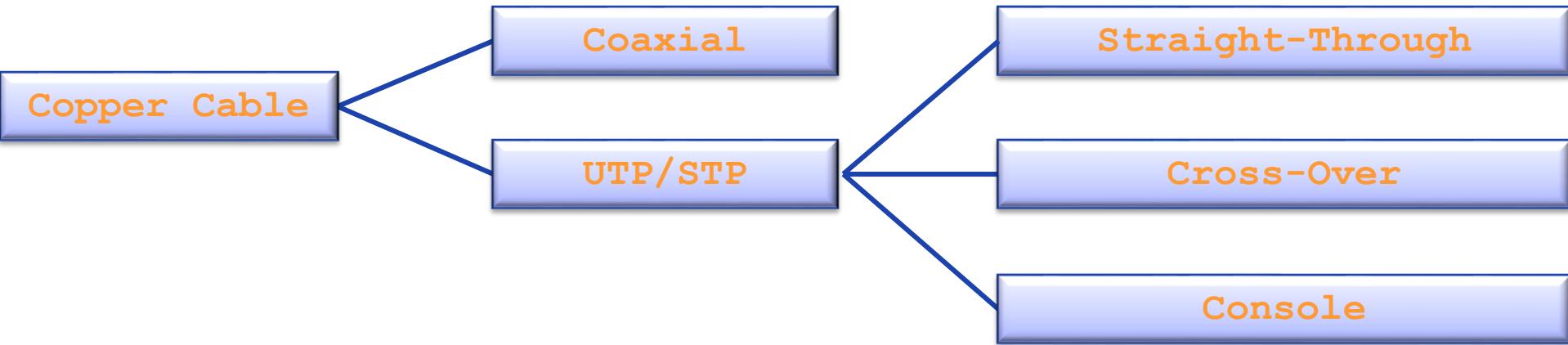
❖ Fast Ethernet

- IEEE 802.3u định nghĩa 2 loại cáp cho mạng 100Mbps:
- Cáp STP (cat 5 hoặc cao hơn) – 100Base - TX.
- Cáp quang 100Base-FX

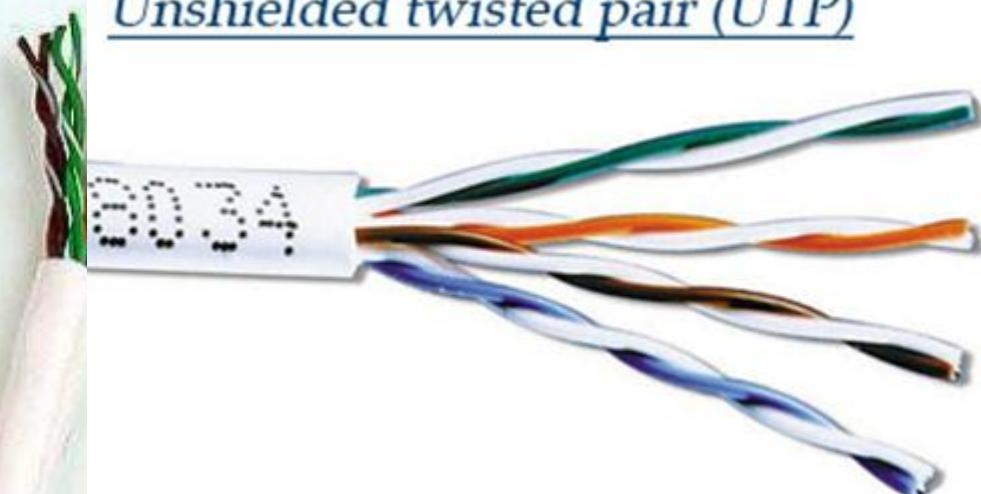
❖ Gigabit Ethernet

- IEEE802.3z và IEEE802.3ab định nghĩa 2 loại cáp cho 1000Mbps:
 - Cáp STP (cat 5e hoặc cao hơn) – 1000Base-T
 - Cáp quang 1000Base-SX và 1000Base-LX.

CÁP MẠNG



Shielded twisted pair (STP)



RJ-45

CÁP CONSOLE



Start → Program → Accessories → Communication → Hyper Terminal

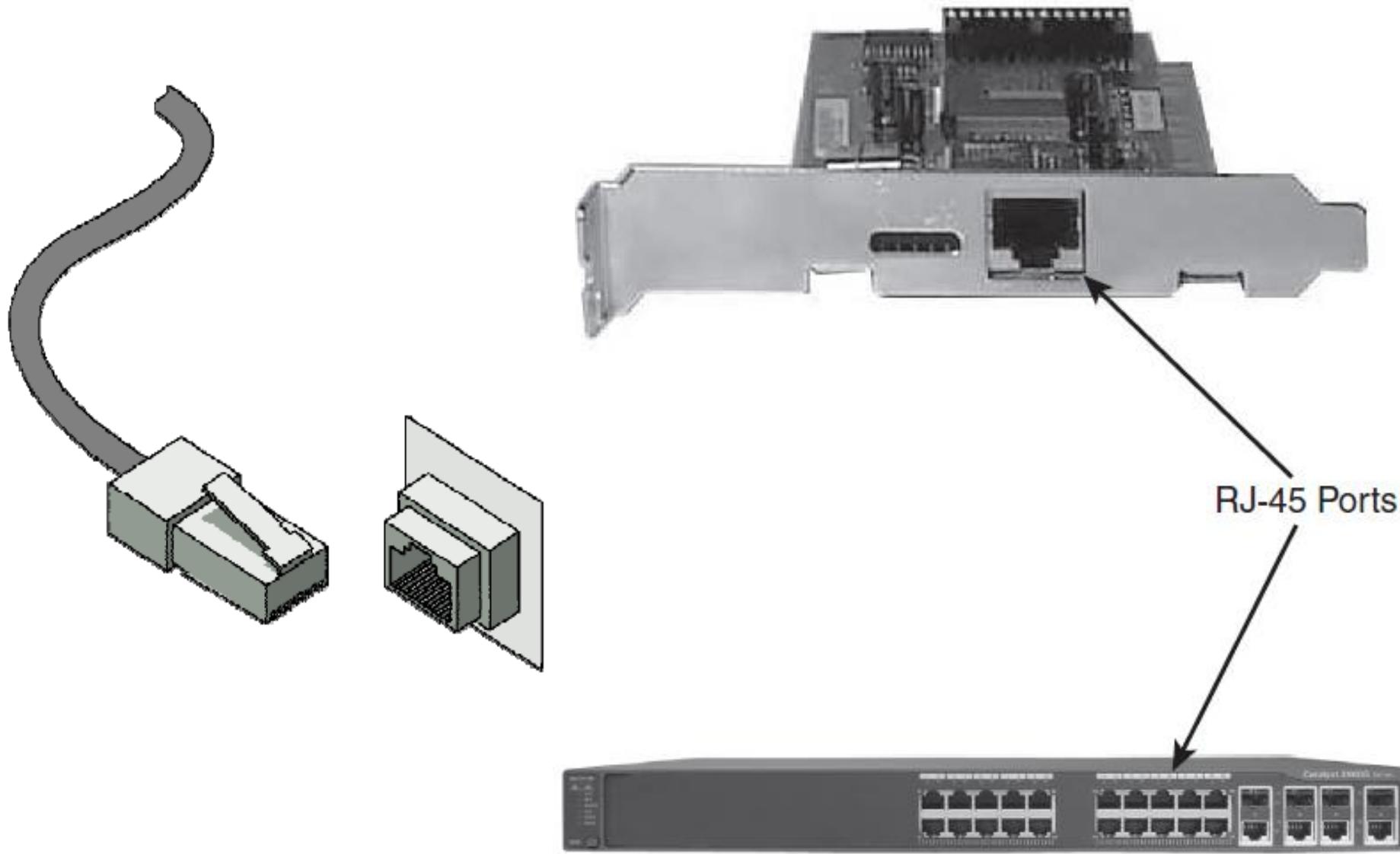
CÁP MẠNG UTP



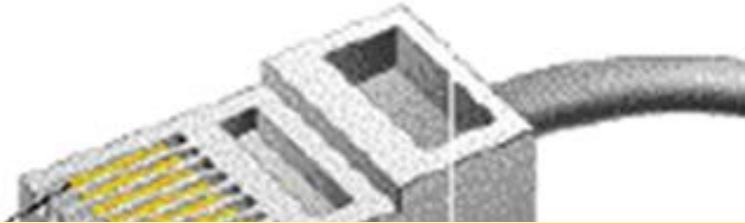
Cáp UTP có 6 loại:

- Cat1: truyền âm thanh, tốc độ <4Mbps
- Cat2: tốc độ 4Mbps
- Cat3: tốc độ 10Mbps
- Cat4: tốc độ 16Mbps
- Cat5: tốc độ 100Mbps
- Cat6: tốc độ 1000Mbps

JACK RJ-45



CHUẨN BẤM DÂY MẠNG RJ45



Pin	T568A	T568B	Signal 10/100BaseTx
1	Wht/Grn	Wht/Org	Tx+
2	Grn	Org	Tx-
3	Wht/Org	Wht/Grn	Rx+
4	Blu	Blu	Unused
5	Wht/Blu	Wht/Blu	Unused
6	Org	Grn	Rx-
7	Wht/Brn	Wht/Brn	Unused
8	Brn	Brn	Unused

CHUẨN BẤM DÂY MẠNG RJ45

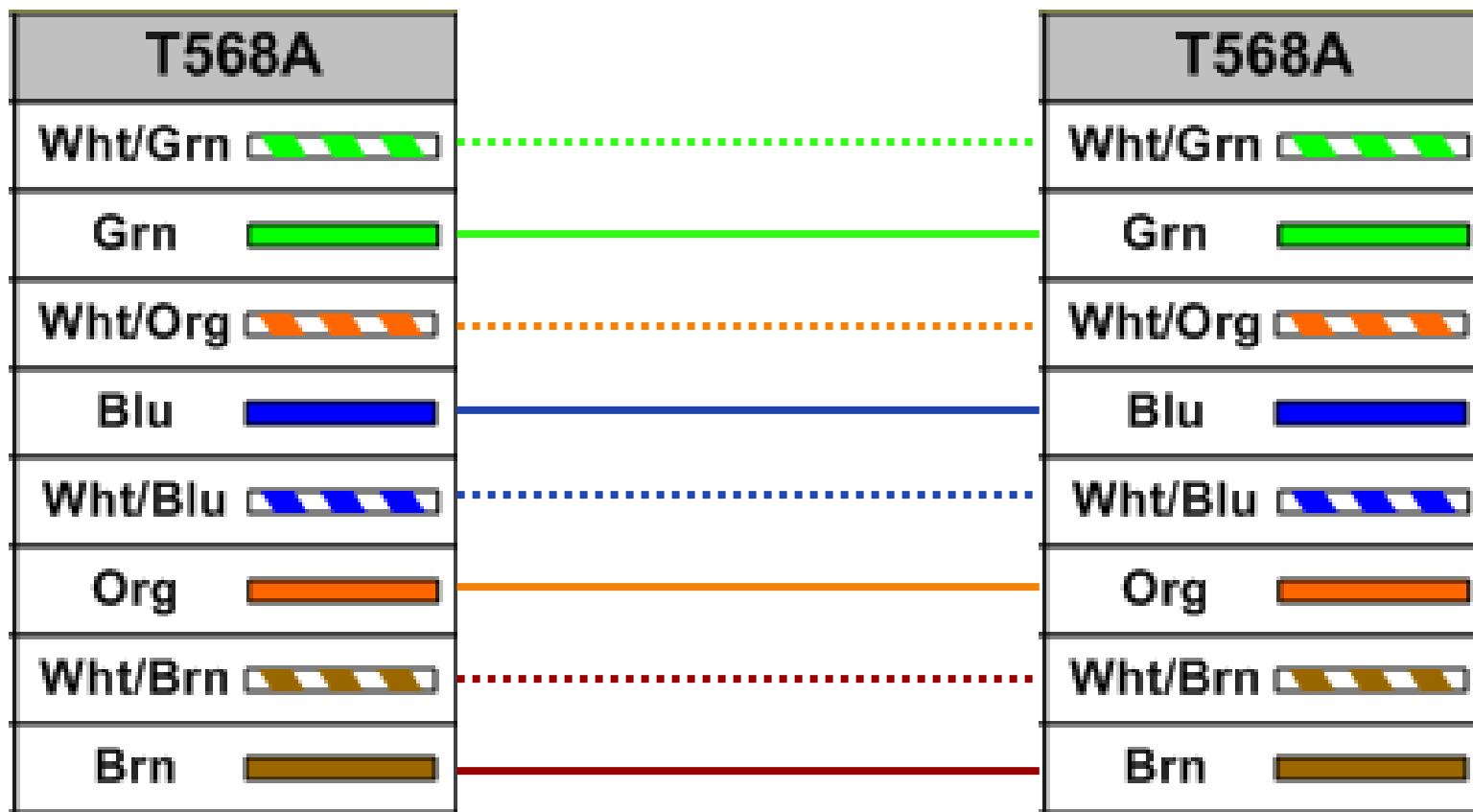
T568B ← **Straight-Through Cable** → **T568B**

T568A ← **Crossover Cable** → **T568B**

Pin	T568A	T568B	Signal 10/100BaseTx
1	Wht/Grn 	Wht/Org 	Tx+
2	Grn 	Org 	Tx-
3	Wht/Org 	Wht/Grn 	Rx+
4	Blu 	Blu 	Unused
5	Wht/Blu 	Wht/Blu 	Unused
6	Org 	Grn 	Rx-
7	Wht/Brn 	Wht/Brn 	Unused
8	Brn 	Brn 	Unused

ĐẦU CÁP THĂNG CHUẨN T568A

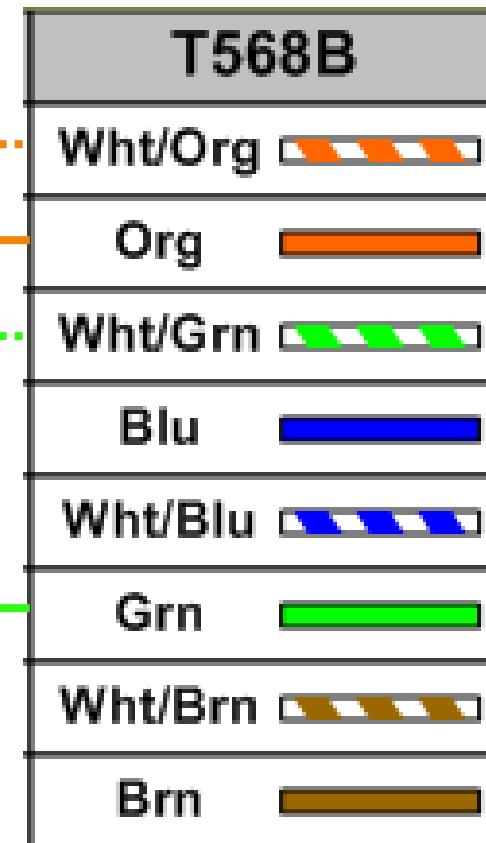
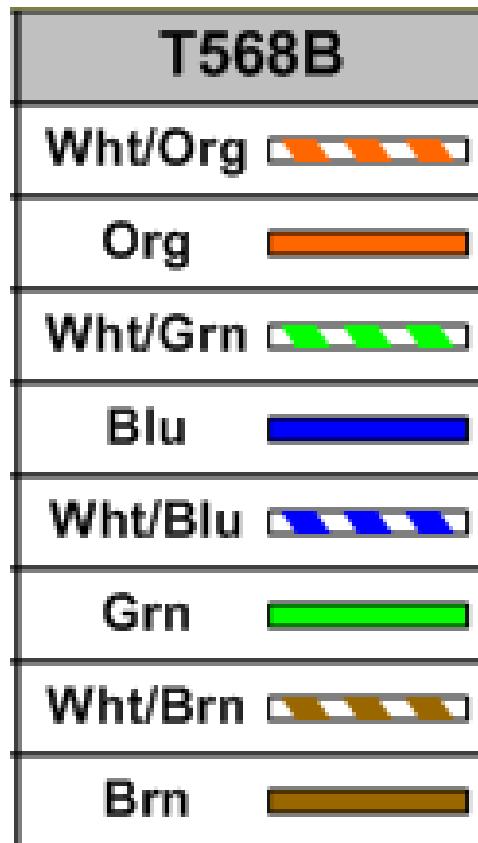
Straight-Through Cable
T568A ← → T568A



ĐẦU CÁP THĂNG CHUẨN T568B

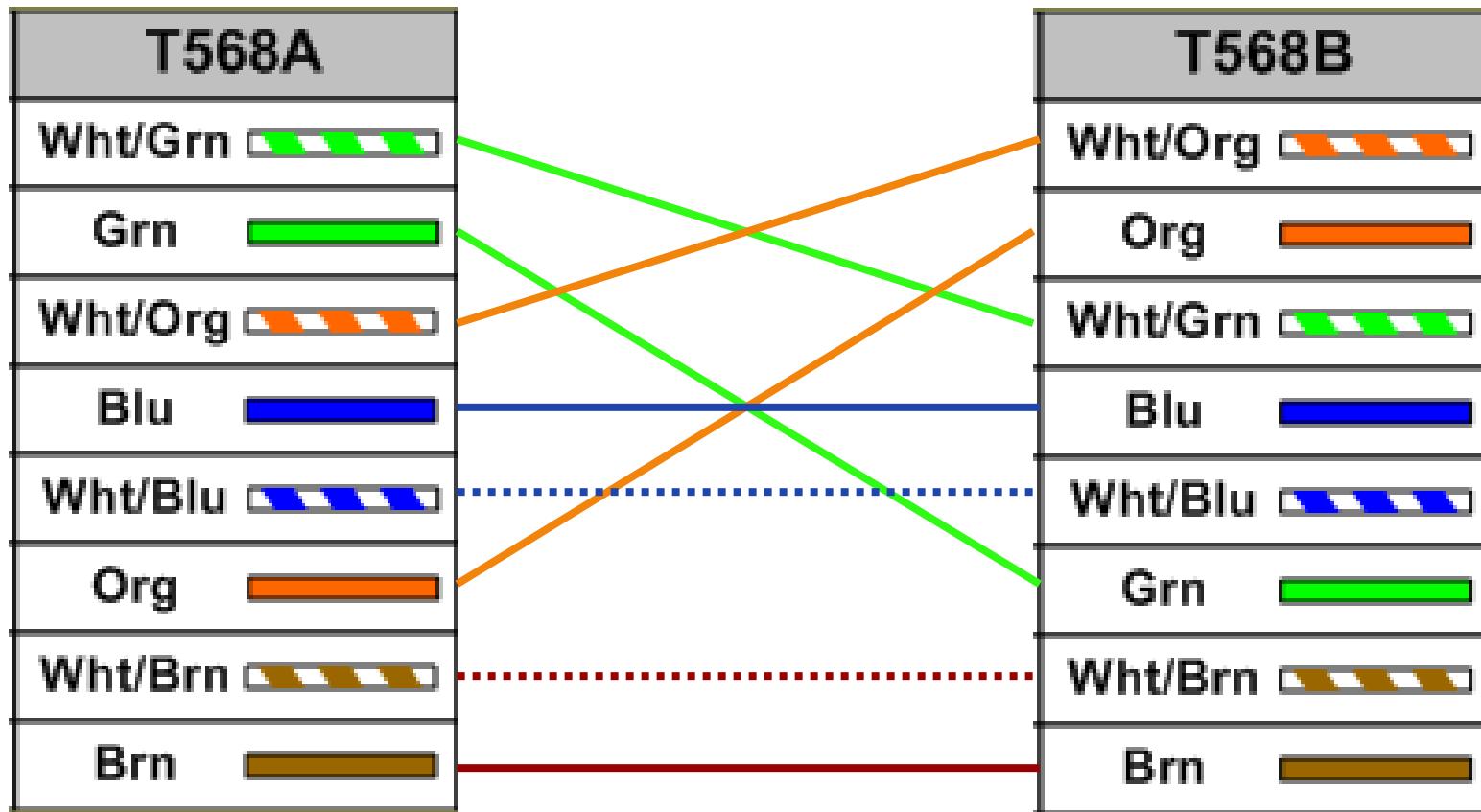
Straight-Through Cable

T568B ← → **T568B**



ĐẦU CÁP CHÉO T568A - T568B

Crossover Cable
T568A ← → T568B



CHUẨN GIGABIT ETHERNET 1Gbps

Pin	Color	Function
1	White with Green	+BI_DA
2	Green	-BI_DA
3	White with Orange	+BI_DB
4	Blue	+BI_DC
5	White with Blue	-BI_DC
6	Orange	-BI_DB
7	White with Brown	+BI_DD
8	Brown	-BI_DD

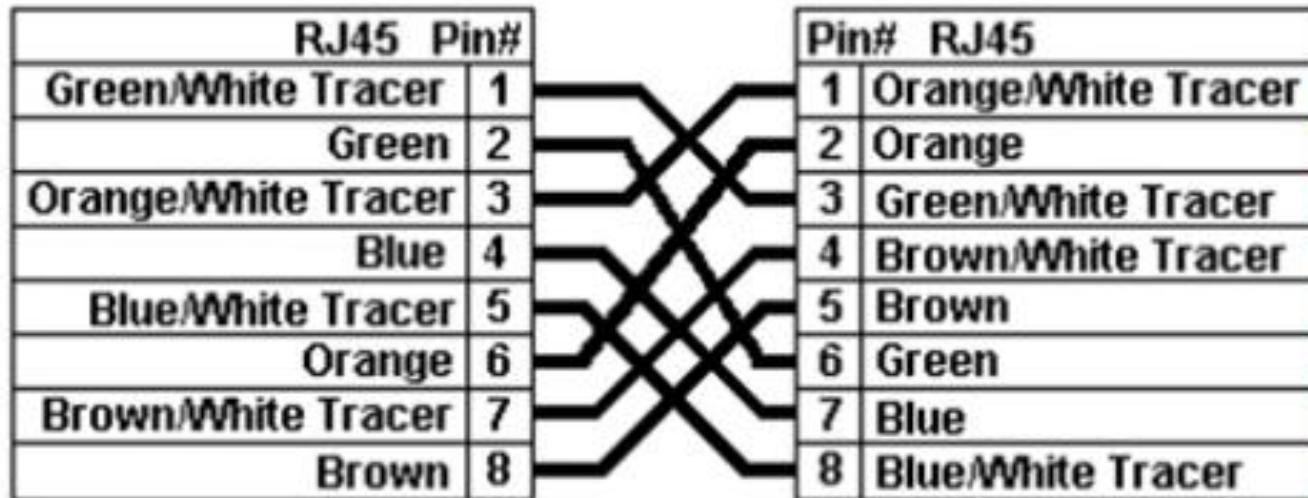
Cặp dây DA và DC là cặp phát Transmit

Cặp dây DB và DD là cặp thu Receive

ĐẦU CÁP CHÉO ETHERNET 1Gbps

Color Standard
EIA/TIA T568A

Ethernet Crossover Cable



"A" is earlier

ĐẦU CÁP CHÉO ETHERNET 1Gbps

Color Standard
EIA/TIA T568B

Ethernet Crossover Cable



RJ45 Pin#	
Orange/White Tracer	1
Orange	2
Green/White Tracer	3
Blue	4
Blue/White Tracer	5
Green	6
Brown/White Tracer	7
Brown	8

Pin# RJ45
1 Green/White Tracer
2 Green
3 Orange/White Tracer
4 Brown/White Tracer
5 Brown
6 Orange
7 Blue
8 Blue/White Tracer



"B" is most recent

Common Ethernet Crossover Cables may only cross connect the Orange & Green pairs

ĐẦU CÁP CHÉO ETHERNET 1Gbps

SƠ ĐỒ BÂM CÁP CHÉO RJ45 (CROSS-OVER)

RJ45 - Ethernet 1000Mbps (1Gbps)

NIC 1			NIC 2		
Màu	Tên	Pin	Pin	Tên	Màu
White/Orange	BI_DA+	1	3	BI_DB+	White/Orange
Orange	BI_DA-	2	6	BI_DB-	Orange
White/Green	BI_DB+	3	1	BI_DA+	White/Green
Blue	BI_DC+	4	7	BI_DD+	Blue
White/Blue	BI_DC-	5	8	BI_DD-	White/Blue
Green	BI_DB-	6	2	BI_DA-	Green
White/Brown	BI_DD+	7	4	BI_DC+	White/Brown
Brown	BI_DD-	8	5	BI_DC-	Brown

❖ Sử dụng đủ 4 đôi dây :

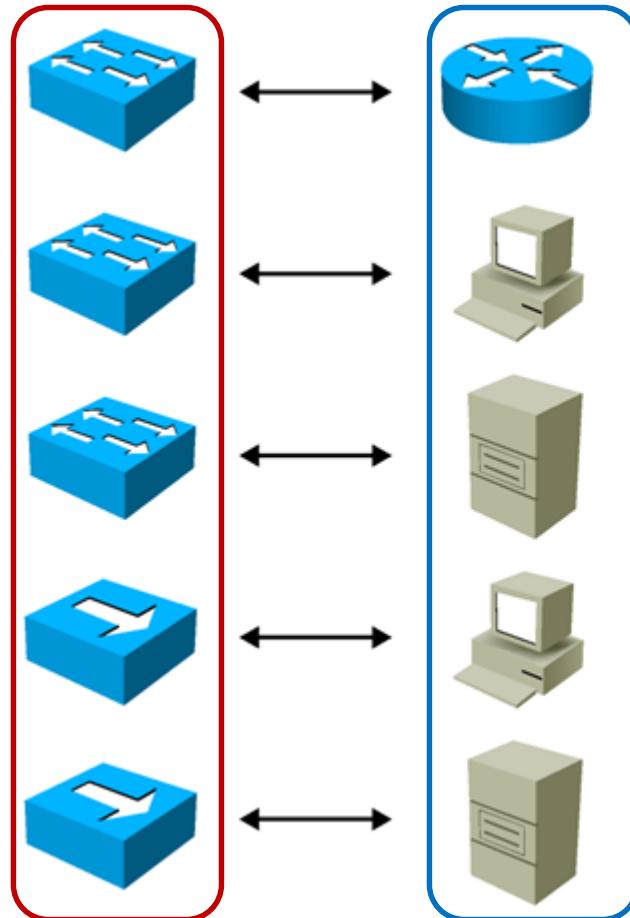
+ Đôi BI_DA (Orange) & BI_DC (Blue) : RECEIVE

+ Đôi BI_DB (Green) & BI_DD (Brown) : TRANSMIT (SEND)

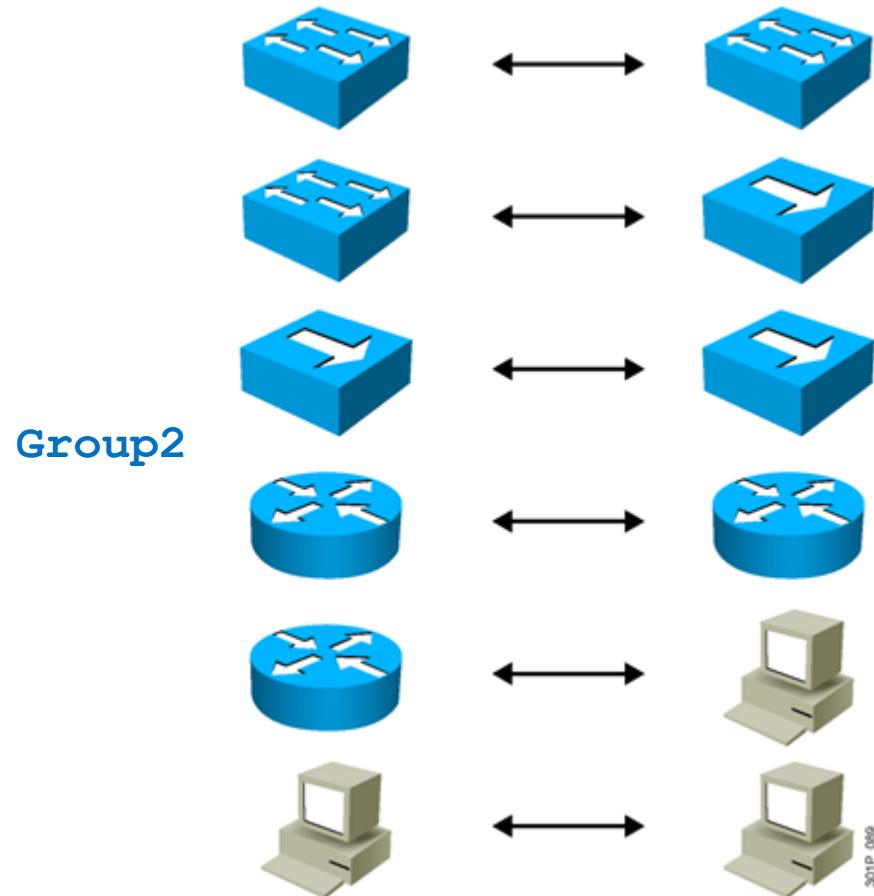
❖ “Phải” dùng cable chuẩn CAT-5E hoặc CAT-6 trở lên.

ĐẦU NỐI CÁC THIẾT BỊ

Straight-Through Cable



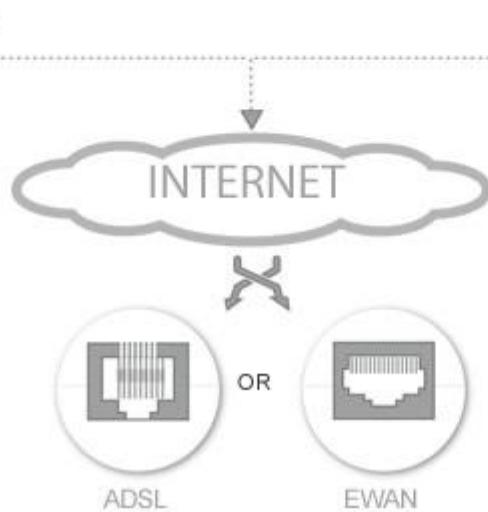
Crossover Cable



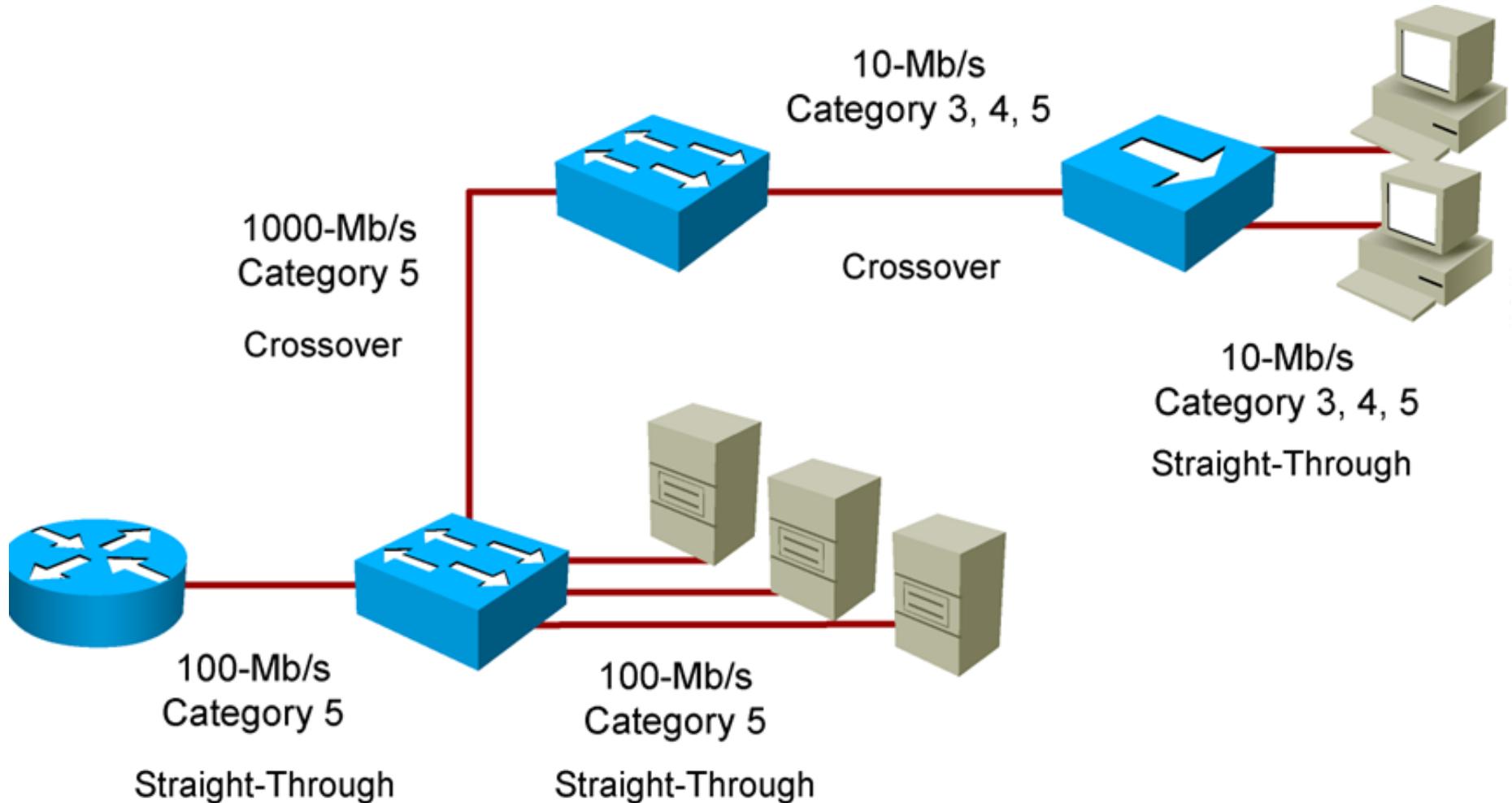
Group1

Group2

JACK RJ11

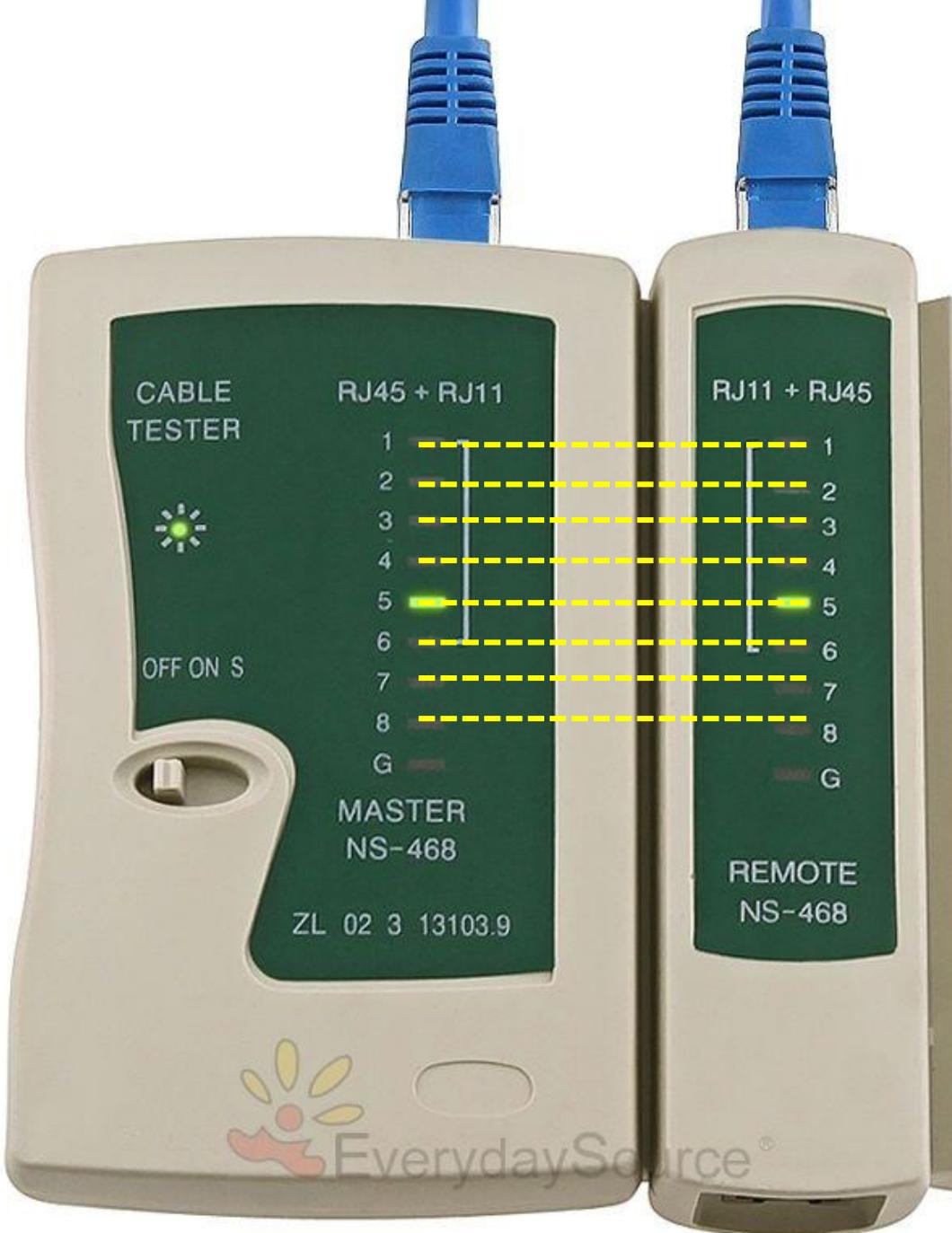


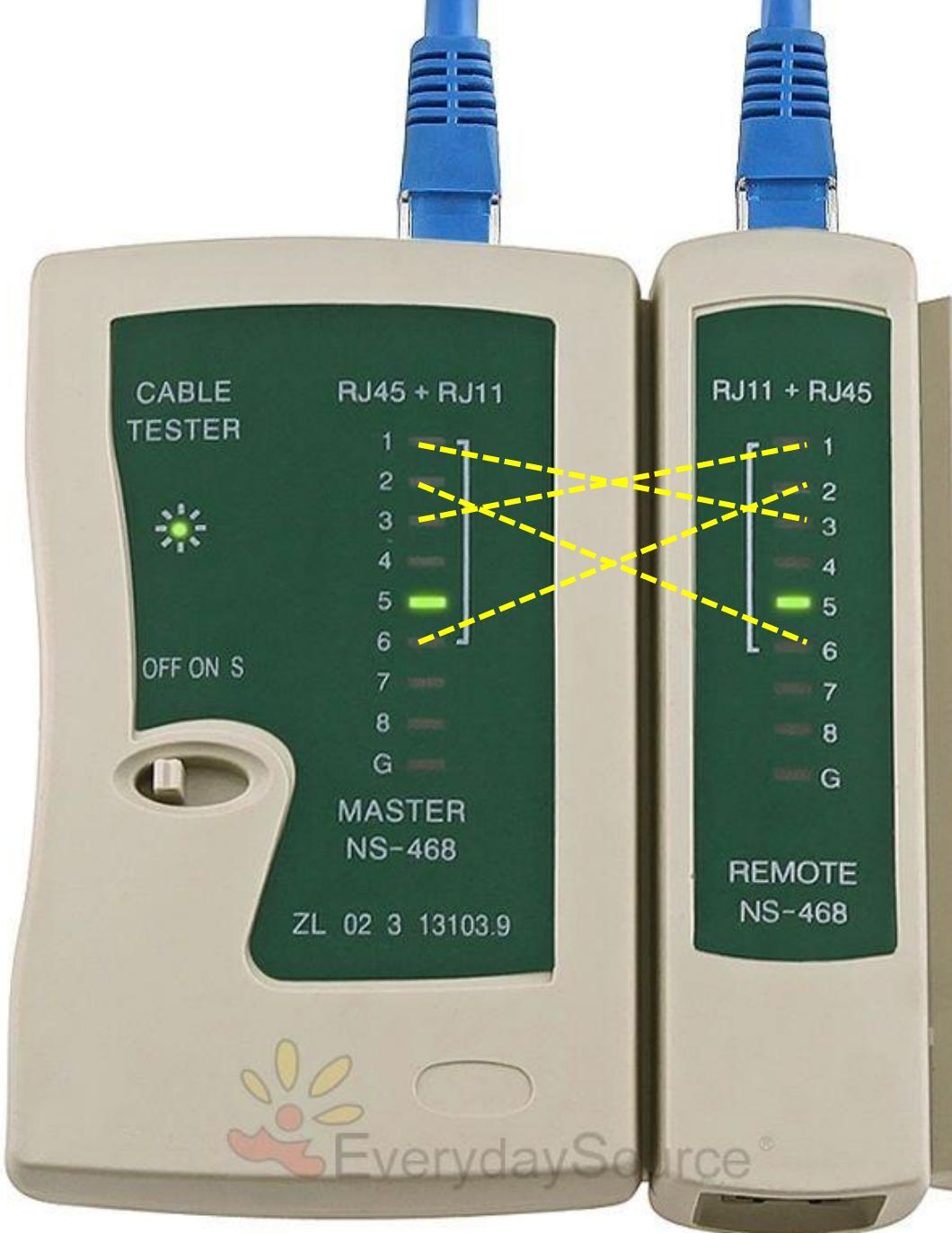
VÍ DỤ



DỤNG CỤ MẠNG

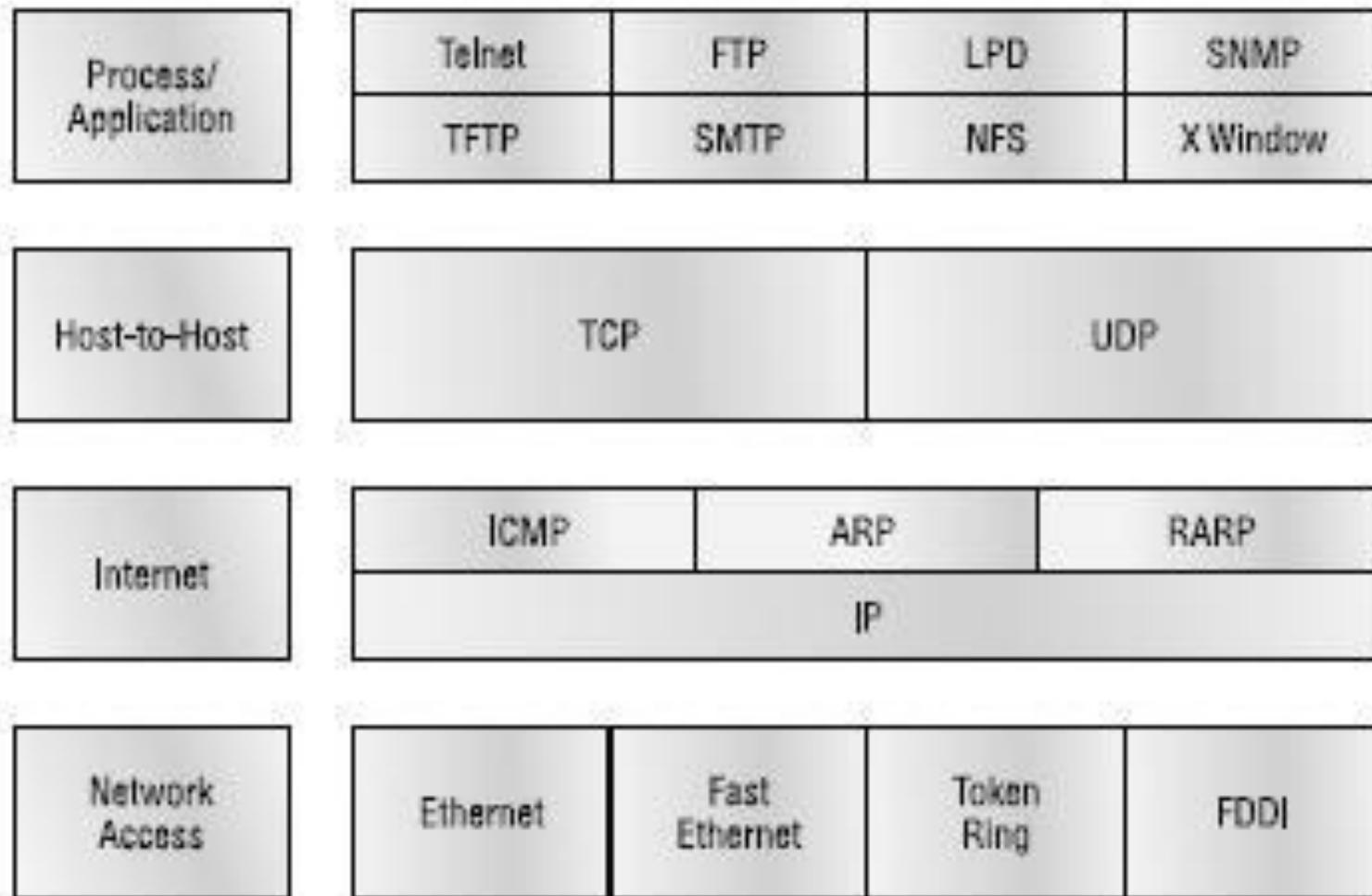






CÁC GIAO THỨC TRONG TCP/IP

DoD Model



CHƯƠNG 1: TỔNG QUAN VỀ MẠNG

1

- Giới thiệu về quản trị mạng

2

- Mô hình OSI và TCP/IP

3

- Địa chỉ IPv4

4

- Địa chỉ IPv6

5

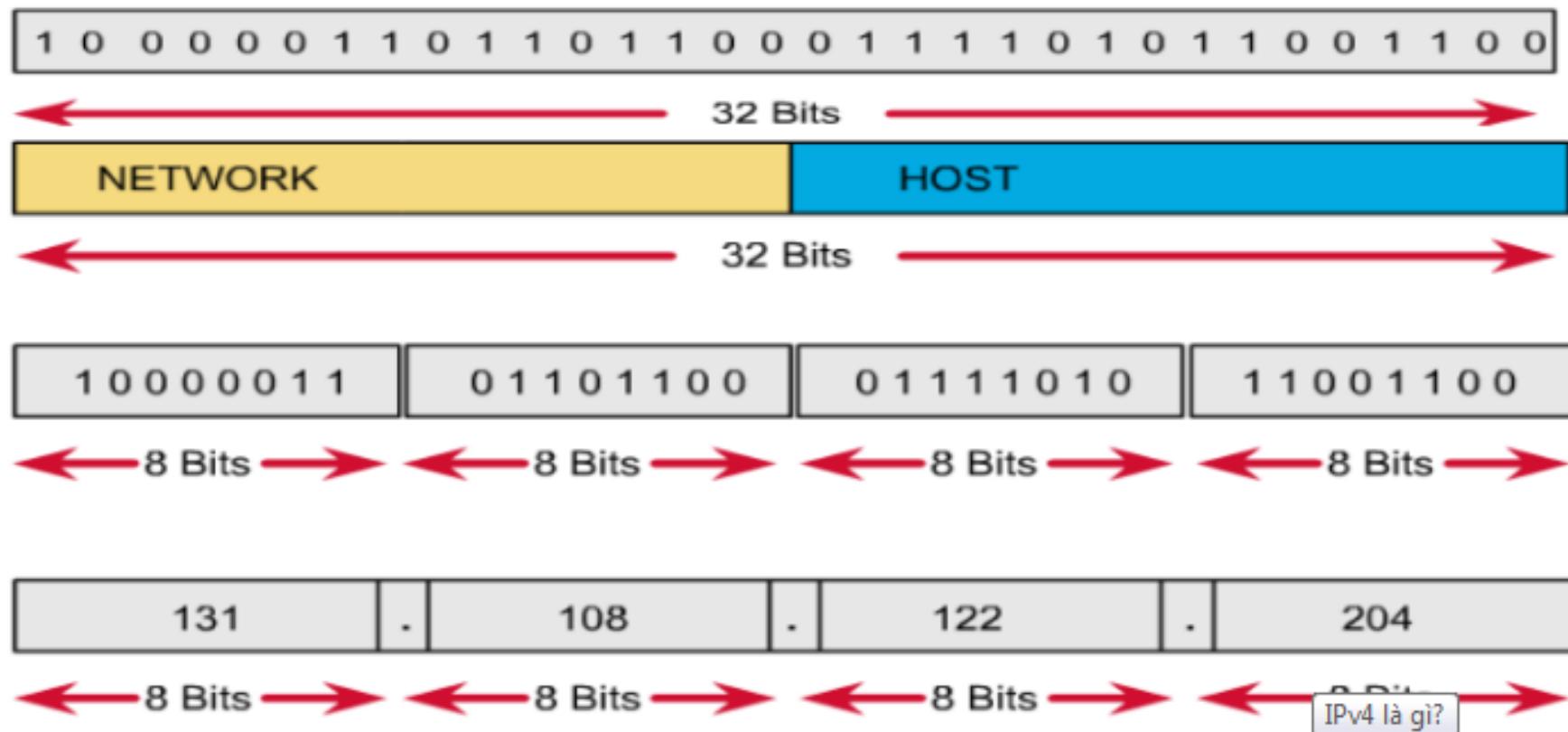
- Chuyển đổi IPv4-IPv6

6

- Cấu hình cơ bản thiết bị mạng

Địa chỉ IPv4 và các lớp địa chỉ

Địa chỉ IPv4 có độ dài 32 bit chia thành 4 octet chia thành 2 phần là network_id và host_id.



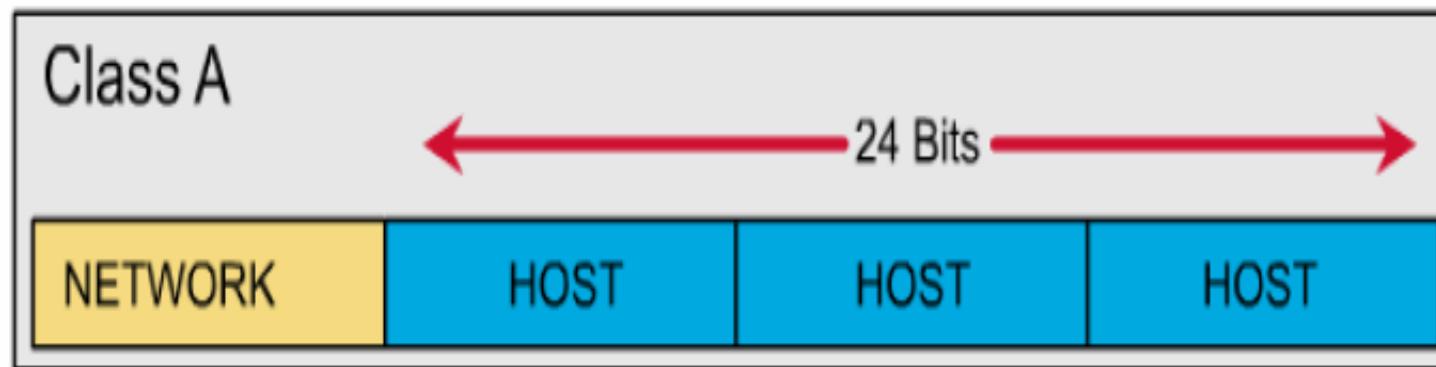
Cấu trúc địa chỉ IPv4

Các lớp địa chỉ IPv4

- Không gian địa chỉ IPv4 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)

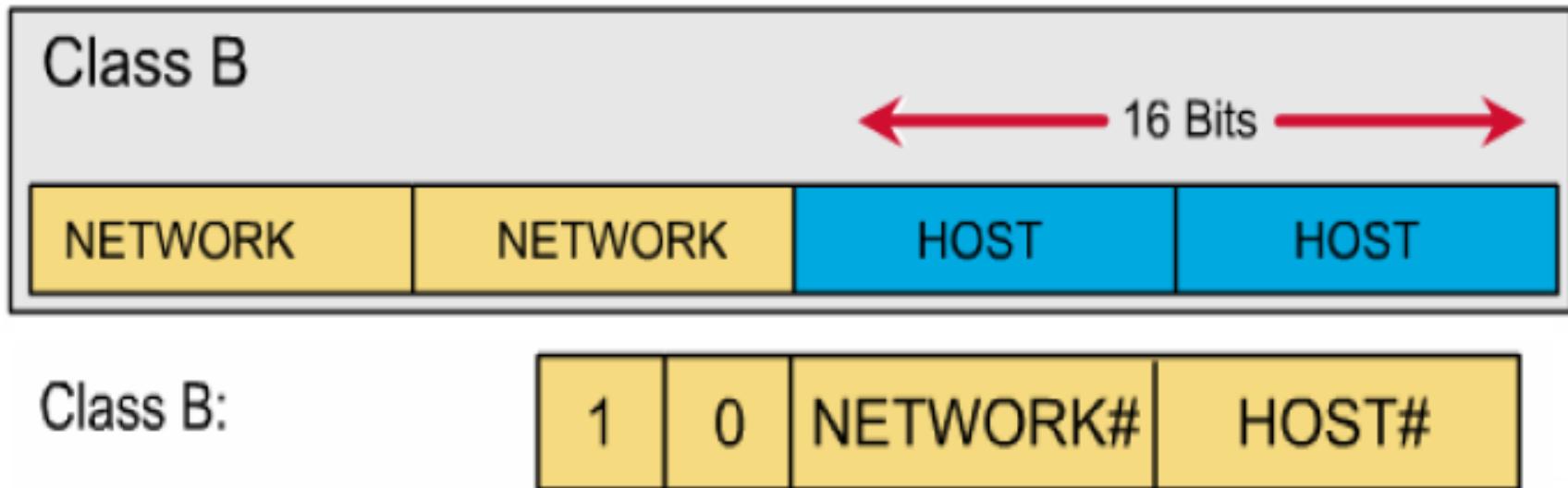
- ❖ Byte đầu tiên này cũng chính là network_id, trừ đi bit đầu tiên làm ID nhận dạng lớp A, còn lại 7 bit để đánh thứ tự các mạng, ta được $128 (=2^7)$ mạng lớp A khác nhau.
- ❖ Bỏ đi hai trường hợp đặc biệt là 0 và 127. Kết quả là lớp A chỉ còn 126 địa chỉ mạng, 1.0.0.0 đến 126.0.0.0.

Lớp A (Class A)

- ❖ Phần host_id chiếm 24 bit, nghĩa là có $2^{24} = 16.777.216$ 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: 16.777.214 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)

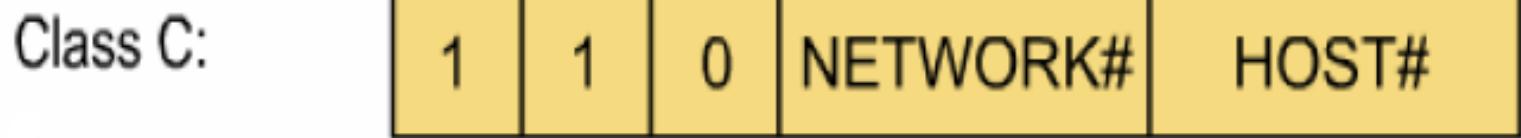
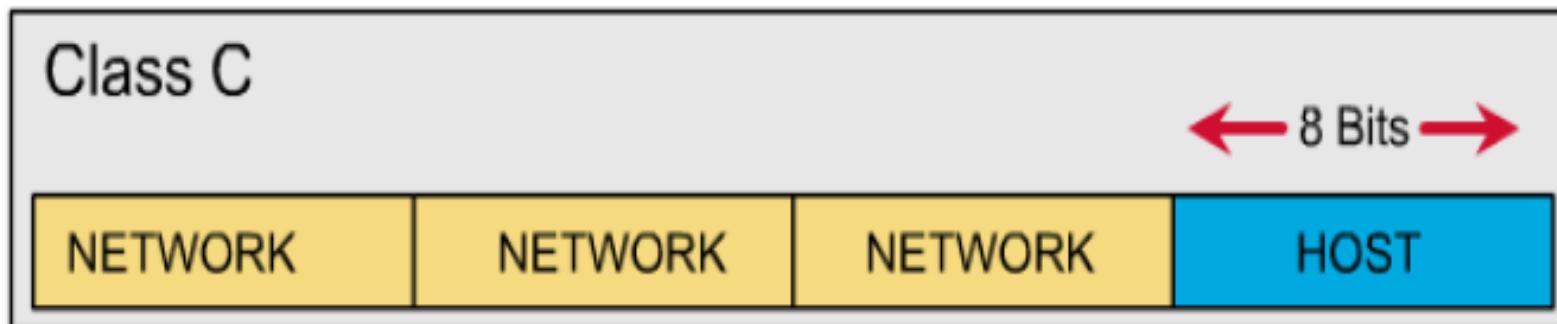
- ❖ Hai bit đầu tiên của byte đầu tiên phải là 10. Dạng nhị phân của octet này là **10xxxxxx**
- ❖ Những địa chỉ IP có byte đầu tiên nằm trong khoảng từ 128 ($=10000000_{(2)}$) đến 191 ($=10111111_{(2)}$) sẽ thuộc về lớp B
- ❖ Ví dụ: 172.29.10.1.

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 16.384 ($=2^{14}$) mạng khác nhau (128.0.0.0 đến 191.255.0.0).
- ❖ Phần host_id dài 16 bit hay có 65.536 ($=2^{16}$) giá trị khác nhau. Trừ đi 2 trường hợp đặc biệt còn lại 65.534 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 **110xxxxx**
- ❖ Những địa chỉ IP có byte đầu tiên nằm trong khoảng từ 192 ($=11000000_{(2)}$) đến 223 ($=11011111_{(2)}$) sẽ thuộc về lớp C.
- ❖ Ví dụ: 203.162.41.235

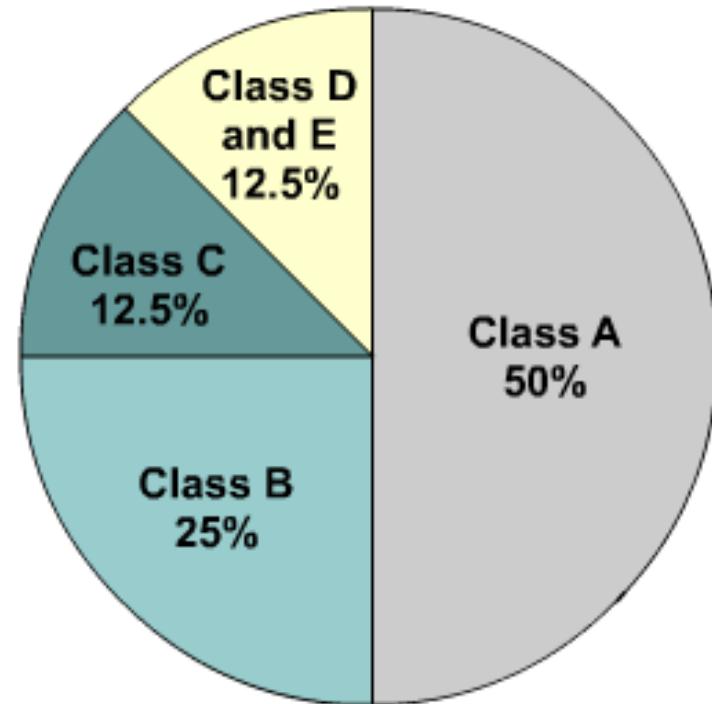
Các lớp địa chỉ IP

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)



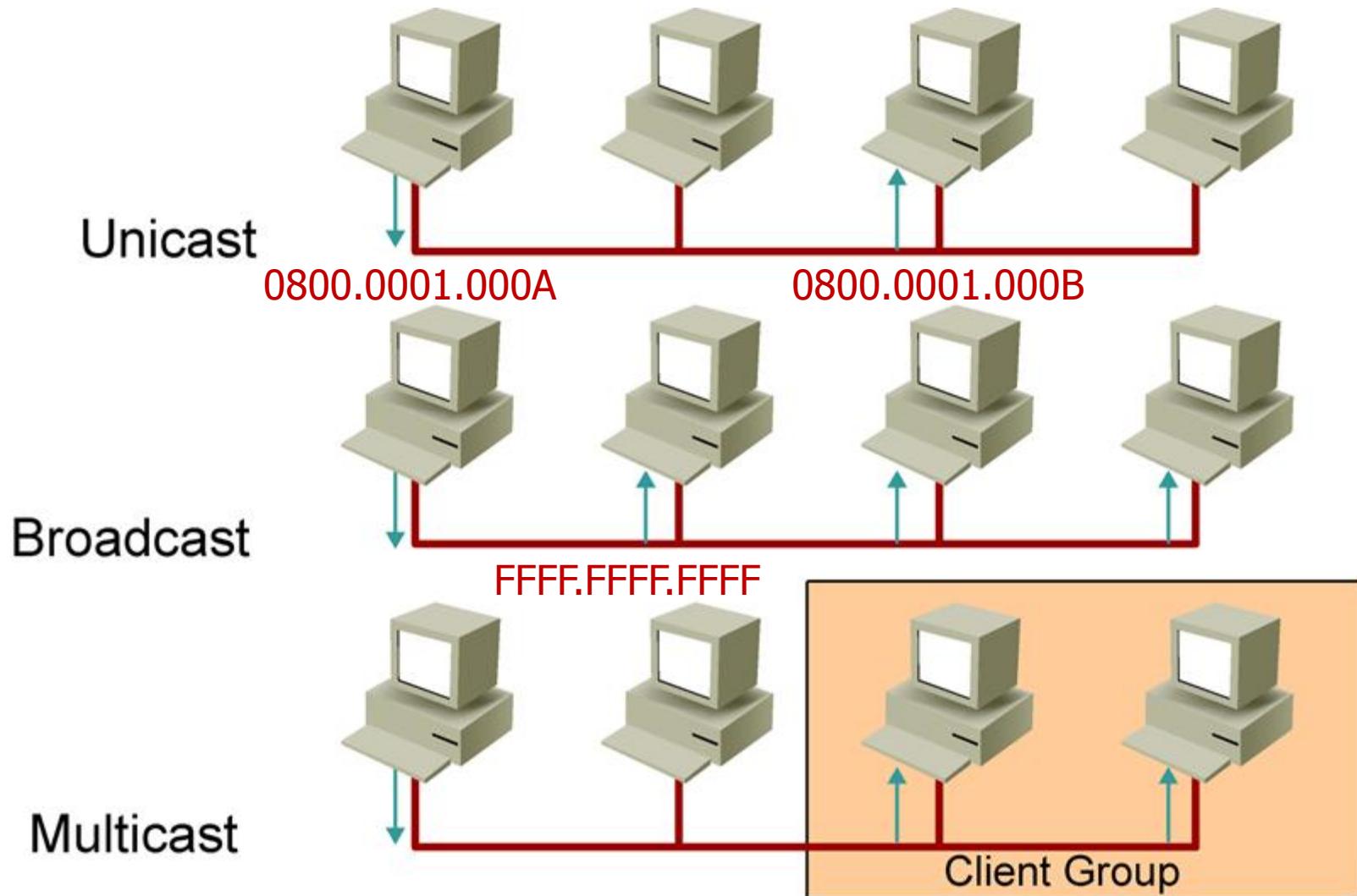
Địa chỉ dành riêng

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

Địa chỉ nào sử dụng trong mạng nội bộ

- ❖ **150.100.255.255**
- ❖ **172.19.255.18**
- ❖ **195.234.253.0**
- ❖ **10.10.110.23**
- ❖ **192.168.221.176**
- ❖ **127.34.25.189**
- ❖ **203.162.217.73**

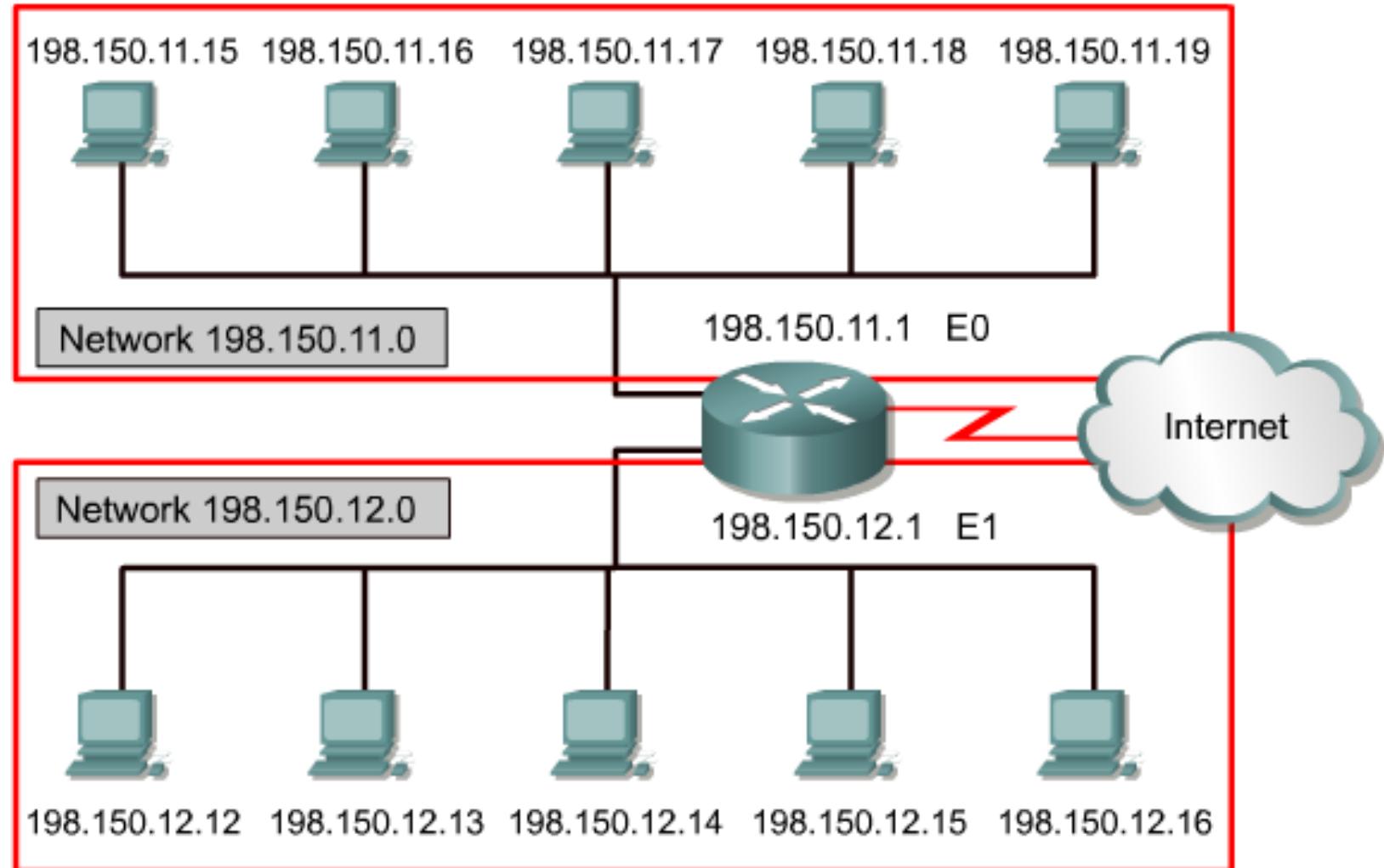
Phân loại địa chỉ IPv4



Địa chỉ mạng, địa chỉ Broadcast

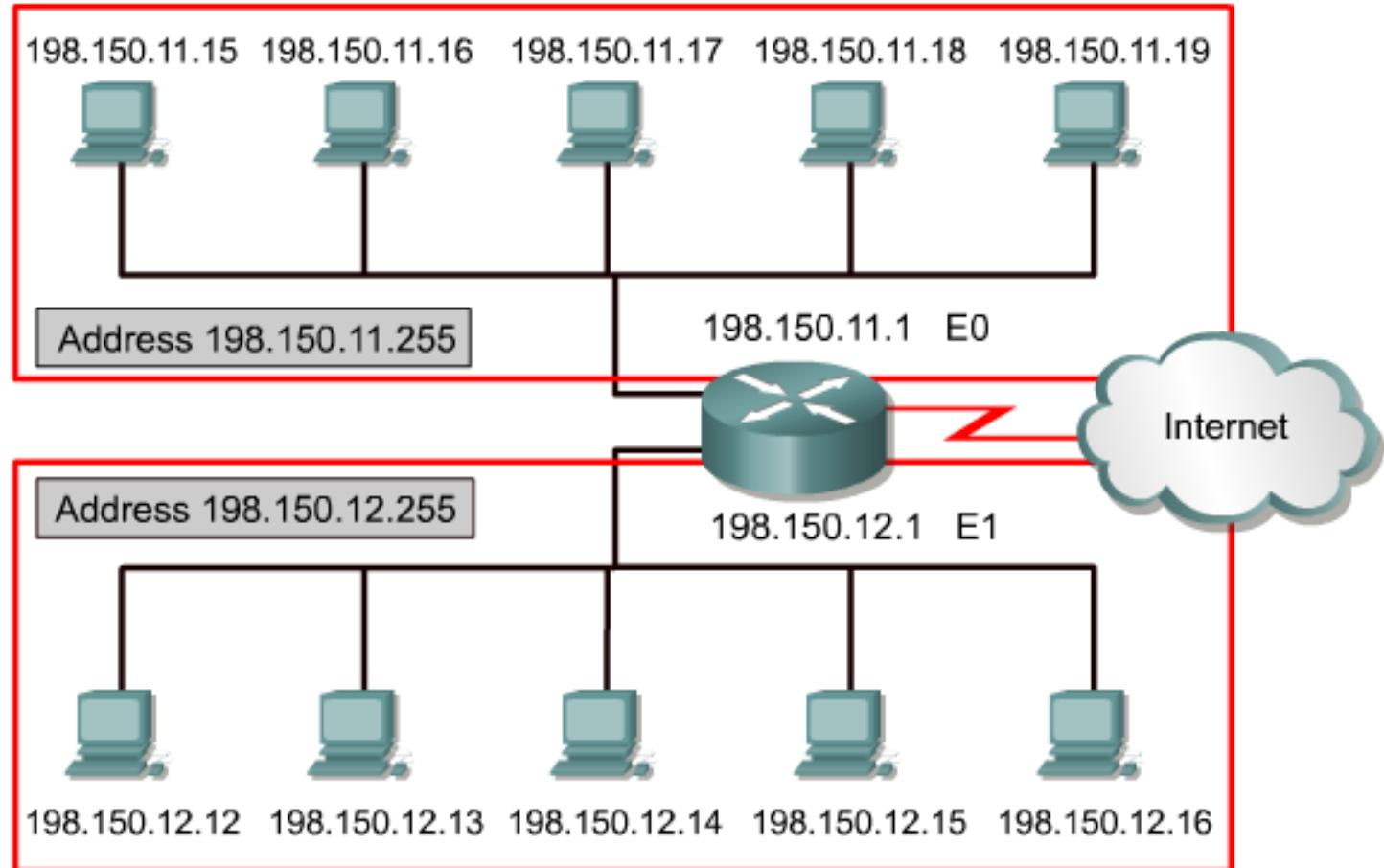
- ❖ Địa chỉ mạng (network address): là địa chỉ IP dùng để đặt cho các mạng. Phần host_id của địa chỉ chỉ chứa các bit 0. Ví dụ: 172.29.0.0
- ❖ Địa chỉ Broadcast: là địa chỉ IP được dùng để đại diện cho tất cả các host trong mạng. Phần host_id chỉ chứa các bit 1. Ví dụ: 172.29.255.255.

Địa chỉ mạng (network address)



Địa chỉ mạng

Địa chỉ Broadcast



Địa chỉ broadcast

CHIA MẠNG CON

❖ Tại sao phải chia mạng con

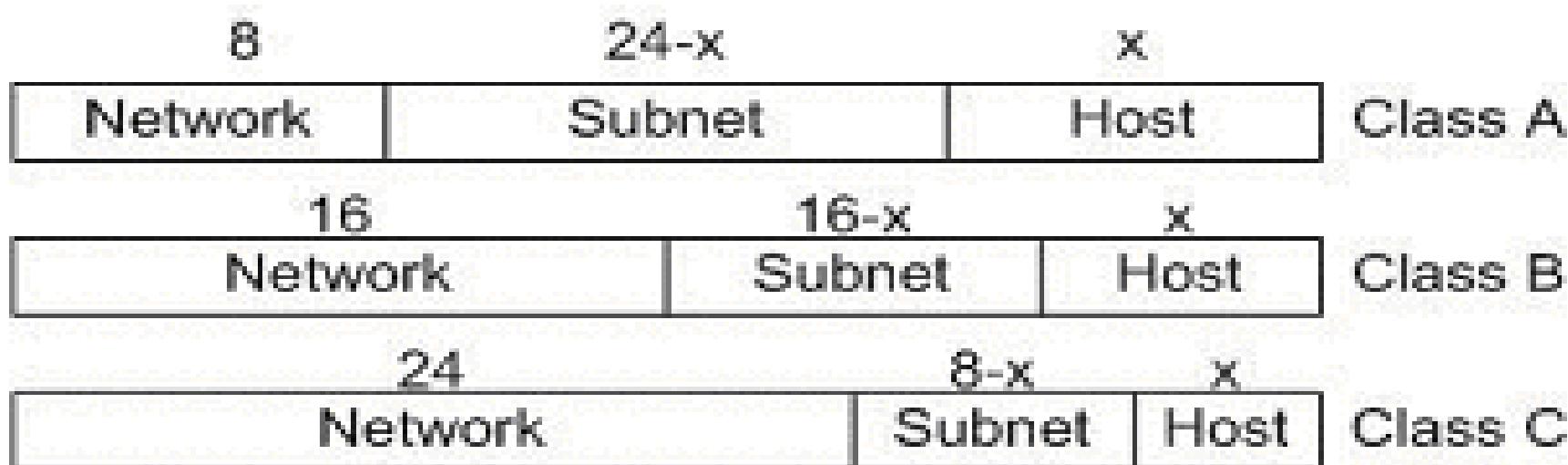
- Mỗi lớp mạng A có đến $2^{24} - 2 = 16.777.214$ địa chỉ IP hay lớp B có $2^{16} - 2 = 65534$ địa chỉ IP.
- Khó có hệ thống đạt số host quá lớn như vậy
- Khó khăn trong công tác quản lý.

Lợi ích khi chia mạng con

- Giảm nghẽn mạng bằng cách tái định hướng các giao vận và giới hạn phạm vi của các thông điệp quảng bá.
- Giới hạn trong phạm vi từng mạng con các trục trặc có thể xảy ra (không ảnh hưởng tới toàn mạng LAN).
- Giảm % thời gian sử dụng CPU do giảm lưu lượng của các giao vận quảng bá.
- Tăng cường bảo mật (các chính sách bảo mật có thể áp dụng cho từng mạng con)
- Cho phép áp dụng các cấu hình khác nhau trên từng 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 tuỳ 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 ($2^4>=12$).

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.

VÍ DỤ

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 thế 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

11111111.11111111.11100000.00000000

Subnet mask
với dạng thập phân

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. 000 00000.00000000	139.12.0.0/19
2	10001011.00001100. 001 00000.00000000	139.12.32.0/19
3	10001011.00001100. 010 00000.00000000	139.12.64.0/19
4	10001011.00001100. 011 00000.00000000	139.12.96.0/19
5	10001011.00001100. 100 00000.00000000	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

Ví dụ tính nhanh vùng địa chỉ IP

- ❖ Cho địa chỉ: 192.168.0.0/24 Chia thành 16 mạng con
- ❖ 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
-

Tính nhanh vùng địa chỉ IP

- ❖ n – số bit làm subnet
- ❖ Số mạng con: $S = 2^n$
- ❖ Số địa chỉ host trong 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 broadcast, ví dụ lớp C: $k*M - 1$ (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 $k=1,2,\dots$)

Kỹ thuật chia mạng con

192.168.1.0 - 255 /24
192.168.1.0 - 127 /25
192.168.1.128 - 255 /25

192.168.1.0000 0000
192.168.1.0000 0001
192.168.1.0000 0010
192.168.1.0000 0011
192.168.1.0000 0100
192.168.1.0000 0101
192.168.1.0000 0110
192.168.1.0111 1111

192.168.1.1000 0000
192.168.1.1000 0001
192.168.1.1000 0010
192.168.1.1000 0011
192.168.1.1000 0100
192.168.1.1000 0101
192.168.1.1000 0110
192.168.1.1111 1111

192.168.1.0 - 255 /24

192.168.1.0 - 63 /26

192.168.1.64 - 127 /26

192.168.1.128 - 191 /26

192.168.1.192 - 255 /26

192.168.1.0**0000** 0000
192.168.1.0**0000** 0001
192.168.1.0**0000** 0010
192.168.1.0000 0011

192.168.1.**0011** 1111

192.168.1.**0100** 0000
192.168.1.**0100** 0001
192.168.1.**0100** 0010
192.168.1.**0100** 0011

192.168.1.**0111** 1111

192.168.1.**1000** 0000
192.168.1.**1000** 0001
192.168.1.**1000** 0010
192.168.1.**1000** 0011

192.168.1.**1011** 1111

192.168.1.**1100** 0000
192.168.1.**1100** 0001
192.168.1.**1100** 0010
192.168.1.**1100** 0011

192.168.1.**1111** 1111

192.168.1.0 - 255 /24

192.168.1.0 - 31 /27

192.168.1.32 - 63 /27

192.168.1.64 - 95 /27

192.168.1.96 - 127 /27

192.168.1.128 - 159 /27

192.168.1.160 - 191 /27

192.168.1.192 - 223 /27

192.168.1.224 - 255 /27

192.168.1.**0000** 0000
192.168.1.**0001** 1111

192.168.1.**0010** 0000
192.168.1.**0011** 1111

192.168.1.**0100** 0000
192.168.1.**0101** 1111

192.168.1.**0110** 0000
192.168.1.**0111** 1111

192.168.1.**1000** 0000
192.168.1.**1001** 1111

192.168.1.**1010** 0000
192.168.1.**1011** 1111

192.168.1.**1100** 0000
192.168.1.**1101** 1111

192.168.1.**1110** 0000
192.168.1.**1111** 1111

Kỹ thuật chia mạng con

192.168.1.0 - 255 /24

192.168.1.0 - 15 /28

192.168.1.16 - 31 /28

192.168.1.32 - 47 /28

192.168.1.48 - 63 /28

192.168.1.0000 0000

192.168.1.0001 0000

192.168.1.0010 0000

192.168.1.0011 0000

192.168.1.64 - 79 /28

192.168.1.80 - 95 /28

192.168.1.96 - 111 /28

192.168.1.112 - 127 /28

192.168.1.0100 0000

192.168.1.0101 0000

192.168.1.0110 0000

192.168.1.0111 0000

192.168.1.128 - 159 /28

192.168.1.144 - 191 /28

192.168.1.160 - 223 /28

192.168.1.176 - 223 /28

192.168.1.1000 0000

192.168.1.1001 0000

192.168.1.1010 0000

192.168.1.1011 0000

192.168.1.192 - 255 /28

192.168.1.208 - 255 /28

192.168.1.224 - 255 /28

192.168.1.240 - 255 /28

192.168.1.1100 0000

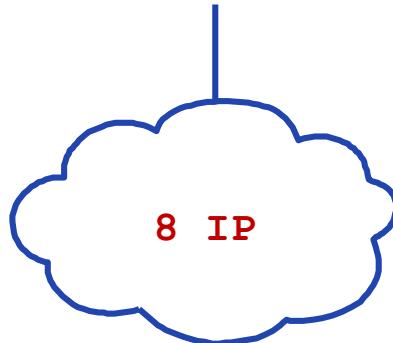
192.168.1.1101 0000

192.168.1.1110 0000

192.168.1.1111 0000

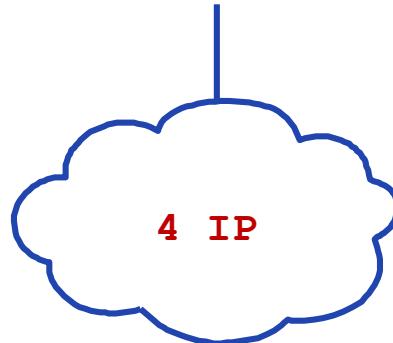
Kỹ thuật chia mạng con

192.168.1.0/29



192.168.1.0000	0000	/ 29
192.168.1.0000	0001	/ 29
192.168.1.0000	0010	/ 29
192.168.1.0000	0011	/ 29
192.168.1.0000	0100	/ 29
192.168.1.0000	0101	/ 29
192.168.1.0000	0110	/ 29
192.168.1.0000	0111	/ 29

192.168.1.0/30



192.168.1.0000	0000	/ 30
192.168.1.0000	0001	/ 30
192.168.1.0000	0010	/ 30
192.168.1.0000	0011	/ 30

Kỹ thuật chia mạng con

Subnet	Network	Host
192.168.1.0 0000000 /25	2 mạng	128 IP
192.168.1.00 000000 /26	4 mạng	64 IP
192.168.1.000 00000 /27	8 mạng	32 IP
192.168.1.0000 0000 /28	16 mạng	16 IP
192.168.1.00000 000 /29	32 mạng	8 IP
192.168.1.000000 00 /30	64 mạng	4 IP
192.168.1.0000000 0 /30	128 mạng	2 IP

	/24	/25	/26	/27	/28
172.16.0.0	0-255	0-127	0-63	0-31	0-15
		128-255	64-127	32-63	16-31
			128-191	64-95	32-47
			192-255	96-127	48-63
				128-159	64-79
				160-191	80-95
				192-223	96-111
				224-255	112-127
					128-143
					144-159
					160-175
					176-191
					192-207
					208-223
					224-239
					240-255

Ví dụ 2

Xác định địa chỉ mạng, địa chỉ Broadcast và dải địa chỉ của mạng sau: **172.16.0. 122 /26**

B1: Chuyển địa chỉ IP và Subnet Mask về dạng nhị phân và thực hiện phép tính IP and Subnet Mask.

	172	16	0	122
IP	10101100	00001000	00000000	01111010
Subnet mask	11111111	11111111	11111111	11000000
Kết quả AND	10101100	00001000	00000000	01000000

B2: Xác định Network_Id và Host_Id, dải host.

Kết quả AND	10101100	00001000	00000000	01000000
Network_Id	172	16	0	64
Host_Id				58
Host đầu	172	16	0	65
Host cuối	172	16	0	126
Broadcast	172	16	0	127

Ví dụ 3

Xác định địa chỉ mạng, địa chỉ Broadcast và dải đại chỉ của mạng sau:

172.16.0.200 /27

172.16.0. 192 (Network Address)

172.16.0. 193

172.16.0. 194

172.16.0. 223 (Broadcast Address)

Ví dụ 4

172.16.0. 50 /28

172.16.0. 48 (Network Address)

172.16.0. 49

172.16.0. 50

172.16.0. 63 (Broadcast Address)

CHƯƠNG 1: TỔNG QUAN VỀ MẠNG

1

- Giới thiệu về quản trị mạng

2

- Mô hình OSI và TCP/IP

3

- Địa chỉ IPv4

4

- Địa chỉ IPv6

5

- Chuyển đổi IPv4-IPv6

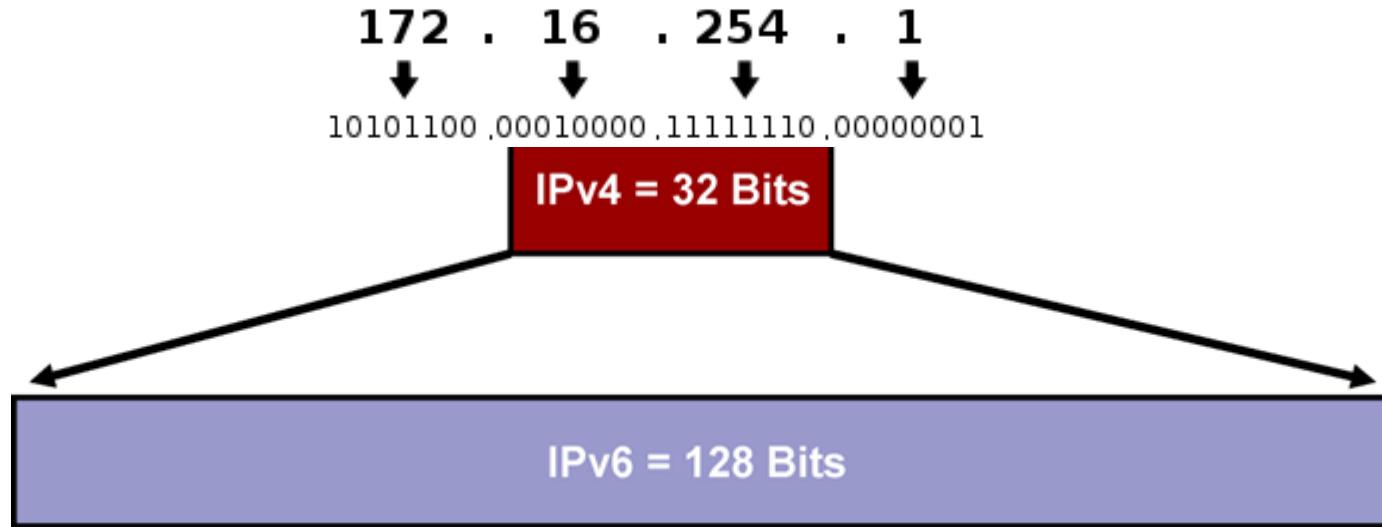
6

- Cấu hình cơ bản thiết bị mạng

NHỮNG HẠN CHẾ CỦA IPv4

- ❖ Sự thiếu hụt địa chỉ
- ❖ Cấu trúc định tuyến không hiệu quả
- ❖ Hạn chế tính bảo mật và kết nối đầu cuối – đầu cuối

Tổng quan về IPv6



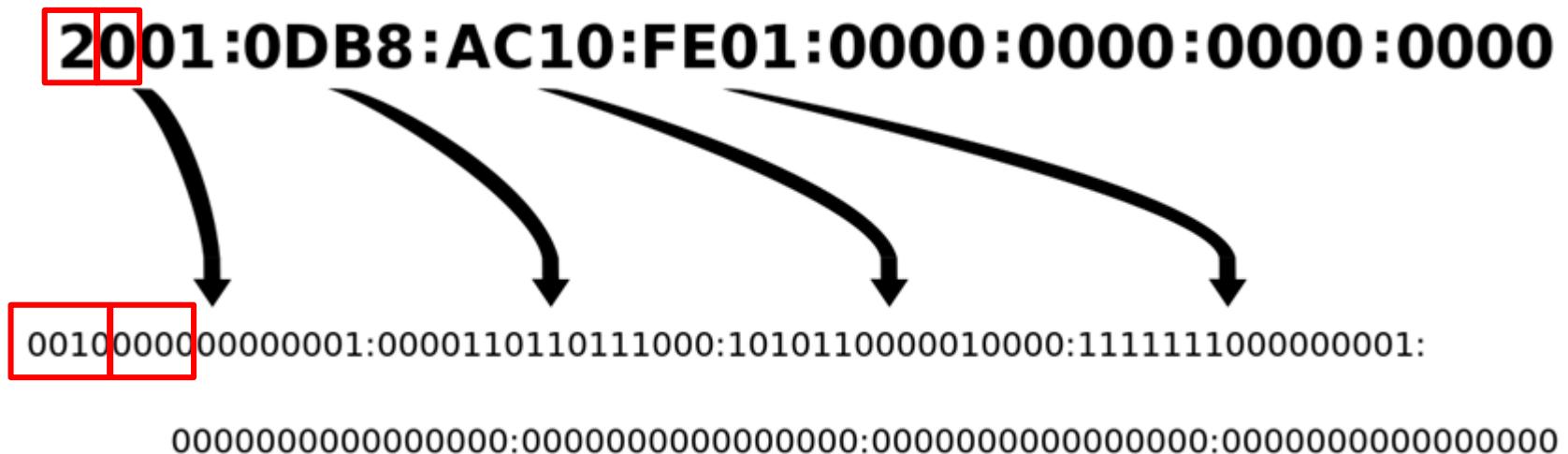
IPv4

- 32 bits chia làm 4 octat, mỗi octat 1 bytes
 $\approx 4,200,000,000$ địa chỉ

IPv6

- 128 bits or 16 bytes: số bít gấp 4 lần IPv4
 $\approx 3.4 * 10^{38}$ địa chỉ
 $\approx 340,282,366,920,938,463,374,607,432,768,211,456$
 $\approx 5 * 10^{28}$ địa chỉ cho một người

Biểu diễn địa chỉ IPv6



Decimal	Hexadecimal	Binary
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Biểu diễn địa chỉ IPv6

Rút gọn địa chỉ IPv6

- ❖ Đối với nhóm có số 0 phía bên trái thì bỏ đi
- ❖ Đối với nhóm toàn số 0 có thể rút gọn ::,
nhưng chỉ rút gọn 1 nhóm

2001:0ABC:00AB:000A:0000:0000:0000:1001

2001:ABC:AB:A:0:0:0:1001 :: 0: 0: 0:1001

2001:ABC:AB:A::1001

Hãy chọn cách viết đúng địa chỉ IPv6

2001:0000:0000:0ABC:00AB:0000:0000:1001

- a. **2001::ABC:AB::1001**
- b. **2001::ABC:AB:0:0:1001**
- c. **2001:0:0:ABC:AB:0:0:1001**
- d. **2001:0:0:ABC:AB::1001**

Cấu trúc IPv6

32-bit IPv4 address

YYY	YYY	YYY	YYY
-----	-----	-----	-----

YYY = 8 bits

128-bit IPv6 address



XXXX							
------	------	------	------	------	------	------	------

XXXX = 16 bits

TIÊU ĐỀ ĐỊA CHỈ IP

IPv4 Header

Version	IHL	Type of Service	Total Length	
Identification		Flags	Fragment Offset	
Time to Live	Protocol	Header Checksum		
Source Address				Destination Address
Options		Padding		

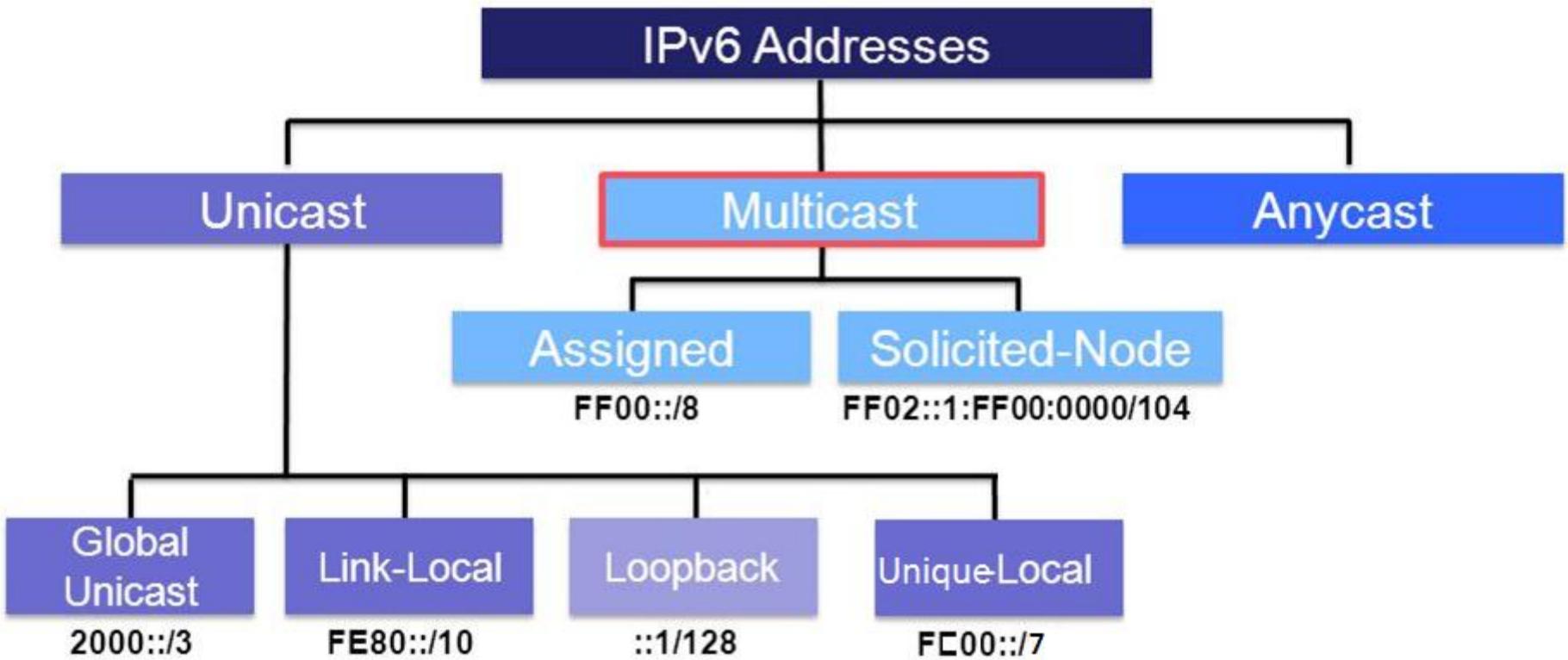
IPv6 Header

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			Destination Address

Legend

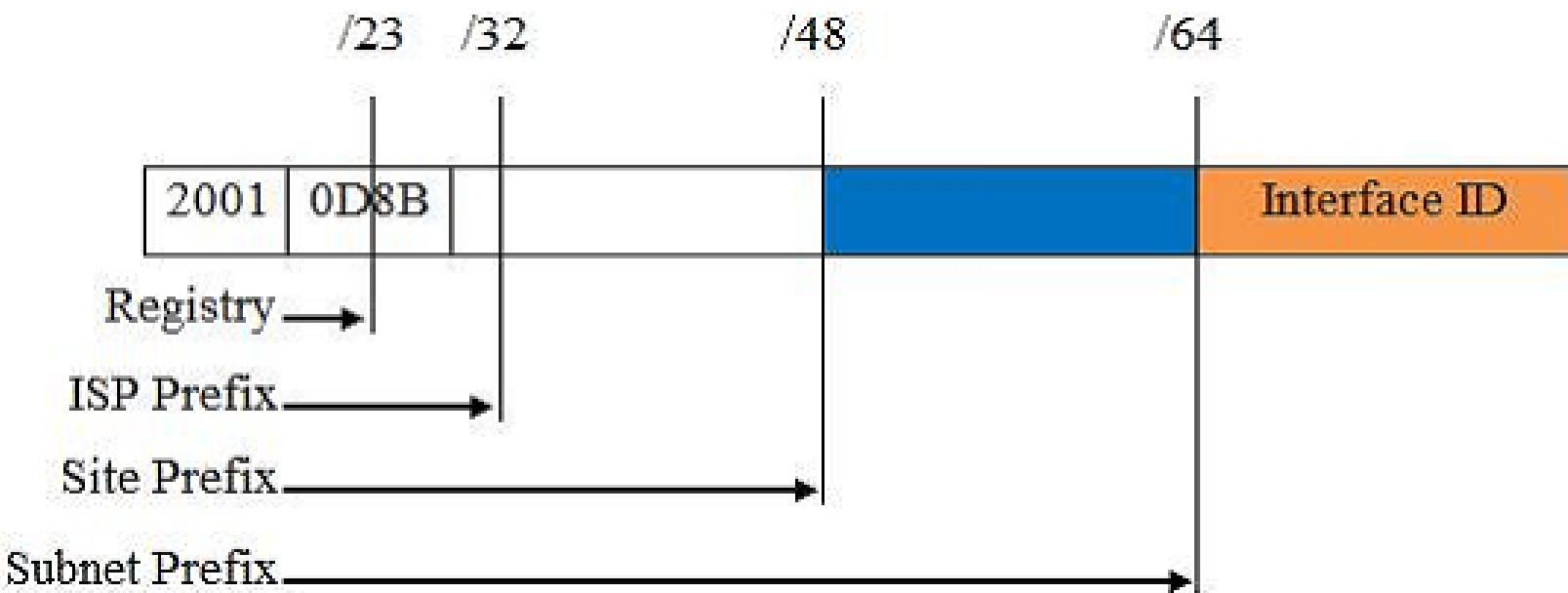
- Field's Name Kept from IPv4 to IPv6
- Fields Not Kept in IPv6
- Name and Position Changed in IPv6
- New Field in IPv6

Phân loại IPv6



IPv6 không có địa chỉ Broadcast

IPv6: Global Unicast Address (2000::/3)



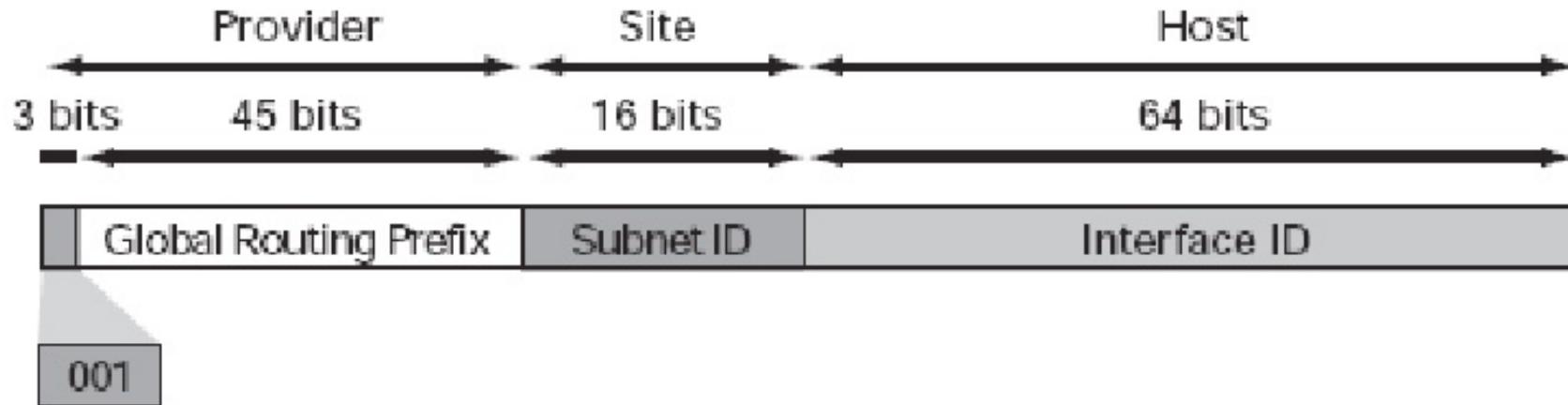
Registry: Định danh các vùng

ISP Prefix: Định danh các nhà cung cấp dịch vụ

Site Prefix: định danh các doanh nghiệp Tổ chức

Subnet Prefix: Định danh mạng nhỏ hơn trong doanh nghiệp tổ chức

IPv6: Global Unicast Address (2000::/3)



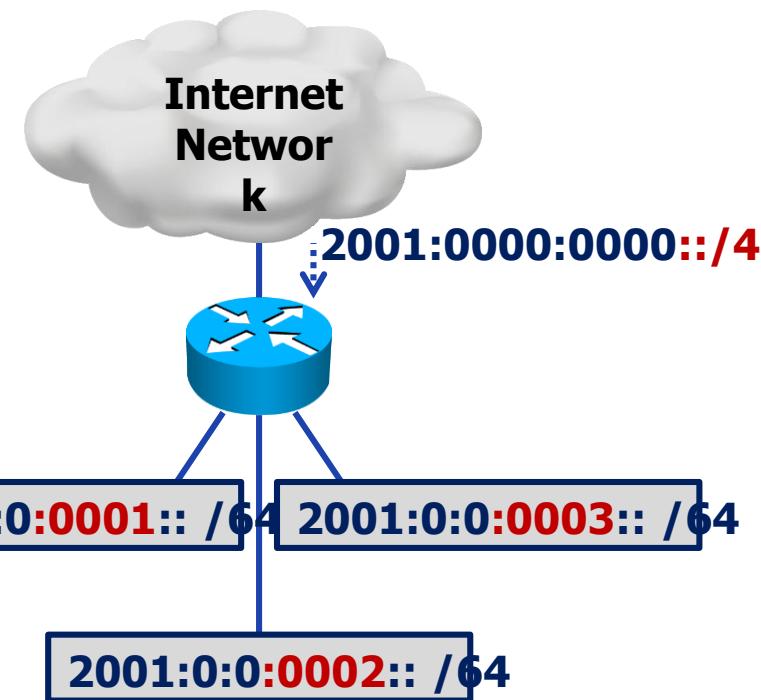
2001:0000:0000::/48

2001:0000:0000:0001:: /64

2001:0000:0000:0002:: /64

2001:0000:0000:0003:: /64

2001:0000:0000:XXXX:: /64



IPv6: Multicast Address

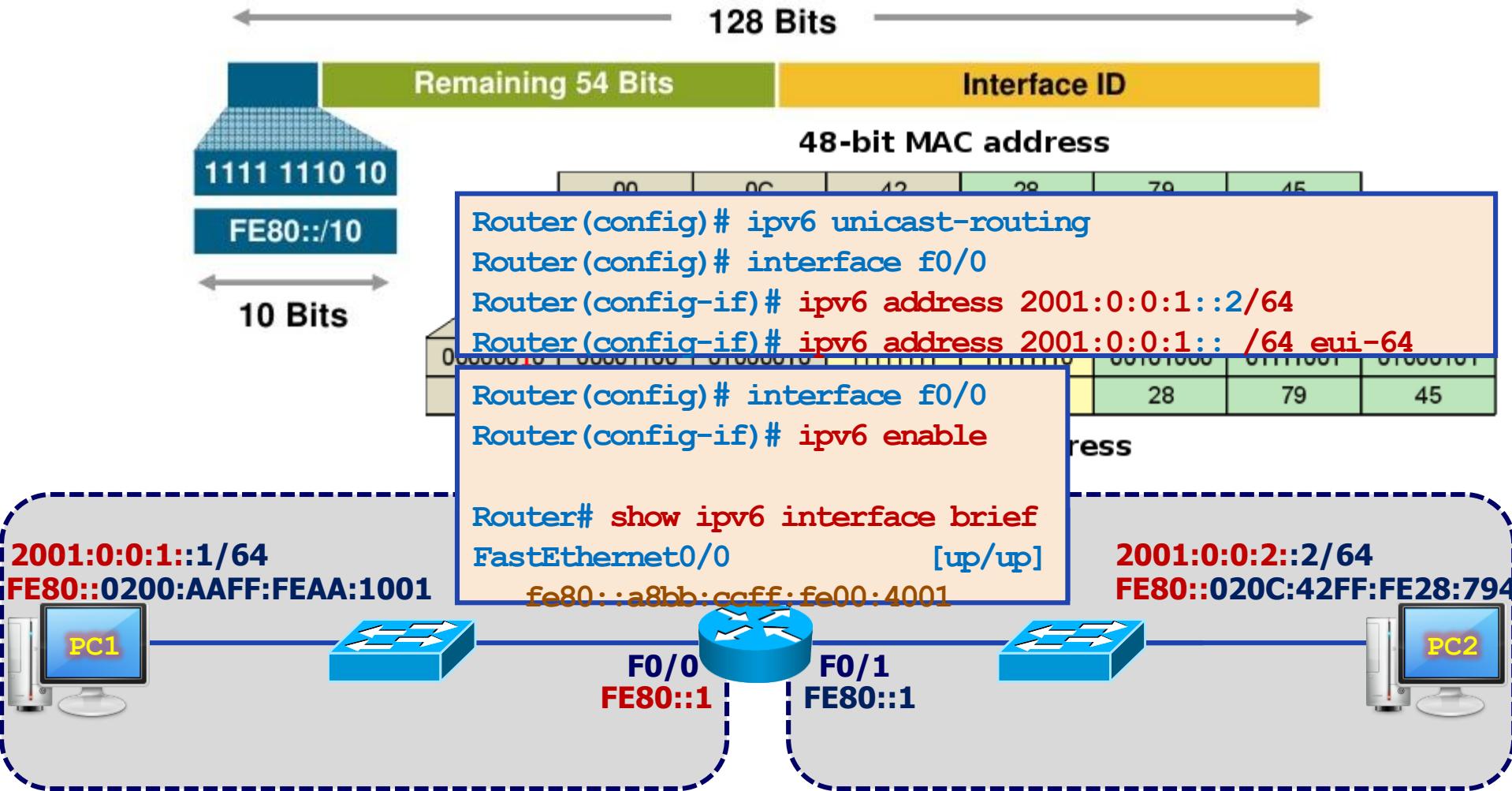
IPv6

Address(s)	Description
FF02:0:0:0:0:0:1	All Nodes Address
FF02:0:0:0:0:0:2	All Routers Address
FF02:0:0:0:0:0:3	Unassigned
FF02:0:0:0:0:0:4	DVMRP Routers
FF02:0:0:0:0:0:5	OSPFIGP
FF02:0:0:0:0:0:6	OSPFIGP Designated Routers
FF02:0:0:0:0:0:7	ST Routers
FF02:0:0:0:0:0:8	ST Hosts
FF02:0:0:0:0:0:9	RIP Routers
FF02:0:0:0:0:0:10	EIGRP Routers
FF02:0:0:0:0:0:11	Mobile-Agents
FF02:0:0:0:0:0:12	SSDP
FF02:0:0:0:0:0:13	All PIM Routers
FF02:0:0:0:0:0:14	RSVP-ENCAPSULATION

IPv4

Address(es)	Description
224.0.0.0	Base Address (Reserved)
224.0.0.1	All Systems on this Subnet
224.0.0.2	All Routers on this Subnet
224.0.0.3	Unassigned
224.0.0.4	DVMRP Routers
224.0.0.5	OSPFIGP OSPFIGP All Routers
224.0.0.6	OSPFIGP OSPFIGP Designated Routers
224.0.0.7	ST Routers
224.0.0.8	ST Hosts
224.0.0.9	RIP2 Routers
224.0.0.10	IIGRP Routers
224.0.0.11	Mobile-Agents
224.0.0.12	DHCP Server / Relay Agent
224.0.0.13	All PIM Routers
224.0.0.14	RSVP-ENCAPSULATION

IPv6: Link-Local Address



IPv6: Link-Local Address



```
C:\Users\Admin>ipconfig
```

```
Windows IP Configuration
```

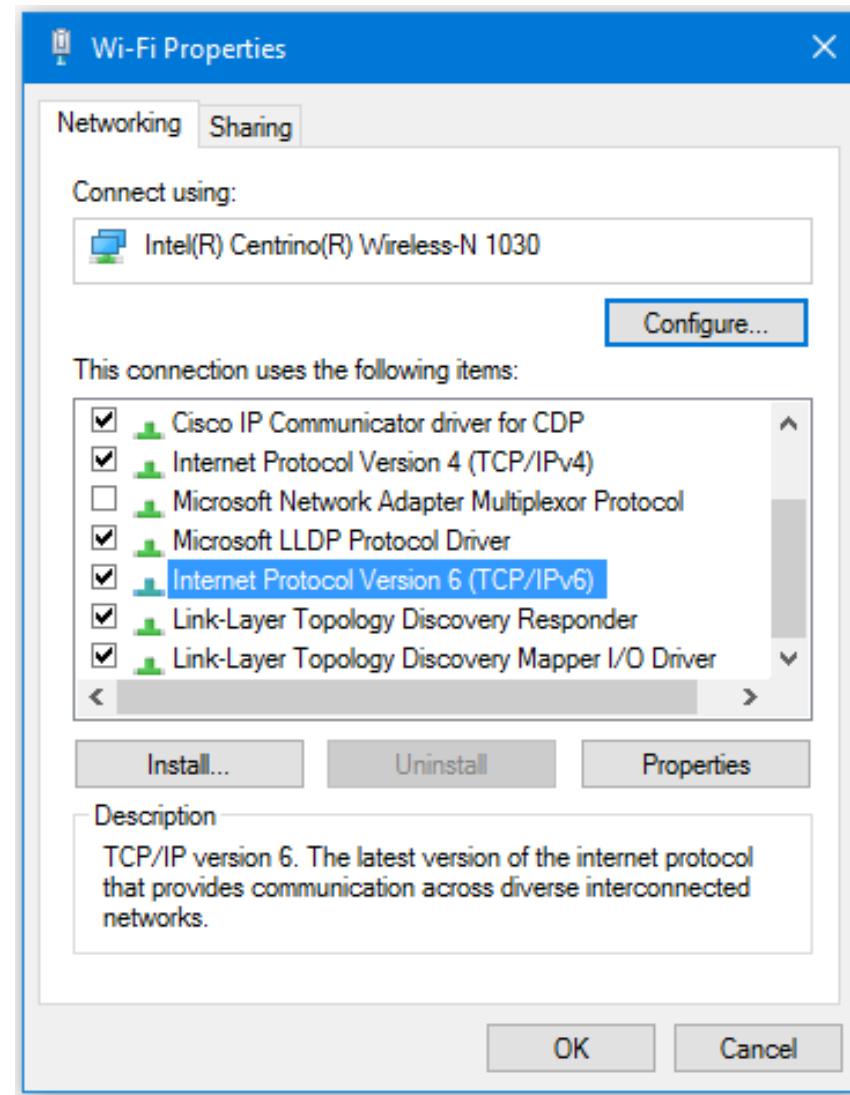
```
Ethernet adapter Local Area Connection:
```

Connection-specific DNS Suffix	:	
IPv6 Address	:	fcab:bebc:abac:100::1000
Link-local IPv6 Address	:	fe80::88c2:66c3:3049:1172%10
IPv4 Address	:	192.168.1.145
Subnet Mask	:	255.255.255.0
Default Gateway	:	192.168.1.1

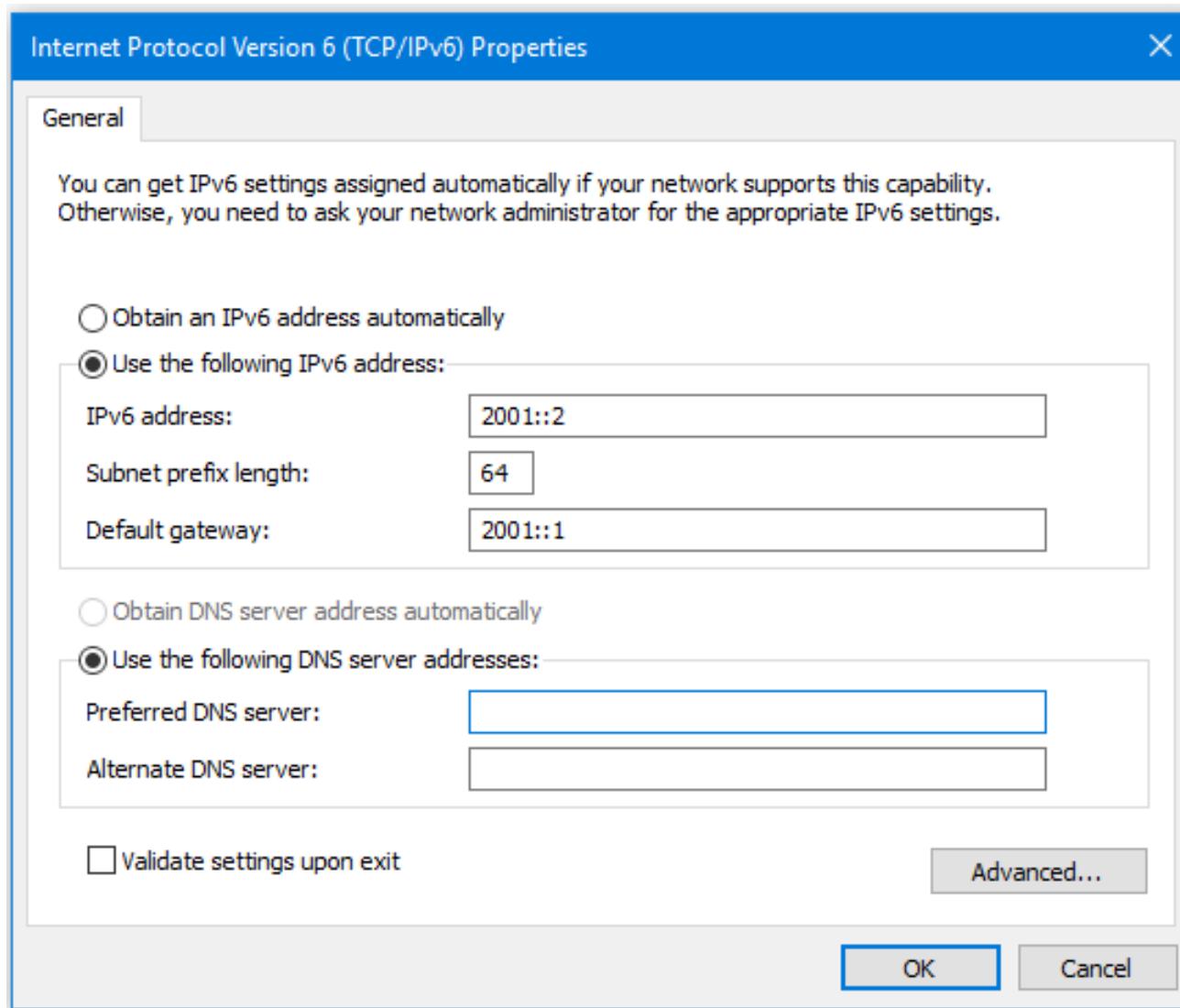
Địa chỉ anycast

- Địa chỉ anycast địa chỉ được gán cho một nhóm các host/interface không cùng trên một node mạng.
- Khi một gói tin được gửi đến địa chỉ anycast, nó sẽ được gửi đến host/interface gần nhất.
- Địa chỉ anycast đó địa chỉ anycast giống địa chỉ unicast.
- Trong gói tin IPv6 thì địa chỉ unicast không được sử dụng trong trường source address.

IPv6: Configuring Address



IPv6: Configuring Address



CHƯƠNG 1: TỔNG QUAN VỀ MẠNG

1

- Giới thiệu về quản trị mạng

2

- Mô hình ISO và TCP/IP

3

- Địa chỉ IPv4

4

- Địa chỉ IPv6

5

- Chuyển đổi IPv4-IPv6

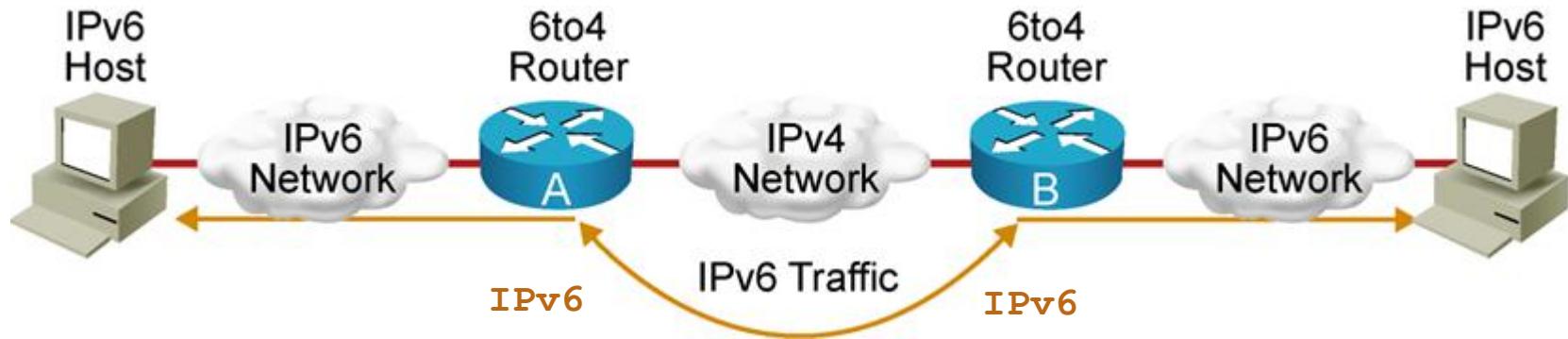
6

- Cấu hình cơ bản thiết bị mạng

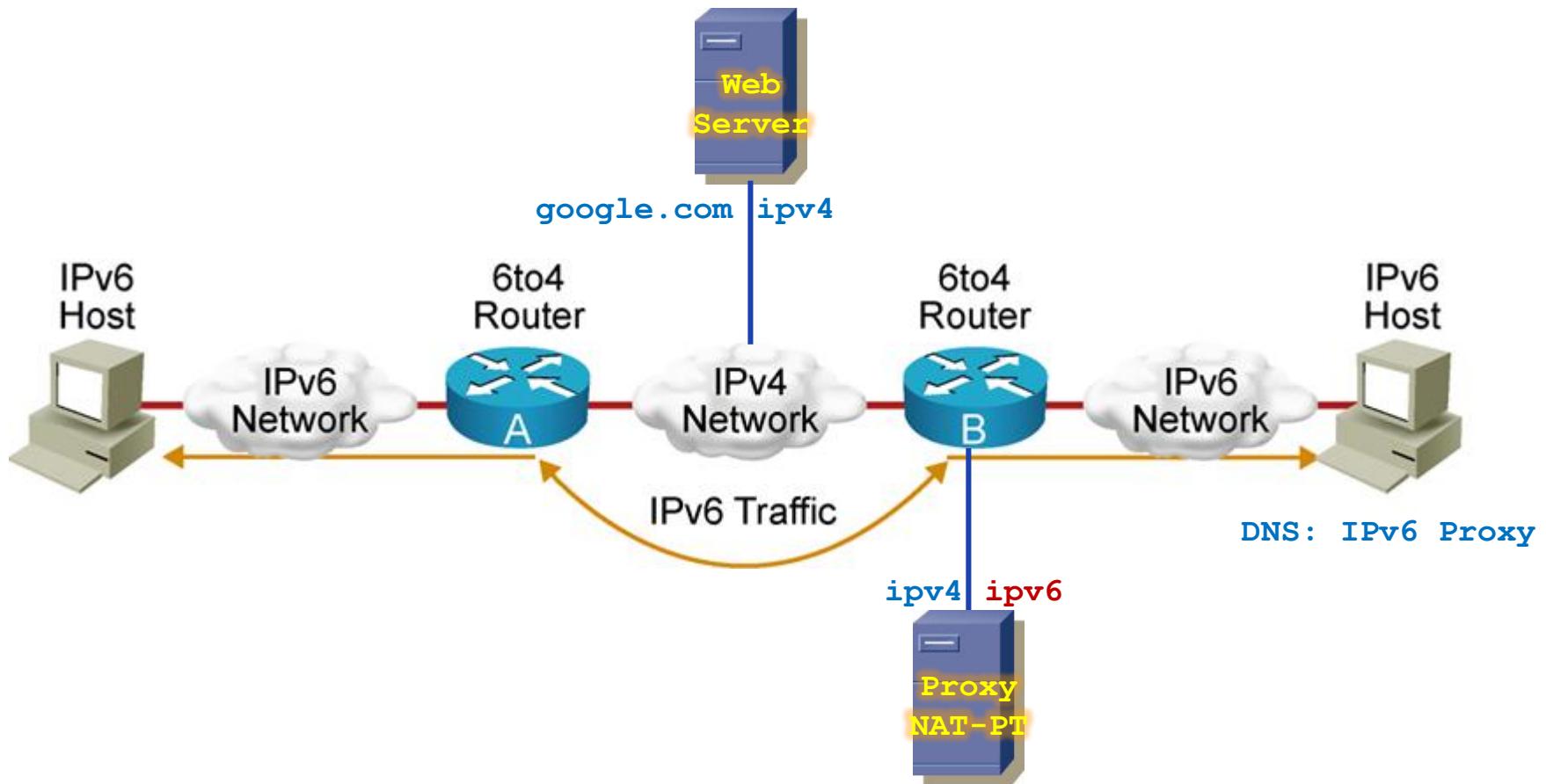
CHUYỂN ĐỔI IPv4-to-IPv6

- ❖ Các phương pháp chuyển đổi IPv4-to-IPv6:
 - Phương pháp đường hầm:
 - Manual tunnel
 - 6to4 tunnel
 - NAT-PT
 - Dual stack
- ❖ Dual stack: Các thiết bị mạng chạy song song giao thức IPv4 và IPv6.

ĐƯỜNG HÀM TUNNEL



NAT-PT (Proxying & Translation)



CHƯƠNG 1: TỔNG QUAN VỀ MẠNG

1

- Giới thiệu về quản trị mạng

2

- Mô hình OSI và TCP/IP

3

- Địa chỉ IPv4

4

- Địa chỉ IPv6

5

- Chuyển đổi IPv4-IPv6

6

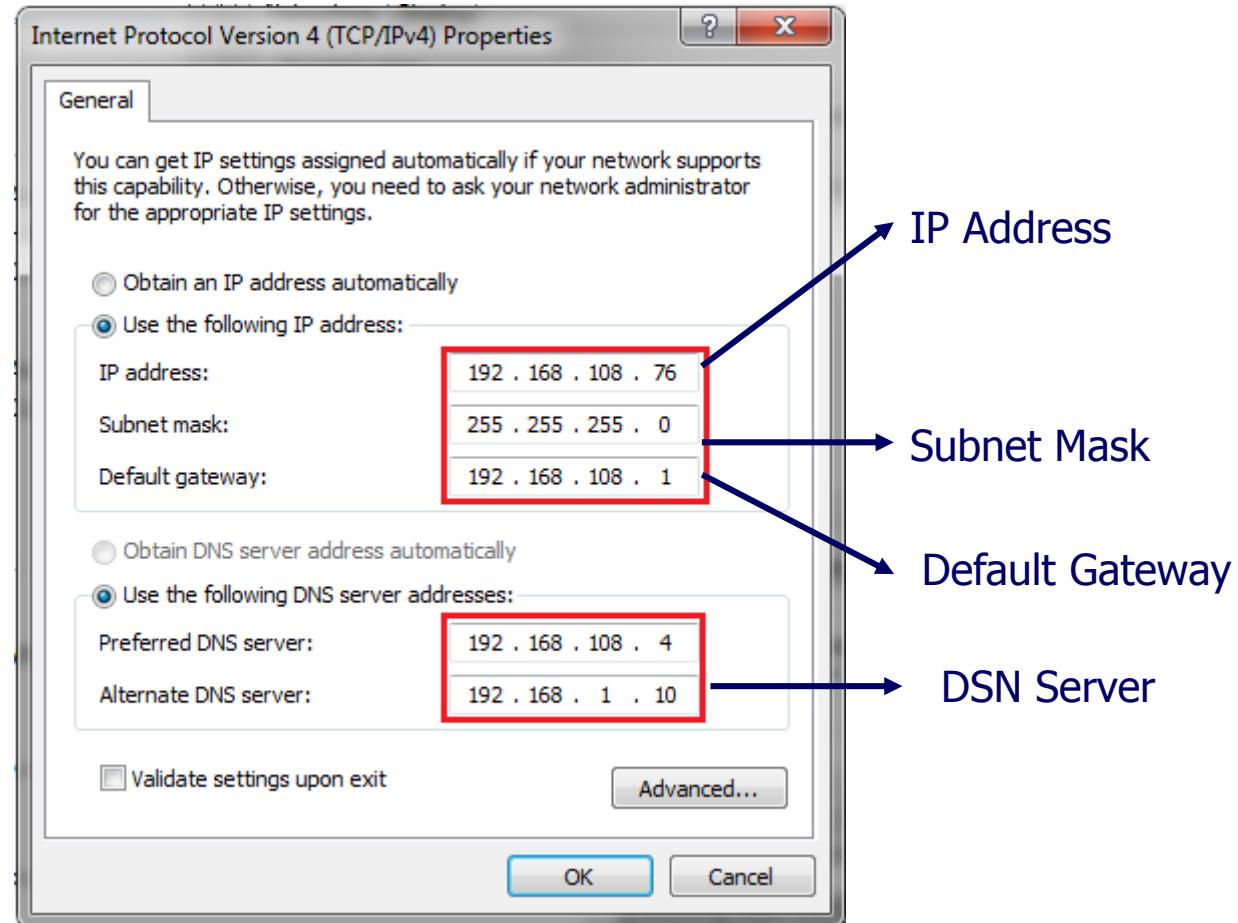
- Cấu hình cơ bản thiết bị mạng

CẤU HÌNH MẠNG

- ❖ Sau khi đã thiết lập mạng, hay nói cách khác là đã thiết lập nối kết về phần cứng giữa thiết bị trung tâm và nút thì các nút vẫn chưa thể thông tin với nhau được.
- ❖ Để giữa các nút có thể thông tin với nhau được thì yêu cầu phải thiết lập các nút (các máy tính, Switch, Router ...) trong LAN theo một chuẩn nhất định (Giao thức – Protocol).
- ❖ Các máy tính trong mạng thường sử dụng hệ điều hành của Microsoft và sử dụng giao thức TCP/IP (Transmission control protocol/ internet protocol).

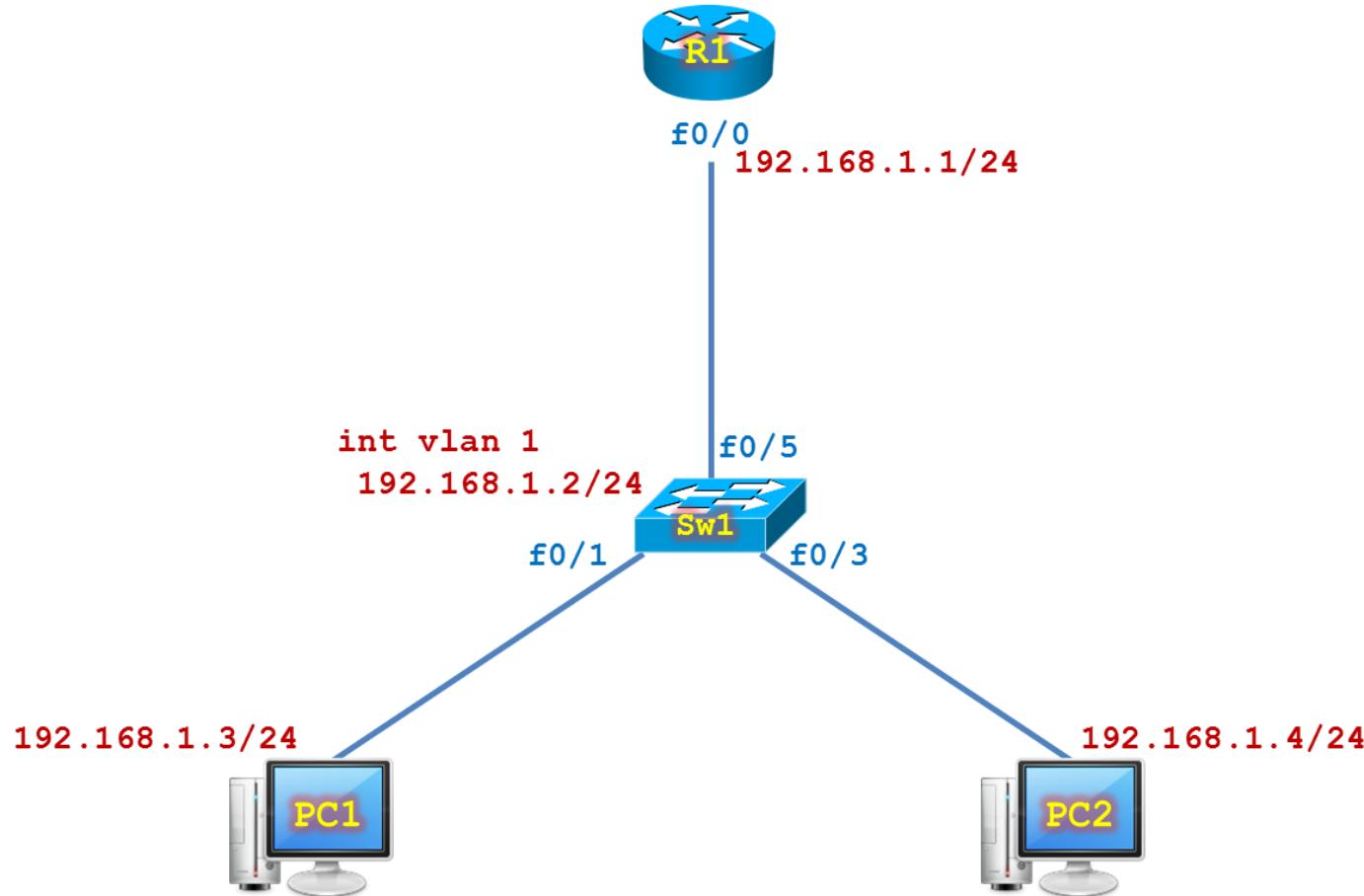
CẤU HÌNH MẠNG

❖ Cài đặt TCP/IP: Để cài đặt TCP/IP cho máy tính:



CẤU HÌNH MẠNG

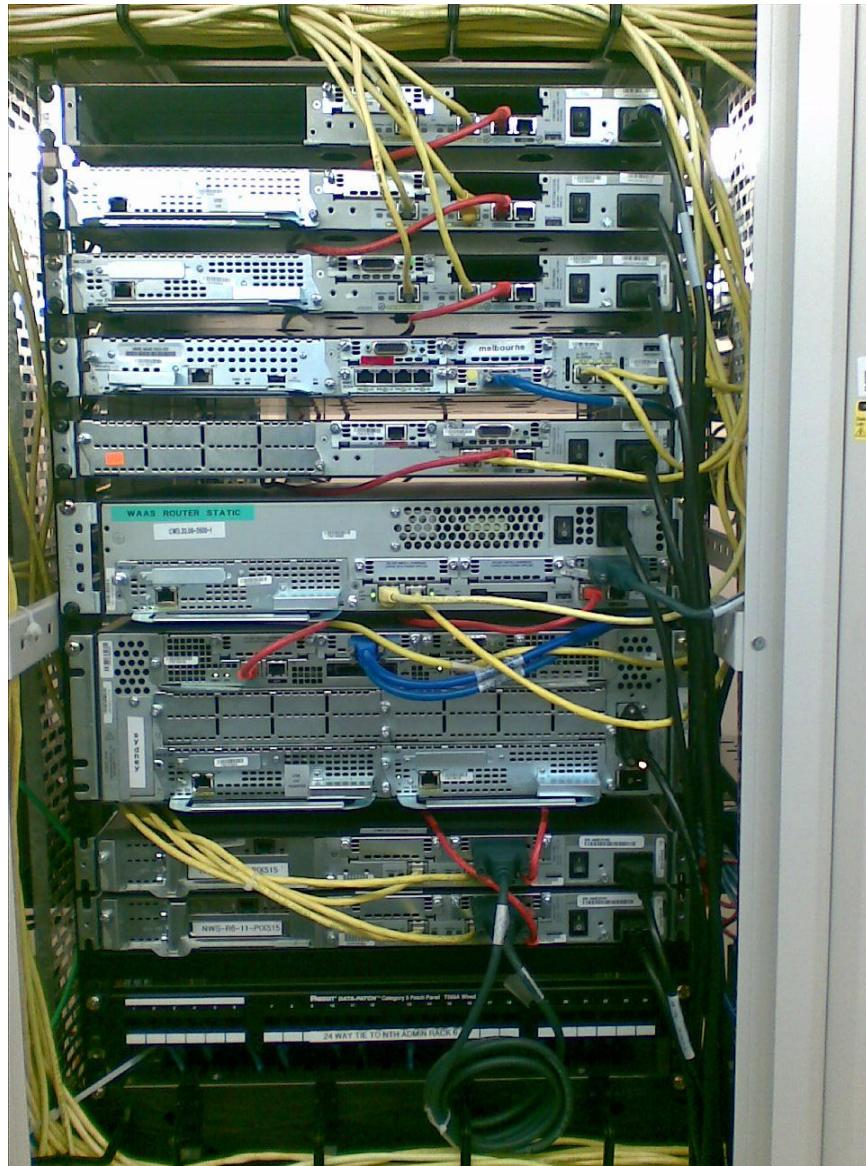
❖ Cấu hình thiết bị mạng: Router, Switch



CẤU HÌNH MẠNG

❖ Cấu hình thiết bị mạng: Router, Switch

- Đặt địa chỉ IP cho các Interface
- Đặt hostname cho Router, Switch.
- Cấu hình password.
- Thiết lập giao thức định tuyến.
- Thiết lập các dịch vụ DNS, DHCP
- ...



CÁC THÀNH PHẦN CỦA ROUTER



Power-On Self-test

Mini IOS used to ROM Monitor > recovery password, upgrade IOS

CÁP CONSOLE CẤU HÌNH

HyperTerminal
CRT
Putty



Console
Rollover
Null-modem

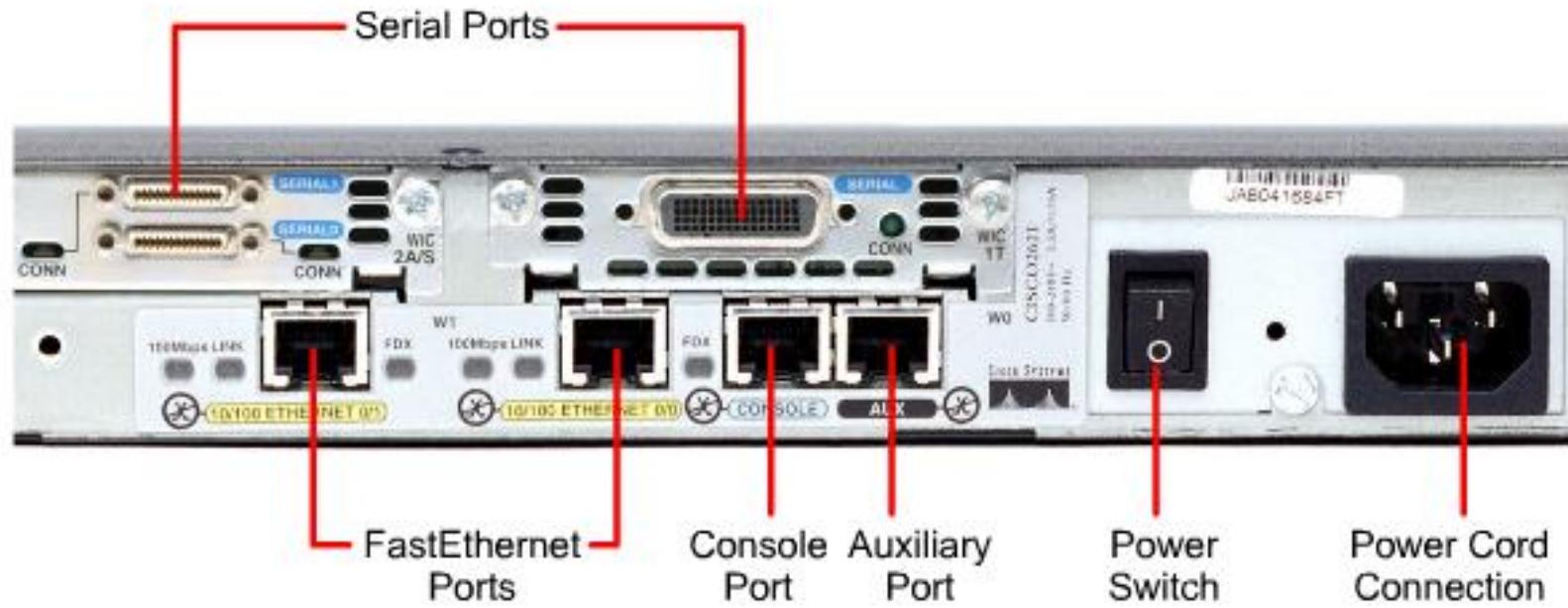


RJ-45
CONSOLE

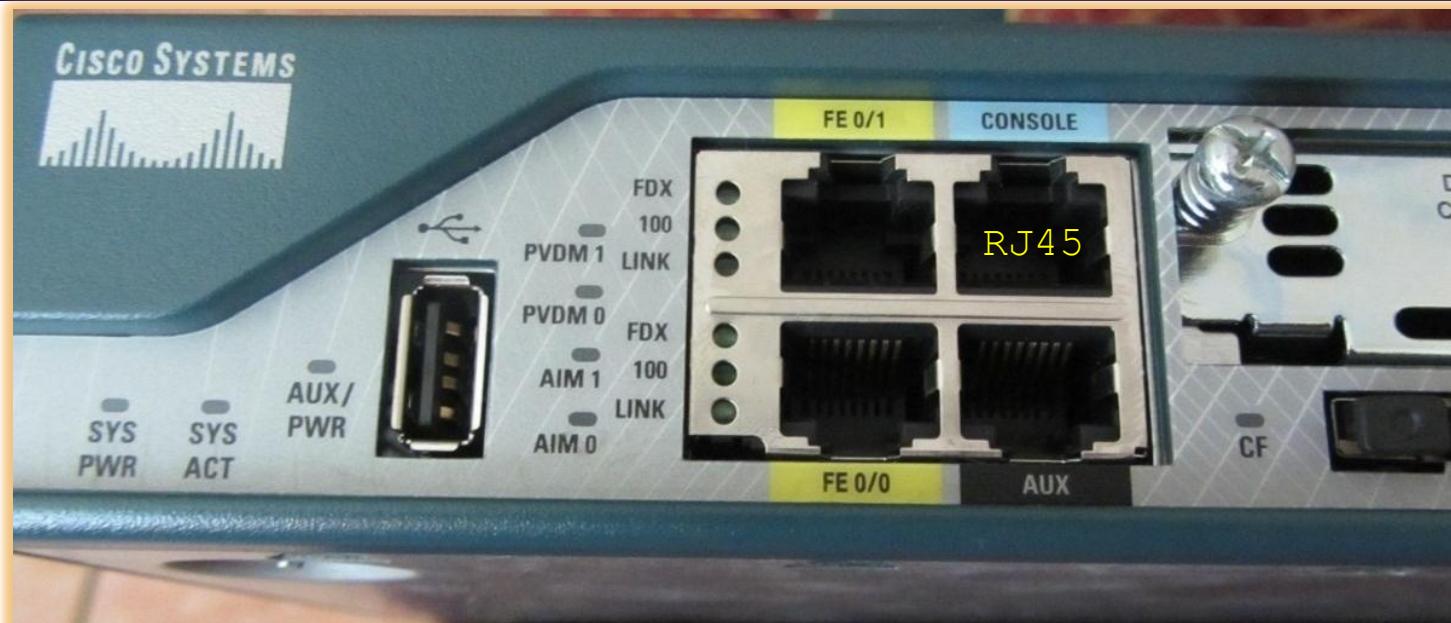


Start → Program → Accessories → Communication → HyperTerminal

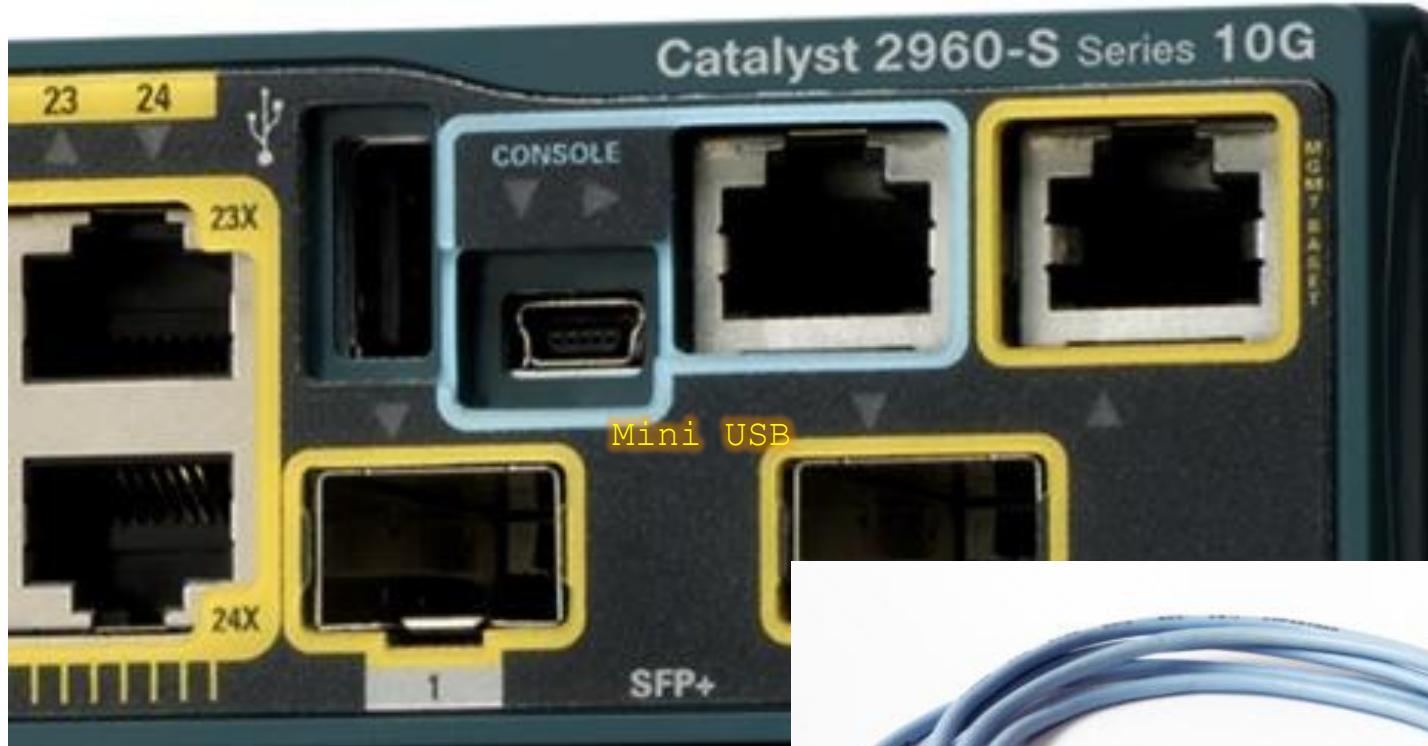
CÔNG KẾT NỐI CỦA ROUTER



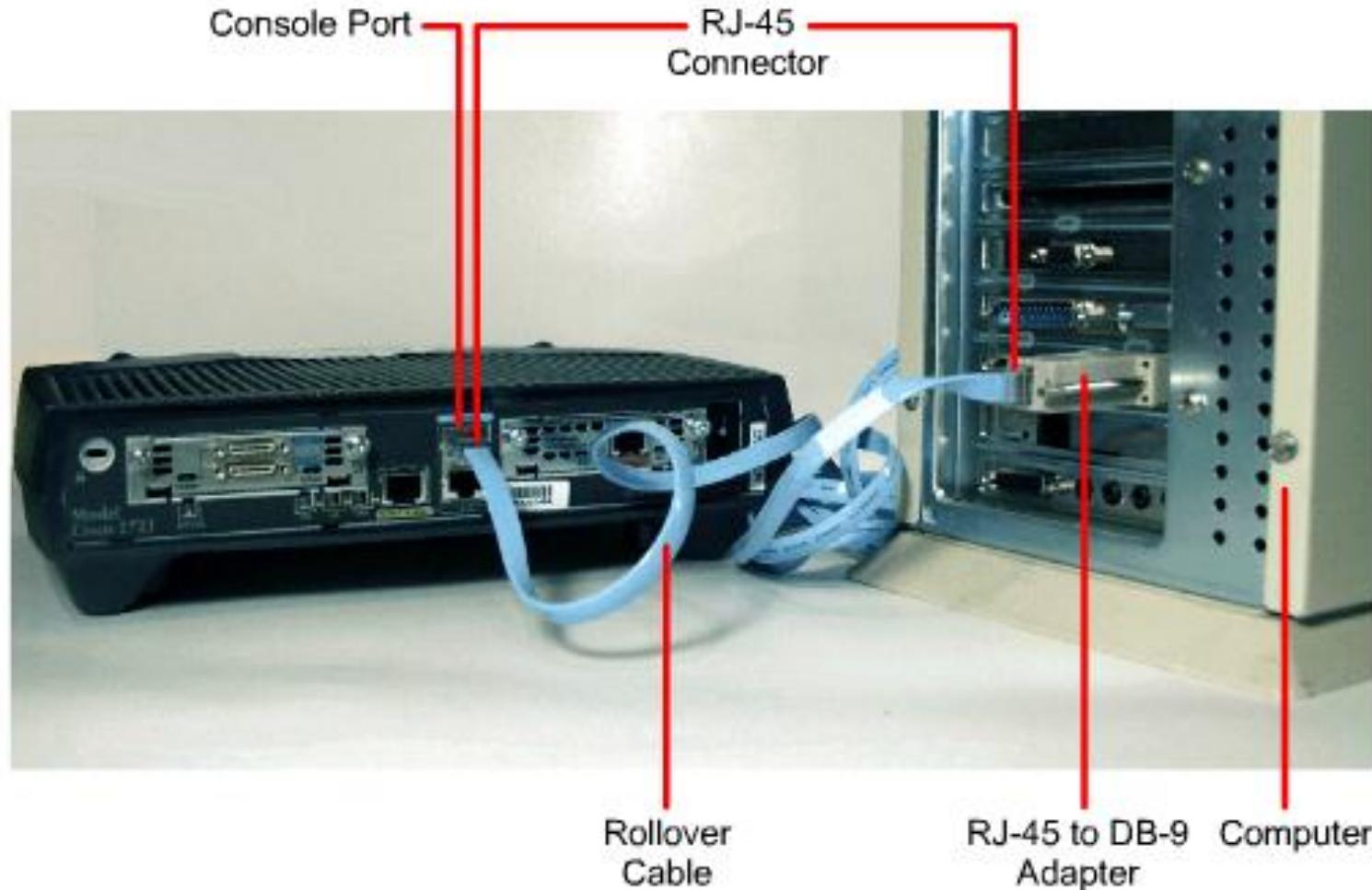
CÔNG KẾT NỐI



CÔNG KẾT NỐI



KẾT NỐI CẤU HÌNH ROUTER



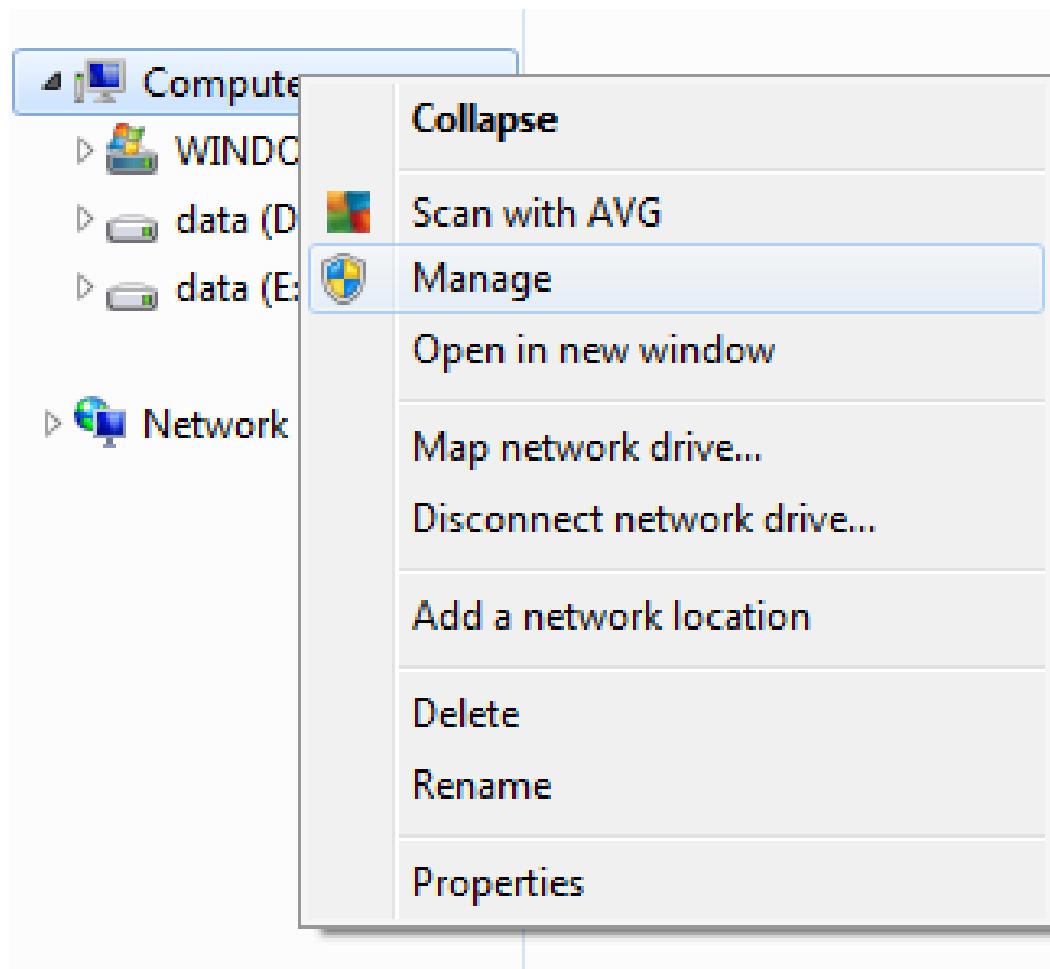
CẤU HÌNH ROUTER DÙNG HYPER TERMINAL



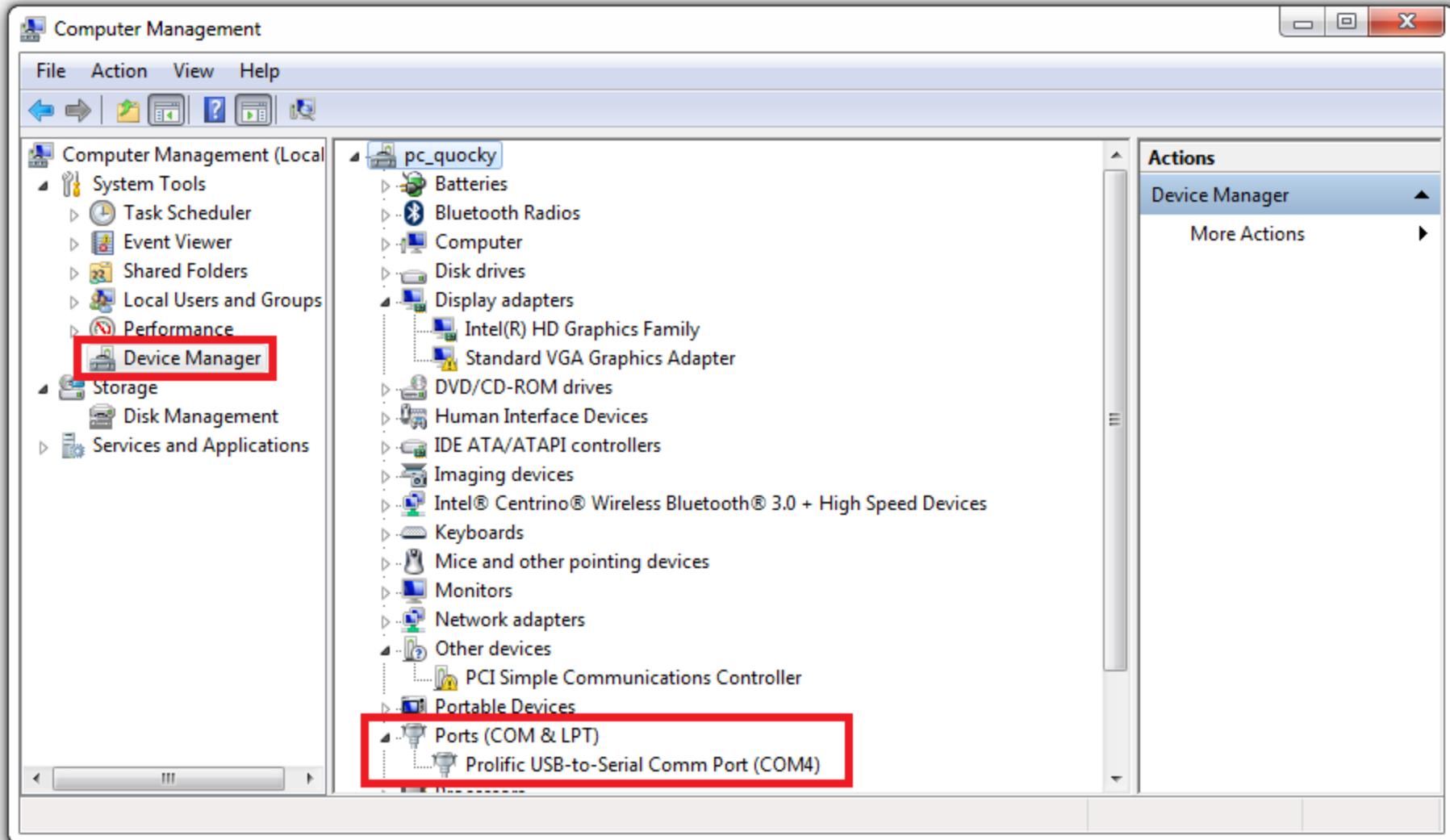
CẤU HÌNH ROUTER DÙNG HYPER TERMINAL



XEM CÔNG KẾT NỐI



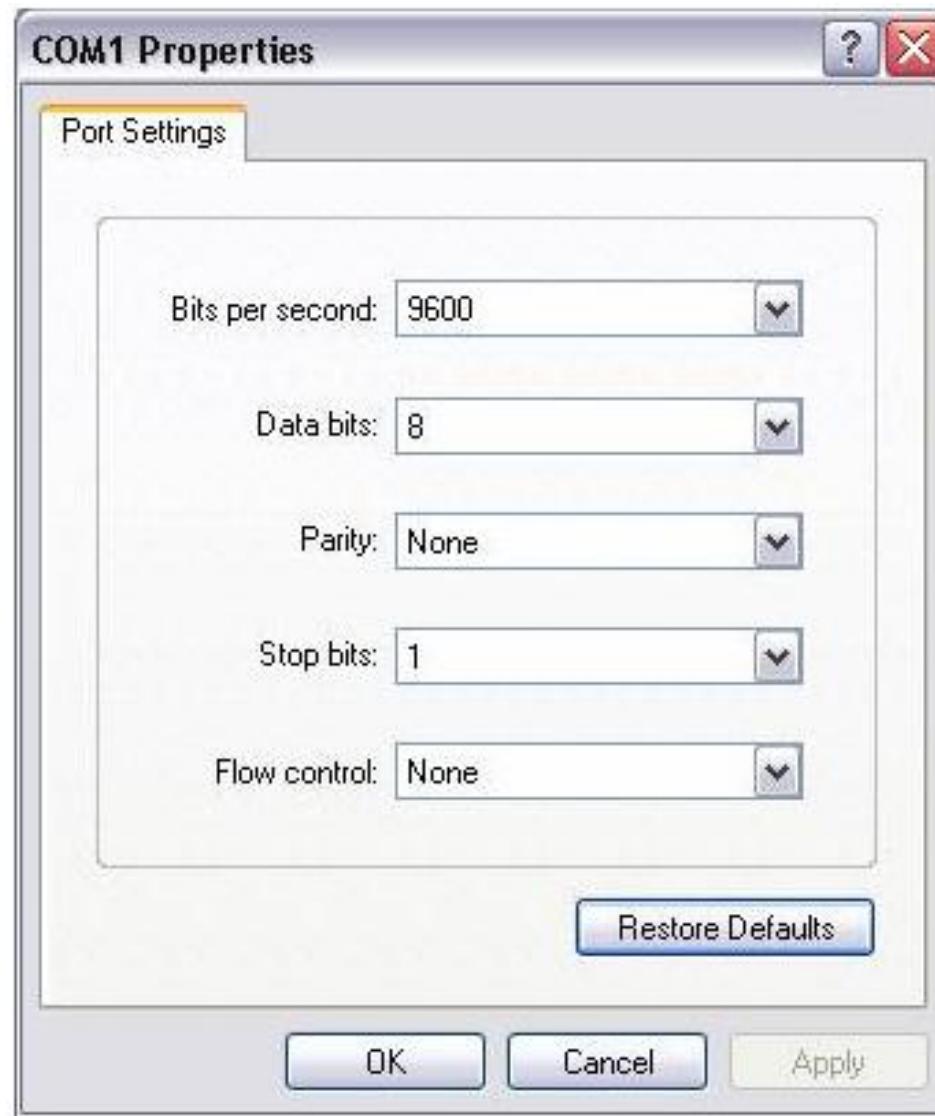
XEM CÔNG KẾT NỐI



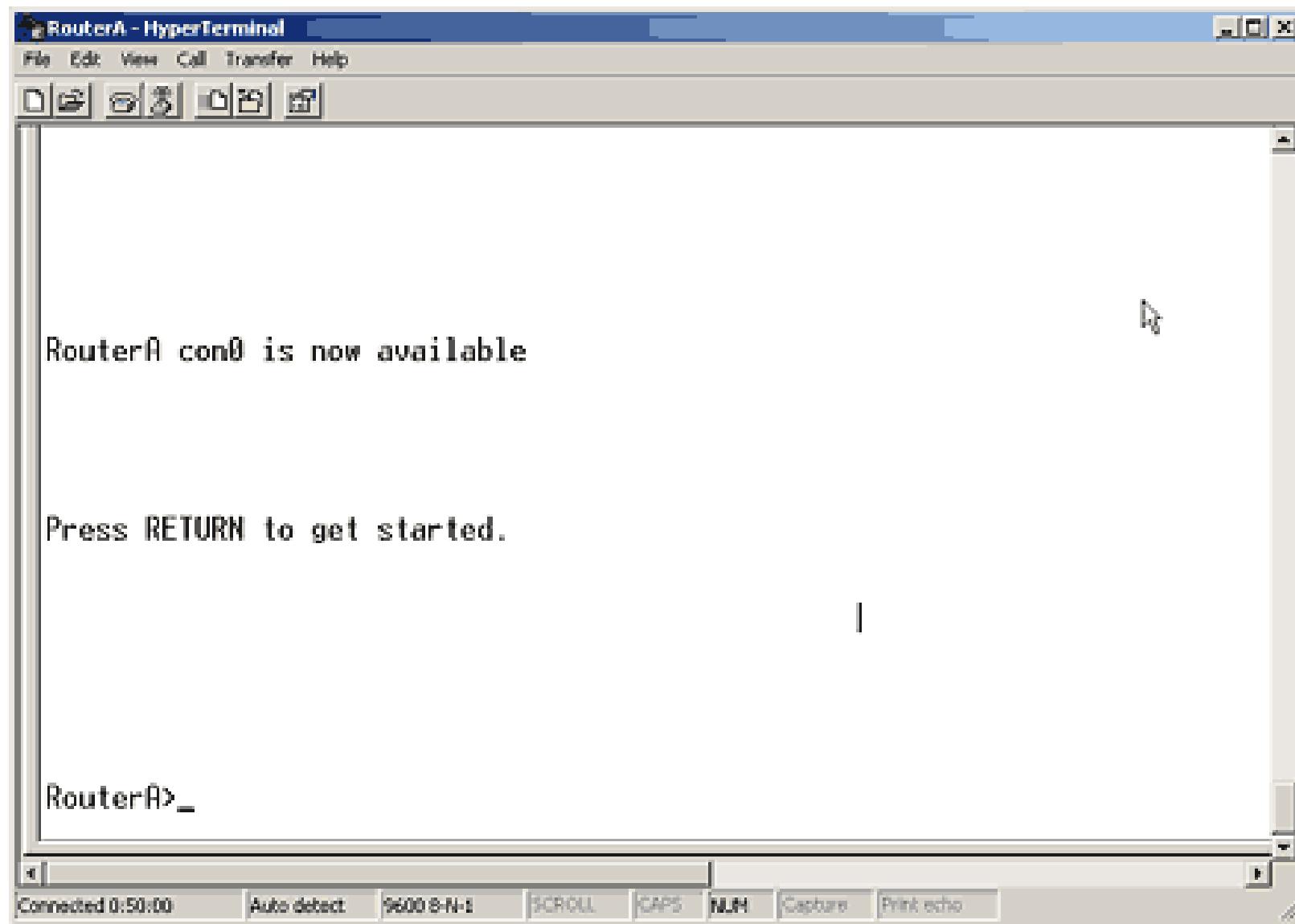
CẤU HÌNH ROUTER DÙNG HYPER TERMINAL



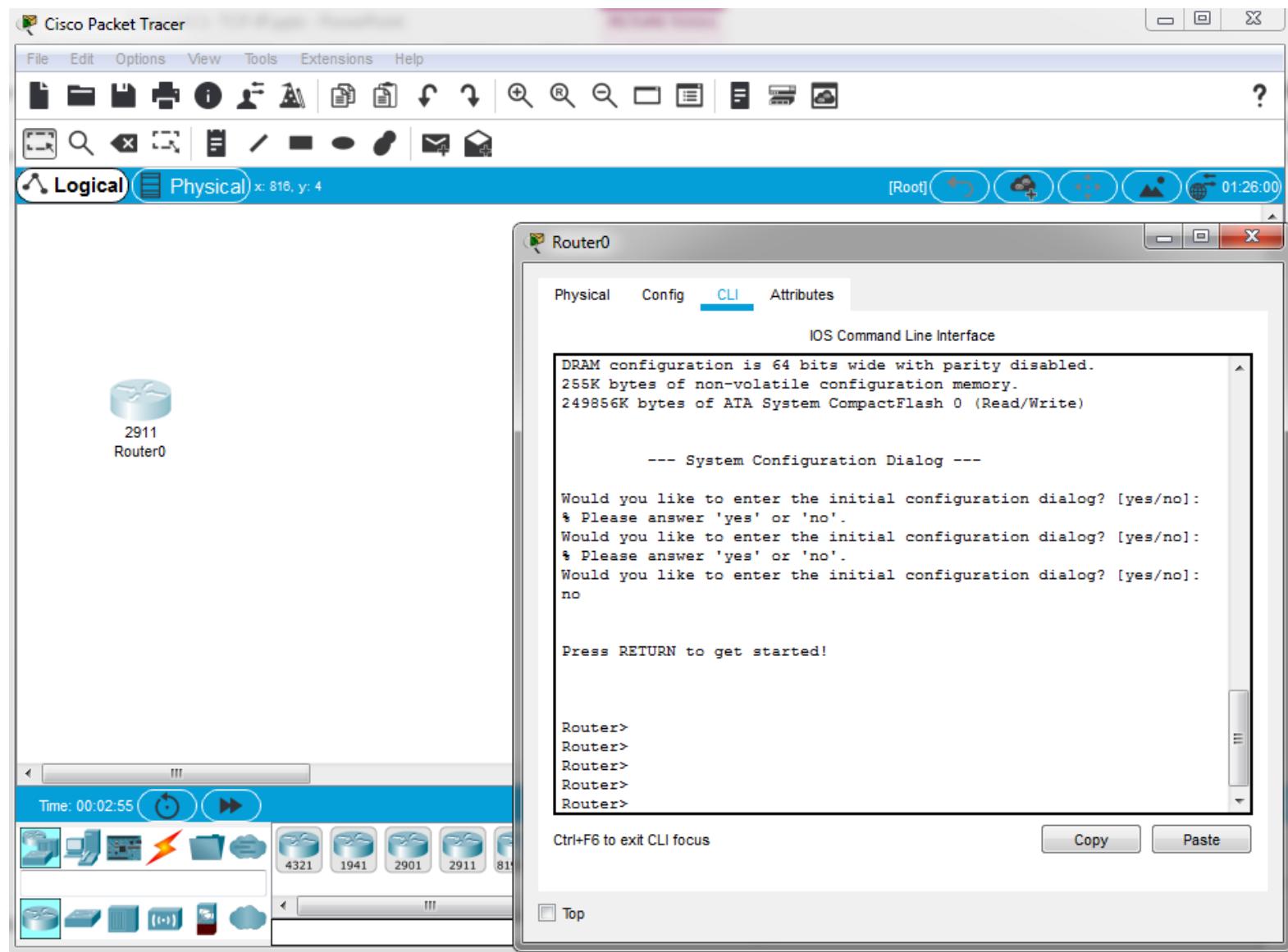
CẤU HÌNH ROUTER DÙNG HYPER TERMINAL



CẤU HÌNH ROUTER DÙNG HYPER TERMINAL



SỬ DỤNG PACKET TRACER



CÁC CHẾ ĐỘ CẤU HÌNH ROUTER

User EXEC Mode

Router>enable

Privileged EXEC Mode

Router#configure terminal

Ctrl-Z (end)

Global Configuration Mode

Router (config) #

Exit

Configuration Mode	Prompt
Interface	Router(config-if) #
Subinterface	Router(config-subif) #
Controller	Router(config-controller) #
Line	Router(config-line) #
Router	Router(config-router) #

CHUYỂN CHẾ ĐỘ NGƯỜI DÙNG

```
Router> exit 5 command show  
Press RETURN to get started.  
Router> enable  
Router#          100 command show  
Router# configure terminal  
Router(config)#  
Router(config)# line console 0  
Router(config-line)# exit  
Router(config)# exit  
Router# disable  
Router>
```

ĐẶT TÊN, BANNER

```
Router> enable
```

```
Router# configure terminal
```

```
Router(config)# hostname TLU
```

```
TLU(config)# hostname Cisco
```

```
Cisco(config) #
```

```
Cisco(config) # banner motd "Day la Router TLU"
```

```
Cisco# exit
```

```
Press RETURN to get started.
```

```
Day la Router TLU
```

```
Cisco>
```

CẤU HÌNH CHỐNG TRÔI DÒNG LỆNH

```
Router# Config t  
Router(config)# line console 0  
Router(config-line)# Logging synchronous
```

Tắt chức năng

```
Router(config)# No logging console
```

CẤU HÌNH IPv4 CHO INTERFACE FA

Cisco> enable

Cisco# configure terminal

Cisco(config)# interface fa0/0 // 1941 gig0/0

Cisco(config-if)# ip address 172.16.10.1 255.255.255.0

Cisco(config-if)# no shutdown

Cisco(config-if)# end

Cisco# Show ip interface brief

Cisco# Show running-config

CẤU HÌNH IPv4 CHO INTERFACE SERIAL

Cisco> enable

Cisco# configure terminal

Cisco(config)# interface se2/0 //Giao diện Serial2/0

Cisco(config-if)# ip address 192.168.1.1 255.255.255.0

Cisco(config-if)# clock rate 64000

Cisco(config-if)# no shutdown

Cisco(config-if)# end

Cisco# Show ip interface brief

Cisco# Show running-config

CẤU HÌNH IPv6 CHO INTERFACE

Cisco> enable

Cisco# configure terminal

Cisco(config)# interface se2/0

Cisco(config-if)# ipv6 enable

Cisco(config-if)# ipv6 address 2001::1/64

Cisco(config-if)# no shutdown

Cisco(config-if)# end

Cisco# Show ipv6 interface brief

Cisco# Show running-config

MỘT SỐ LỆNH SHOW

Router#show ip interface brief

```
Router# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	10.0.0.1	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/1/0	unassigned	YES	unset	administratively down	down
Serial0/2/0	unassigned	YES	unset	administratively down	down
Serial0/3/0	unassigned	YES	unset	administratively down	down

```
Router# ping 10.0.0.2
```

MỘT SỐ LỆNH SHOW

- ❖ Hiển thị thông tin phần cứng của một interface
 - ❖ Router#show controllers serial 0/0/0
- ❖ Hiển thị thời gian được cấu hình trên router
 - ❖ Router#show clock
- ❖ Hiển thị bảng thông tin host
 - ❖ Router#show host
- ❖ Hiển thị thông tin user đang kết nối trực tiếp vào thiết bị
 - ❖ Router#show users
- ❖ Hiển thị các câu lệnh đã thực thi trên router
 - ❖ Router#show history

MỘT SỐ LỆNH SHOW

- ❖ Hiển thị thông tin về bộ nhớ Flash của Router
 - ❖ Router#show flash
- ❖ Hiển thị các thông tin về IOS của Router
 - ❖ Router#show version
- ❖ Hiển thị bảng thông tin ARP trên router
 - ❖ Router#show arp

LUU FILE CẤU HÌNH ĐANG CHẠY

- ❖ Xem nội dung cấu hình đang chạy trên RAM
 - ❖ Router#show running-config
- ❖ Kiểm tra nội dung file cấu hình đã lưu ở NVRAM
 - ❖ Router#show startup-config
- ❖ Lưu file cấu hình vào NVRAM
 - ❖ Router# copy running-config startup-config
- ❖ Xóa file cấu hình khởi động
 - ❖ Router# erase startup-config
 - ❖ Router# reload

MỘT SỐ LỆNH CẤU HÌNH KHÁC

- ❖ Cấu hình không phân giải hostname
 - Router(config)# no ip domain-lookup

❖ Lab 1: Hướng dẫn sử dụng phần mềm Cisco Packet Tracer 7

1. Mở Cisco Packet Tracer
2. Chọn Guest Login để vào đăng ký

3. Trên trình duyệt đã mở

<https://www.netacad.com/virtual/app/introduction-packet-tracer>

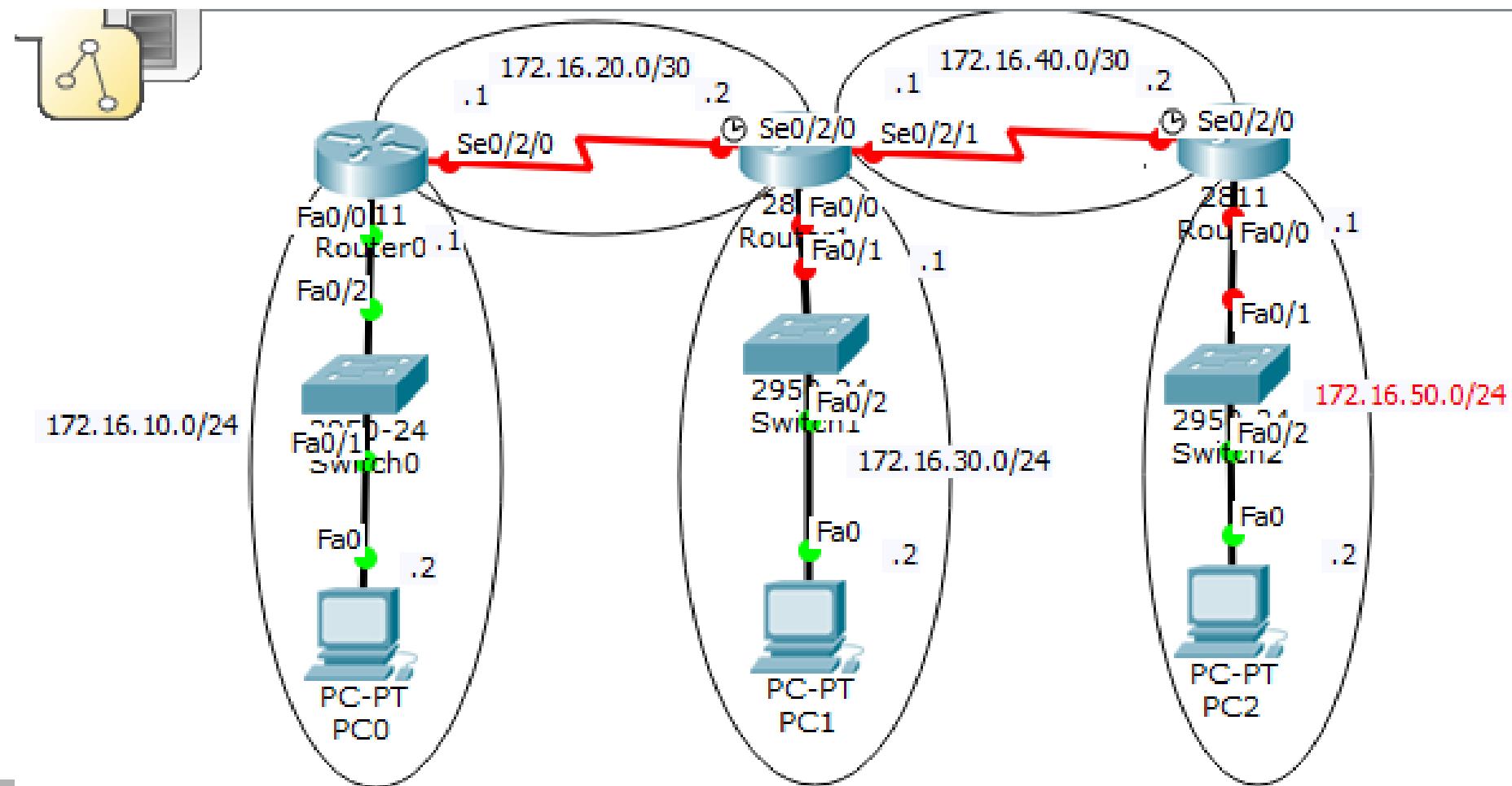
vào địa chỉ Email và nhấn vào Enroll Now

4. Vào các thông tin cá nhân

Bài tập Thực hành

Lab 1: Hướng dẫn sử dụng phần mềm Cisco Packet Tracer 7

Lab 2: Thực hiện cấu hình cơ bản router trong mạng sau



CẤU HÌNH ROUTER BOSTON

Router> enable

Router# configure terminal

Router(config)# hostname Boston

Boston config)#

Boston(config)# interface fastethernet 0/0

Boston(config)# interface f0/0

Boston(config-if)# ip address 172.16.10.1 255.0.0.0

Boston(config-if)# no shutdown

Boston(config-if)# end

Boston#

CẤU HÌNH ROUTER BOSTON

Boston > enable

Boston # configure terminal

Boston config)#

Boston(config)# interface Serial 0/0/0

Boston(config)# interface se0/0/0

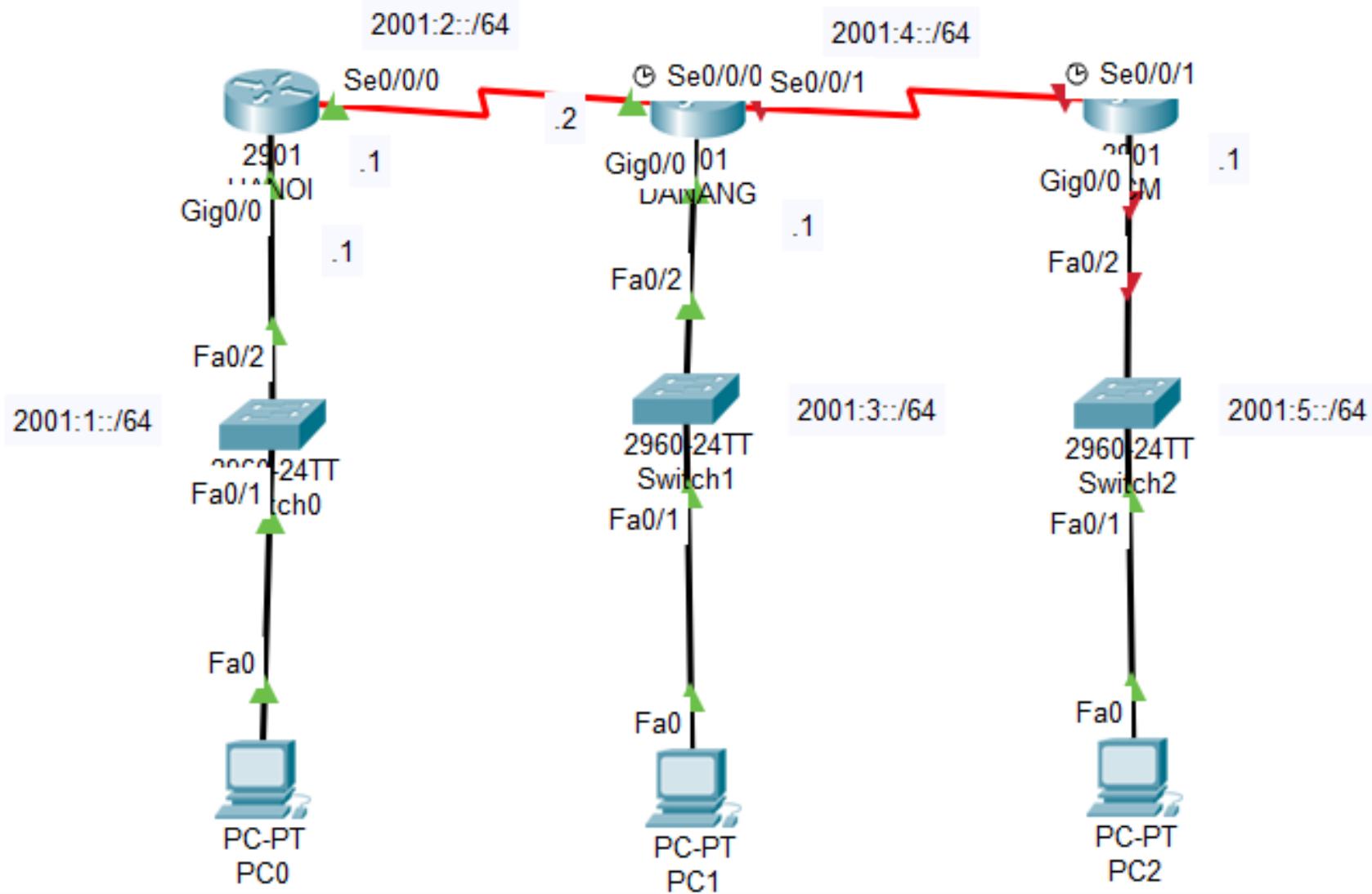
Boston(config-if)# ip address 172.16.20.1 255.0.0.0

Boston(config-if)# no shutdown

Boston(config-if)# end

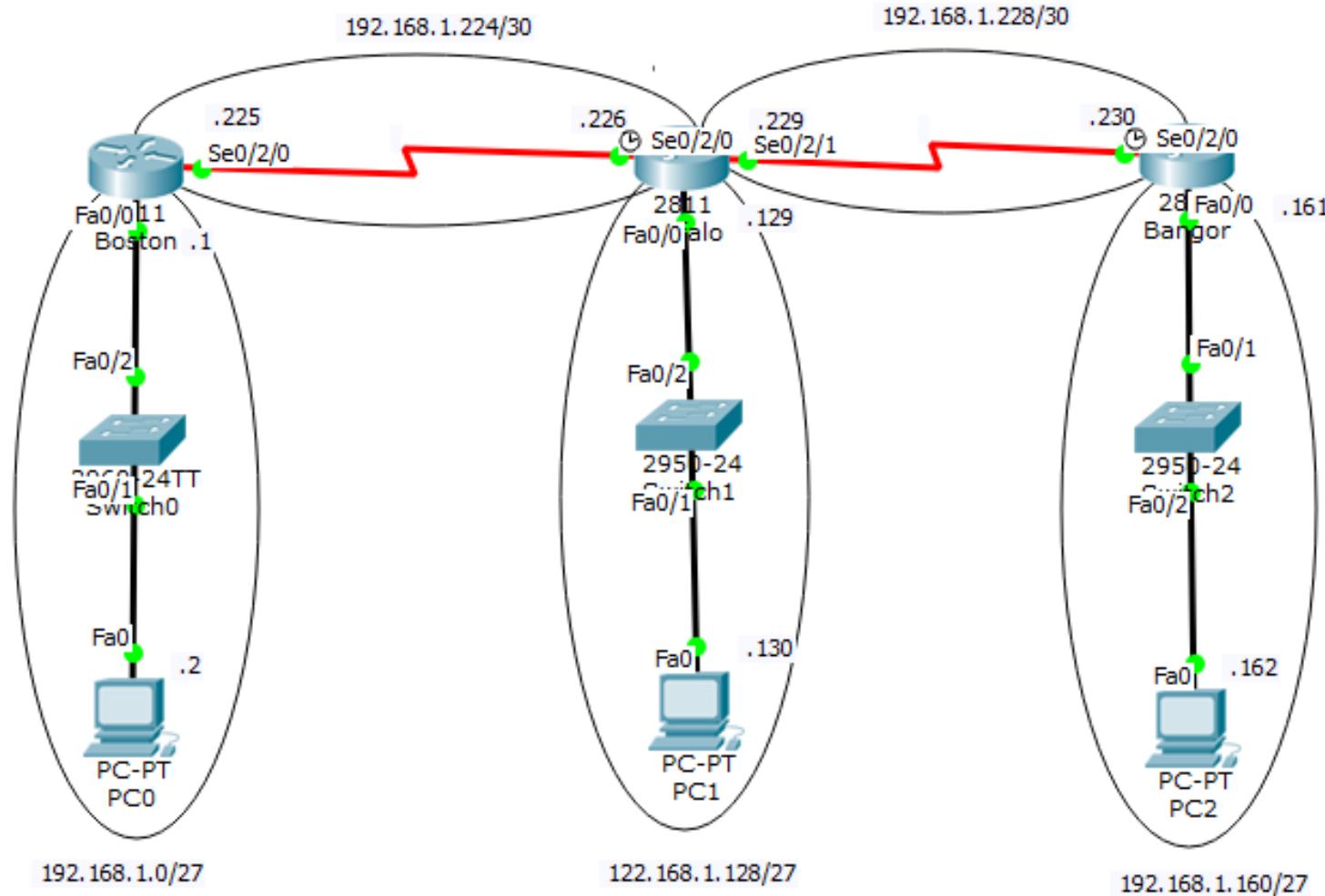
Boston#

CẤU HÌNH CƠ BẢN IPv6



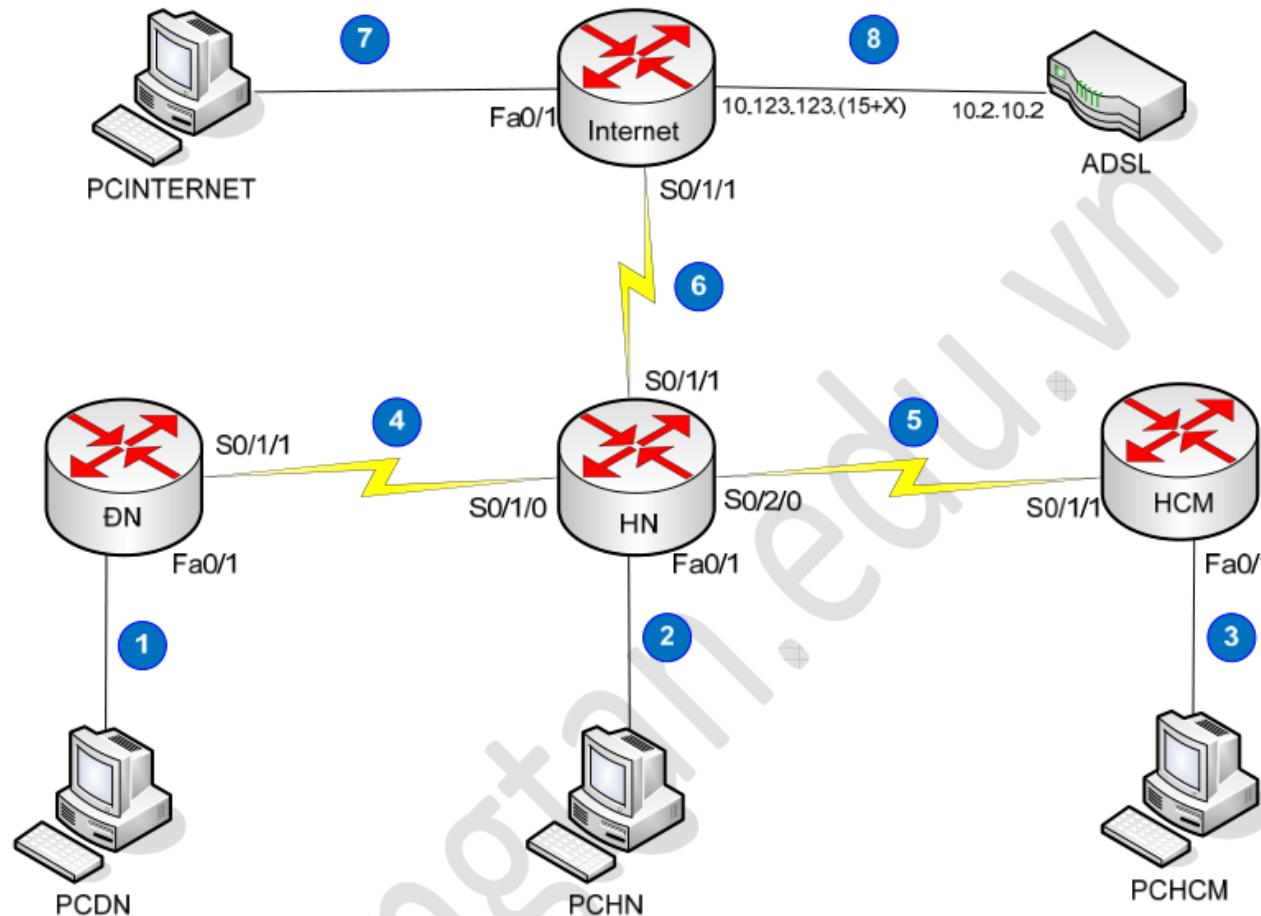
Bài tập Thực hành

Lab 3: Thực hiện cấu hình cơ bản router trong mạng sau



Bài tập Thực hành

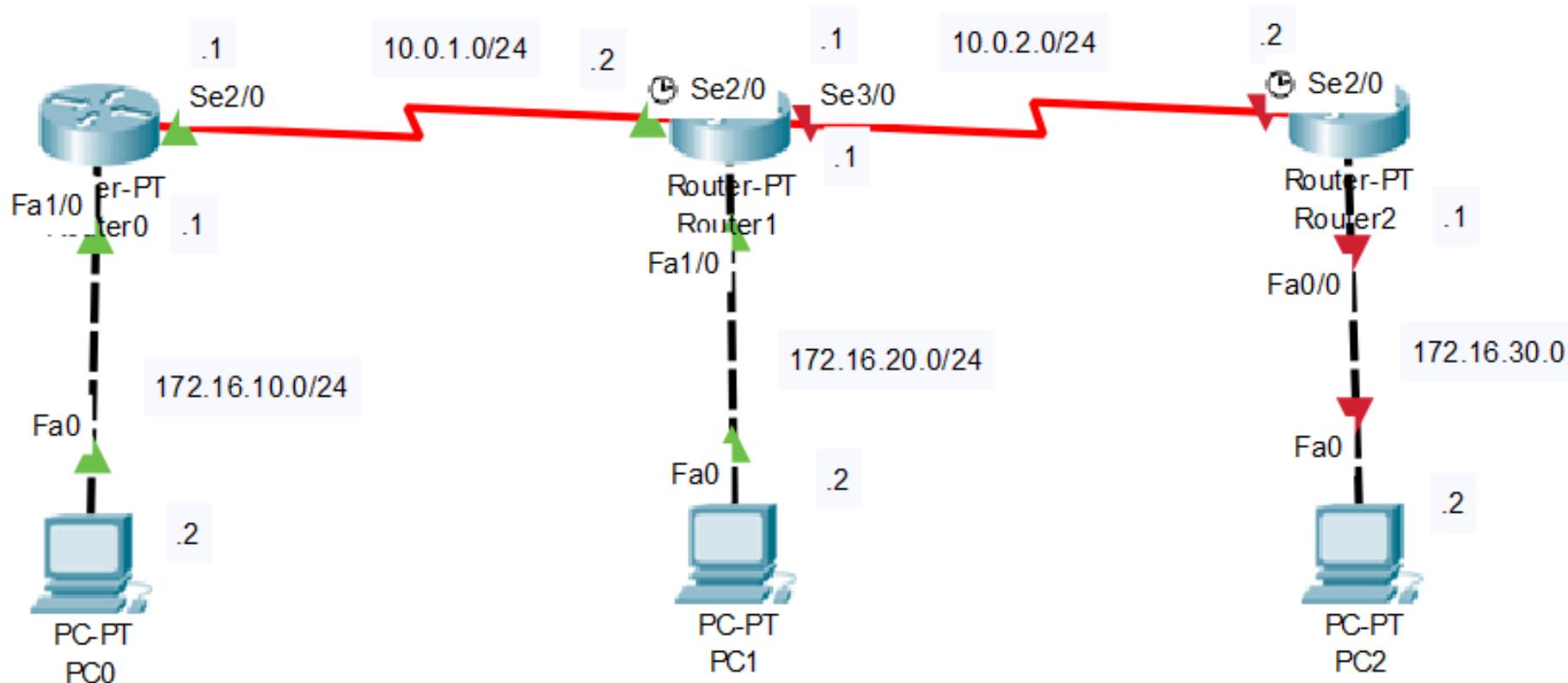
Lab 4: Thực hiện cấu hình cơ bản router trong mạng sau



YÊU CẦU

1. Sử dụng mạng $172.(15+X).0.0/16$ để chia subnet với X là số thứ tự của nhóm
2. Kiểm tra lại thông tin định tuyến bằng các lệnh
 - + Show ip route
 - + Ping ra internet
 - + Từ PC dùng lệnh tracert ra internet để liệt kê đường đi

Lab 5: Thực hiện cấu hình cơ bản router trong mạng sau





TRƯỜNG ĐẠI HỌC THỦY LỢI

KHOA CÔNG NGHỆ THÔNG TIN
Bộ môn: Kỹ thuật máy tính và mạng

QUẢN TRỊ MẠNG

Giảng viên: Trần Văn Hội

Email: hoitv@tlu.edu.vn

Điện thoại: 0944.736.007

NỘI DUNG MÔN HỌC



Chương 1: Tổng quan về mạng



Chương 2: Các kỹ thuật định tuyến



Chương 3: Chuyển mạch trong mạng LAN



Chương 4: Công nghệ mạng WAN



Chương 5: Bảo mật mạng

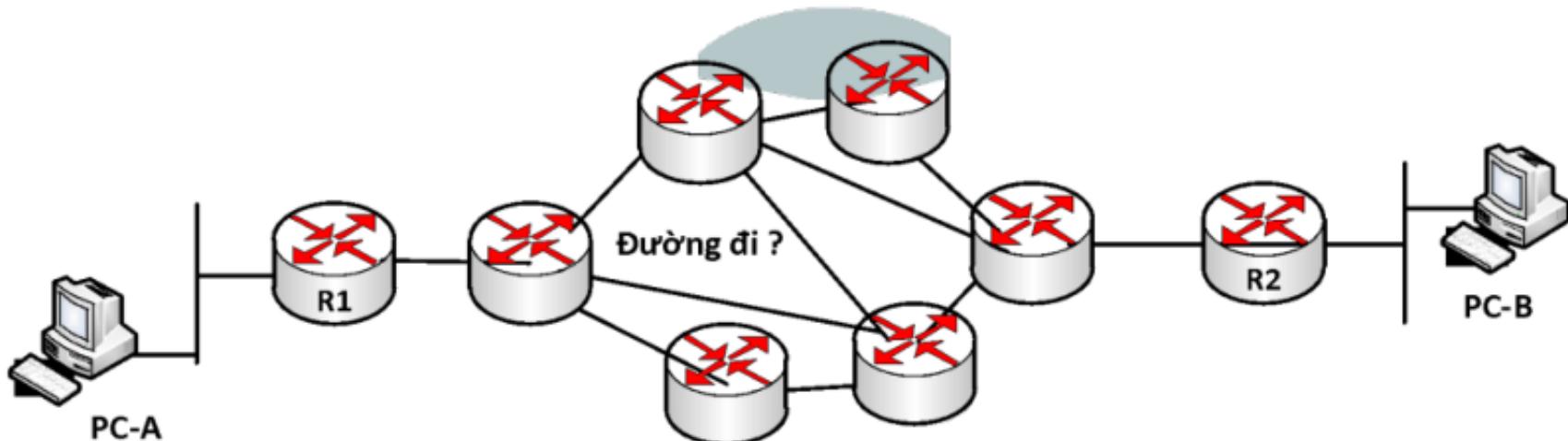
CHƯƠNG 2: CÁC KỸ THUẬT ĐỊNH TUYẾN

- 1 • Tổng quan về định tuyến
- 2 • Định tuyến tĩnh
- 3 • Giao thức định tuyến RIP
- 4 • Giao thức định tuyến OSPF
- 5 • Giao thức định tuyến EIGRP
- 6 • Giao thức định tuyến BGP

BÀI 1: TỔNG QUAN VỀ ĐỊNH TUYẾN

1. ROUTING - ĐỊNH TUYẾN

- Định tuyến là chức năng của Router giúp xác định quá trình tìm đường đi cho các gói tin để truyền dữ liệu từ nguồn tới đúng đích cần gửi.



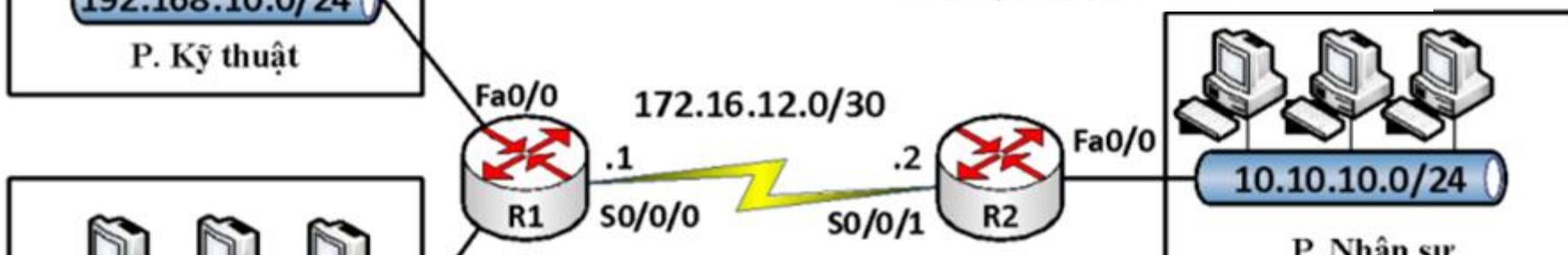
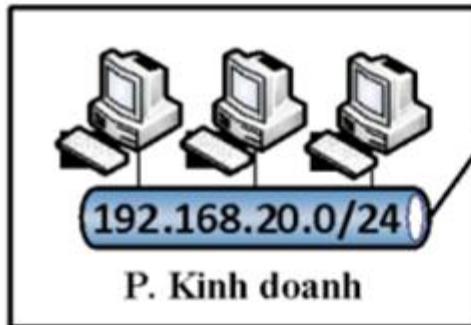
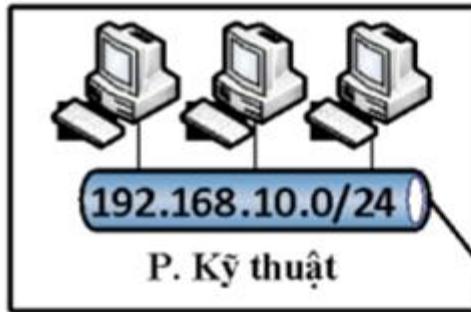
ROUTER

- ❖ Router là một thiết bị ở lớp 3. Router quyết định chuyển gói dựa trên địa chỉ mạng của gói dữ liệu. Router sử dụng bảng định tuyến để ghi lại địa chỉ lớp 3 của các mạng kết nối trực tiếp vào router và các mạng mà router học được từ các router láng giềng.
- ❖ Mục tiêu của router là thực hiện các việc sau:
 - Kiểm tra dữ liệu lớp 3 của gói nhận được
 - Chọn đường tốt nhất cho gói dữ liệu
 - Chuyển mạch gói ra cổng tương ứng
- ❖ Router ko bị bắt buộc phải chuyển các gói quảng bá

ROUTING - ĐỊNH TUYẾN

- Router dựa vào địa chỉ IP đích (destination IP) trong các gói tin và sử dụng bảng định tuyến (routing table) để xác định đường đi cho chúng.
- Trong bảng định tuyến, mỗi mạng mà router có thể chuyển đi (mạng đích) thể hiện bằng một dòng.
- Mỗi mạng này có được có thể do chúng đang kết nối trực tiếp với router đang xét hay router học được thông qua việc cấu hình định tuyến.

BẢNG ĐỊNH TUYẾN



Network	Interface or Next hop
172.16.12.0/30	Connected – S0/0/1
10.10.10.0/24	Connected – Fa0/0
192.168.10.0/24	172.16.12.1
192.168.20.0/24	172.16.12.1

Bảng định tuyến



Network	Interface or Next hop
172.16.12.0/30	Connected – S0/0/0
192.168.10.0/24	Connected – Fa0/0
192.168.20.0/24	Connected – Fa0/1
10.10.10.0/24	172.16.12.2

```
Router>en
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

      20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        20.0.0.0/24 is directly connected, Serial0/1/0
L        20.0.0.2/32 is directly connected, Serial0/1/0
S*      0.0.0.0/0 is directly connected, Serial0/1/0
                  [1/0] via 20.0.0.1

Router#
```

2. PHÂN LOẠI ĐỊNH TUYẾN (1)

- ❖ **Có 2 phương pháp định tuyến:**

- Định tuyến tĩnh (Static Route)
- Định tuyến động (Dynamic Route)

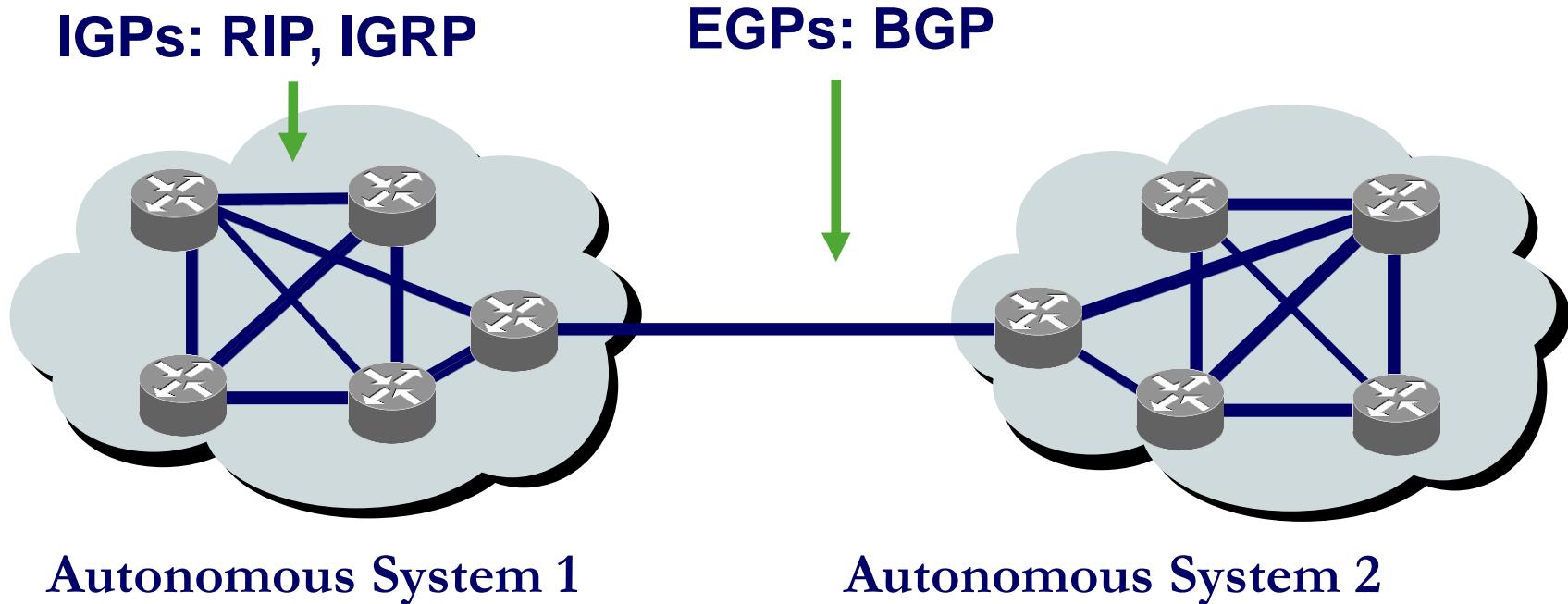
- ❖ **Định tuyến tĩnh (Static Route)**

- Định tuyến tĩnh là loại định tuyến mà trong đó router sử dụng các tuyến đường đi tĩnh để vận chuyển dữ liệu đi.
- Các tuyến đường đi tĩnh này có được do người quản trị cấu hình thủ công vào các router.

ĐỊNH TUYẾN ĐỘNG - DYNAMIC ROUTING

- ❖ Định tuyến động là loại định tuyến mà trong đó router sử dụng các tuyến đường đi động để vận chuyển dữ liệu đi.
- ❖ Các tuyến đường đi động này có được do các router sử dụng các giao thức định tuyến động trao đổi thông tin định tuyến với nhau tạo ra.
- ❖ Một số giao thức định tuyến động phổ biến: RIP, OSPF, BGP,...

ĐỊNH TUYẾN ĐỘNG - DYNAMIC ROUTING



- ❖ **Kỹ thuật định tuyến động chia làm hai nhóm:**
 - **Định tuyến ngoài EGP (Exterior Gateway Protocol):** là giao thức trao đổi thông tin giữa các AS (Autonomous System) khác nhau. Tiêu biểu là giao thức BGP (Border Gateway Protocol)
 - **Định tuyến trong IGP (Interior Gateway Protocol):** là giao thức định tuyến bên trong 1 AS như (RIP, IGRP, EIGRP, OSPF...).

IGP (Interior Gateway Protocol)

- ❖ IGP lại được chia thành 3 nhóm:
- ❖ Distance – vector: Mỗi router gửi cho láng giềng của nó toàn bộ bảng định tuyến của nó theo định kì. Giao thức tiêu biểu là RIP.
- ❖ Link – state: Mỗi router sẽ gửi bản tin trạng thái đường link (LSA) cho các router khác. Các Router sau khi xây dựng xong bảng định tuyến sẽ vẽ ra được một bản đồ mạng của toàn bộ hệ thống. Tiêu biểu là giao thức OSPF.
- ❖ Hybrid: tiêu biểu là giao thức EIGRP. Loại hình này kết hợp các đặc điểm của hai loại trên.

IGP (Interior Gateway Protocol)

- ❖ Các giao thức IGP cũng có thể chia làm 2 loại:
 - Các giao thức Classfull: Router sẽ không gửi kèm subnet-mask trong bảng tin định tuyến của mình. Từ đó giao thức classful không hỗ trợ sơ đồ VLSM và mạng gián đoạn (Discontiguous networks). Giao thức tiêu biểu là RIPv1 .
 - Các giao thức Classless: ngược lại với classful, Router có thể gửi kèm subnet-mask trong bảng định tuyến. Từ đó các giao thức classless có hỗ trợ sơ đồ VLSM và mạng gián đoạn. Các giao thức tiêu biểu là: RIPv2, OSPF, EIGRP.

THAM SỐ ĐỊNH TUYẾN

- ❖ **Giá trị AD (Administrative Distance):** là giá trị được sử dụng để chỉ độ tin cậy của các giao thức định tuyến.
- Trong trường hợp router học được một mạng đích thông qua nhiều giao thức định tuyến khác nhau, thì tuyến của giao thức định tuyến nào có AD nhỏ nhất thì sẽ được lựa chọn và đưa vào bảng định tuyến.
- Giá trị AD này khác nhau theo từng Vendor qui định.

Bảng giá trị AD của Cisco qui định

Route type	AD
Kết nối trực tiếp	0
Static	1
EIGRP summary route	5
Exterior BGP	20
EIGRP (internal)	90
OSPF	110
IS-IS	115
RIP	120
EGP (Exterior Gateway Protocol)	140
On-Demand Routing	160
EIGRP (External)	170
Internal BGP	200
Unknown	255

THAM SỐ ĐỊNH TUYẾN

- ❖ **Metric:** là giá trị dùng để định lượng mức độ tối ưu của 1 đường đi trong tính toán định tuyến.
- ❖ Mỗi kĩ thuật Routing sẽ có Metric khác nhau:
 - RIP dựa vào số router trên đường đi đến đích gọi là hop-count.
 - OSPF tính metric dựa vào băng thông (Bandwidth) đường truyền.
 - EIGRP tính metric dựa vào một bộ các thông số khác nhau trên đường đi đến đích như băng thông (Bandwidth), độ trễ (delay), độ tin cậy (reliability), tải (load) của đường truyền.

CHƯƠNG 2: CẤU HÌNH ĐỊNH TUYẾN

- 1 • Tổng quan về định tuyến
- 2 • Định tuyến tĩnh
- 3 • Giao thức định tuyến RIP
- 4 • Giao thức định tuyến OSPF
- 5 • Giao thức định tuyến EIGRP
- 6 • Giao thức định tuyến BGP

BÀI 2: ĐỊNH TUYẾN TĨNH

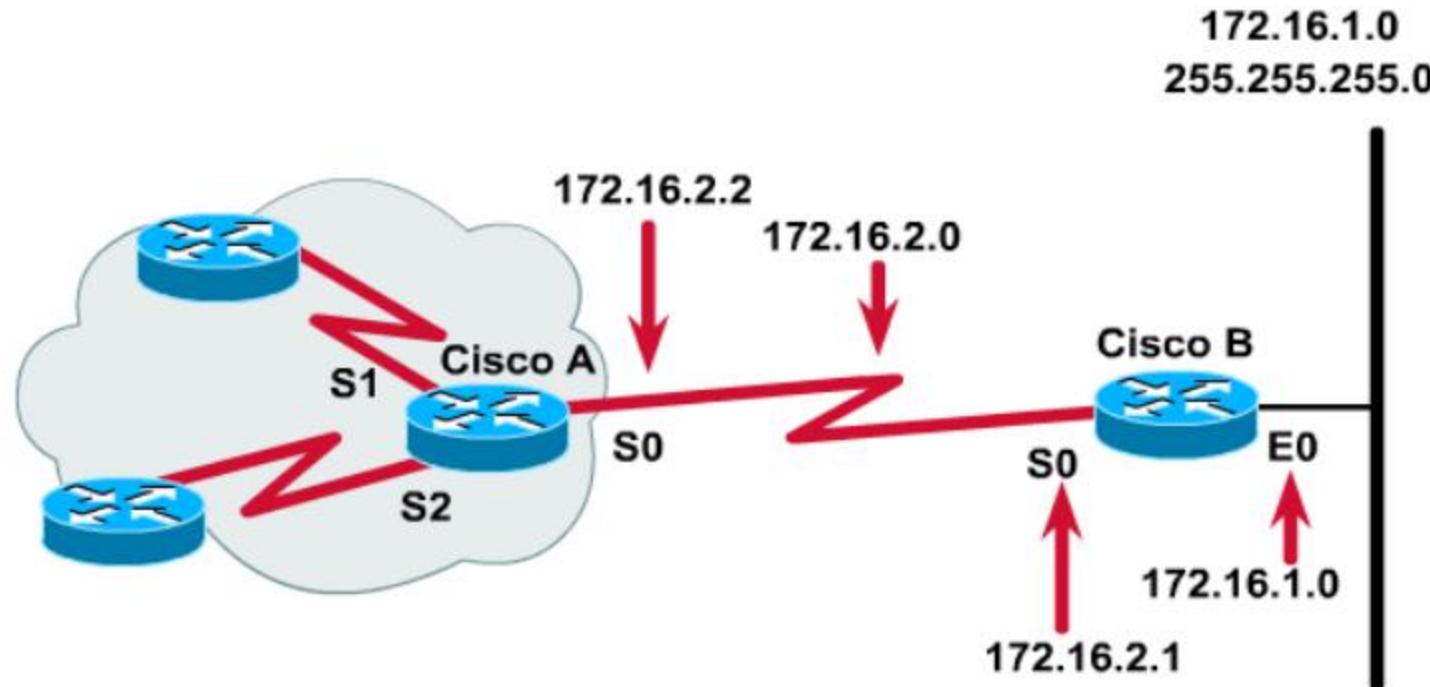
1. Định tuyến tĩnh IPv4:

```
R(config)#ip route <destination-net> <subnet-mask> <NextHop  
|OutPort>
```

- ❖ Trong đó:
 - destination-network: Là địa chỉ mạng cần đi tới
 - subnet-mask: subnet mask của destination-network
 - next-hop: địa chỉ IP của router kế tiếp kết nối trực tiếp với router đang xét
 - OutPort: cổng của router mà packet sẽ đi ra

ĐỊNH TUYẾN TĨNH (STATIC ROUTING)

- ❖ Ví dụ: Cấu hình trên router Cisco A để học mạng 172.16.1.0/24



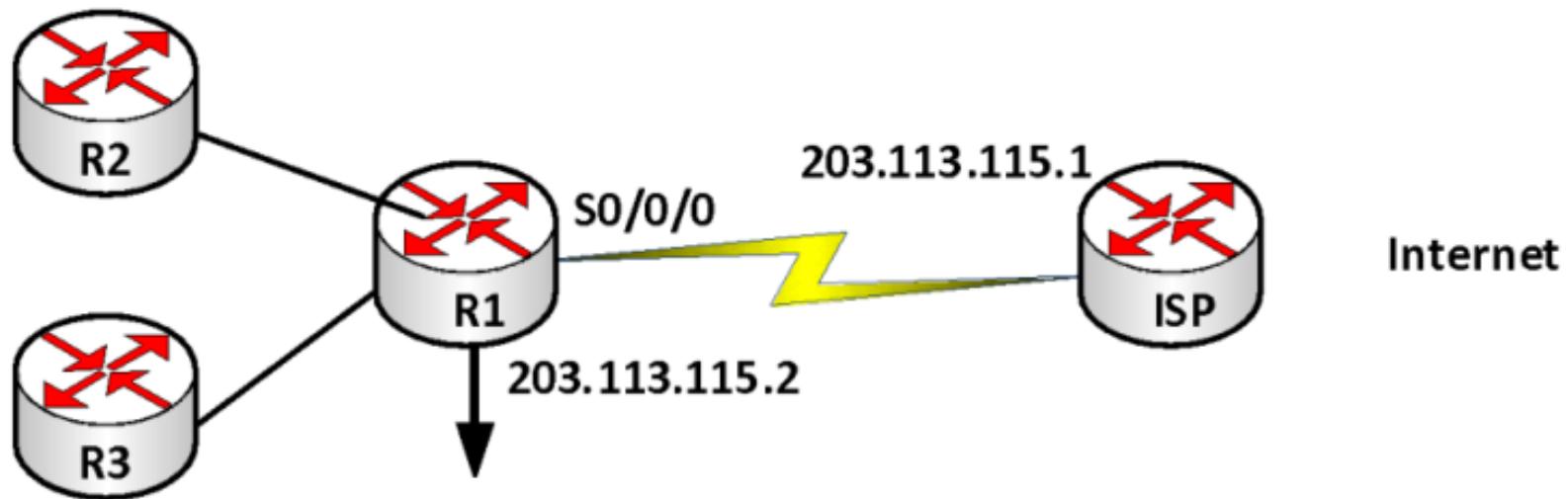
```
CiscoA(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1
```

```
CiscoA(config)#ip route 172.16.1.0 255.255.255.0 S0
```

DEFAULT ROUTE

- ❖ Default route nằm ở cuối bảng định tuyến và được sử dụng để gửi các gói tin đi trong trường hợp mạng đích không tìm thấy trong bảng định tuyến.
- ❖ Nó rất hữu dụng trong các mạng dạng “stub network” như kết nối từ mạng nội bộ ra ngoài Internet.

DEFAULT ROUTE



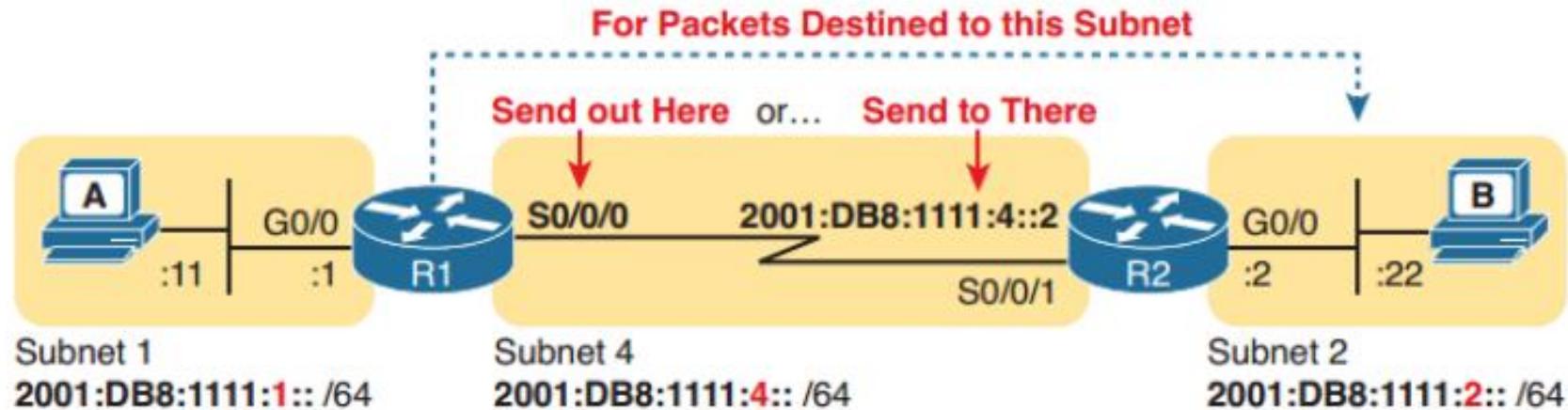
```
R1(config)#ip route 0.0.0.0 0.0.0.0 203.113.115.1
```

```
R1(config)#ip route 0.0.0.0 0.0.0.0 S0/0/0
```

2. ĐỊNH TUYẾN TÍNH CHO IPv6

R(config)#Ipv6 unicast-routing

R(config)#ipv6 route prefix-network/prefix-length [OutGoing Interface | Next-Hop]



```
! Static route on router R1
```

```
R1(config)# ipv6 route 2001:db8:1111:2::/64 s0/0/0
```

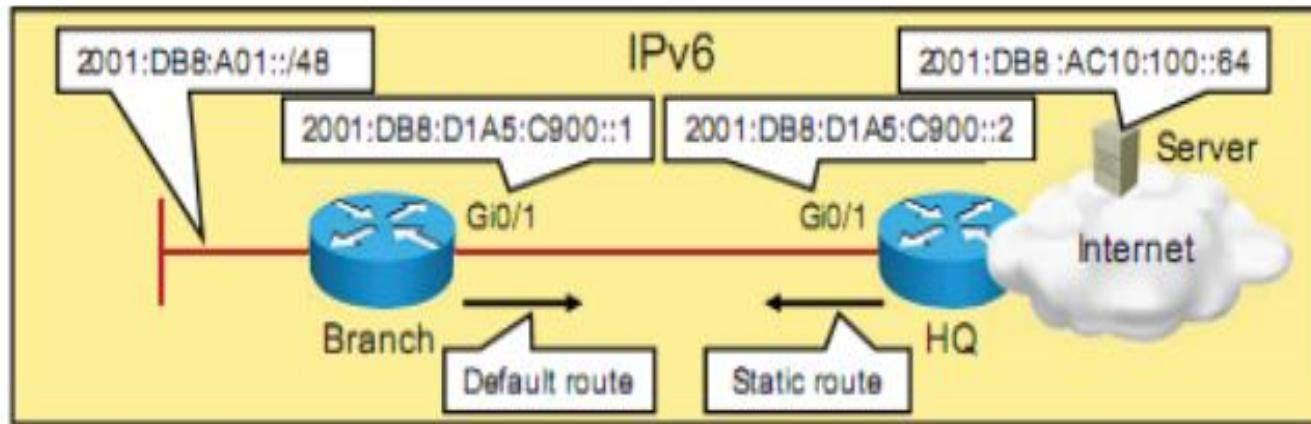
```
! The first command is on router R1, listing R2's global unicast address
```

```
R1(config)# ipv6 route 2001:db8:1111:2::/64 2001:DB8:1111:4::2
```

```
! The first command is on router R1, listing R2's link-local address
```

```
R1(config)# ipv6 route 2001:db8:1111:2::/64 s0/0/0 FE80::FF:FE00:2
```

DEFAULT ROUTE VIPv6



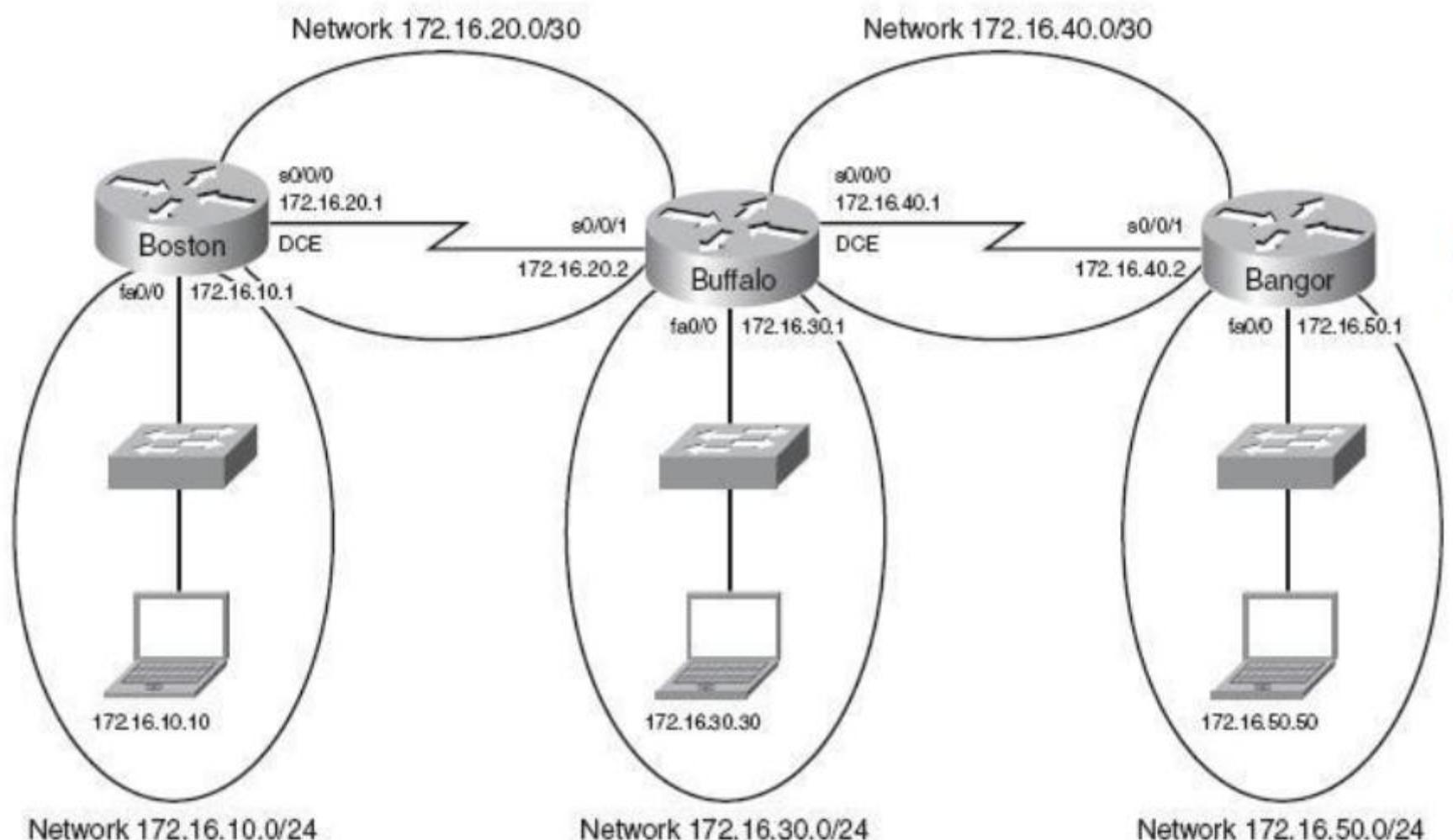
The static IPv6 route is configured on the HQ router:

```
HQ(config)#ipv6 route 2001:DB8:A01::/48 Gi0/1 2001:DB8:D1A5:C900::1
```

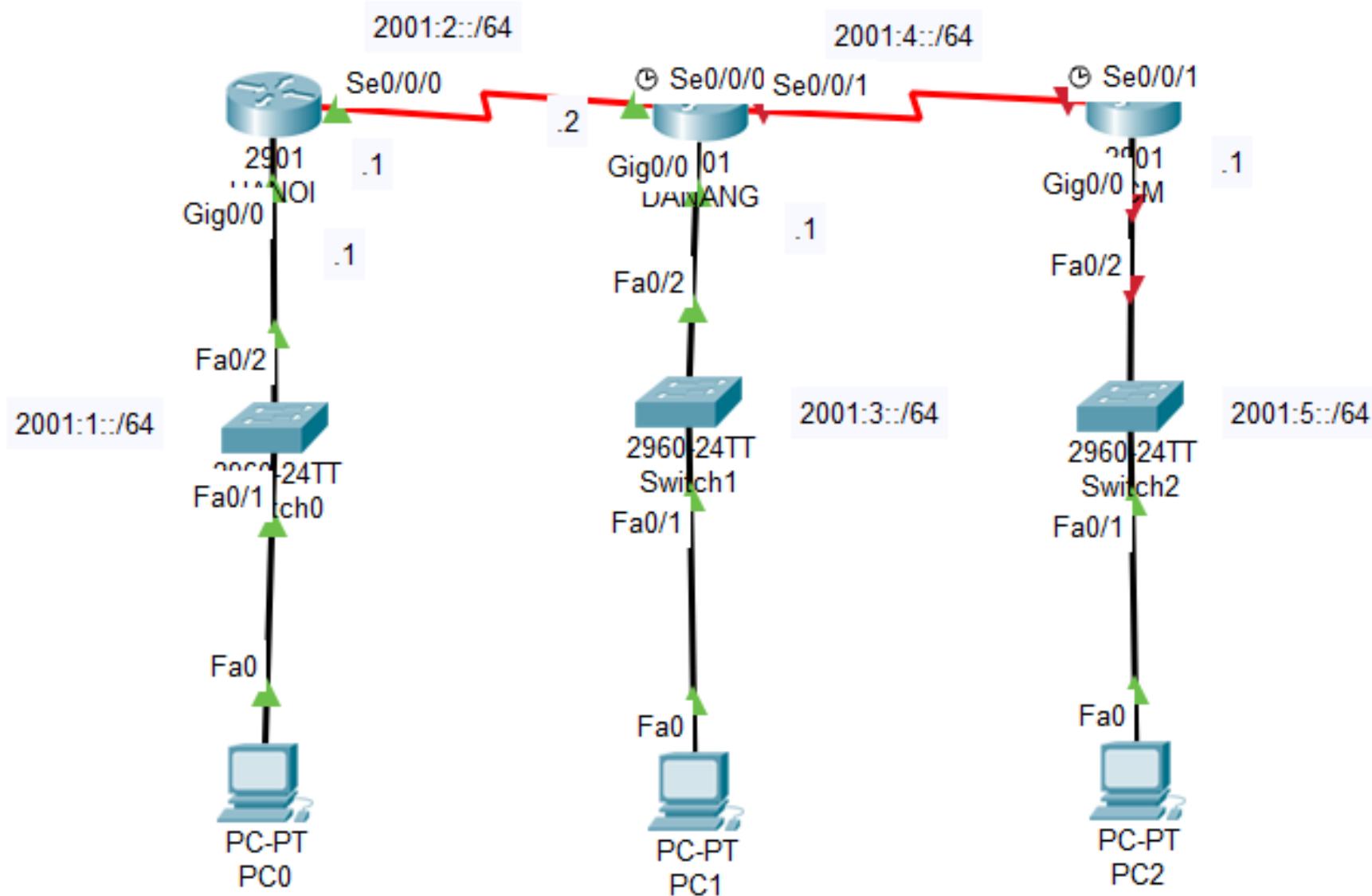
The default IPv6 route is configured on the Branch router:

```
Branch(config)#ipv6 route ::/0 Gi0/1 2001:DB8:D1A5:C900::2
```

BÀI TẬP 1: ĐỊNH TUYỀN TĨNH IPv4



BÀI TẬP 2: ĐỊNH TUYỀN TĨNH IPv6



Boston Router

Boston> enable	Chuyển vào chế độ Privileged
Boston# configure terminal	Chuyển vào chế độ cấu hình Global Configuration
Boston(config)# ip route 172.16.30.0 255.255.255.0 172.16.20.2	Cấu hình một static route sử dụng địa chỉ next-hop
Boston(config)# ip route 172.16.40.0 255.255.255.252 172.16.20.2	Cấu hình một static route sử dụng địa chỉ next-hop
Boston(config)# ip route 172.16.50.0 255.255.255.0 172.16.20.2	Cấu hình một static route sử dụng địa chỉ next-hop
Boston(config)# exit	Chuyển về chế độ cấu hình Privileged
Boston# copy run start	Lưu file cấu hình đang chạy trên RAM vào NVRAM.

Buffalo Router

Buffalo> enable	Chuyển về chế độ cấu hình Privileged.
Buffalo# configure terminal	Chuyển vào chế độ cấu hình Global Configuration
Buffalo(config)# ip route 172.16.10.0 255.255.255.0 s0/0/1	Cấu hình một static route sử dụng một interface đang tồn tại.
Buffalo(config)# ip route 172.16.50.0 255.255.255.0 s0/0/0	Cấu hình một static route sử dụng một interface đang tồn tại.
Buffalo(config)# exit	Thoát ra chế độ Privileged.
Buffalo# copy run start	Lưu file cấu hình đang chạy trên RAM vào NVRAM

Bangor Router

Bangor> enable	Chuyển vào chế độ cấu hình Privileged.
Bangor# configure terminal	Chuyển vào chế độ cấu hình Global Configuration.
Bangor(config)# ip route 0.0.0.0 0.0.0.0 s0/0/1	Cấu hình static route sử dụng default route
Bangor# copy run start	Lưu file cấu hình đang chạy trên RAM vào NVRAM.

Bangor#show ip route	Xem bảng định tuyến
----------------------	---------------------

CHƯƠNG 2: CẤU HÌNH ĐỊNH TUYẾN

- 1 • Tổng quan về định tuyến
- 2 • Định tuyến tĩnh
- 3 • Giao thức định tuyến RIP
- 4 • Giao thức định tuyến OSPF
- 5 • Giao thức định tuyến EIGRP
- 6 • Giao thức định tuyến BGP

BÀI 3: GIAO THỨC ĐỊNH TUYẾN RIP

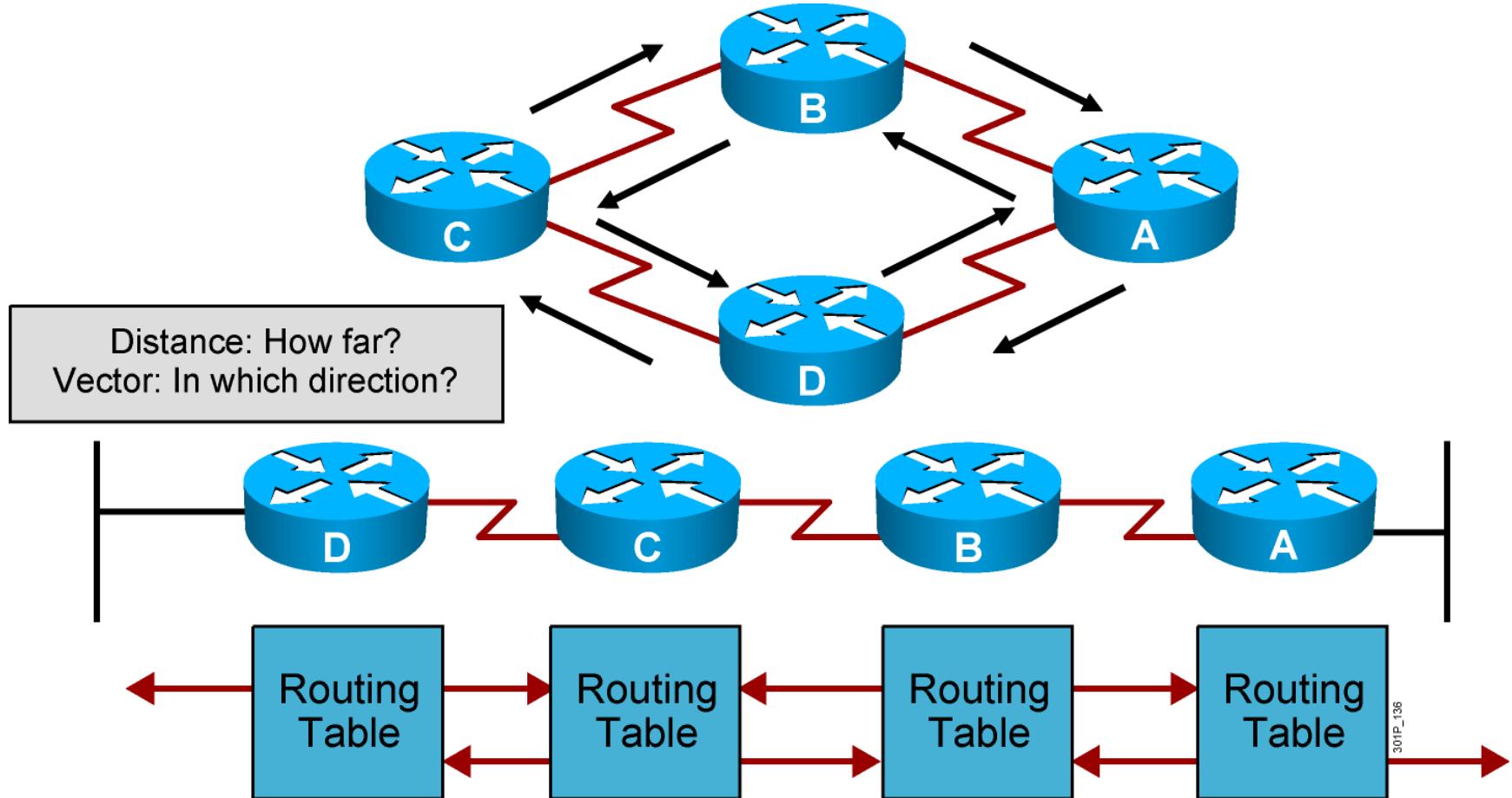
1. RIP (Routing Information Protocol).

- Giao thức định tuyến nội vùng (Interior routing protocols)
- Sử dụng thuật toán tìm đường Bellman Ford.
- 30 giây các router update thông tin định tuyến.
- Metric = hop count (số nút mạng đi qua).
 - (Maximum is 16 equal-cost paths, if metric =16 -> infinity.)
- Đường đi tốt nhất là đường đi có metric nhỏ nhất.
- Dùng UDP-port 520 để chuyển có gói tin update với IPv4 và 521 với IPv6.
- AD (Administrative Distance) = 120 (độ tin cậy).

RIP (Routing Information Protocol)

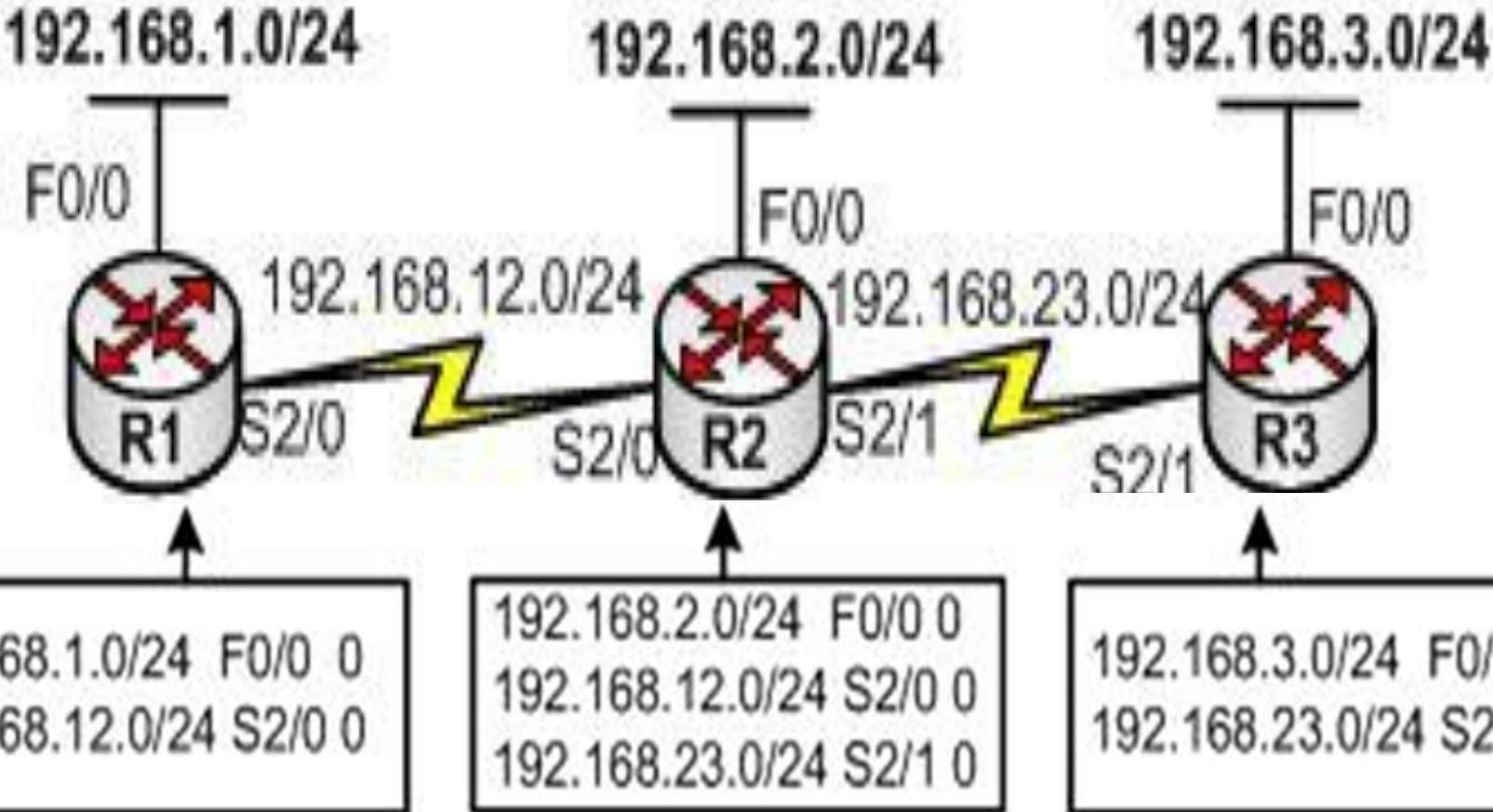
- ❖ RIP v1 và RIP v2, RIPng
- ❖ Thông tin cập nhật routing table theo địa chỉ 224.0.0.9
đối với IPv4 và FF02::09 với IPv6
- ❖ Người quản trị có thể tính lại đường đi một cách thủ công.
- ❖ Các gói tin RIP với router được chứng thực

Distance Vector

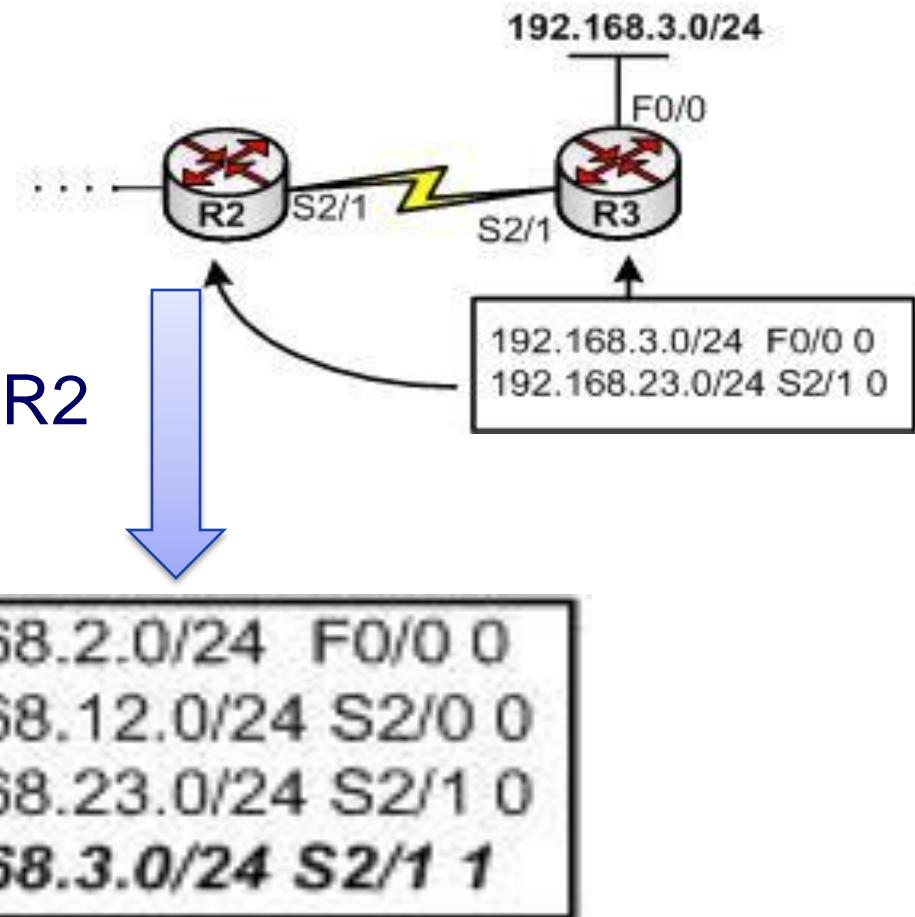


Các router định kỳ gửi các routing table đến các router láng giềng

Hoạt Động RIP



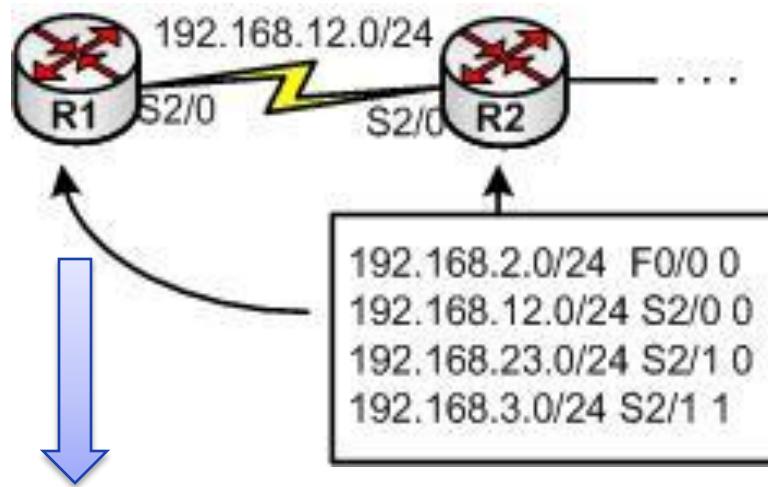
Hoạt Động RIP tt



Routing table send from R3 to R2

Routing table of R2 ?

Hoạt Động RIP tt

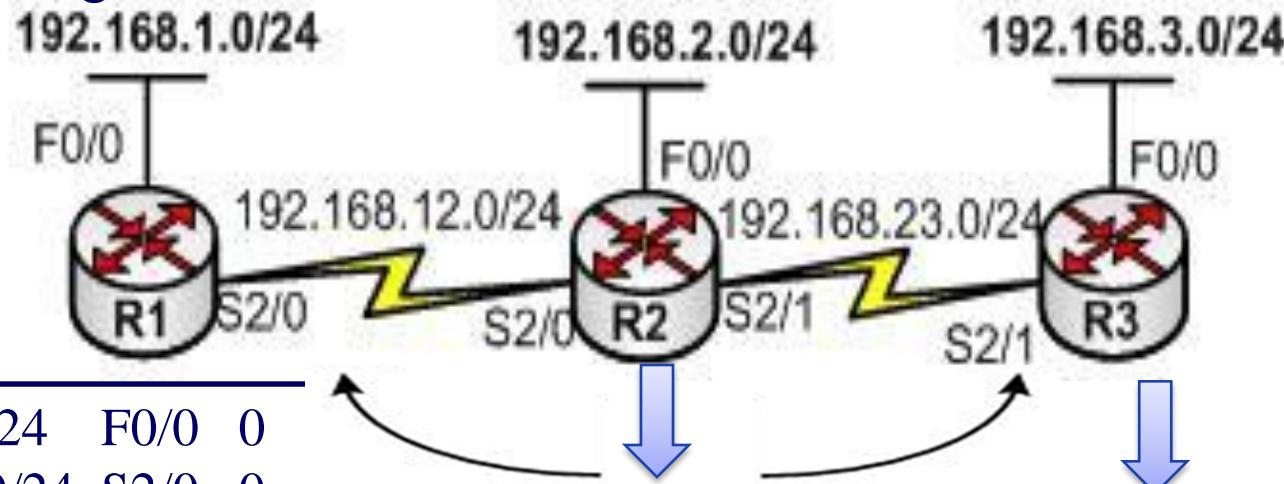


192.168.1.0/24	F0/0	0
192.168.12.0/24	S2/0	0
192.168.23.0/24	S2/0	1
192.168.2.0/24	S2/0	1
192.168.3.0/24	S2/0	2

Routing table send from R2 to **R1** and **R3**
Routing table of **R1**

Hoạt Động RIP tt

Routing table send from R1 to R2



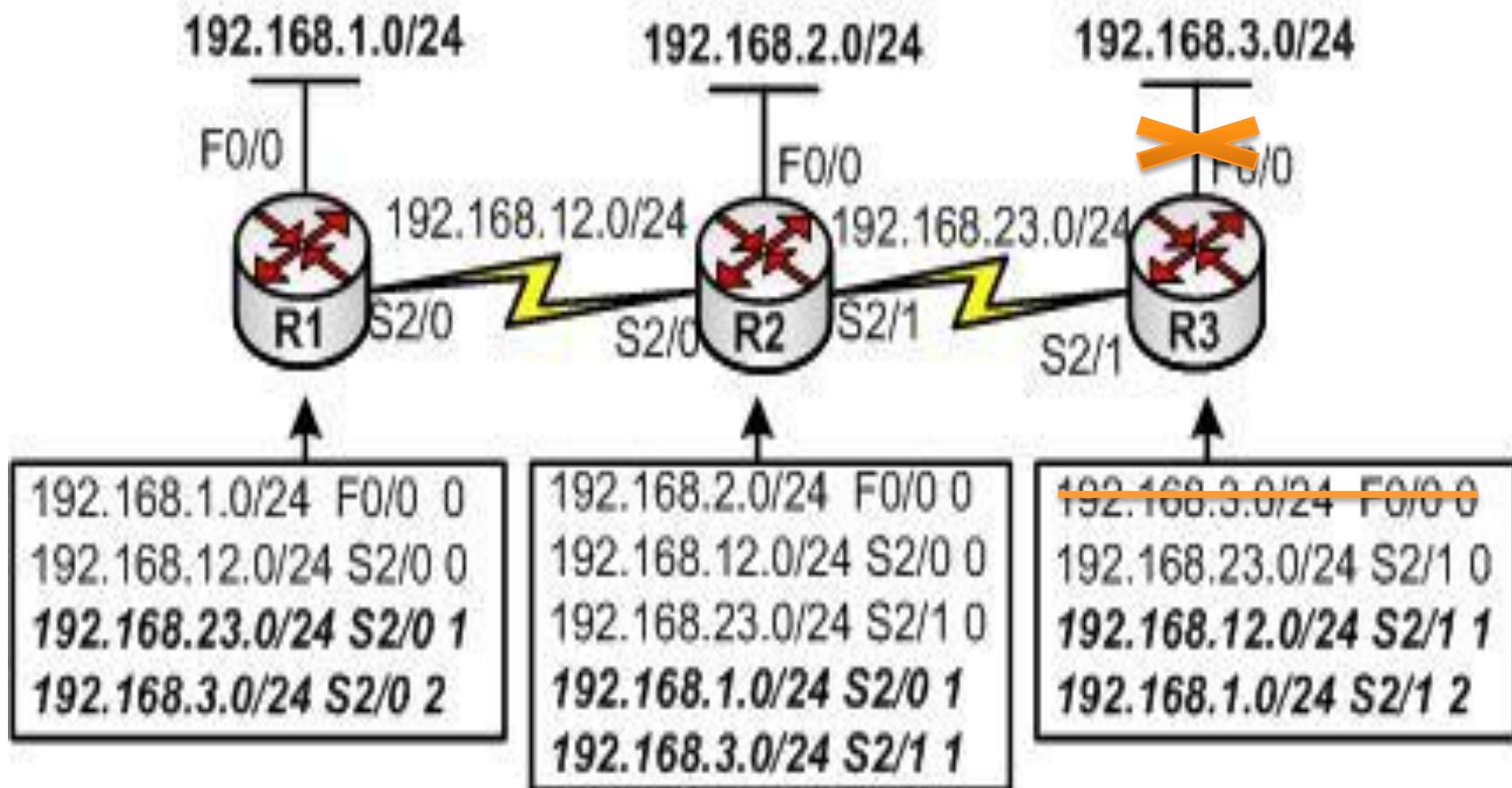
192.168.1.0/24	F0/0	0
192.168.12.0/24	S2/0	0
192.168.23.0/24	S2/0	1
192.168.2.0/24	S2/0	1
192.168.3.0/24	S2/0	2

192.168.12.0/24	S2/0	0
192.168.2.0/24	F0/0	0
192.168.23.0/24	S2/1	0
192.168.3.0/24	S2/1	1
192.168.1.0/24	S2/0	1

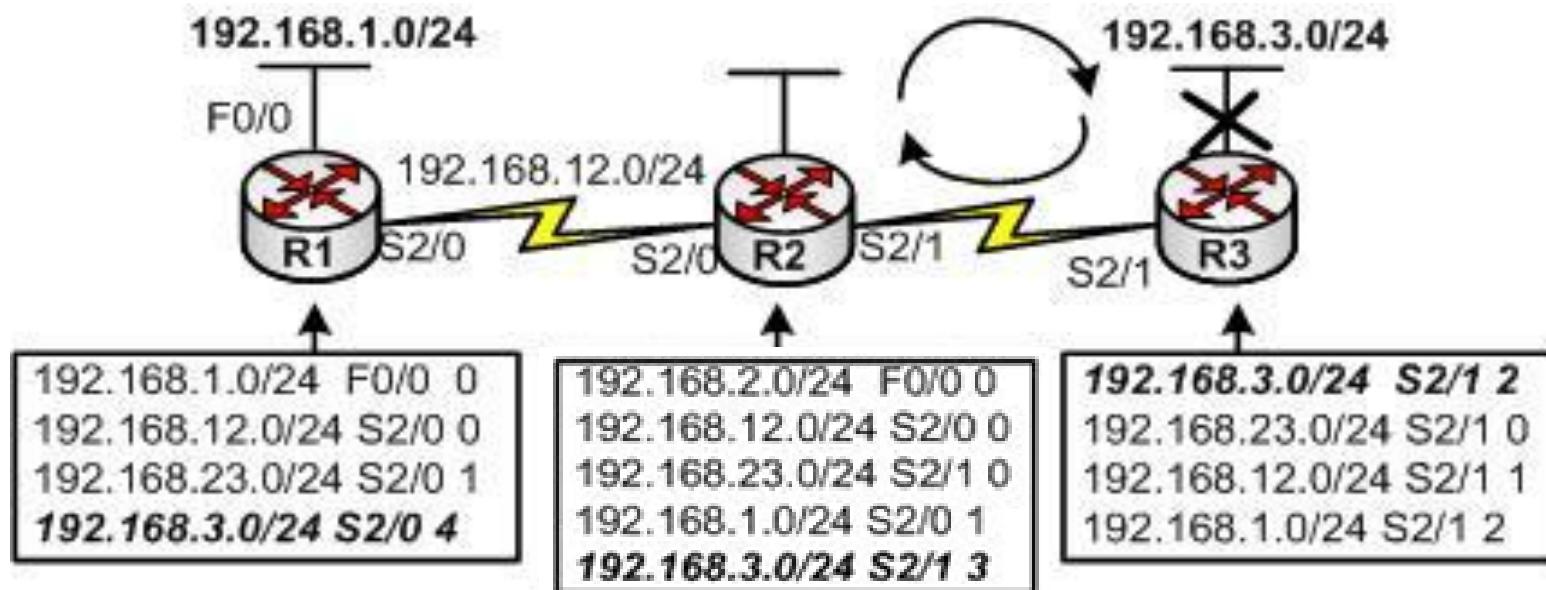
192.168.12.0/24		
192.168.2.0/24		
192.168.23.0/24		
192.168.3.0/24		
192.168.1.0/24		

Routing table of R2

Hoạt động RIP (tt)

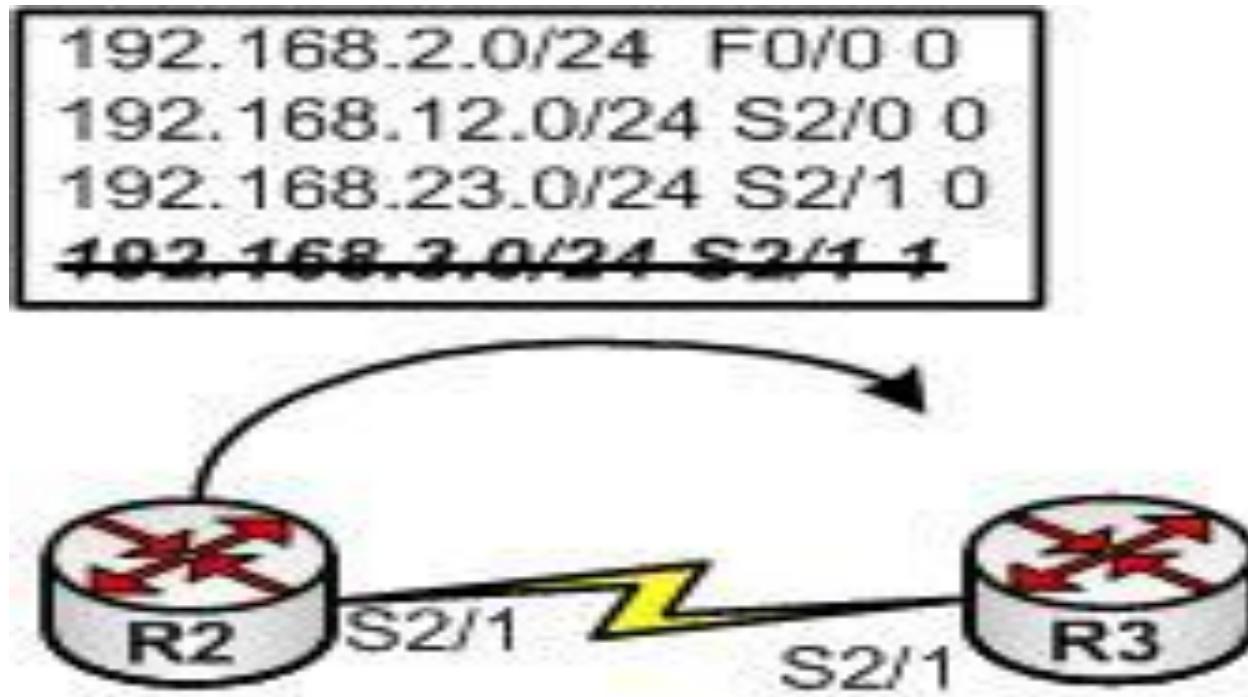


Routing Loops



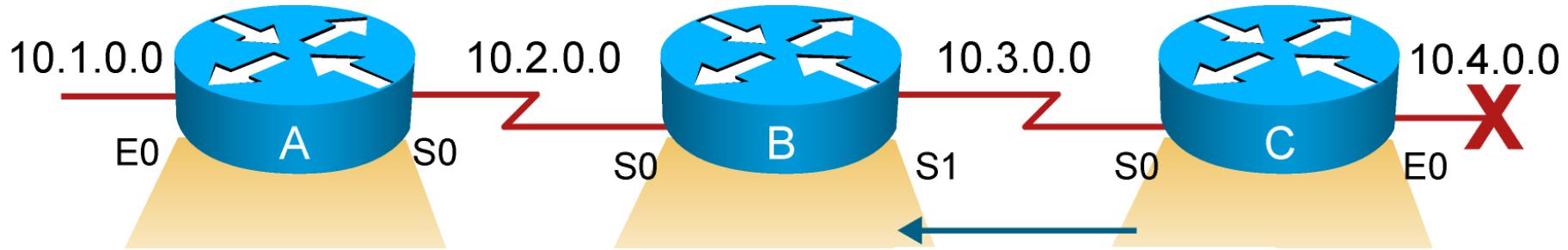
- ❖ Net 192.68.3.0/24 down
- ❖ Cause network loops

Giải pháp chống Loops - Split Horizon



Router R2 không gửi mạng mà Router R3 đã gửi

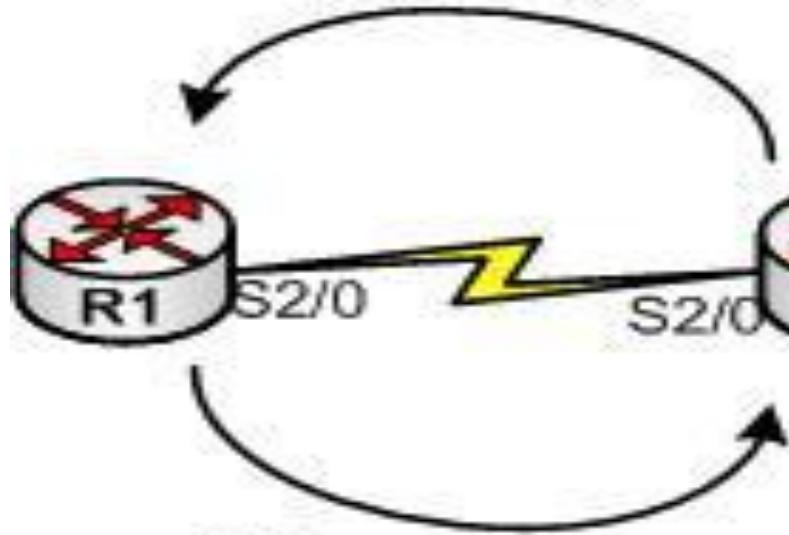
Giải pháp chống Loops - Route Poisoning



Giải pháp chống Loops

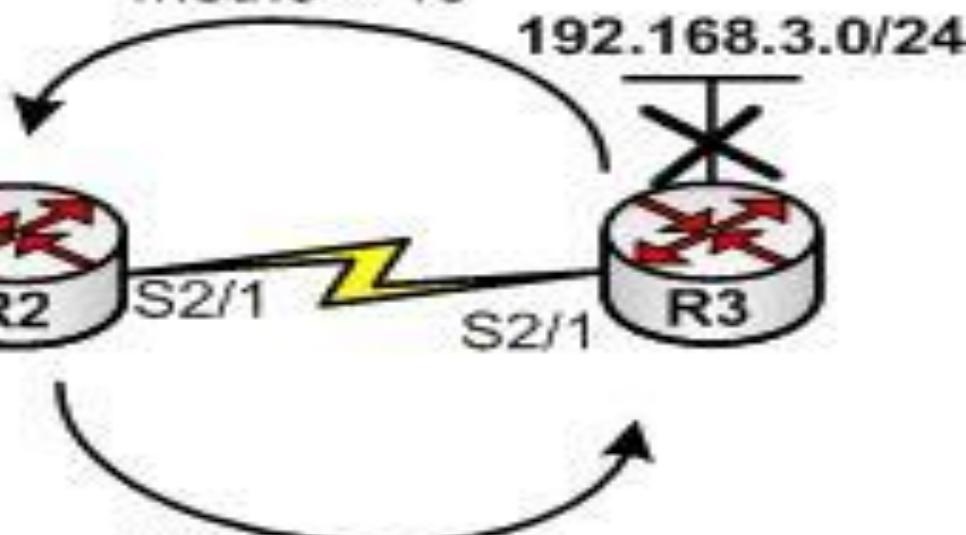
Route Poisoning and Poison Reverse

Route – poisoning
192.168.3.0/24,
metric = 16



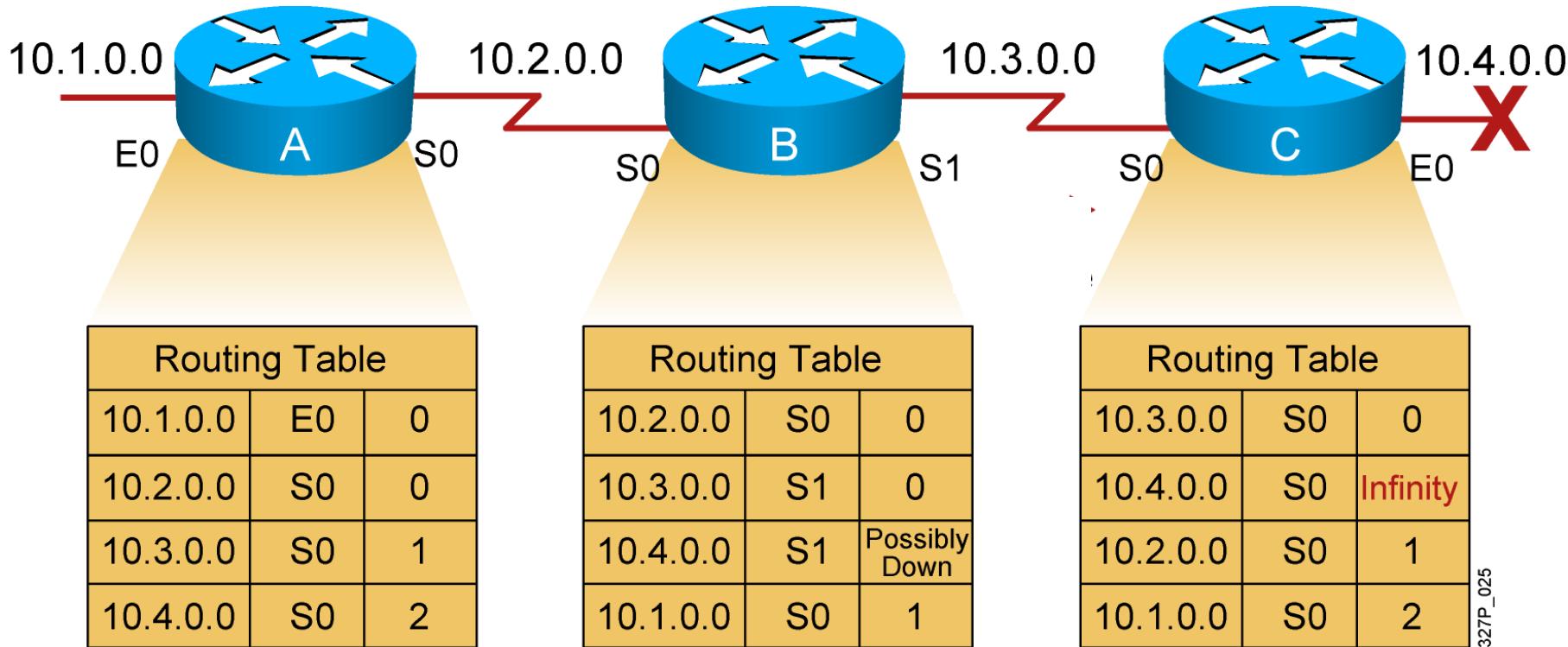
Poison – reverse
192.168.3.0/24,
metric = 16

Route – poisoning
192.168.3.0/24,
metric = 16



Poison – reverse
192.168.3.0/24,
metric = 16

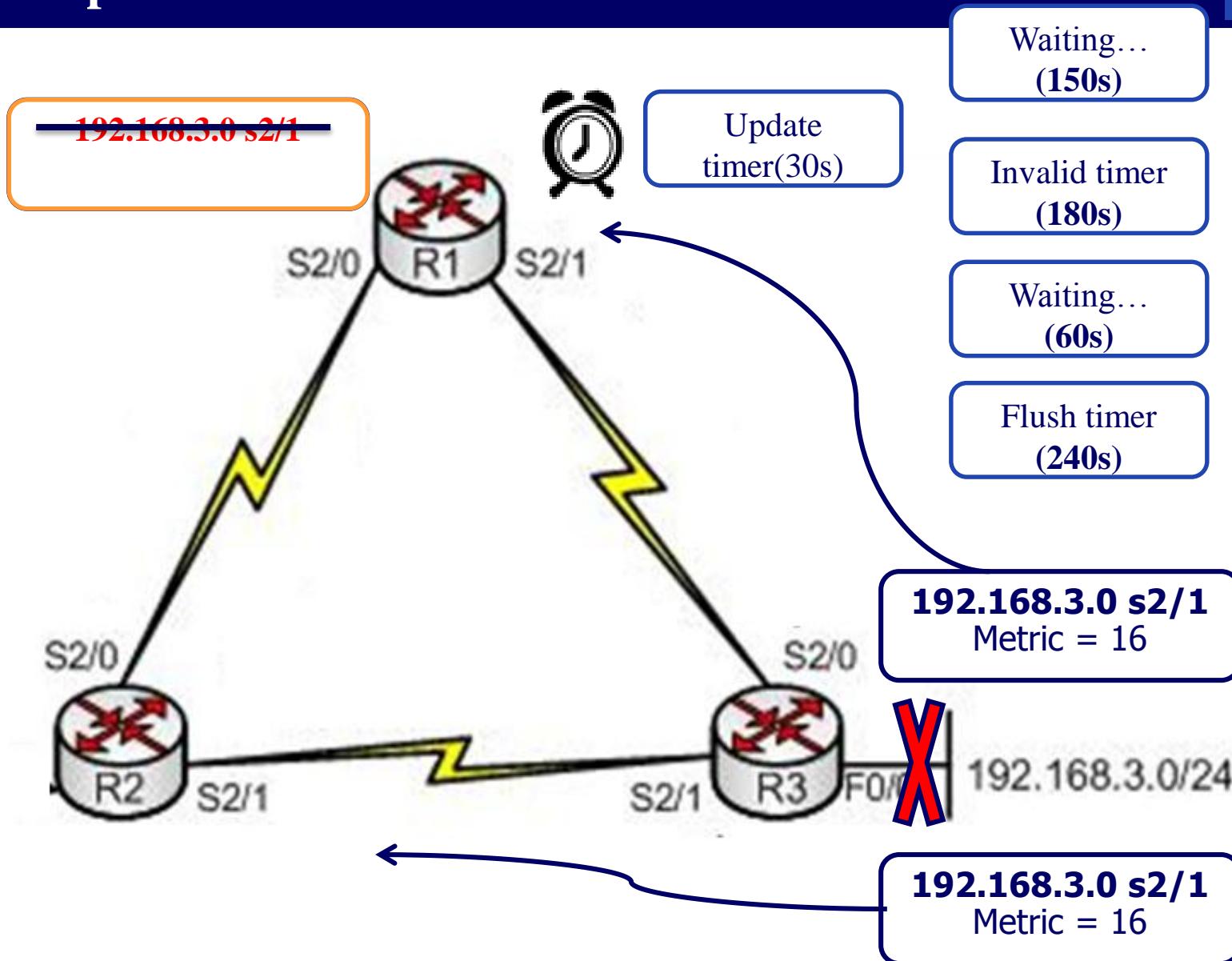
Giải pháp chống Loops - Timer



Timer: Update timer – Invalid timer – Flush timer

Giải pháp chống Loops - Timer

Update timer - Invalid timer – Flush timer

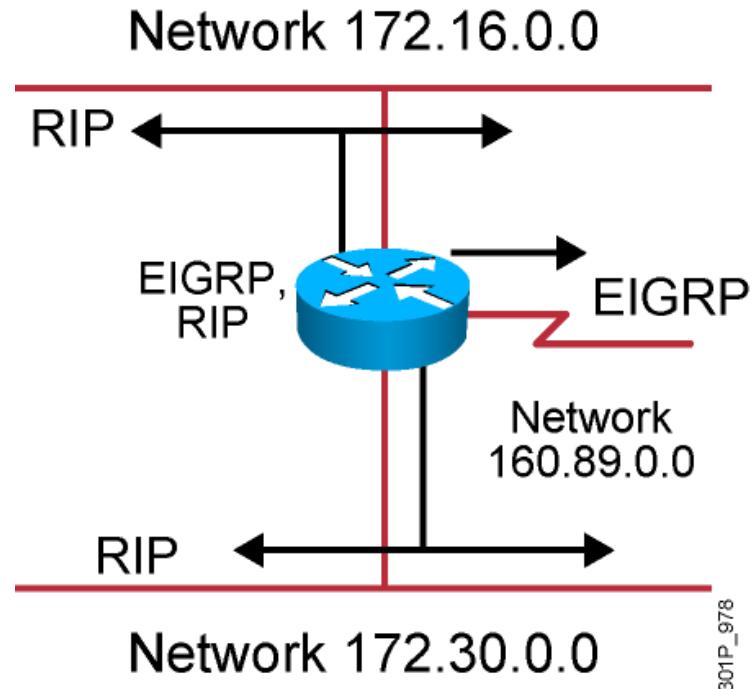


So sánh RIPv1 và RIPv2

	RIPv1	RIPv2
Routing protocol	Classful	Classless
Supports variable-length subnet mask?	No	Yes
Sends the subnet mask along with the routing update?	No	Yes
Addressing type (update route)	Broadcast 255.255.255.255	Multicast 224.0.0.9
Defined in ...	RFC 1058	RFCs 1721, 1722, and 2453
Supports manual route summarization?	No	Yes
Authentication support?	No	Yes

2. Cấu hình RIP IPv4

- Router configuration
 - Select routing protocols
 - Specify networks or interfaces



301P_978

Cấu hình RIPv2

- Bước 1: Khởi tạo tiến trình định tuyến RIP

```
RouterX(config)# router rip
```

- Bước 2: Thiết lập version cho RIP

```
RouterX(config-router)# version 2
```

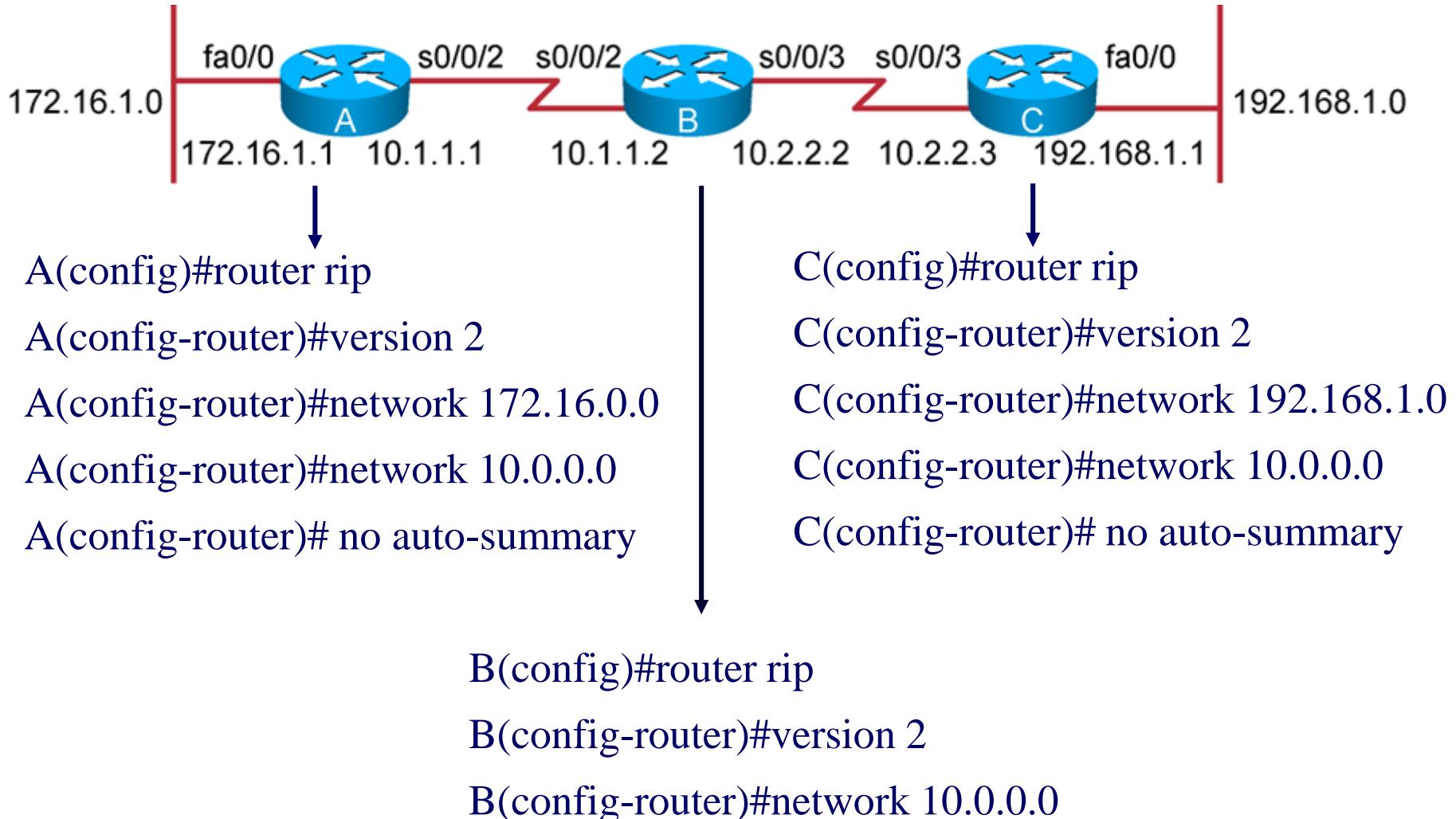
- Bước 3: Thiết lập cổng tham gia định tuyến (yêu cầu mạng chính theo đúng lớp mạng)

```
RouterX(config-router)# network network-number
```

Để quảng bá các mạng con và hỗ trợ mạng không liên tục, chúng ta phải sử dụng lệnh sau:

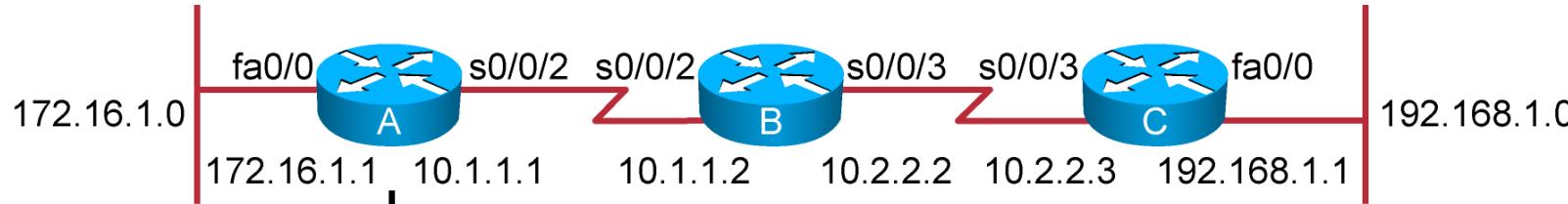
```
Router(config-router)#no auto-summary
```

Ví dụ cấu hình RIP



Thông tin cấu hình RIP

Router#Show ip protocol



30IP_97%

Routing Protocol is "rip"

Sending updates every 30 seconds, next due in 6 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip

Default version control: send version 2, receive version 2
Interface Send Recv Triggered RIP Key-chain
FastEthernet0/0 2 2
Serial0/0/2 2 2

Automatic network summarization is in effect

Maximum path: 4

Routing for Networks:

10.0.0.0
172.16.0.0

Routing Information Sources:

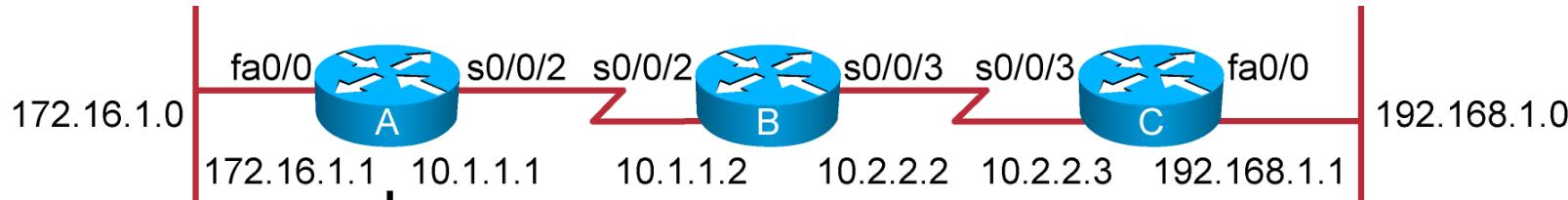
Gateway	Distance	Last Update
10.1.1.2	120	00:00:25

Distance: (default is 120)

RouterA#

Hiển thị bảng định tuyến

Router#Show ip route



301P_976

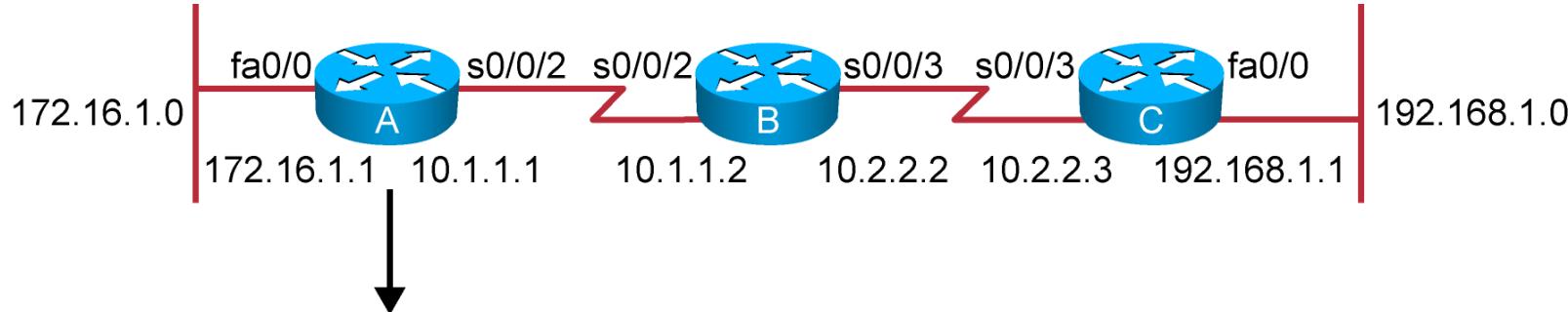
```
RouterA# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
      U - per-user static route, o - ODR
      T - traffic engineered route
```

Gateway of last resort is not set

```
      172.16.0.0/24 is subnetted, 1 subnets
C        172.16.1.0 is directly connected, fastethernet0/0
      10.0.0.0/24 is subnetted, 2 subnets
R        10.2.2.0 [120/1] via 10.1.1.2, 00:00:07, Serial0/0/2
C        10.1.1.0 is directly connected, Serial0/0/2
R        192.168.1.0/24 [120/2] via 10.1.1.2, 00:00:07, Serial0/0/2
```

Hiển thị thông tin gõ rối IP RIP

RouterA# debug ip rip



```
00:06:24: RIP: received v1 update from 10.1.1.2 on Serial0/0/2
00:06:24:      10.2.2.0 in 1 hops
00:06:24:      192.168.1.0 in 2 hops
00:06:33: RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (172.16.1.1)
00:06:34:      network 10.0.0.0, metric 1
00:06:34:      network 192.168.1.0, metric 3
00:06:34: RIP: sending v1 update to 255.255.255.255 via Serial0/0/2 (10.1.1.1)
00:06:34:      network 172.16.0.0, metric 1
```

3. Cấu hình RIP IPv6

B1: Cho phép định tuyến IPv6: R(config)#**ipv6 unicast-routing**

B2: Chọn giao thức định tuyến: R(config)#**ipv6 router rip tag**

Trong đó: tag là một chuỗi định danh, do người cấu hình tự đặt

B3. Chọn cổng tham gia vào quá trình trao đổi thông tin định tuyến: R(config-if)#**ipv6 rip tag enable**

Các lệnh kiểm tra cấu hình:

R#**show ipv6 rip**

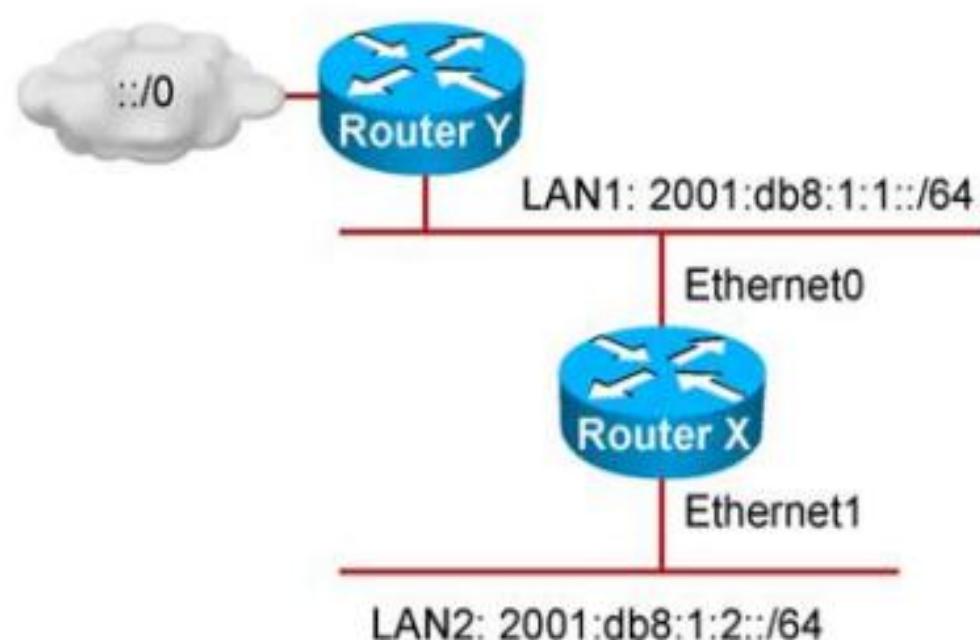
R#**show ipv6 route [rip]**

VÍ DỤ

❖ Trên Router Y

```
Y(config)#ipv6 unicast-routing
```

```
Y(config)#ipv6 router rip R1
```



```
Y#config terminal
```

```
Y(config)#int Ethernet0
```

```
Y(config-if)#ipv6 address 2001:db8:1:1::/64 eui-64
```

```
Y(config-if)#ipv6 rip R1 enable
```

❖ Trên Router X

```
X(config)#ipv6 unicast-routing
```

```
X(config)#ipv6 router rip R1
```

```
X#conf t
```

```
X(config)#int Ethernet0
```

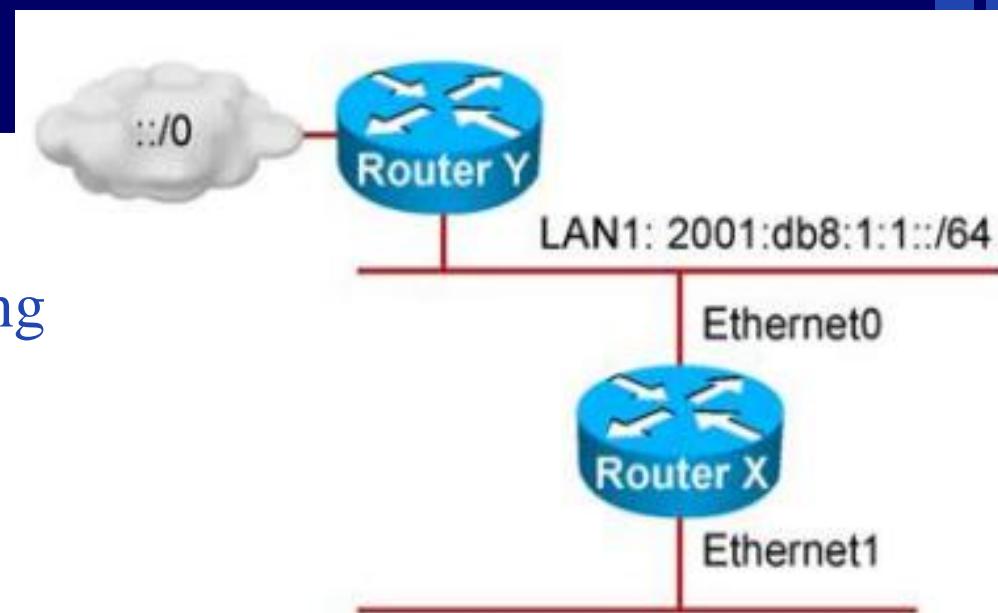
```
X(config-if)#ipv6 address 2001:db8:1:1::/64 eui-64
```

```
X(config-if)#ipv6 rip R1 enable
```

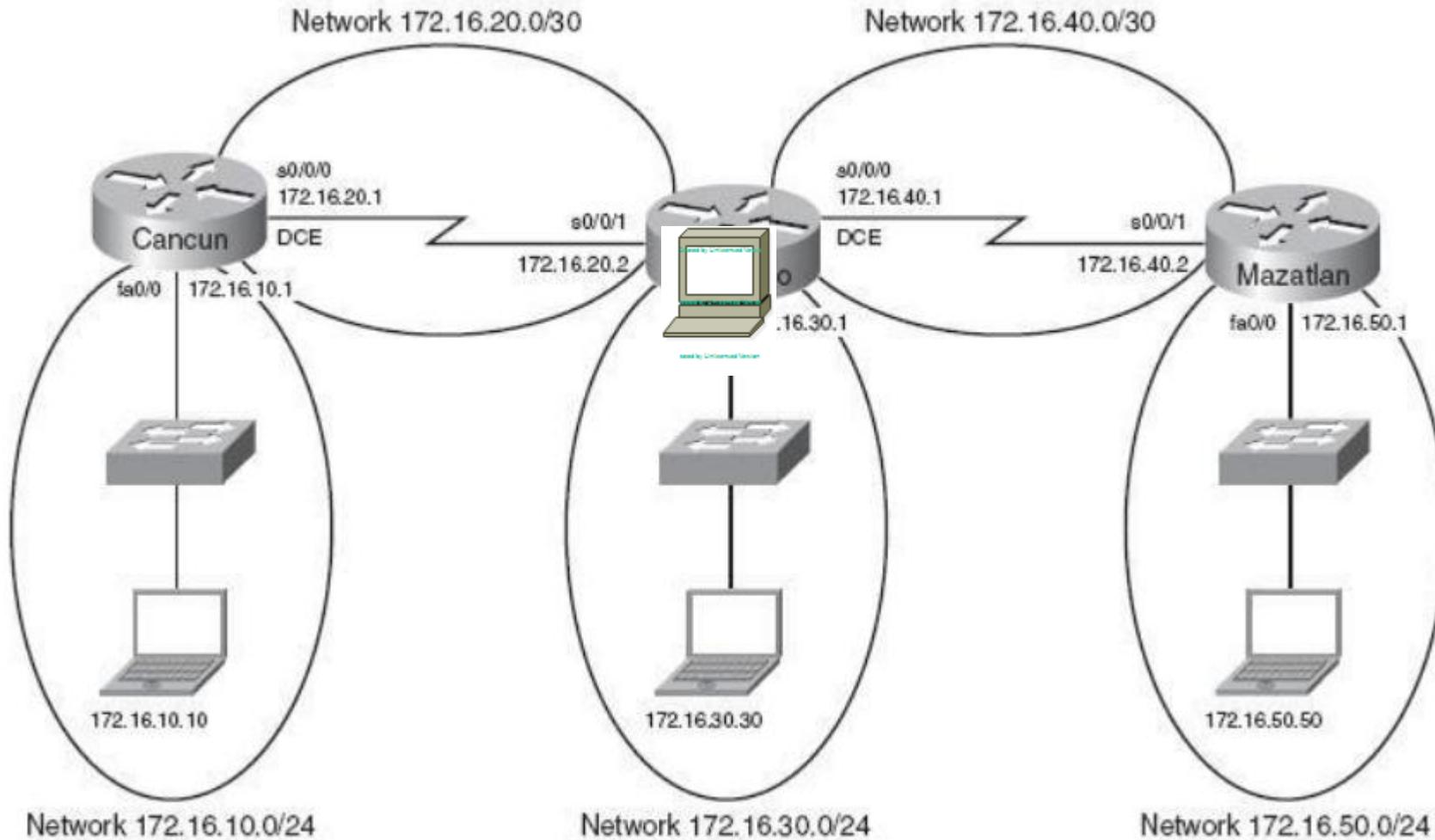
```
X(config)#int Ethernet1
```

```
X(config-if)#ipv6 address 2001:db8:1:2::/64 eui-64
```

```
X(config-if)#ipv6 rip R1 enable
```



BÀI TẬP 1: CẤU HÌNH RIPv2



Cancun Router

Cancun> enable	Chuyển cấu hình vào chế độ Privileged
Cancun# configure terminal	Chuyển cấu hình vào chế độ Global Configuration.
Cancun(config)# router rip	Enable giao thức định tuyến RIP.
Cancun(config-router)# version 2	Enable RIPv2
Cancun(config-router)# network 172.16.0.0	Quảng bá các mạng kết nối trực tiếp vào router
Cancun(config-router)# no auto-summary	Tắt tính năng auto-summarization
Cancun# copy run start	Lưu file cấu hình đang chạy trên RAM vào NVRAM

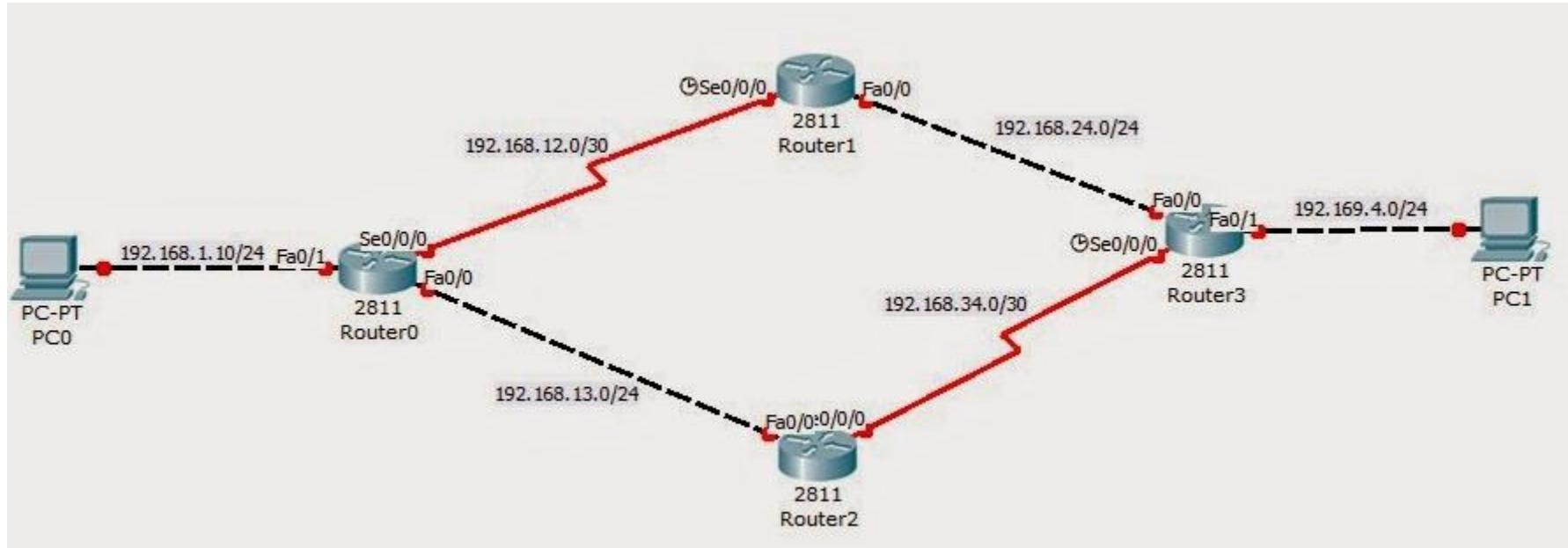
Acapulco Router

Acapulco> enable	Chuyển cấu hình vào chế độ Privileged.
Acapulco# configure terminal	Chuyển cấu hình vào chế độ Global Configuration.
Acapulco(config)# router rip	Enable giao thức định tuyến RIP.
Acapulco(config-router)# version 2	Enable RIPv2
Acapulco(config-router)# network 172.16.0.0	Quảng bá các mạng kết nối trực tiếp vào router
Acapulco(config-router)# no auto-summary	Tắt tính năng auto-summarization
Acapulco# copy run start	Lưu file cấu hình đang chạy trên RAM vào NVRAM.

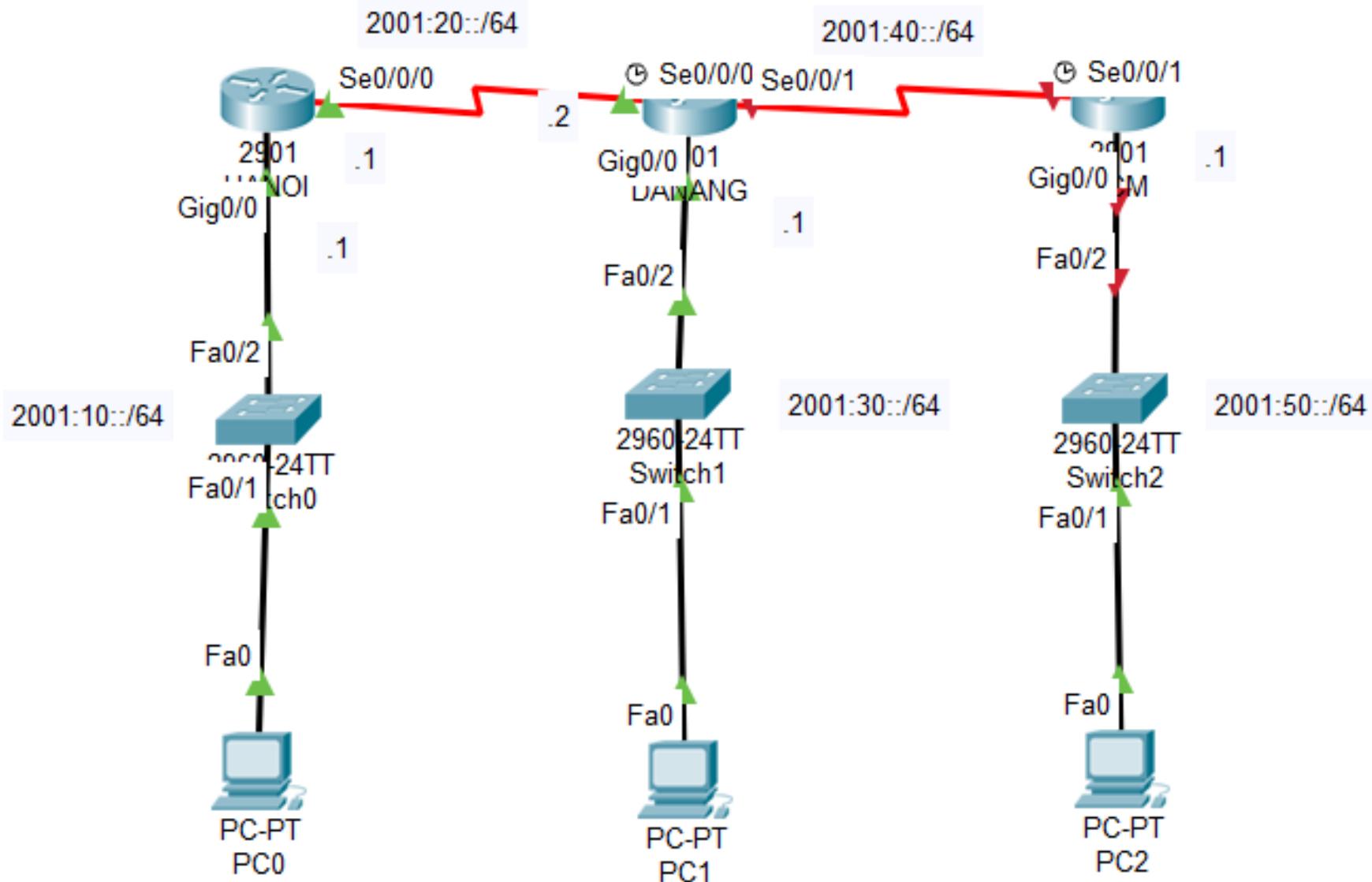
Mazatlan Router

Mazatlan> enable	Chuyển cấu hình vào chế độ Privileged.
Mazatlan# configure terminal	Chuyển cấu hình vào chế độ Global Configuration.
Mazatlan(config)# router rip	Enable giao thức định tuyến RIP.
Mazatlan(config-router)# version 2	Enable RIPv2
Mazatlan(config-router)# network 172.16.0.0	Quảng bá các mạng kết nối trực tiếp vào router
Mazatlan(config-router)# no auto-summary	Tắt tính năng auto-summarization
Mazatlan# copy run start	Lưu file cấu hình đang chạy trên RAM vào NVRAM.

BÀI TẬP 2: CẤU HÌNH RIPv2



BÀI TẬP 3: CẤU HÌNH RIPng



CHƯƠNG 2: CẤU HÌNH ĐỊNH TUYẾN

- 1 • Tổng quan về định tuyến
- 2 • Định tuyến tĩnh
- 3 • Giao thức định tuyến RIP
- 4 • Giao thức định tuyến OSPF
- 5 • Giao thức định tuyến EIGRP
- 6 • Giao thức định tuyến BGP

BÀI 4: Giao thức định tuyến OSPF

- ❖ Giao thức định tuyến OSPF (Open Shortest Path First) là giao thức định tuyến động thuộc nhóm Link-State, là chuẩn mở do IEEE đưa ra.
- ❖ Trên mỗi Router đều có bản đồ mạng của cả vùng (bảng định tuyến) thông qua việc đồng nhất bảng cơ sở dữ liệu trạng thái đường link (LSDB - Link State Database).
- ❖ Từ bản đồ mạng này Router sẽ tự tính toán ra đường đi ngắn nhất và xây dựng bảng định tuyến cho nó.
- ❖ Giao thức OSPF được sử dụng rộng rãi trong các công ty cho hệ thống mạng lớn.

1. TỔNG QUAN VỀ OSPF

- ❖ **AD = 110**
- ❖ **Metric** phụ thuộc vào Bandwidth
- ❖ Sử dụng thuật toán Dijkstra để tìm đường đi ngắn nhất.
- ❖ Hoạt động ở nhóm classless
- ❖ Chạy trên nền giao thức IP, Protocol-id = 89
- ❖ Trao đổi thông tin qua địa chỉ 224.0.0.5 và 224.0.0.6

HOẠT ĐỘNG CỦA OSPF

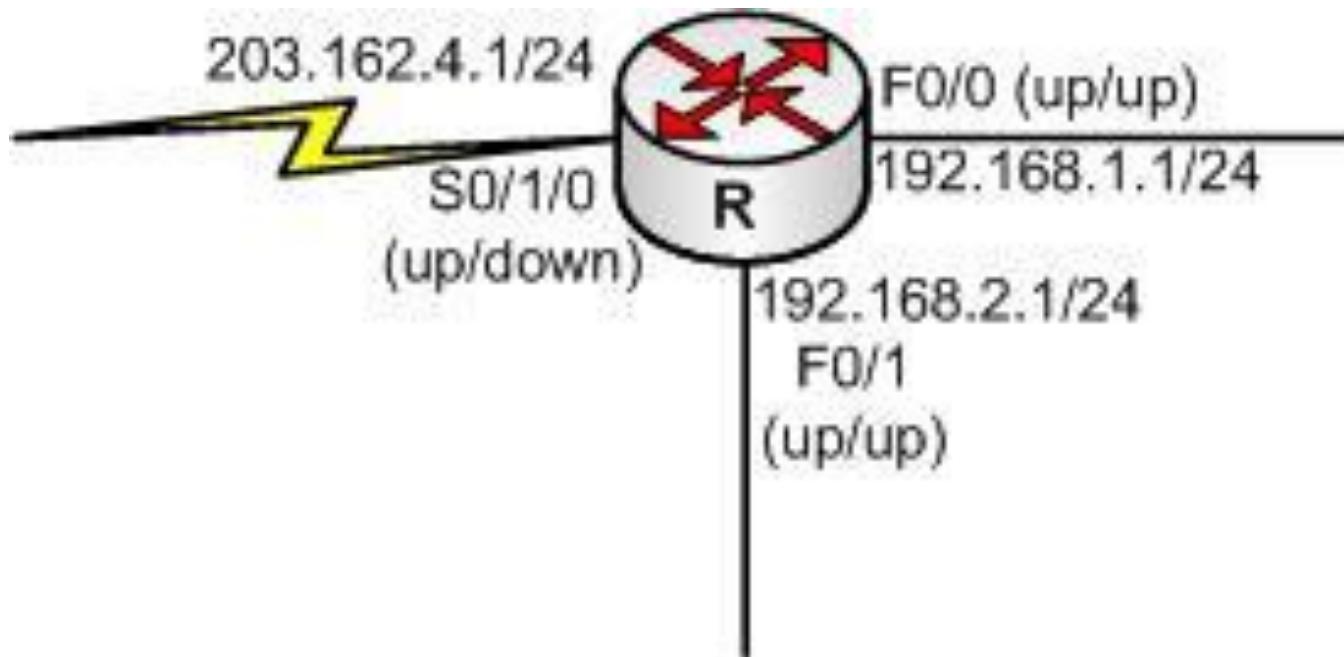
- ❖ **Bầu chọn Router-id**
- ❖ **Thiết lập quan hệ neighbor**
- ❖ **Trao đổi cơ sở dữ liệu LSDB**
- ❖ **Xây dựng bảng định tuyến**

ROUTER-ID

- ❖ Để chạy OSPF nó phải tạo ra 1 định danh để chạy gọi là Router-id (giống như CMND) có định dạng A.B.C.D (vd: IPv4:192.168.1.1)
- ❖ Để tạo ra Router-id có 2 cách
 - Cách 1: Router tự động tạo ra
 - Cách 2: Do mình tạo bằng cách config

Cách 1: Tự động tạo

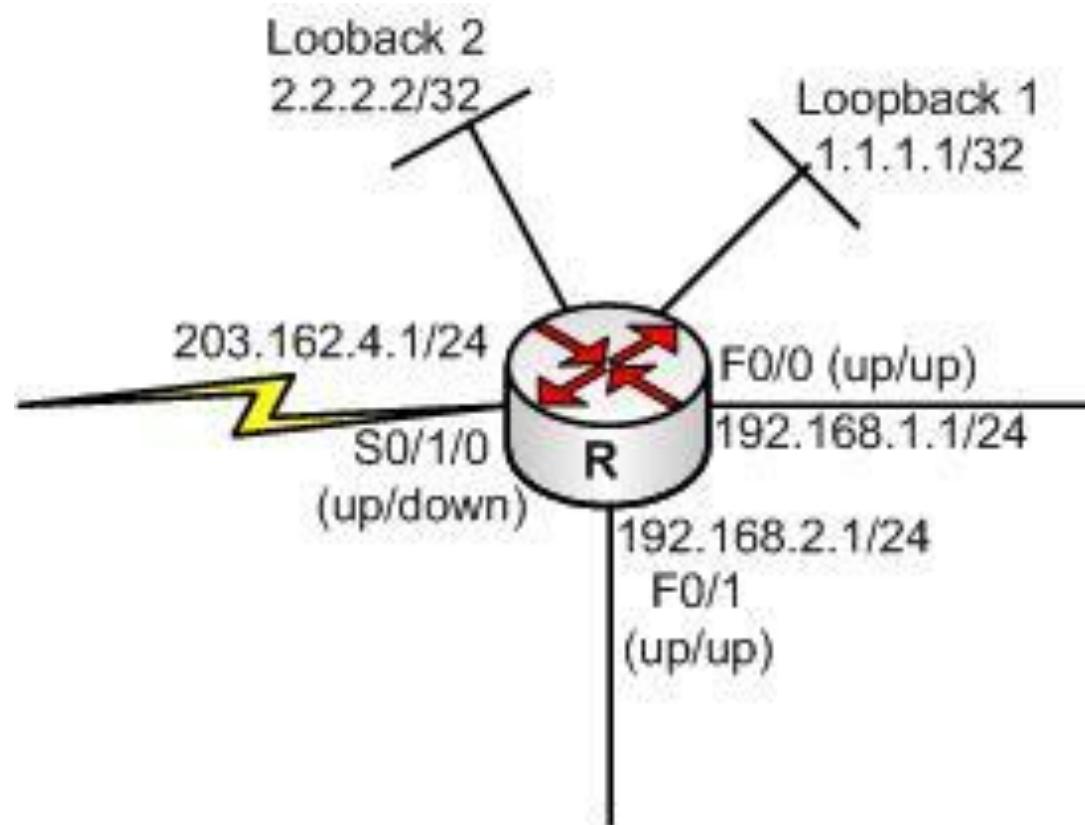
- ❖ Dựa vào interface nào có địa chỉ IP *cao nhất* trong các interface active và ưu tiên loopback để lấy IP đó làm Router-id.



=> Router-id = 192.168.2.1

Cách 1: Tự động tạo

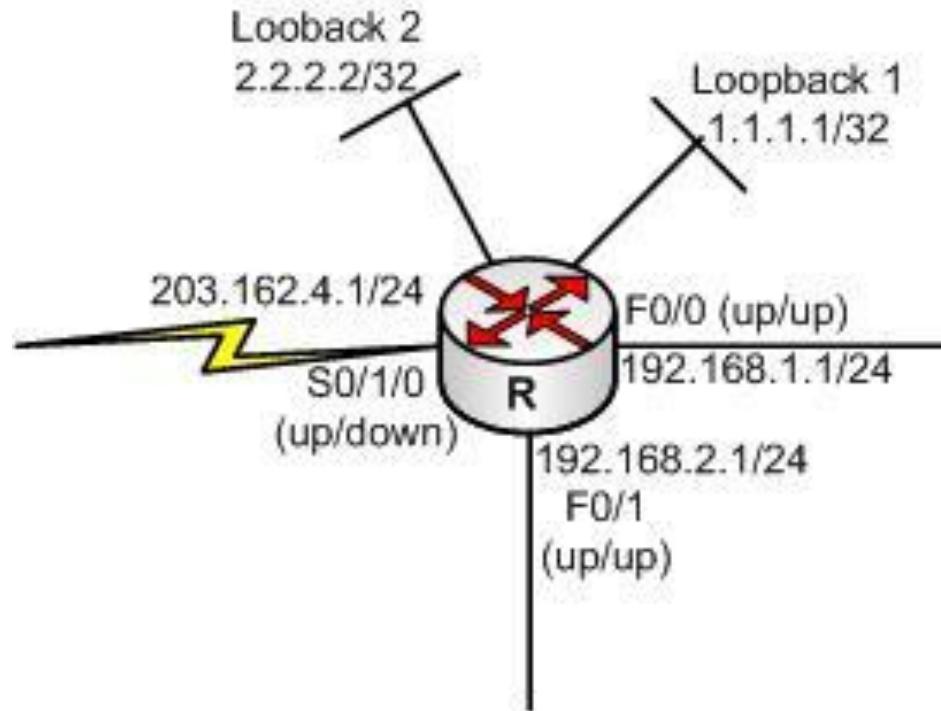
- ❖ Nếu Router có Loopback tồn tại và cho tham gia định tuyến thì Router-id ưu tiên cho Loopback trước.



=> Router-id = 2.2.2.2

Cách 2 : Admin tạo

- ❖ Router-id không nhất thiết là phải chọn IP có trên interface

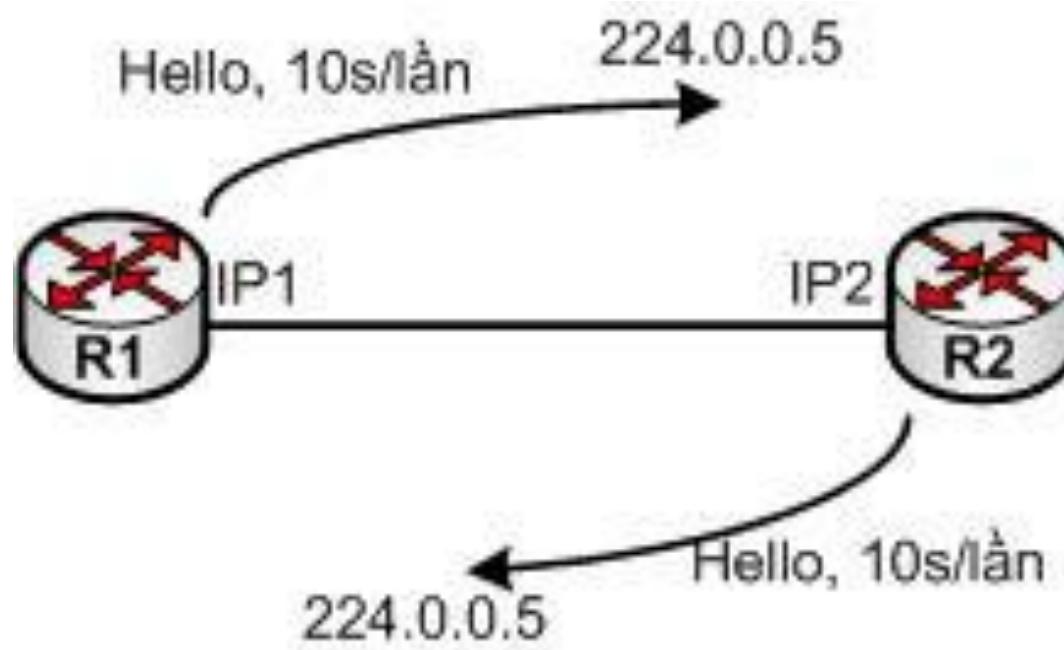


- Có thể cấu hình **Router-id = 100.100.100.100**. Ip này không thuộc interface nào của router cả.

Thiết lập Neighbor trong OSPF

Neighbor trong giao thức định tuyến OSPF

- ❖ Khi cả 2 Router đã chạy OSPF thì chúng bắt đầu gửi gói tin Hello để thiết lập neighbor.



Thiết lập Neighbor trong OSPF

Để làm neighbor của nhau thì gói tin hello của 2 router phải giống nhau 1 số thông số:

Điều kiện 1: *Cùng Area_id.*

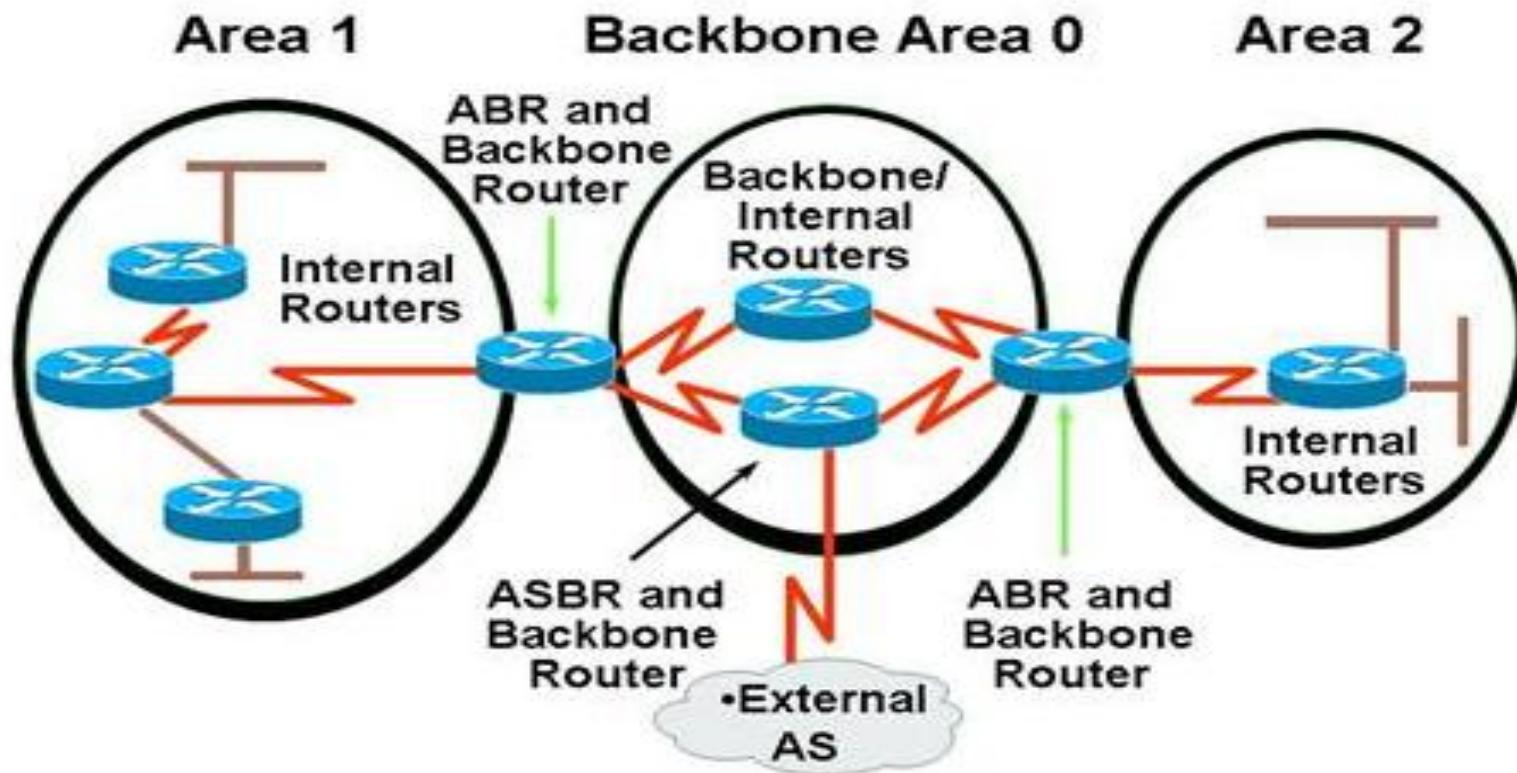
Điều kiện 2: *2 router phải cùng subnet và subnet-mask.*

Điều kiện 3: *Có cùng hello-timer/die-timer(10s/40s).*

Điều kiện 4: *Cùng loại xác thực (Authentication).*

Thiết lập Neighbor trong OSPF

Điều kiện 1: Cùng Area_id



Điều kiện 1: Cùng Area_id

- ❖ **Backbone area:** Phải có ít nhất 1 vùng. Kí hiệu: 0
- ❖ **Non-backbone are:** phải kết nối trực tiếp với vùng Backbone area. Kí hiệu: 1- 2^{52} . \Rightarrow sẽ có 1 Router đứng giữa 2 vùng
- ❖ **Backbone Router:** là Router nằm trong vùng backbone area.
- ❖ **Internal Router:** là Router nằm trong vùng non-backbone area.
- ❖ **Area Boder Router (ABR):** Router nằm giữa ranh giới backbone area và non-backbone area.
- ❖ **Autonomous System Boder Router (ASBR):** là Router biên giới giữa định tuyến OSPF và 1 giao thức định tuyến khác (nghĩa là nó vừa chạy OSPF vừa chạy RIPv2 chẳng hạn)

Thiết lập Neighbor trong OSPF

Điều kiện 2 : 2 router phải cùng subnet và subnet-mask

Ví dụ 1: R1 = 192.168.1.110/25

R2 = 192.168.1.130/25

⇒ Major-network = 192.168.1.0/24

⇒ mượn 1 bít --> bước nhảy = 128

⇒ Có 2 mạng 192.168.1.0/25 và 192.168.1.128/25

⇒ 2 router không thể là neighbor của nhau được vì 2 IP
trên khác mạng.

Thiết lập Neighbor trong OSPF

Điều kiện 2 : 2 router phải cùng subnet và subnet-mask

❖ **Ví dụ 2:**

192.168.1.110/25 và 192.168.1.11/26

2 router cùng mạng nhưng không thể làm neighbor của nhau vì *không cùng subnet-mask*

Thiết lập Neighbor trong OSPF

- ❖ **Điều kiện 3:** *Có cùng hello-timer/die-timer(10s/40s)*
- ❖ **Điều kiện 4:** *Cùng loại xác thực.*
cùng là plain-text cùng xác thực MD5
=> khi cả 4 điều kiện trên giống nhau thì 2 Router có thể làm neighbor của nhau (Two – Way).

CÁC BƯỚC THỰC HIỆN ĐỊNH TUYẾN OSPF

- ❖ B1: Thiết lập được neighbor của nhau. Sau đó liệt kê các neighbor vào trong neighbor của mình. Lúc này, mỗi quan hệ giữa các neighbor gọi là 2-way.
- ❖ B2: Bắt đầu gửi thông tin trạng thái đường link để dựng lên 1 bảng database (bảng topology).
- ❖ B3: Từ bảng topology nó bắt đầu dùng thuật toán Dijkstra để tìm ra đường đi tối ưu để đưa ra bảng định tuyến.

QUÁ TRÌNH TRAO ĐỔI BẢN TIN

- ❖ Sau khi ở trạng thái 2-way thì nó bắt đầu gửi thông tin cho nhau để hình thành lên 1 bảng database gọi là LSDB (Link-state database)
- ❖ **Gđ1:** Router gửi 1 bản tin *DBD* (*Database Description*) để mô tả những thông tin mà nó có được cho router neighbor.
- ❖ **Gđ2:** Khi neighbor nhận được DBD nếu nó thấy thông tin nào trong DBD mà nó không có thì nó sẽ gửi *LSR* (*link state request*) để xin thông tin thiếu.

QUÁ TRÌNH TRAO ĐỔI BẢN TIN

- ❖ **Gđ3:** Khi router nhận được request LSR thì nó phải cho những thông tin thiếu cho router xin bằng LSA (Link state Advertisement) nằm bên trong *LSU (Link state update)*.
- ❖ **Gđ4:** Khi router xin nhận được LSU thì nó bỏ phần LSU lấy phần LSA. Khi nhận xong nó phải trả lời lại là đã nhận được bằng *LSACK (link state acknowledgment)*
- ❖ ==> Sau khi có LSDB thì router có thể tự chọn được đường đi tốt nhất dựa vào thuật toán Dijkstra

MÔI TRƯỜNG MẠNG

- ❖ Tùy thuộc vào mỗi 1 môi trường mạng thì nó có 1 cách trao đổi khác nhau để nó tìm được đường đi tốt nhất.
- ❖ Trong môi trường mạng có 2 môi trường chính:

1. Point to point:

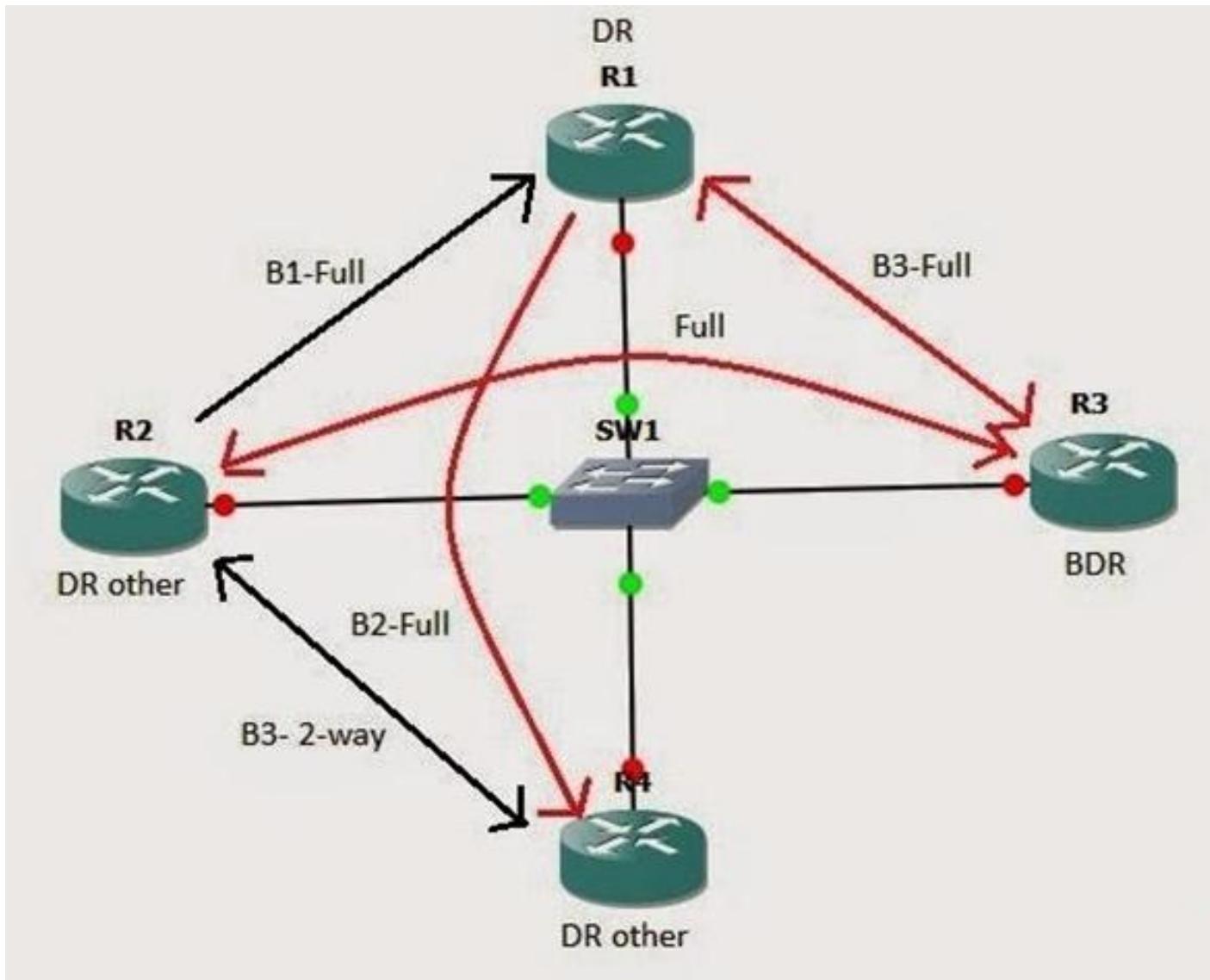
- ❖ Là môi trường mà 2 router kết nối với nhau bằng cổng serial (WAN).
- ❖ Khi ở môi trường này thì các router gửi SLDB trực tiếp qua nhau thì từ mối quan hệ 2-way chuyển sang mối quan hệ FULL (nếu không quan hệ trực tiếp với nhau thì ko cần chuyển quan hệ 2-way)

MÔI TRƯỜNG MẠNG

2. Broadcast multi access:

- ❖ Các router kết nối với nhau = interface LAN.
- ❖ Trước khi trao đổi thông tin thì các router sẽ bầu chọn ra 1 router đóng vai trò làm chủ đạo gọi là **DR (designated router)** có nhiệm vụ tiếp nhận các thông tin trao đổi và gửi qua cho các router khác.
- ❖ **BDR (backup designated router)** là router dự phòng cho DR.
- ❖ **DR other:** Những router còn lại. Những router không nói chuyện trực tiếp với nhau (vẫn giữ trạng thái 2-way) mà phải thông qua DR. Đồng thời DR gửi thông tin copy cho BDR để backup

MÔI TRƯỜNG MẠNG



TÍNH COST TRONG OSPF

- ❖ Trong OSPF không còn gọi là Metric mà gọi là Cost (Cost trên interface)
- ❖ *Cost được tính khi đi vào 1 cổng và đi ra không tính*
- ❖ Công thức tính cost như sau:

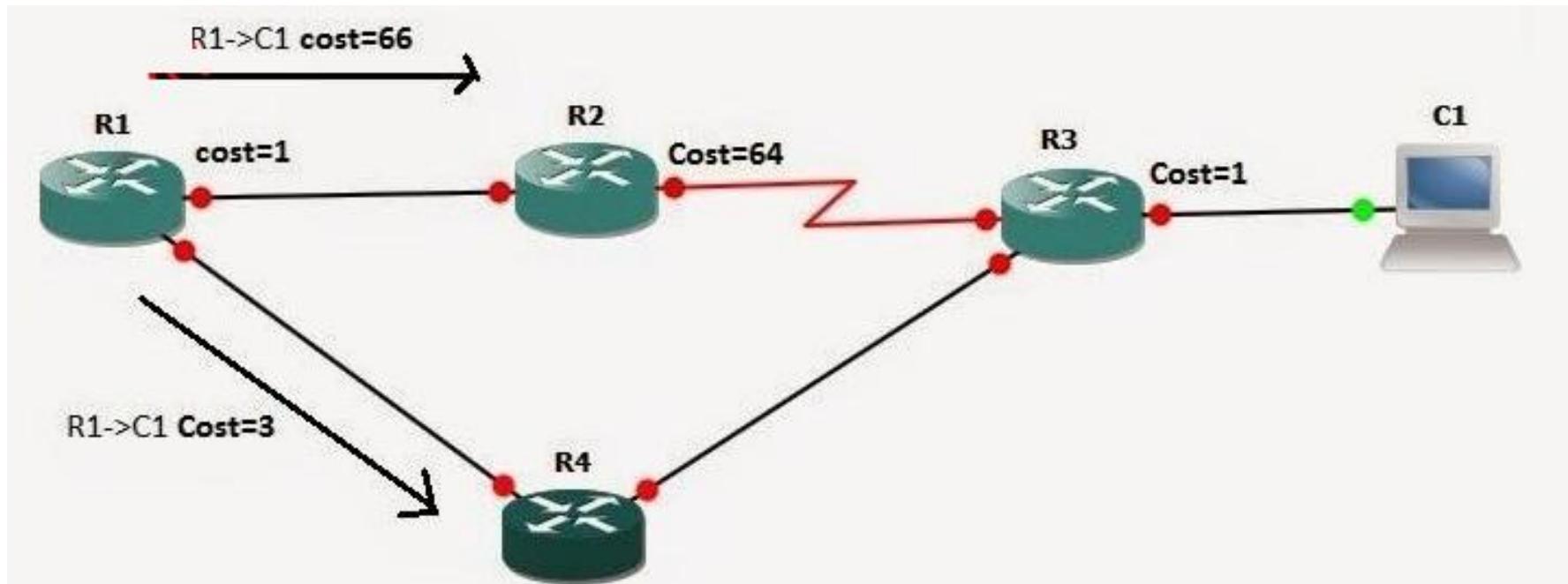
$$\text{Cost} = 10^8 / \text{bandwidth}$$

- Ethernet(10Mbps) --> Cost = 10
- FastEthernet(100Mbps) --> cost=1
- Serial(1,544Mbps) --> cost=64

COST MẶC ĐỊNH TRONG OSPF

Link Bandwidth	Default OSPF cost
56Kbps serial link	1785
64Kbps serial link	1562
T1 (1.544Mbps) serial link	65
E1 (2.048Mbps) serial link	48
4Mbps Token Ring	25
Ethernet	10
16Mbps Token Ring	6
FDDI or Fast Ethernet	1
Gigabit Ethernet / 10G network	1

Ví dụ:



❖ Để tính cost từ R1--> C1 ta tính ngược lại như sau:

Từ C1 --> đi vào f0/1 R3(+cost=1) --> đi ra s0/0/0 R3(+0) --> đi vào f0/1 R2(+64) --> đi ra f0/0 R2(+0) --> đi vào f0/0 R1(+1).

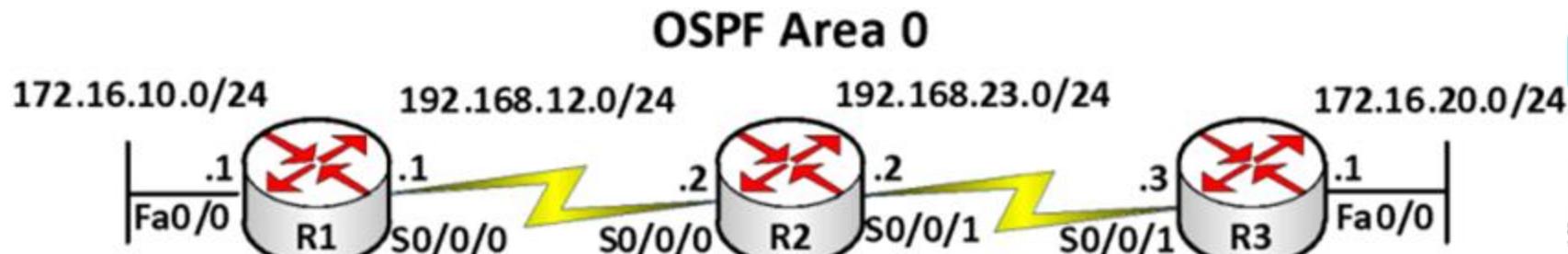
Ví dụ:

- ❖ Ở đây để Router sẽ chọn đường có cost = 3. Để có thể loadbalancing trong sơ đồ này ta cần thay đổi **Bandwidth**: việc thay đổi bandwidth nào chỉ nhằm mục đích thay đổi giá trị cost nó không ảnh hưởng gì đến traffic của interface
- ❖ **Cost**: ở đường dưới ta thấy tại f0/0 của R3 cost=1 ta không thể hạ cost được nữa vì cost = 1 là giá trị minimum. Vì vậy trong sơ đồ trên ta nên tăng cost ở f0/1 lên sao cho tổng cost của 2 đường đều = 66.

2. CẤU HÌNH ĐỊNH TUYẾN OSPF IPv4

- ❖ Bước 1: Khởi tạo tiến trình định tuyến OSPF
 - Router(config)#**router ospf <process-id>**
- ❖ Bước 2: Chọn cổng tham gia trao đổi thông tin định tuyến
 - Router(config-router)#**network <address> <wildcard-mask> area <area-id>**
- *Process-id: chỉ số tiến trình của OSPF, mang tính chất cục bộ, có giá trị 1 đến 65535.*
- *Address: địa chỉ cổng tham gia định tuyến*
- *Wildcard mask: điều kiện kiểm tra giữa địa chỉ cấu hình trong address và địa chỉ các cổng trên router, tương ứng bit 0 – phải so khớp, bit 1 – không cần kiểm tra.*
- *Area-id: vùng mà cổng tương ứng thuộc về trong kiến trúc OSPF.*

CẤU HÌNH ĐỊNH TUYẾN OSPF



R1> Enable

R1# configure terminal

R1(config)# router ospf 1

R1(config-router)# network 172.16.10.1 0.0.0.0 area 0

R1(config-router)# network 192.168.12.1 0.0.0.0 area 0

R2(config-router)# network 192.168.12.0 0.0.0.255 area 0

R2(config-router)# network 192.168.23.0 0.0.0.255 area 0

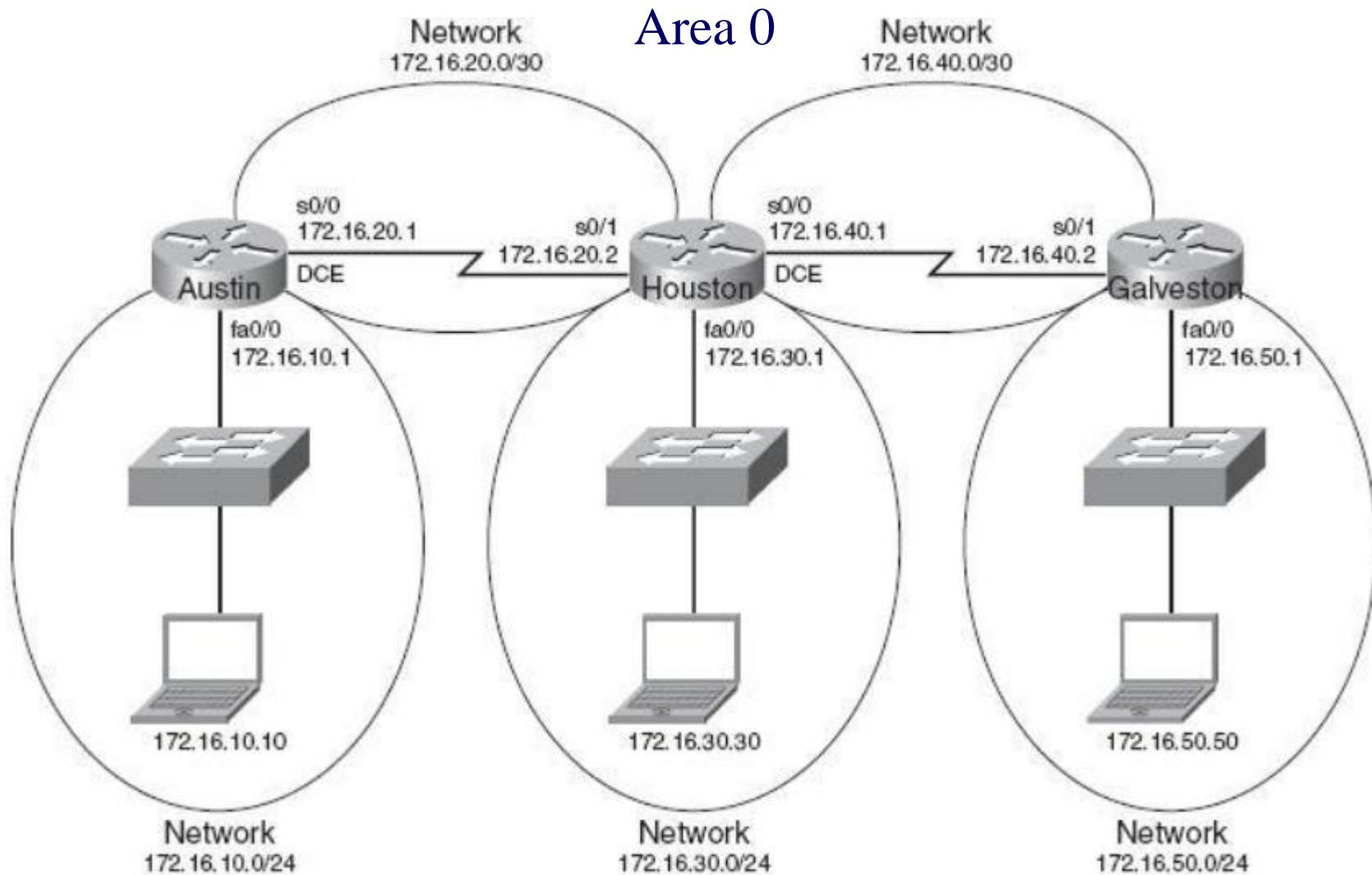
R3(config-router)# network 192.168.23.3 0.0.0.0 area 0

R3(config-router)# network 192.168.20.1 0.0.0.0 area 0

Các câu lệnh kiểm tra cấu hình OSPF

- ❖ Router#show ip protocol
- ❖ Router#show ip route
- ❖ Router#show ip ospf interface
- ❖ Router#show ip ospf neighbor
- ❖ Router#debug ip ospf events
- ❖ Router#debug ip ospf packet

VÍ DỤ: CẤU HÌNH ĐỊNH TUYẾN OSPF CHO IPv4



Router Austin

Router>enable	Chuyển cấu hình vào chế độ Privileged
Router#configure terminal	Chuyển cấu hình vào chế độ Global Configuration
Router(config)#hostname Austin	Cấu hình tên router là Austin
Austin(config)#interface fastethernet 0/0	Chuyển cấu hình vào chế độ interface fa0/0
Austin(config-if)#ip address 172.16.10.1 255.255.255.0	Gán địa chỉ IP và subnetmask cho interface fa0/0
Austin(config-if)#no shutdown	Enable Interface.
Austin(config-if)#interface serial 0/0	Chuyển vào chế độ cấu hình của interface s0/0
Austin(config-if)#ip address 172.16.20.1 255.255.255.252	Gán địa chỉ ip và subnetmask cho interface

Router Austin

Austin(config-if)#clock rate 56000	Cấu hình clock rate cho interface DCE
Austin(config-if)#no shutdown	Enable Interface
Austin(config-if)#exit	Trở về chế độ cấu hình Global Configuration
Austin(config)#router ospf 1	Cho phép router chạy giao thức định tuyến OSPF với Process ID là 1
Austin(config-router)#network 172.16.10.0 0.0.0.255 area 0	Thực hiện quảng bá các mạng kết nối trực tiếp vào interface của router trong area 0
Austin(config-router)#network 172.16.20.0 0.0.0.255 area 0	Thực hiện quảng bá các mạng kết nối trực tiếp vào interface của router trong area 0
Austin#copy running-config startup-config	Lưu file cấu hình đang chạy trên RAM vào NVRAM

Router Houston

Router>enable	Chuyển cấu hình vào chế độ Privileged
Router#configure terminal	Chuyển cấu hình vào chế độ Global Configuration
Router(config)#hostname Houston	Cấu hình tên router là Houston
Houston(config)#interface fastethernet 0/0	Chuyển cấu hình vào chế độ interface fa0/0
Houston(config-if)#ip address 172.16.30.1 255.255.255.0	Gán địa chỉ IP và subnetmask cho interface fa0/0
Houston(config-if)#no shutdown	Enable Interface
Houston(config-if)#interface serial0/0	Chuyển vào chế độ cấu hình của interface s0/0
Houston(config-if)#ip address 172.16.40.1 255.255.255.252	Gán địa chỉ ip và subnetmask cho interface

Router Houston

Houston(config-if)#clock rate 56000	Cấu hình clock rate cho interface DCE
Houston(config-if)#no shutdown	Enable Interface
Houston(config)#interface serial 0/1	Chuyển vào chế độ cấu hình của interface s0/1
Houston(config-if)#ip address 172.16.20.2 255.255.255.252	Gán địa chỉ ip và subnetmask cho interface
Houston(config-if)#no shutdown	Enable Interface
Houston(config-if)#exit	Chuyển cấu hình vào chế độ Global Configuration
Houston(config)#router ospf 1	Cho phép router chạy giao thức định tuyến OSPF với Process ID là 1
Houston(config-router)#network 172.16.0.0 0.0.255.255 area 0	Thực hiện quảng bá các mạng kết nối trực tiếp vào interface của router trong area 0
Houston(config-router)#<ctrl> z	Trở về chế độ cấu hình Privileged
Houston#copy running-config startupconfig	Lưu file cấu hình đang chạy trên RAM vào NVRAM

Router Galveston

Router>enable	Chuyển cấu hình vào chế độ Privileged
Router#configure terminal	Chuyển cấu hình vào chế độ Global Configuration
Router(config)#hostname Galveston	Cấu hình tên router là Galveston
Galveston(config)#interface fastethernet 0/0	Chuyển cấu hình vào chế độ interface fa0/0
Galveston(config-if)#ip address 172.16.50.1 255.255.255.0	Gán địa chỉ ip và subnetmask cho interface
Galveston(config-if)#no shutdown	Enable Interface
Galveston(config-if)#interface serial 0/1	Chuyển vào chế độ cấu hình của interface s0/1
Galveston(config-if)#ip address 172.16.40.2 255.255.255.252	Gán địa chỉ ip và subnetmask cho interface

Router Galveston

Galveston(config-if)#no shutdown	Enable Interface
Galveston(config-if)#exit	Chuyển cấu hình vào chế độ Global Configuration
Galveston(config)#router ospf 1	Cho phép router chạy giao thức định tuyến OSPF với Process ID là 1
Galveston(config-router)#network 172.16.40.2 0.0.0.0 area 0	Thực hiện quảng bá các mạng kết nối trực tiếp vào interface của router trong area 0
Galveston(config-router)#network 172.16.50.1 0.0.0.0 area 0	Thực hiện quảng bá các mạng kết nối trực tiếp vào interface của router trong area 0
Galveston(config-router)#<ctrl> z	Trở về chế độ cấu hình Privileged
Galveston#copy running-config startup-config	Lưu file cấu hình đang chạy trên RAM vào NVRAM

3. CẤU HÌNH ĐỊNH TUYẾN OSPF IPv6

- ❖ **B1: Bật tính năng định tuyến cho Ipv6**

R(config)#ipv6 unicast-routing

- ❖ **B2: Chọn giao thức định tuyến**

R(Config)#ipv6 router ospf <process-id>

R(config-router)#router-id H.H.H.H

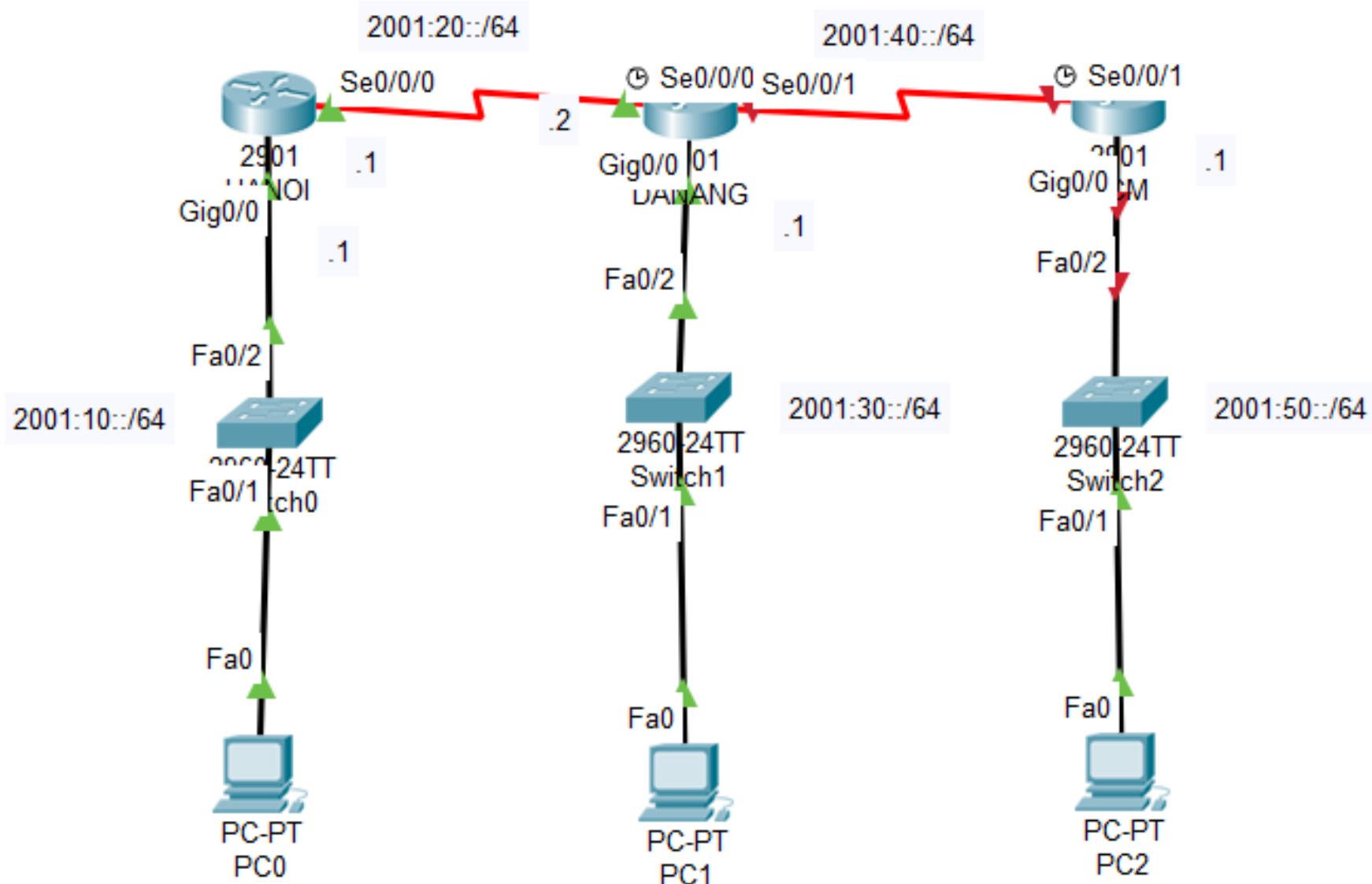
- ❖ **B3. Chọn cổng tham gia vào quá trình trao đổi thông tin định tuyến**

R(Config-if)#ipv6 ospf <process-id> area <area-id>

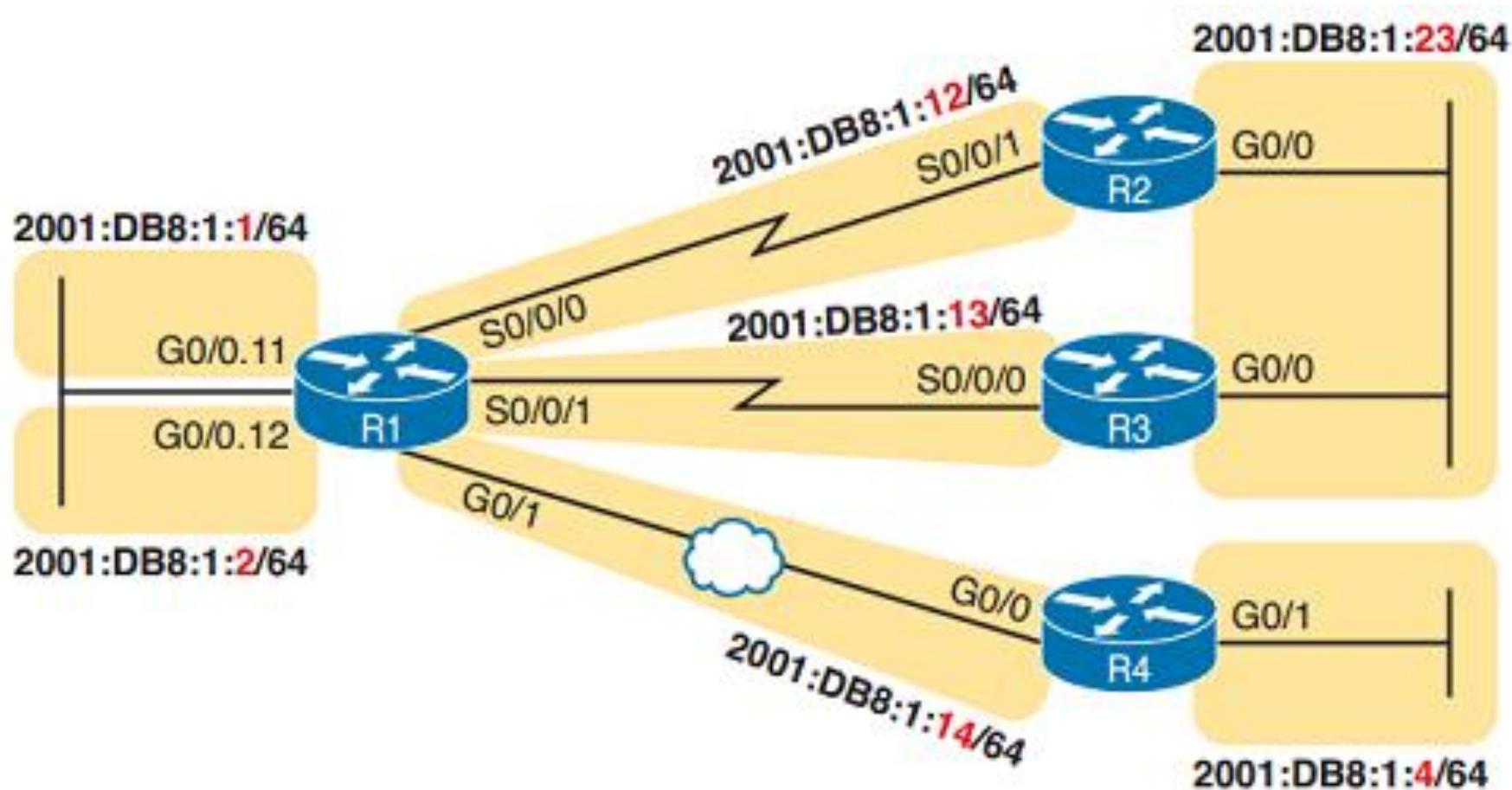
CÁC LỆNH KIỂM TRA CẤU HÌNH

- ❖ R#show ipv6 protocols
- ❖ R#show ipv6 ospf neighbor
- ❖ R#show ipv6 ospf database
- ❖ R#show ipv6 route [ospf]

BÀI TẬP 1: CẤU HÌNH OSPF CHO IPv6



BÀI TẬP 2: CẤU HÌNH OSPF CHO IPv6



CHƯƠNG 2: CẤU HÌNH ĐỊNH TUYẾN

- 1 • Tổng quan về định tuyến
- 2 • Định tuyến tĩnh
- 3 • Giao thức định tuyến RIP
- 4 • Giao thức định tuyến OSPF
- 5 • Giao thức định tuyến EIGRP
- 6 • Giao thức định tuyến BGP

BÀI 5: GIAO THỨC ĐỊNH TUYẾN EIGRP

- ❖ EIGRP là giao thức định tuyến do cisco tạo ra, chỉ hoạt động trên các thiết bị của cisco.
- ❖ EIGRP là một giao thức định tuyến lai nó vừa mang những đặc điểm của distance-vector vừa mang một số đặc điểm của link-state.
- ❖ EIGRP là giao thức định tuyến classless.
- ❖ EIGRP hỗ trợ VLSM và CIDR nên sử dụng hiệu quả không gian địa chỉ sử dụng địa chỉ multicast 224.0.0.10 để trao đổi thông tin cập nhật định tuyến.
- ❖ Khả năng cân bằng tải load balancing.

METRIC CỦA EIGRP

$$metric_{EIGRP} = \left[K1 * BW + \frac{K2 * BW}{(256 - load)} + K3 * Delay \right] * \frac{K5}{(reliability + K4)}$$

Với K_1, K_2, K_3, K_4, K_5 là hàng số

Mặc định $K_1 = 1, K_2 = 0, K_3 = 1, K_4 = 0, K_5 = 0$

Do đó, ta có: Metric = bandwidth + delay

Default	K1	K2	K3	K4	K5
	1	0	1	0	0
tos	BW	Load	Delay	Reliability	

EIGRP HỌC CÁC MẠNG ĐÍCH

- ❖ Các router phát hiện các láng giềng của nó, danh sách các láng giềng được lưu giữ trong “neighbor table”.
- ❖ Mỗi router sẽ trao đổi các thông tin về cấu trúc mạng với các láng giềng của nó.
- ❖ Router đặt những thông tin về cấu trúc hệ thống mạng học được vào cơ sở dữ liệu về cấu trúc mạng (topology table).
- ❖ Router chạy thuật toán DUAL với cơ sở dữ liệu đã thu thập được ở bước trên để tính toán tìm ra đường đi tốt nhất đến mỗi một mạng trong cơ sở dữ liệu.

IGRP CHỐNG “ROUTING LOOP”

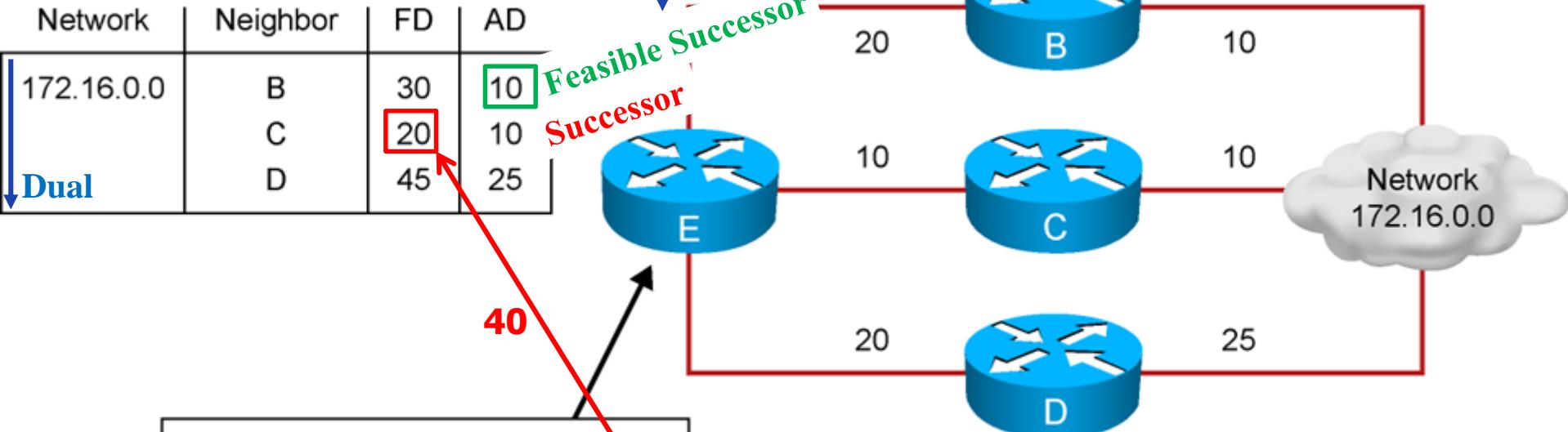
- ❖ Các giao thức định tuyến dạng “link-state” vượt qua vấn đề này bằng cách mỗi router đều nắm giữ toàn bộ cấu trúc mạng.
- ❖ Trong giao thức EIGRP, khi tuyến đường đi chính gặp sự cố, router có thể kịp thời đặt đường đi dự phòng vào bảng định tuyến đóng vai trò như đường đi chính.
- ❖ Trường hợp không có đường đi dự phòng, EIGRP sử dụng thuật toán DUAL cho phép router gửi các yêu cầu và tính toán lại các đường đi đến đích.

EIGRP HỌC CÁC MẠNG ĐÍCH

- ❖ Router đặt các đường đi tốt nhất đến mỗi mạng đích vào bảng định tuyến.
- ❖ Trong EIGRP có hai tuyến ta cần quan tâm là “successor route” và “fossible successor route”.
- Successor route: là tuyến đường đi chính được sử dụng để chuyển dữ liệu đến đích, được lưu trong bảng định tuyến. EIGRP cho phép chia tải tối đa trên 16 đường (mặc định là 4 đường) đến mỗi mạng đích.
- Fossible successor route: là đường đi dự phòng cho đường đi chính và được lưu trong bảng cấu trúc mạng (topology table).

EIGRP: Load Balancing

```
RouterE# show ip route
D 172.16.0.0 [90/409600] via RouterC, F0/2
D 172.16.0.0 [90/409600] via RouterB, F0/1
```



```
(config)#router eigrp 200
(config-router)#variance 2
```

Chọn AD < Variance*FDmin

FD = feasible distance
AD = advertised distance
AD = advertised distance

HOẠT ĐỘNG CỦA EIGRP

❖ Thiết lập Neighbor trong EIGRP

Để làm neighbor của nhau thì gói tin hello của 2 router phải giống nhau 1 số thông số:

Điều kiện 1: *Cùng AS.*

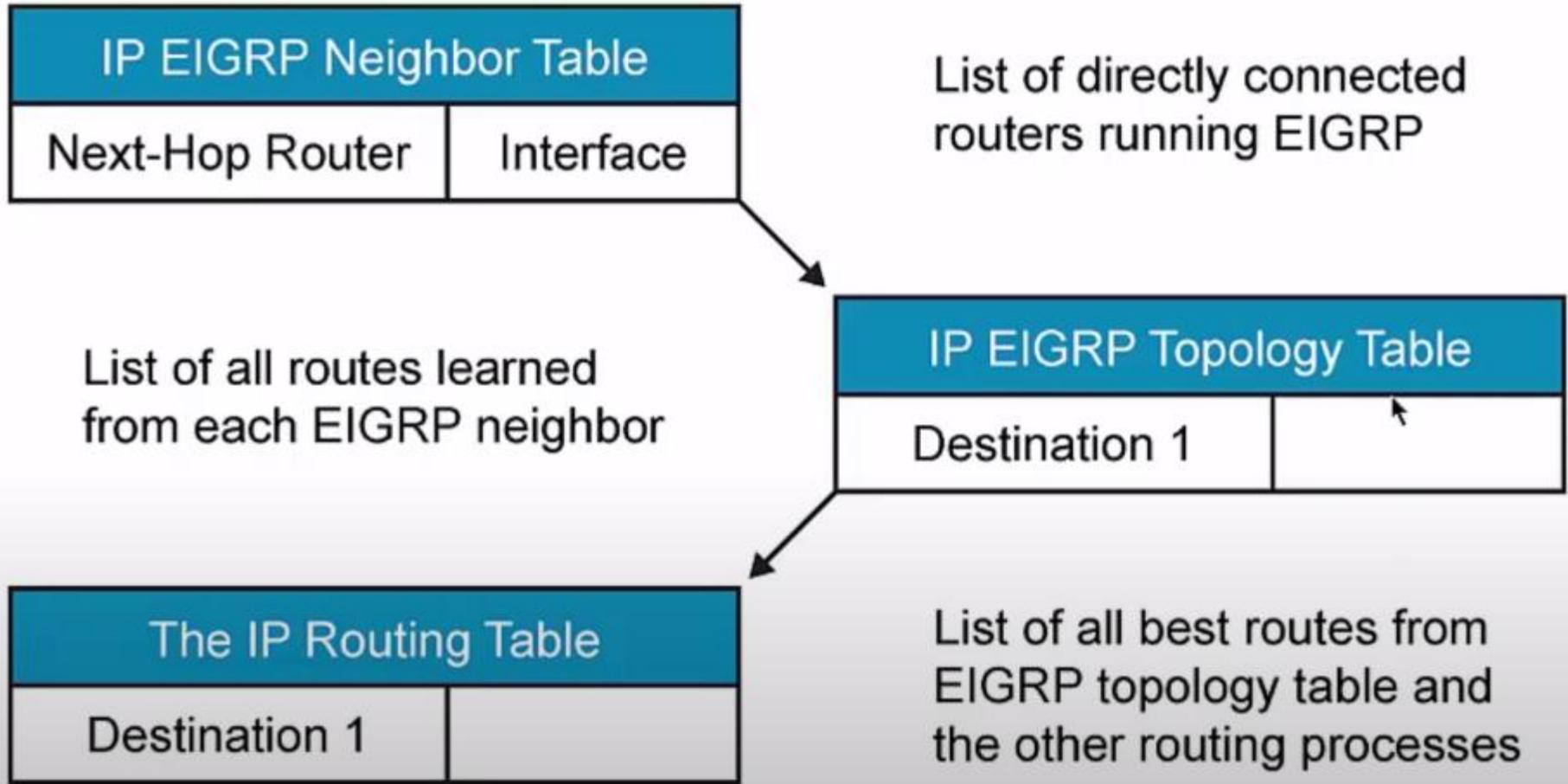
Điều kiện 2: *2 router phải cùng subnet và subnet-mask.*

Điều kiện 3: *Cùng loại xác thực (Authentication).*

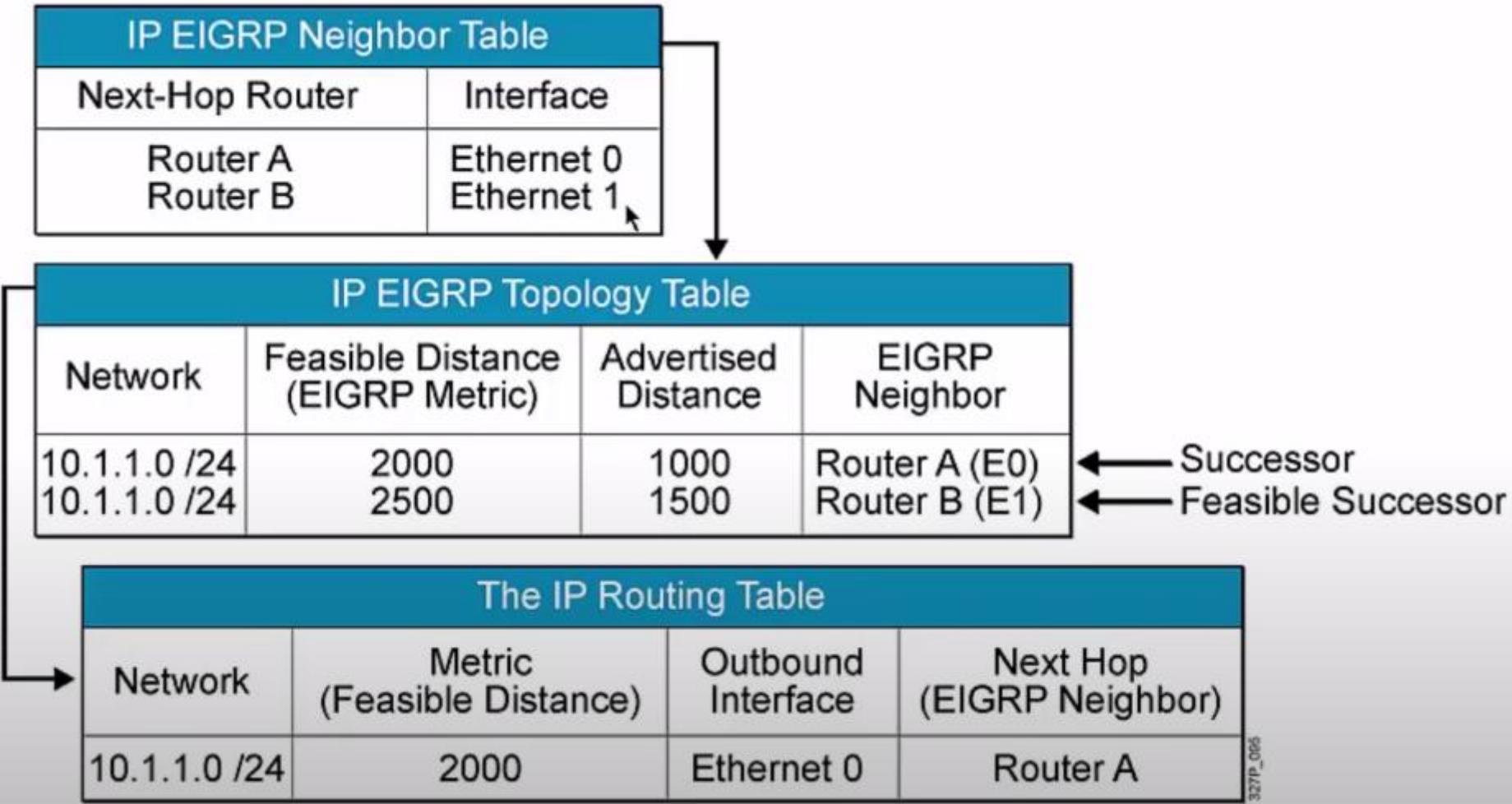
Điều kiện 4: Cùng bộ tham số K

❖ Sau khi thiết lập Neighbor, các router gửi bảng định tuyến cho các láng giềng sau đó chỉ gửi thông tin có thay đổi. EIGRP cập nhật tất cả các mạng vào Topology để thiết lập bảng định tuyến.

EIGRP Table



VÍ DỤ



CẤU HÌNH EIGRP CHO IPv4

❖ **Bước 1. Kích hoạt giao thức định tuyến EIGRP**

Router(config)#router eigrp <autonomous-system>

Trong đó: autonomous-system: có giá trị từ 1 đến 65535, giá trị này phải giống nhau ở tất cả các router chạy EIGRP

❖ **Bước 2. Chọn cổng tham gia vào quá trình trao đổi thông tin định tuyến**

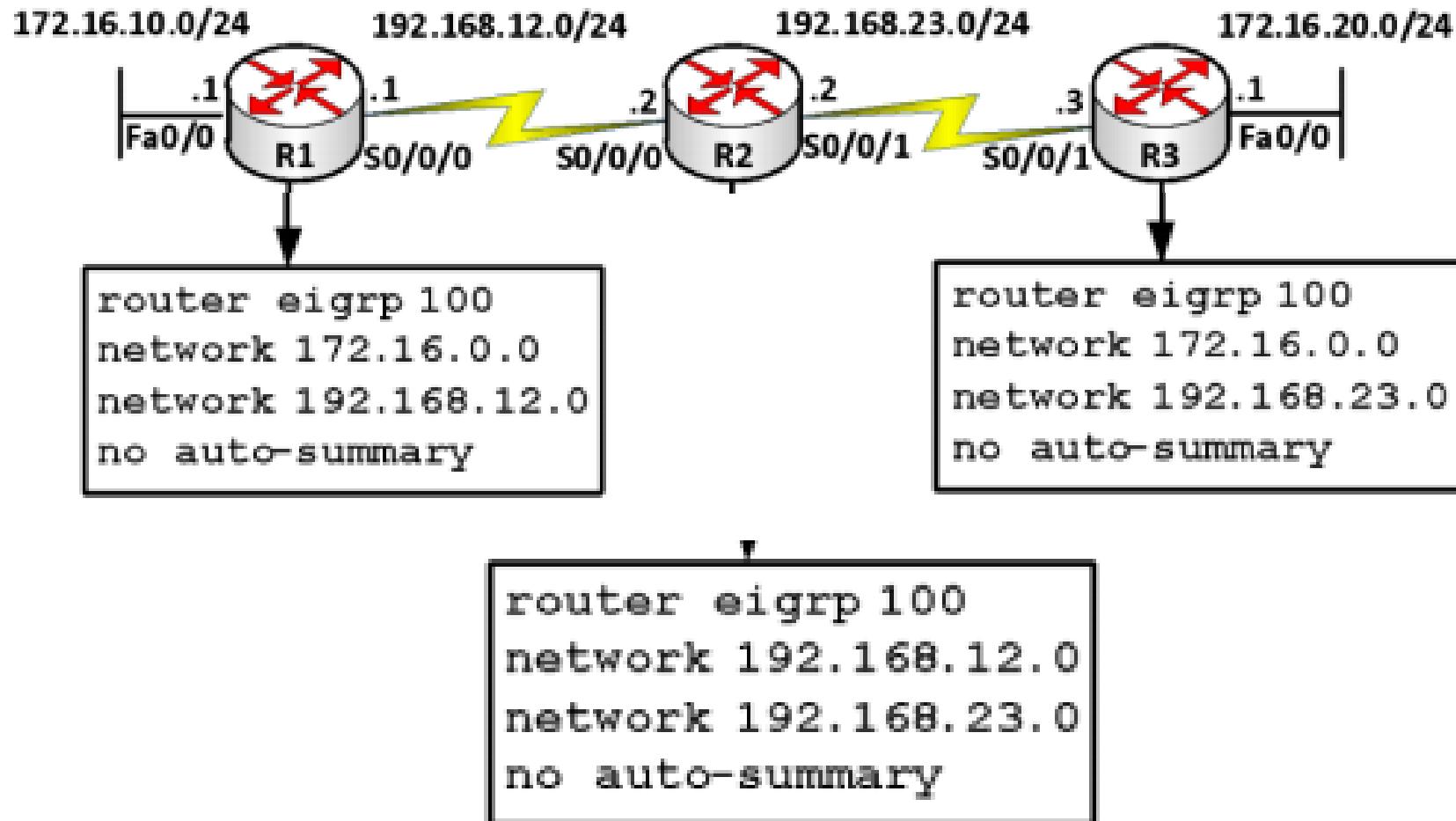
Router(config-router)#network <network-number>

Với network-number là địa chỉ cổng theo đúng lớp mạng của nó.

Để quảng bá các mạng con và hỗ trợ mạng không liên tục, chúng ta phải sử dụng lệnh sau:

Router(config-router)#no auto-summary

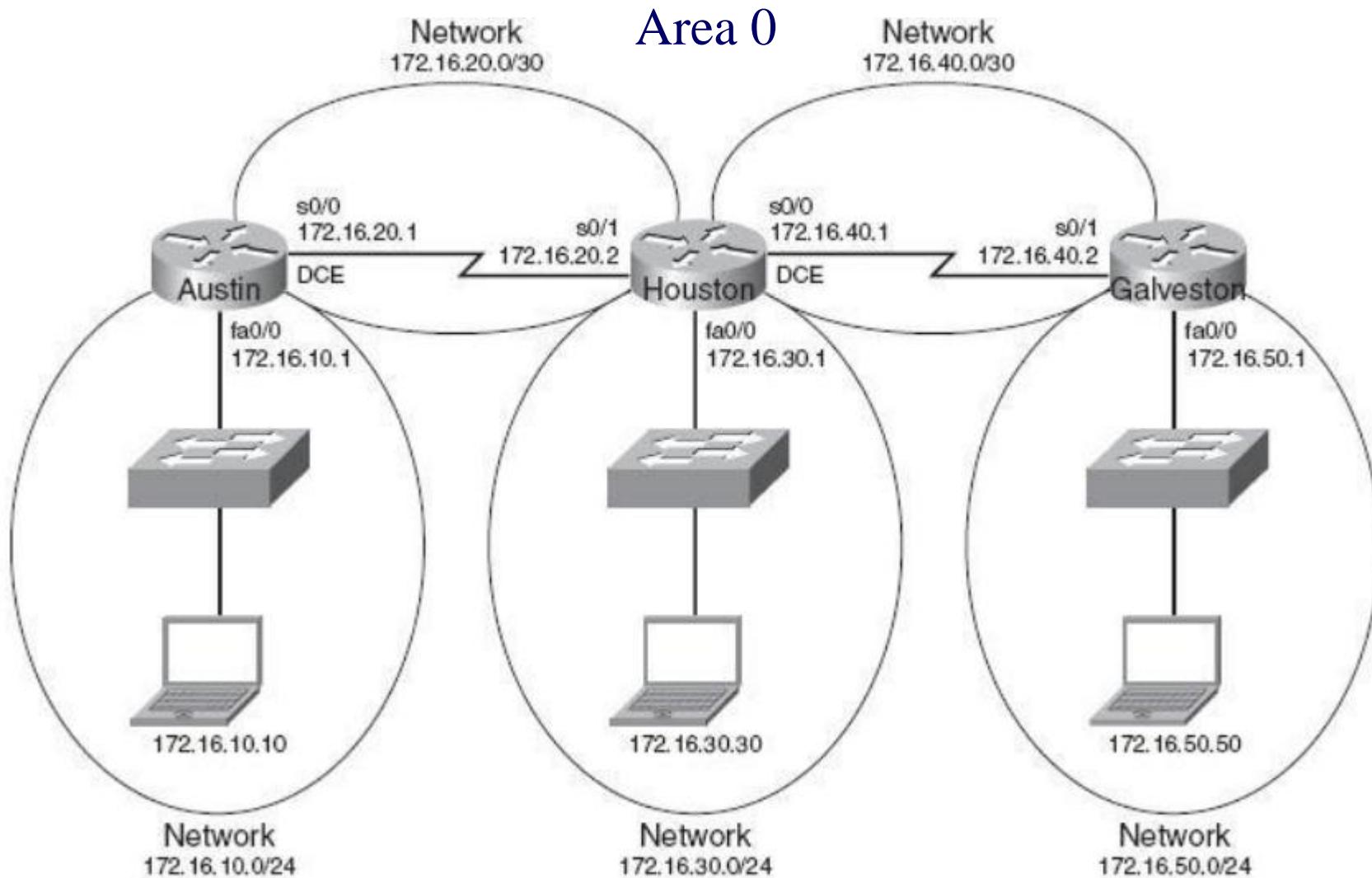
Ví dụ: Cấu hình định tuyến EIGRP cho mạng



LỆNH KIỂM TRA CẤU HÌNH EIGRP

- ❖ Router#show ip eigrp neighbors
- ❖ Router#show ip eigrp topology
- ❖ Router#show ip route eigrp
- ❖ Router#show ip protocols
- ❖ Router#show ip eigrp traffic

CẤU HÌNH ĐỊNH TUYẾN EIGRPv4



LỆNH CẤU HÌNH EIGRP CHO IPv6

❖ Bước 1: Chọn giao thức định tuyến

R(config)#ipv6 router eigrp <AS>

❖ Bước 2: Xác định router-id

R(config-router)#eigrp router-id H.H.H.H -> tham số tùy chọn

R(config-router)#no shutdown

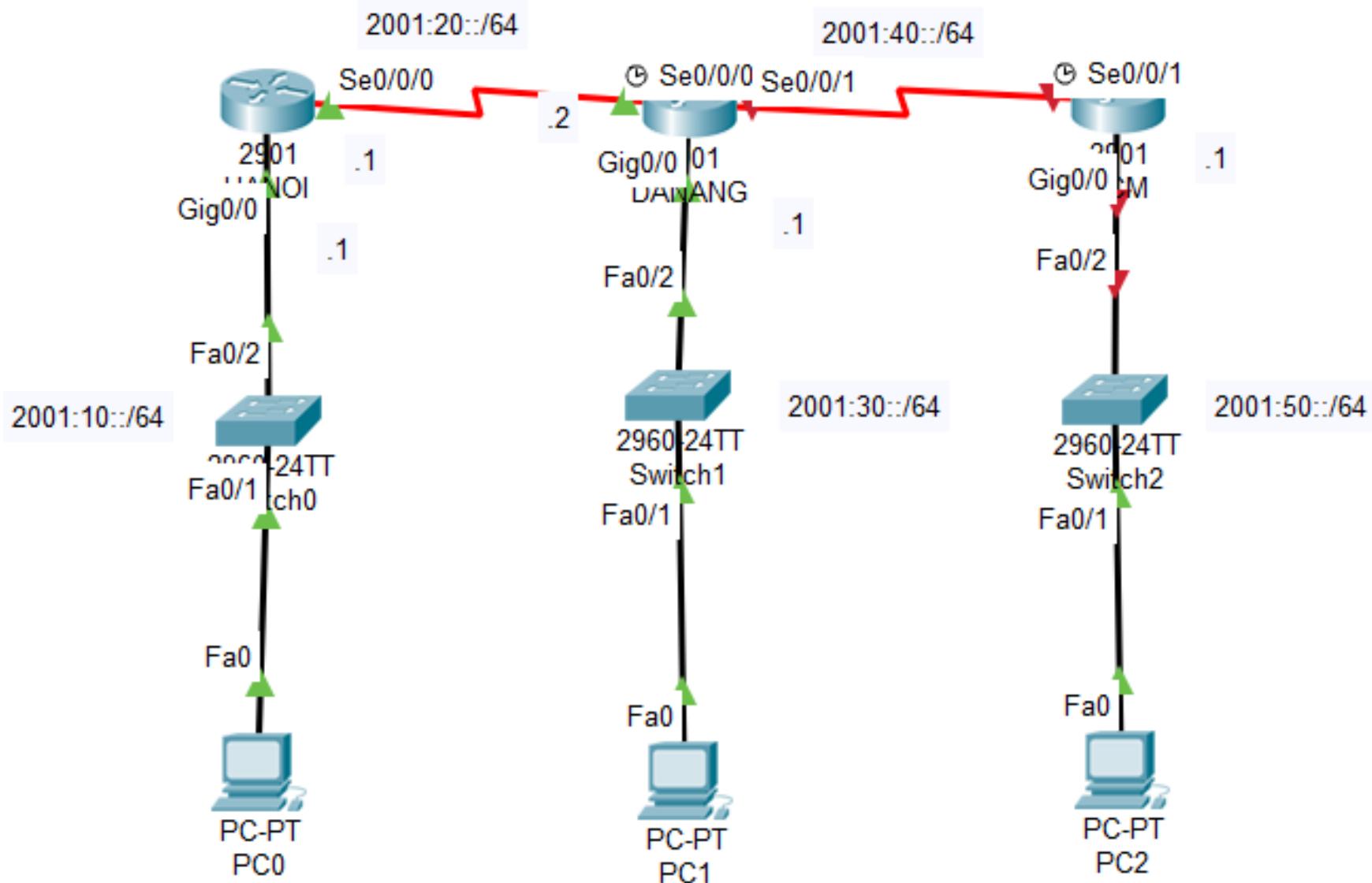
❖ Bước 3: Chọn cổng tham gia vào quá trình trao đổi thông tin định tuyến.

R(config-if)#ipv6 eigrp <AS>

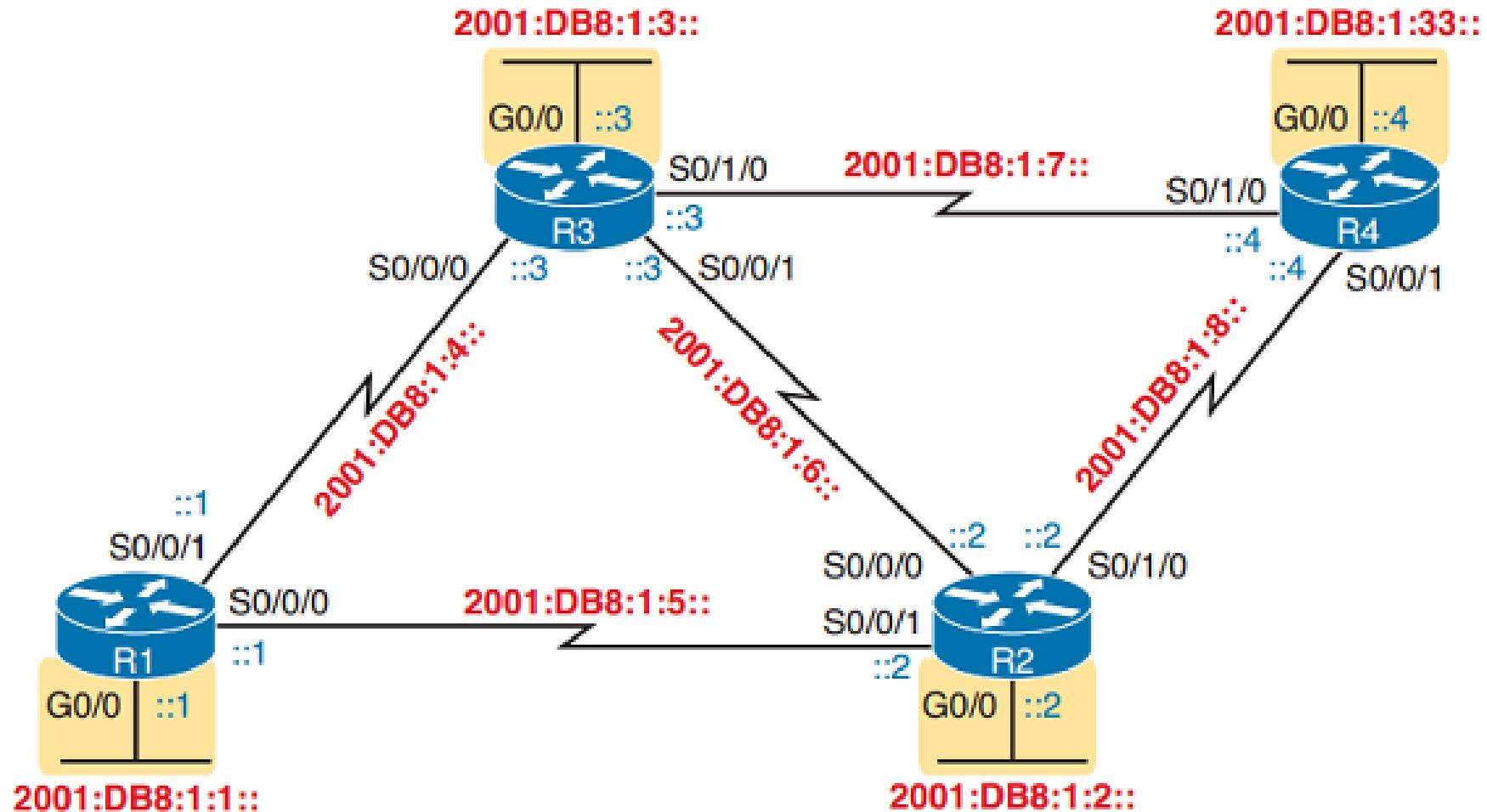
CÁC LỆNH KIỂM TRA CẤU HÌNH

- ❖ R#show ipv6 protocols
- ❖ R#show ipv6 eigrp neighbors
- ❖ R#show ipv6 eigrp topology
- ❖ R#show ipv6 route [eigrp]

CẤU HÌNH EIGRP CHO IPv6



BÀI TẬP 1: CẤU HÌNH EIGRP



CHƯƠNG 2: CẤU HÌNH ĐỊNH TUYẾN

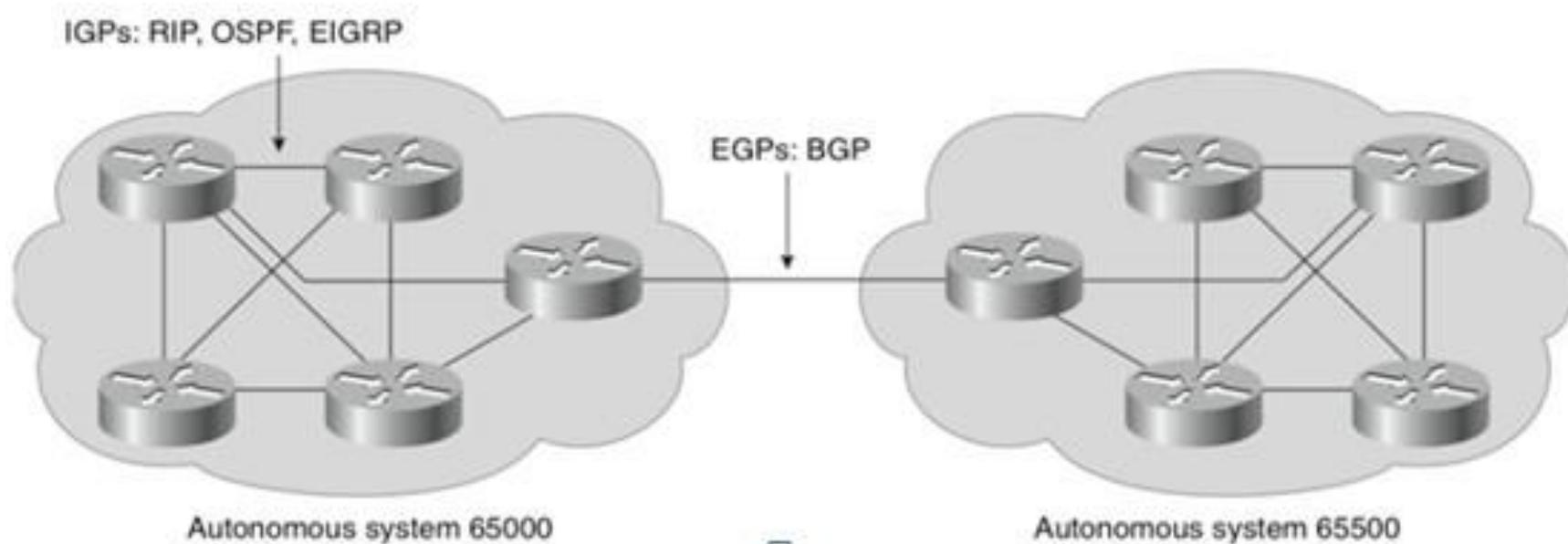
- 1 • Tổng quan về định tuyến
- 2 • Định tuyến tĩnh
- 3 • Giao thức định tuyến RIP
- 4 • Giao thức định tuyến OSPF
- 5 • Giao thức định tuyến EIGRP
- 6 • Giao thức định tuyến BGP

BÀI 6: GIAO THỨC ĐỊNH TUYẾN BGP

- ❖ BGP, viết tắt của từ tiếng Anh Border Gateway Protocol, là giao thức định tuyến đa miền sử dụng trên Internet từ 1994
- ❖ Là giao thức định tuyến liên vùng (giữa các AS), là kiểu định tuyến path vector dựa trên các luật, thuộc tính. Mỗi tuyến đường là danh sách các AS cần phải đi qua.
- ❖ Phiên bản BGP hiện nay là phiên bản 4, dựa trên RFC 4271.
- ❖ BGP hỗ trợ định tuyến liên vùng không phân lớp địa chỉ và dùng kỹ thuật kết hợp đường đi để giảm kích thước bảng định tuyến.

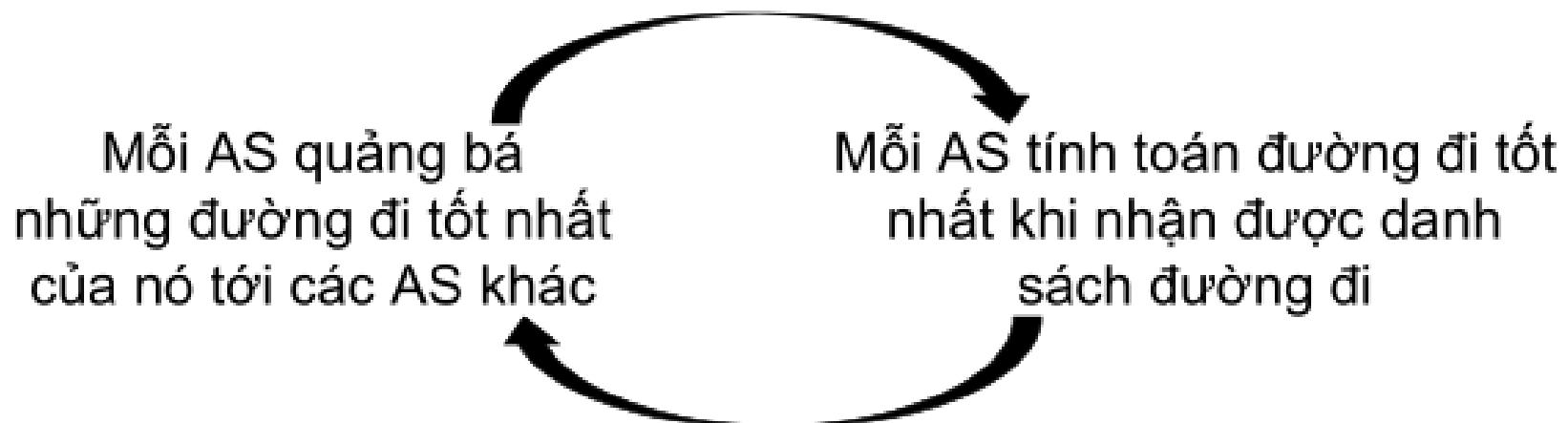
GIAO THỨC BGP

- ❖ Khi BGP chạy trên những AS khác nhau thì nó được gọi là External BGP – EBGP, chạy trong cùng 1 AS thì gọi là Internal BGP - IBGP



Ý TƯỞNG TÌM ĐƯỜNG

- ❖ Mỗi một địa chỉ IP Public sẽ được quản lý và gắn liền bởi một số AS do các tổ chức quy định và đối với BGP nó sẽ dựa vào các địa chỉ IP Public mà tham chiếu tới số AS để định tuyến Traffic.
- ❖ Ví dụ: Một mạng chiếm 255 địa chỉ lớp C từ 203.162.0.0/24 - 203.162.254.0/24 thì chỉ dùng 1 địa chỉ 203.162.0.0/16 để định danh mạng.



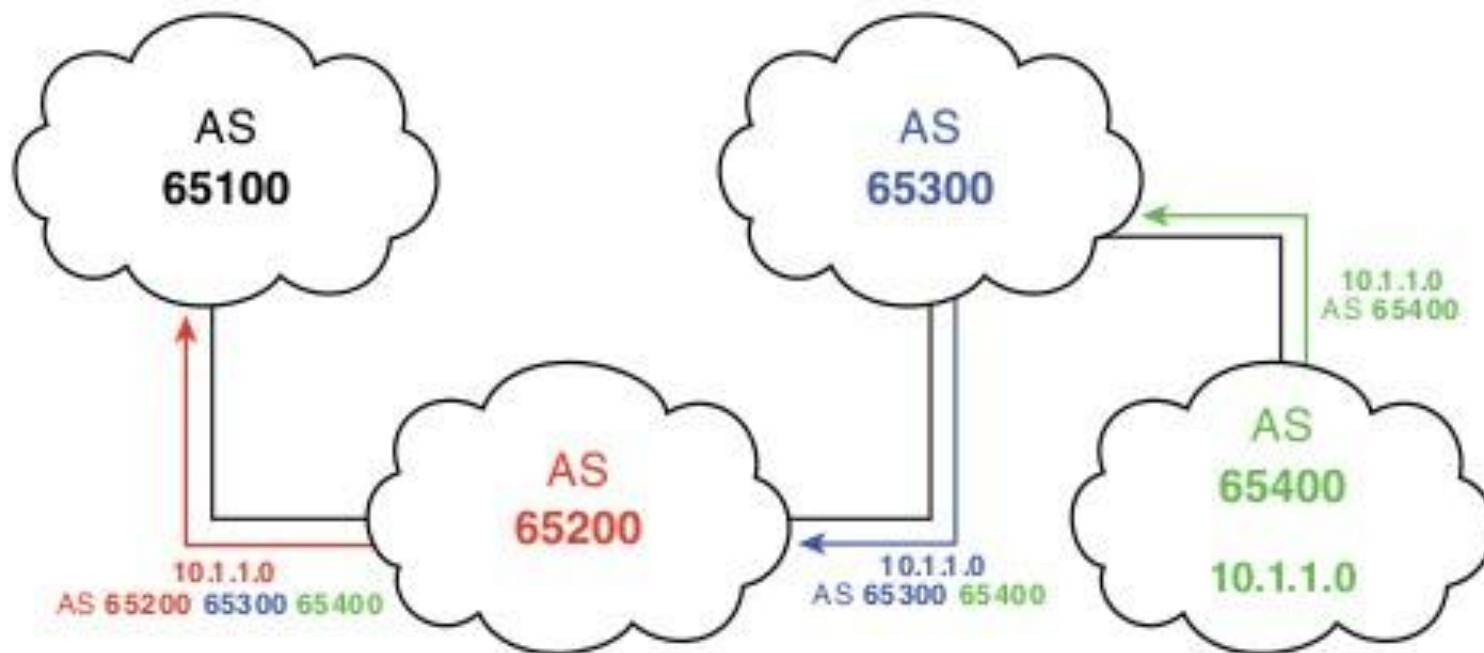
Các khái niệm liên quan đến BGP

- ❖ Giá trị AD của EBGP là 20. Giá trị AD của IBGP là 200.
- ❖ Các BGP láng giềng được gọi là các peers phải được cấu hình trực tiếp theo kiểu tĩnh.
- ❖ BGP sử dụng TCP port 179. Các BGP peers sẽ trao đổi các thông tin như thông tin cập nhật update, gói tin keepalive...
- ❖ Các Routers chỉ có thể chạy một BGP tại một thời điểm.
- ❖ BGP là một giao thức kiểu path-vector. Đường đi của nó đến một mạng bao gồm một danh sách các AS.

BGP Database

- ❖ BGP dùng 3 loại database, 2 loại dùng riêng cho giao thức, 1 loại dùng cho toàn bộ quá trình routing trên router.
- ❖ **Neighbor database:** một danh sách tất cả các BGP láng giềng được cấu hình.
- ❖ **BGP database,** hay còn gọi RIB (Routing Information Base): một danh sách các mạng mà BGP biết, kèm theo là paths (đường đi) và attributes.
- ❖ **Routing table:** danh sách các paths đến mỗi mạng được sử dụng bởi Router và next hop cho mỗi mạng.

BGP sử dụng Router là các AS



Cơ chế chống loop là một ASN-AS number. Khi một Router cập nhật về một mạng đi ra khỏi 1 AS, ASN của AS đó được đính kèm vào bản cập nhật. Khi một AS nhận một cập nhật, nó sẽ xem trong AS list. Nếu nhận ra ASN của chính nó, cập nhật sẽ bị loại bỏ.

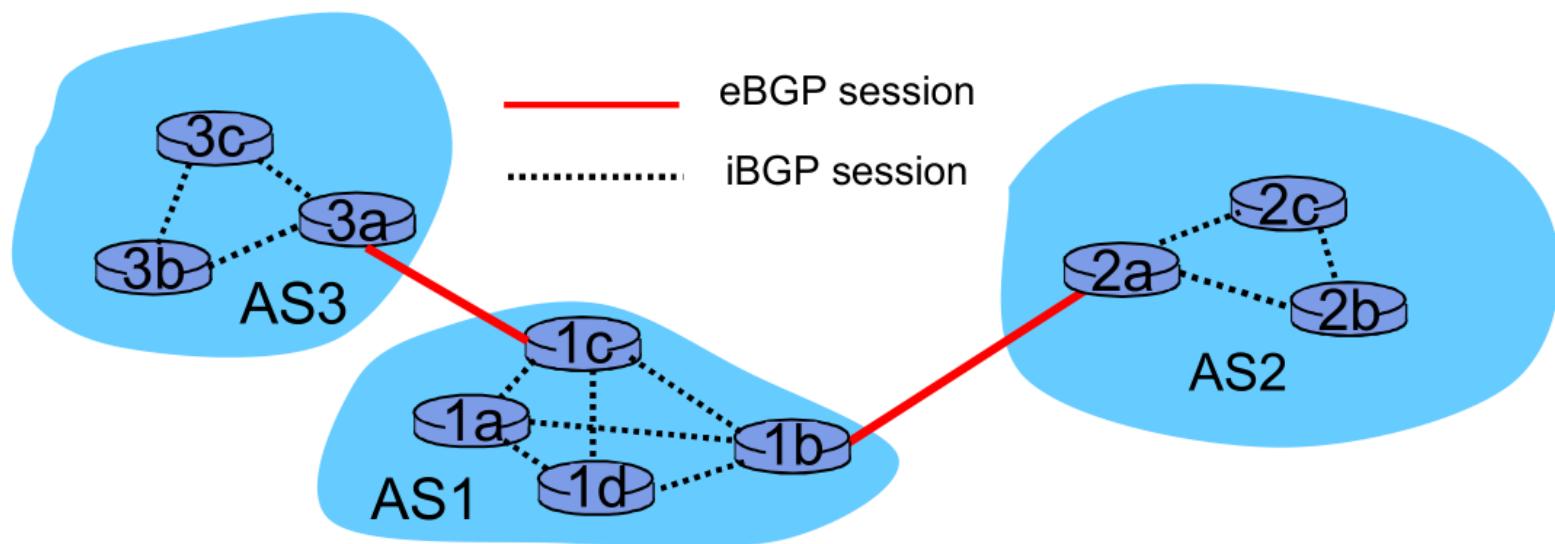
HOẠT ĐỘNG CỦA BGP

- ❖ eBGP, iBGP và IGP
- ❖ BGP cài đặt trên các router biên của AS (kết nối tới các AS khác) với 2 phiên hoạt động:
 - External BGP (eBGP): thực hiện trao đổi thông điệp với các router biên trên AS khác để tìm đường đi tới đích nằm ngoài AS của nó
 - Internal BGP (iBGP): trao đổi thông điệp với các router biên và router nội vùng cùng AS để quảng bá đường đi tới đích nằm ngoài AS của nó.
- ❖ IGP: Interior Gateway Protocol = Intra-domain Routing Protocol
 - Cài đặt trên router nội vùng
 - Tìm đường đi tới đích nằm trong vùng AS
 - Dữ liệu tới đích ngoài AS sẽ được chuyển tới router biên.

EBGP và IBGP

❖ Quảng bá thông tin đường đi

1. 3a gửi tới 1c bằng eBGP
2. 1c gửi thông tin nội bộ tới (1b, 1d, ...) trong AS1 bằng iBGP
 - 1b: Router biên cài BGP
 - 1a, 1d: Router nội vùng cài IGP
3. 2a nhận thông tin từ 1b bằng eBGP

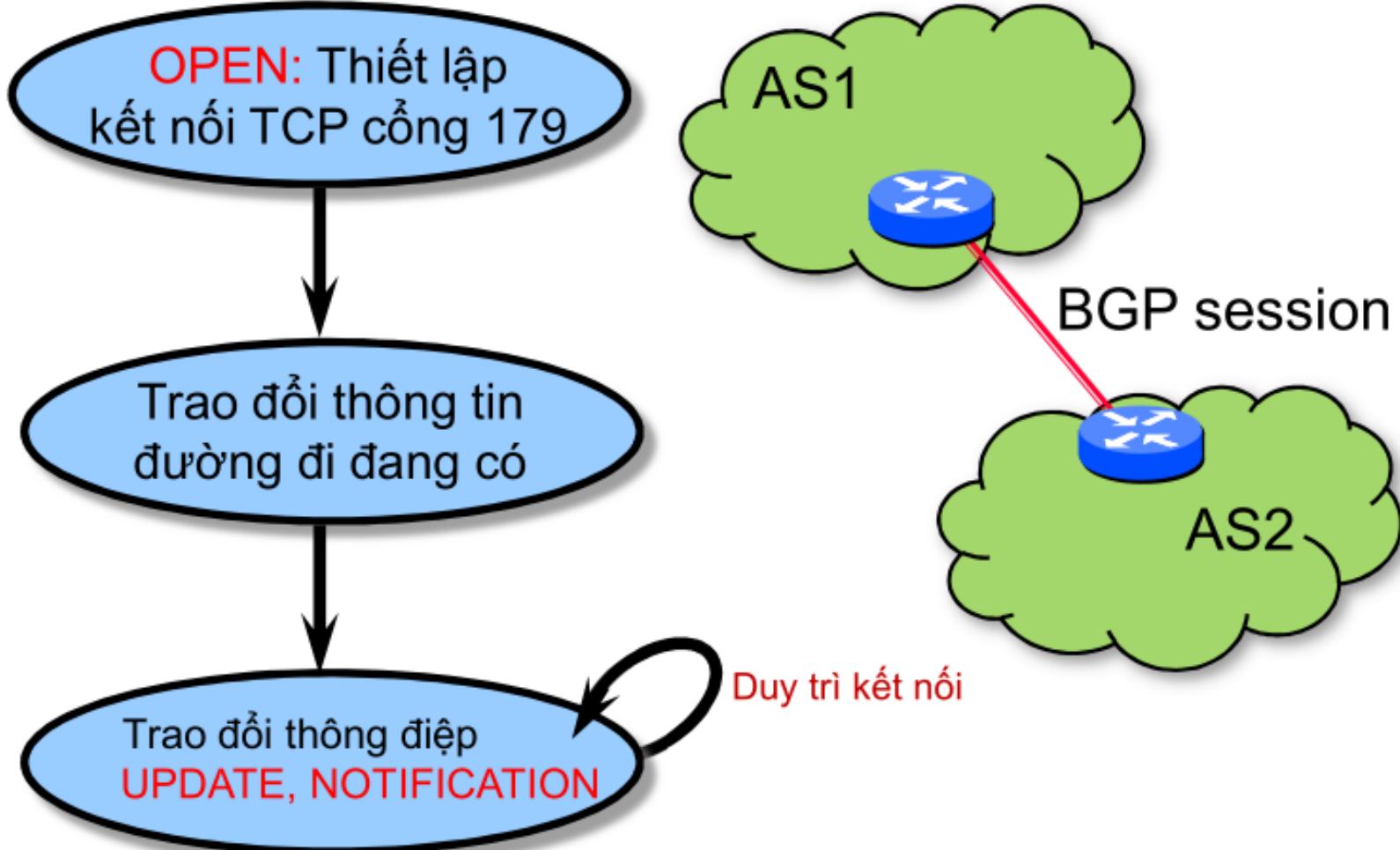


Các kiểu thông điệp BGP

Có 4 kiểu thông điệp

- ❖ *Open*: sau khi một láng giềng được cấu hình, BGP gửi một thông điệp open để cố gắng kết nối với láng giềng đó. Bao gồm thông tin như ASN, RIB, và hold time. Sử dụng TCP, cổng 179.
- ❖ *Update*: thông điệp này được sử dụng để trao đổi thông tin định tuyến giữa các peers. Chứa thông tin về các routes mới, các routes bị down, và các thuộc tính của đường (path attributes).
- ❖ *Keepalive*: mặc định, các BGP peers trao đổi thông điệp này sau mỗi 60 giây. Chúng sẽ giữ phiên làm việc giữa các peer được active.
- ❖ *Notification*: khi xảy ra 1 vấn đề làm cho Router phải kết thúc phiên làm việc BGP, một thông điệp notification sẽ được gửi đến BGP neighbor và việc kết nối sẽ chấm dứt.

PHIÊN TRAO ĐỔI THÔNG TIN CỦA BGP

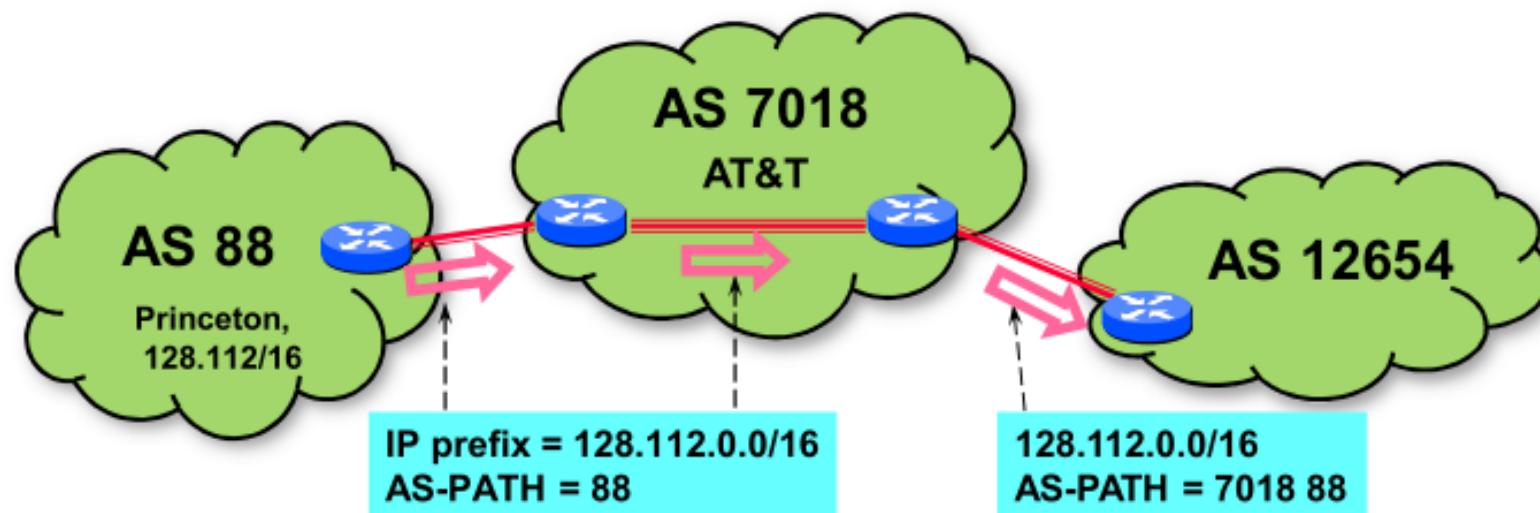


UPDATE = <IP prefix: Thuộc tính>

- ❖ IP prefix: địa chỉ của đích
- ❖ Thuộc tính gán cho đường đi: Sử dụng cho mục đích lựa chọn/quảng bá đường đi nào:
 - Các thuộc tính nội bộ: Chỉ dùng cho các thông điệp trao đổi trong AS. Ví dụ: LOCAL-PREF.
 - Các thuộc tính sử dụng cho EBGP: ORIGIN, AS-PATH, NEXT-HOP, MED.
 - Các thuộc tính khác: ATOMIC_AGGREGATE, AGGREGATOR, COMMUNITY...

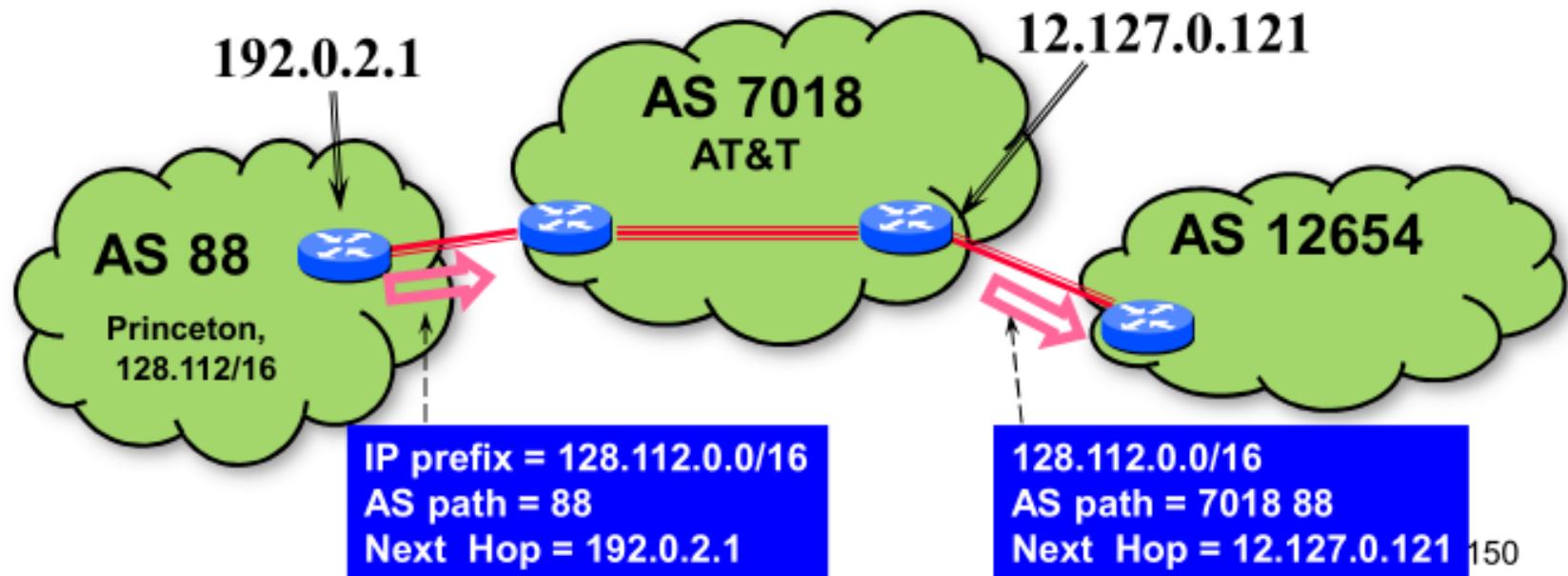
Thuộc tính (1): AS-PATH

- ❖ Thông tin về đường đi tới một đích (IP prefix)
- ❖ Liệt kê số hiệu các AS trên đường đi tới đích (theo thứ tự gần đích tới xa đích)



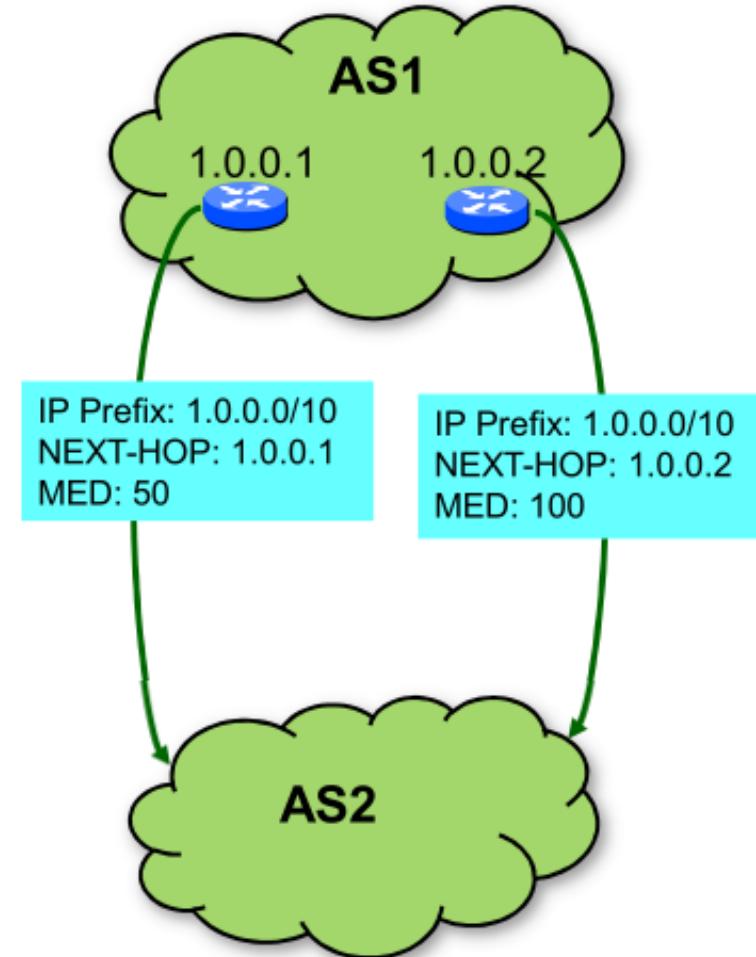
Thuộc tính (2): NEXT-HOP

- ❖ Địa chỉ IP của router tiếp theo trên đường đi tới đích
- ❖ Cập nhật trên thông điệp UPDATE ra khỏi AS.



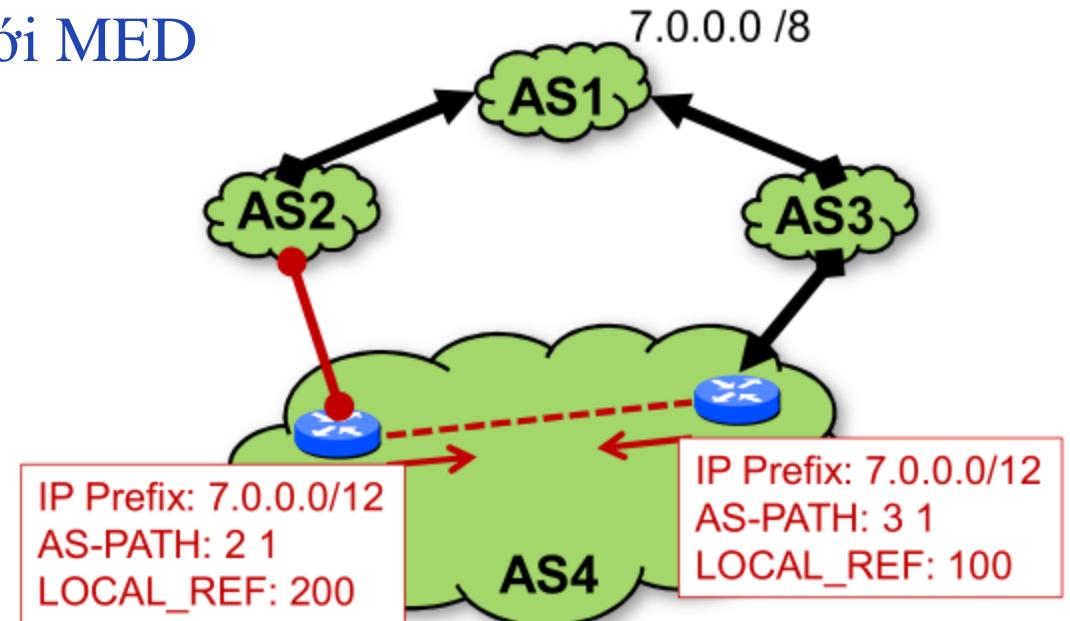
Thuộc tính (3): MED

- ❖ Multi-Exit Discriminator
- ❖ Dùng cho eBGP
- ❖ Sử dụng trong trường hợp một AS có nhiều liên kết tới một AS khác:
- ❖ AS quảng bá đường đi với giá trị MED khác nhau qua các liên kết khác nhau.
- ❖ AS nhận thông tin sẽ chọn đường đi có MED nhỏ hơn.
-> điều khiển lưu lượng vào.



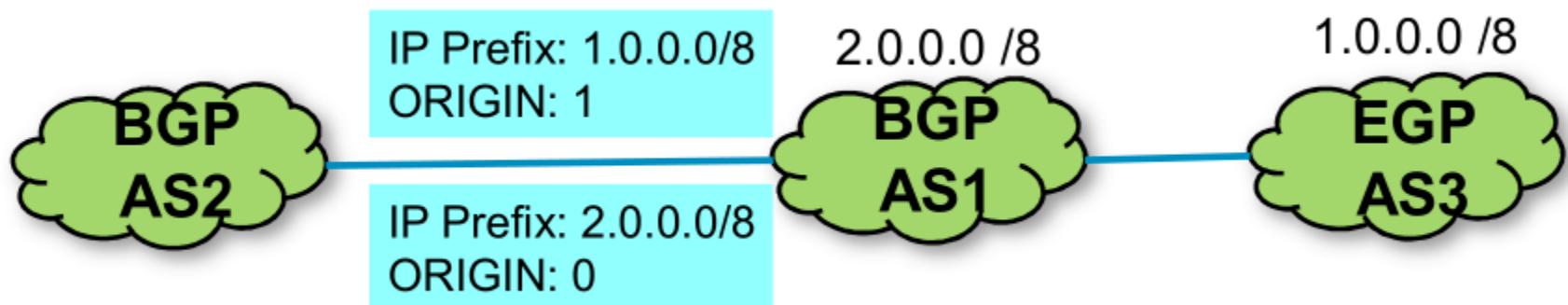
Thuộc tính (4): LOCAL_REF

- ❖ Local reference
- ❖ Trao đổi trên các thông điệp iBGP
- ❖ Gán cho các đường đi tới cùng đích
- ❖ Chọn đường đi có LOCAL_REF lớn hơn -> điều khiển lưu lượng ra.
- ❖ Không nhầm lẫn với MED



Thuộc tính (5): ORIGIN

- ❖ Chỉ ra nguồn gốc của thông tin về đường đi
- ❖ Sử dụng 1 trong 3 giá trị:
 - 0-IGP: thông tin đường đi học được từ trong AS qua giao thức IGP
 - 1-EGP: thông tin đường đi học được từ ngoài AS qua giao thức EGP (Exterior Gateway Protocol) [RFC904]
 - ?-INCOMPLETE: đường đi học được từ nguồn không xác định (thường do định tuyến tĩnh)

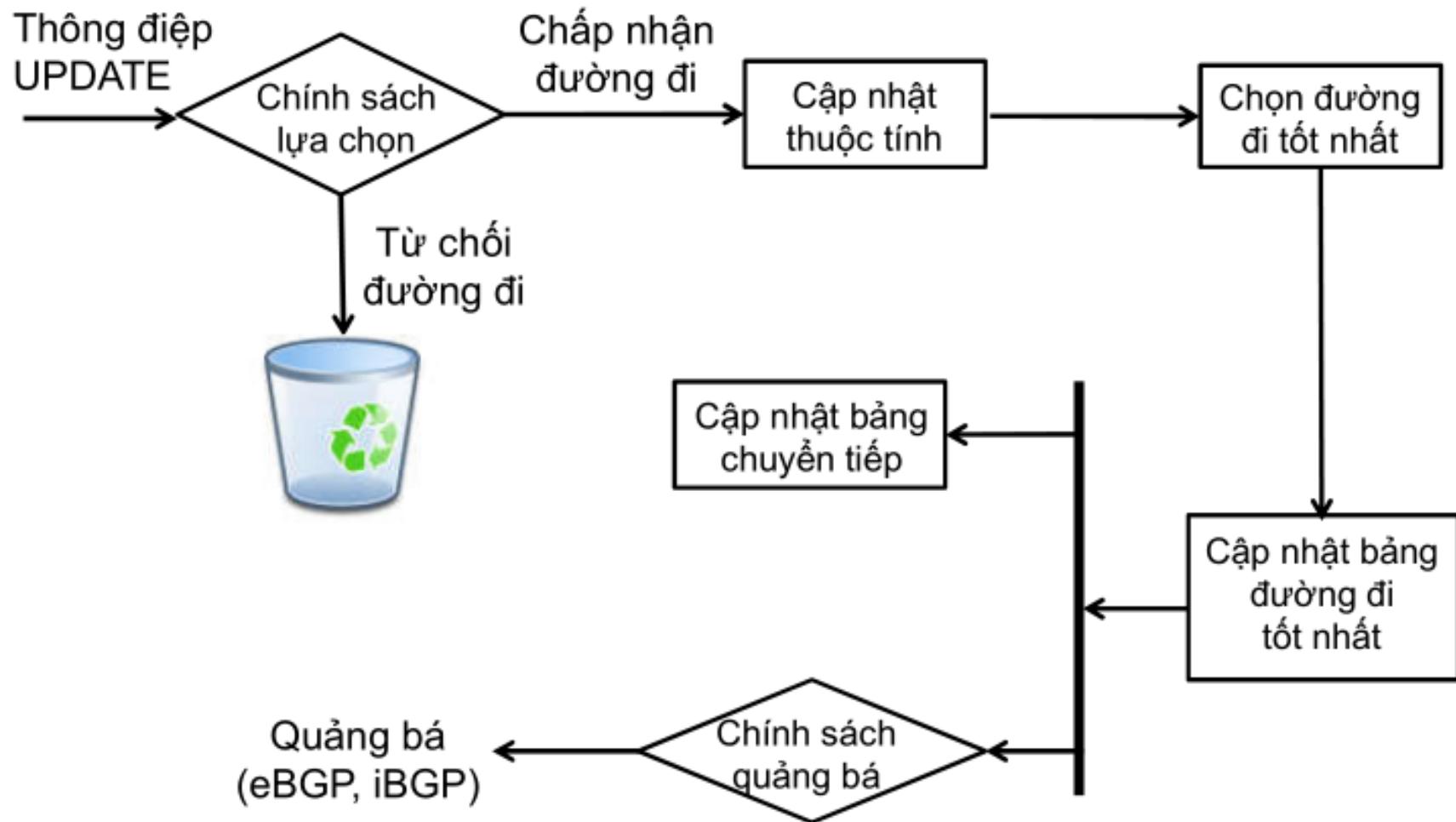


Sử dụng các thuộc tính

❖ Thứ tự ưu tiên khi chọn đường

Độ ưu tiên	Tiêu chí	Mục tiêu
1	LOCAL PREF	Cao nhất
2	ASPATH	Qua ít AS nhất
3	MED	Thấp nhất
4	eBGP > iBGP	Chọn đường đi học từ AS khác
5	iBGP path	Đường đi tới router biên gần nhất
6	Router ID	Địa chỉ IP nhỏ nhất

Quá trình xử lý thông điệp UPDATE



Một số vấn đề tồn tại của BGP

- ❖ An toàn bảo mật:
 - Tấn công vào BGP có thể gây thiệt hại lớn
- ❖ Không đảm bảo hiệu năng
 - Vì ưu tiên tìm đường theo chính sách trước tìm đường ngắn nhất
- ❖ Hội tụ chậm
 - Dưới 35% router có thời gian hoạt động 99.99%
 - Khoảng 10% có thời gian hoạt động dưới 95%
 - 40% số đường bị lỗi cần 30 phút để cập nhật xong
 - May mắn là hầu hết đường đi đều ổn định.
- ❖ Phức tạp khi cần triển khai các chính sách

CẤU HÌNH BGP TRÊN ROUTER CISCO

- ❖ Thiết lập giao thức định tuyến BGP

R1(config)#**router bgp <AS-Number>**

- ❖ Thiết lập láng giềng

R1(config-router)#**neighbor <Address> remote-as <AS-Number>**

- ❖ Quảng bá mạng

R1(config-router)#**network <Network> mask <Subnet-mask>**

- ❖ Phân phối giao thức định tuyến

R1(config-router)#**redistribute static**

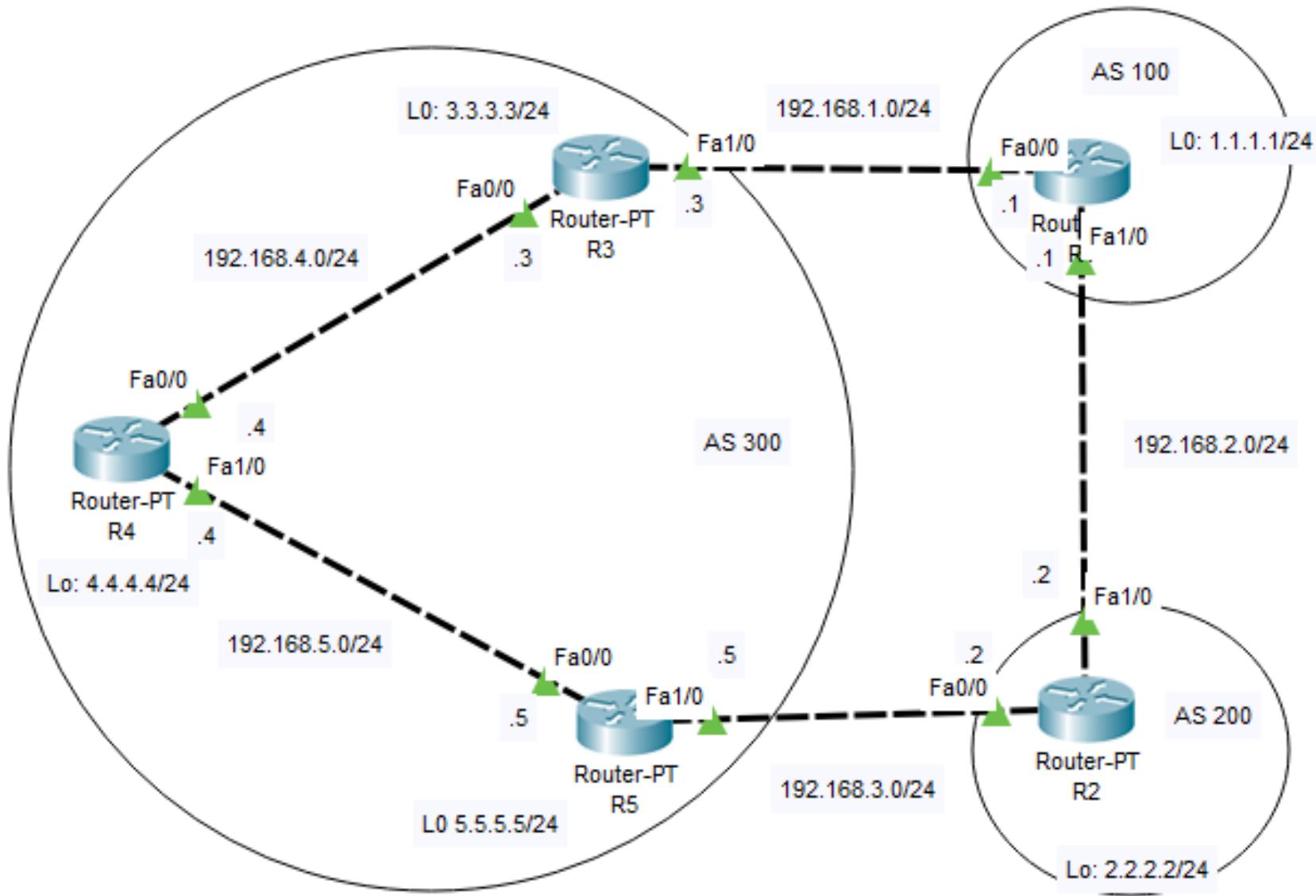
- ❖ Nếu sử dụng card loopback để thiết lập neighbor nên cần phải “update-source” cho card loopback0

R1(config-router)# **neighbor <address> update-source Loopback0**

REDISTRIBUTE

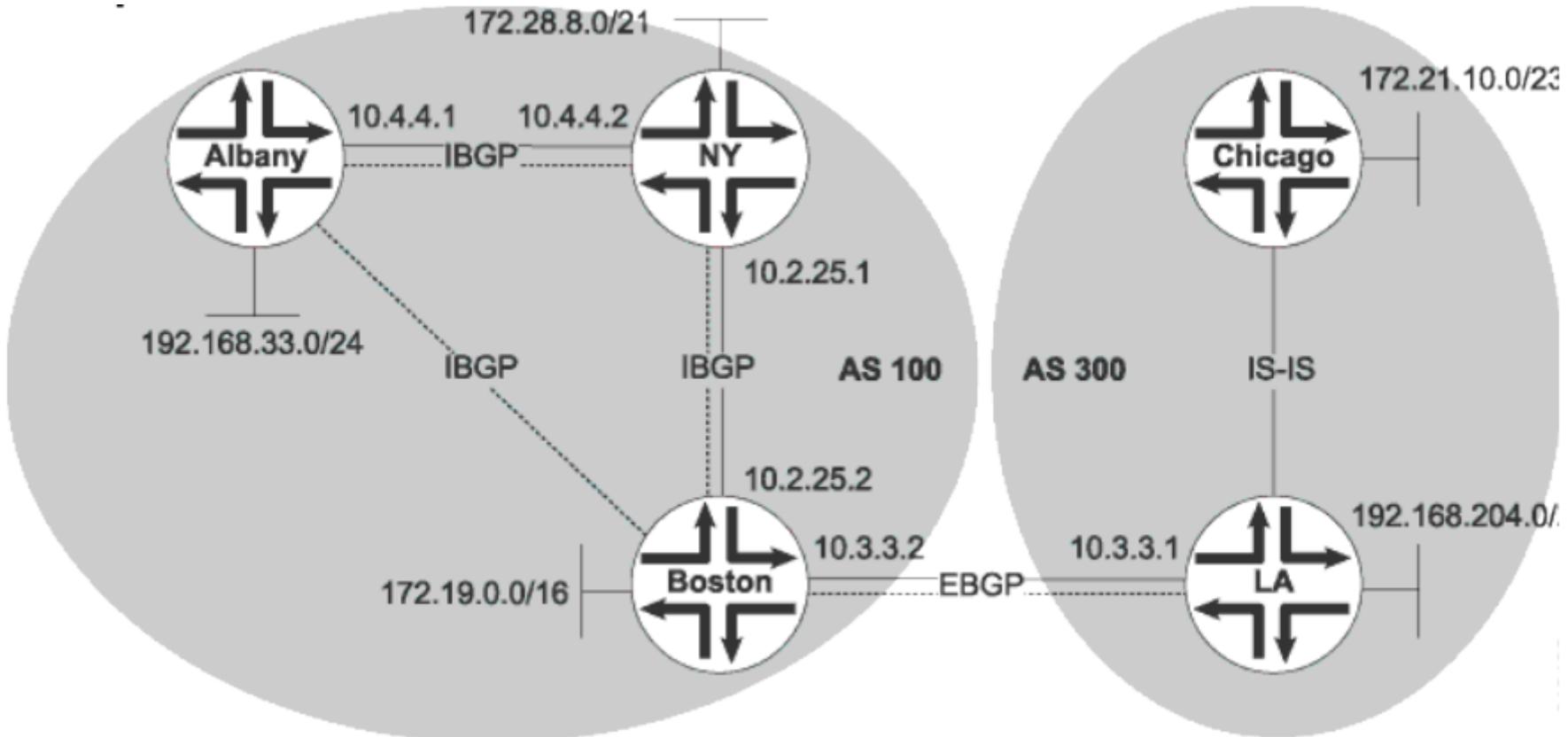
- ❖ Phân phối định tuyến định nghĩa cách thức trao đổi thông tin định tuyến giữa các giao thức định tuyến. Mỗi giao thức có metric khác nhau, nên phải chuyển đổi cho phù hợp.
- ❖ Quảng bá các tuyến học được từ OSPF vào RIP
 - R(config)#**router rip**
 - R(config-router)#**redistribute ospf 1 metric <number>**
- ❖ Quảng bá các tuyến học được từ RIP vào OSPF
 - R(config)#**router ospf <process-id>**
 - R(config-router)#**redistribute rip metric <metric> subnets**

CẤU HÌNH ĐỊNH TUYỀN BGP



```
R1(config)#  
R1(config-if)  
R1(config)#  
R1(config-route)  
R1(config-route)  
R1(config-route)
```

CẤU HÌNH BGP TRÊN ROUTER CISCO



CẤU HÌNH TRÊN ROUTER BIÊN BOSTON

- ❖ Boston(config)#**router bgp 100**
- ❖ Boston(config-router)#**neighbor 10.2.25.1 remote-as 100**
- ❖ Boston(config-router)#**neighbor 10.4.4.1 remote-as 100**
- ❖ Boston(config-router)#**neighbor 10.3.3.1 remote-as 300**
- ❖ Boston(config-router)#**network 172.19.0.0**
- ❖ Boston(config-router)#**redistribute static**

CẤU HÌNH TRÊN ROUTER NY

- ❖ NY(config)#**router bgp 100**
- ❖ NY(config-router)#**neighbor 10.4.4.1 remote-as 100**
- ❖ NY(config-router)#**neighbor 10.2.25.2 remote-as 100**
- ❖ NY(config-router)#**network 172.28.8.0 mask 255.255.248.0**

CẤU HÌNH TRÊN ROUTER LA

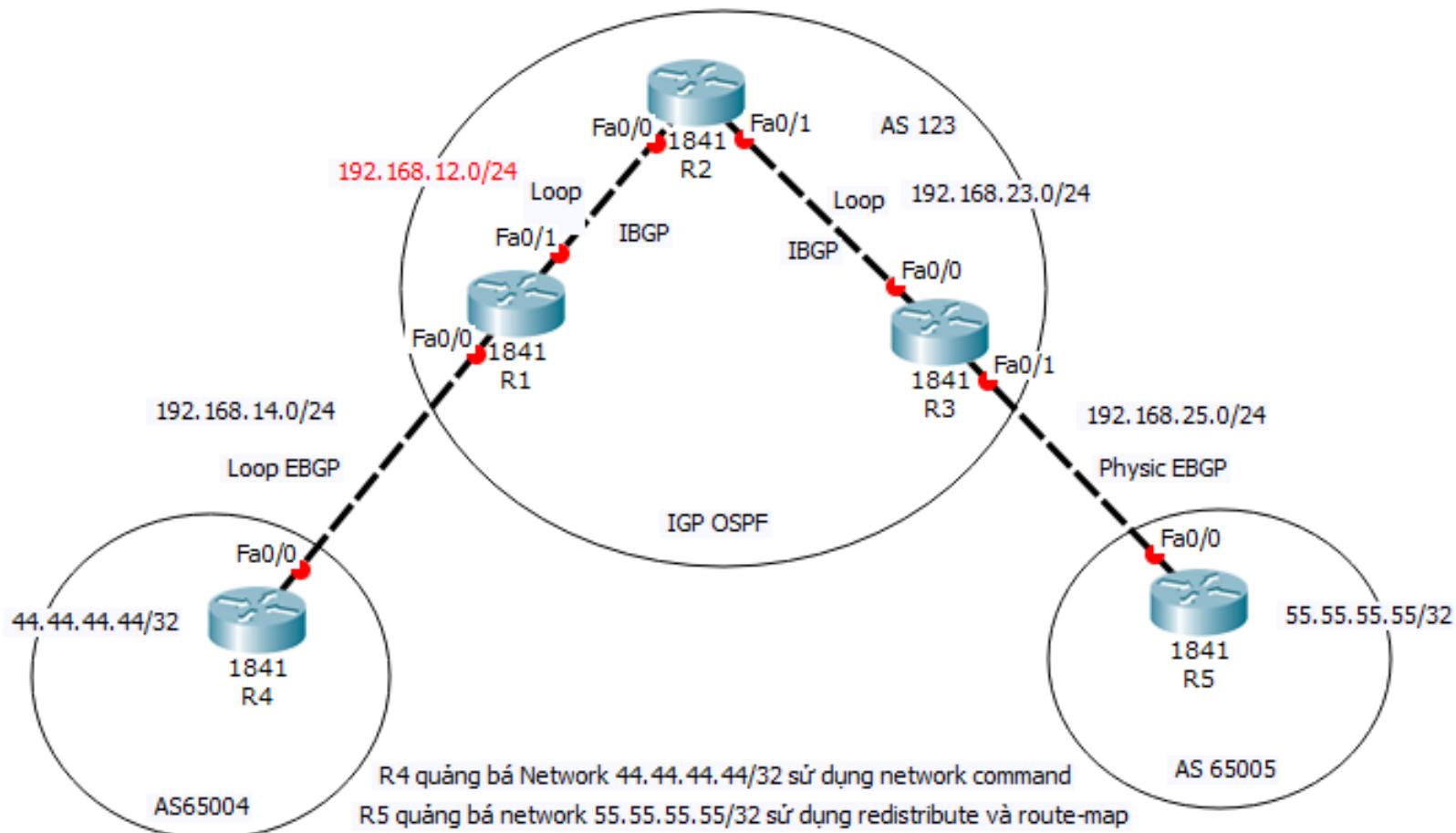
- ❖ LA(config)#**router bgp 300**
- ❖ LA(config-router)#**neighbor 10.3.3.2 remote-as 100**
- ❖ LA(config-router)#**network 192.168.204.0 mask
255.255.252.0**
- ❖ LA(config-router)#**redistribute isis**

CẤU HÌNH TRÊN ROUTER ALBANY

- ❖ Albany(config)#**router bgp 100**
- ❖ Albany(config-router)#**neighbor 10.4.4.2 remote-as 100**
- ❖ Albany(config-router)#**neighbor 10.2.25.2 remote-as 100**
- ❖ Albany(config-router)#**network 192.168.33.0 mask 255.255.255.0**

BÀI TẬP

❖ Cho sơ đồ mạng như hình vẽ:



- ❖ Cấu hình eBGP sử dụng loopback và physical interface sử dụng update-source và ebgp-multihop
- ❖ Cấu hình iBGP ở dạng full mesh và cấu hình next-hop-self cho các Router biên

YÊU CẦU

- ❖ Cấu hình R1, R2, R3 tham gia định tuyến OSPF với Area 0. (tất cả các interface loopback0 cũng tham gia định tuyến OSPF).
- ❖ Cấu hình R1 và R4 tham gia định tuyến BGP sử dụng card loopback để tham gia neighbor. R4 sẽ quảng bá network 44.44.44.44/43
- ❖ Cấu hình R3 và R5 tham gia định tuyến BGP sử dụng interface physical để tham gia neighbor. R5 sẽ quảng bá network 55.55.55.55/43.

PHÂN BỐ IP CHO CÁC ROUTER

Router	Interface	IP address
R1	f0/0	192.168.14.1/24
	f0/1	192.168.12.1/24
	loopback 0	1.1.1.1/24
R2	f0/0	192.168.12.2/24
	f0/1	192.168.23.2/24
	loopback 0	2.2.2.2/24
R3	f0/0	192.168.23.3/24
	f0/1	192.168.35.3/24
	loopback 0	3.3.3.3/24
R4	f0/0	192.168.14.4/24
	loopback 0	4.4.4.4/24
	loopback 1	44.44.44.44/32
R5	f0/0	192.168.35.5/24
	loopback 0	5.5.5.5/24
	loopback 1	55.55.55.55/32

CẤU HÌNH CƠ BẢN CÁC ROUTER

//Config Router R1

R1(config)# interface f0/0

R1(config-if)# ip address 192.168.14.1 255.255.255.0

R1(config-if)# interface f0/1

R1(config-if)# ip address 192.168.12.1 255.255.255.0

R1(config-if)# interface loopback0

R1(config-if)# ip address 1.1.1.1 255.255.255.0

CẤU HÌNH CƠ BẢN CÁC ROUTER

//Config Router R2

R2(config)# interface f0/0

R2(config-if)# ip address 192.168.12.2 255.255.255.0

R2(config-if)# interface f0/1

R2(config-if)# ip address 192.168.23.2 255.255.255.0

R2(config-if)# interface loopback0

R2(config-if)# ip address 2.2.2.2 255.255.255.0

CẤU HÌNH CƠ BẢN CÁC ROUTER

//Config Router R3

R3(config)# interface f0/0

R3(config-if)# ip address 192.168.23.3 255.255.255.0

R3(config-if)# interface f0/1

R3(config-if)# ip address 192.168.35.3 255.255.255.0

R3(config-if)# interface loopback0

R3(config-if)# ip address 3.3.3.3 255.255.255.0

CẤU HÌNH CƠ BẢN CÁC ROUTER

//Config Router R4

R4(config)# interface f0/0

R4(config-if)# ip address 192.168.14.4 255.255.255.0

R4(config-if)# interface loopback0

R4(config-if)# ip address 4.4.4.4 255.255.255.0

R4(config-if)# interface loopback1

R4(config-if)# ip address 44.44.44.44 255.255.255.255

CẤU HÌNH CƠ BẢN CÁC ROUTER

//Config Router R5

R5(config)# interface f0/0

R5(config-if)# ip address 192.168.35.5 255.255.255.0

R5(config-if)# interface loopback0

R5(config-if)# ip address 5.5.5.5 255.255.255.0

R5(config-if)# interface loopback1

R5(config-if)# ip address 55.55.55.55 255.255.255.255

Cấu hình định tuyến OSPF cho Router 1, 2, 3

R1(config)#router ospf 1

R1(config-router)#router-id 1.1.1.1

R1(config-router)#network 1.1.1.1 0.0.0.0 area 0

R1(config-router)#network 192.168.12.1 0.0.0.0 area 0

❖ Kiểm tra bảng định tuyến:

R1#Show ip route ospf

Cấu hình định tuyến OSPF cho Router 1, 2, 3

```
R2(config)#router ospf 1
```

```
R2(config-router)#router-id 2.2.2.2
```

```
R2(config-router)#network 2.2.2.2 0.0.0.0 area 0
```

```
R2(config-router)#network 192.168.12.2 0.0.0.0 area 0
```

```
R2(config-router)#network 192.168.23.2 0.0.0.0 area 0
```

❖ Kiểm tra bảng định tuyến:

```
R2#Show ip route ospf
```

Cấu hình định tuyến OSPF cho Router 1, 2, 3

```
R3(config)#router ospf 1
```

```
R3(config-router)#router-id 3.3.3.3
```

```
R3(config-router)# network 3.3.3.3 0.0.0.0 area 0
```

```
R3(config-router)# network 192.168.23.3 0.0.0.0 area 0
```

❖ Kiểm tra bảng định tuyến:

```
R3#Show ip route ospf
```

Cấu hình định tuyến BGP sử dụng card loopback

- ❖ Cấu hình định tuyến BGP giữa Router R1 và R4 sử dụng card loopback để thiết lập Neighbor.

R1(config)#router bgp 123

R1(config-router)# neighbor 4.4.4.4 update-source Loopback0

R1(config-router)# neighbor 4.4.4.4 remote-as 65004

//vì sử dụng card loopback để thiết lập neighbor nên cần phải “update-source” cho card loopback0

R1(config-router)# neighbor 4.4.4.4 update-source Loopback0

// Vì SD card loopback để thiết lập neighbor nên TTL phải >=2

R1(config-router)# neighbor 4.4.4.4 ebgp-multihop 255

// Để R1 thiết lập Neighbor được với R4 thì R1 phải nhìn thấy loopback của R4.

R1(config)# ip route 4.4.4.4 255.255.255.255 14.14.14.4

// Cấu hình BGP trên Router R4

```
R4(config)# router bgp 65004
```

```
R4(config-router)# network 44.44.44.44 mask 255.255.255.255
```

```
R4(config-router)# neighbor 1.1.1.1 remote-as 123
```

```
R4(config-router)# neighbor 1.1.1.1 ebgp-multihop 5
```

```
R4(config-router)# neighbor 1.1.1.1 update-source Loopback1
```

```
R4(config)# ip route 1.1.1.1 255.255.255.255 14.14.14.1
```

Cấu hình định tuyến BGP sử dụng interface physical

❖ Cấu hình định tuyến BGP giữa Router R3 và R5.

```
R3(config)#router bgp 123
```

```
R3(config-router)# neighbor 35.35.35.5 remote-as 65005
```

```
R5(config)# router bgp 65005
```

```
R5(config-router)# network 55.55.55.55 mask 255.255.255.255
```

```
R5(config-router)# neighbor 35.35.35.3 remote-as 123
```

Cấu hình BGP full mesh

- ❖ Cấu hình định tuyến BGP full mesh giữa các Router R1, R2 và R3.

// Cấu hình bgp trên Router R1

```
R1(config)#router bgp 123
```

```
R1(config-router)#neighbor 2.2.2.2 remote-as 123
```

```
R1(config-router)#neighbor 2.2.2.2 update-source loopback 0
```

```
R1(config-router)#neighbor 3.3.3.3 remote-as 123
```

```
R1(config-router)#neighbor 3.3.3.3 update-source loopback 0
```

Cấu hình BGP full mesh

// Cấu hình bgp trên Router R2

```
R2(config)#router bgp 123
```

```
R2(config-router)#neighbor 1.1.1.1 remote-as 123
```

```
R2(config-router)#neighbor 1.1.1.1 update-source loopback 0
```

```
R2(config-router)#neighbor 3.3.3.3 remote-as 123
```

```
R2(config-router)#neighbor 3.3.3.3 update-source loopback 0
```

Cấu hình BGP full mesh

// Cấu hình bgp trên Router R3

```
R3(config)#router bgp 123
```

```
R3(config-router)#neighbor 1.1.1.1 remote-as 123
```

```
R3(config-router)#neighbor 1.1.1.1 update-source loopback 0
```

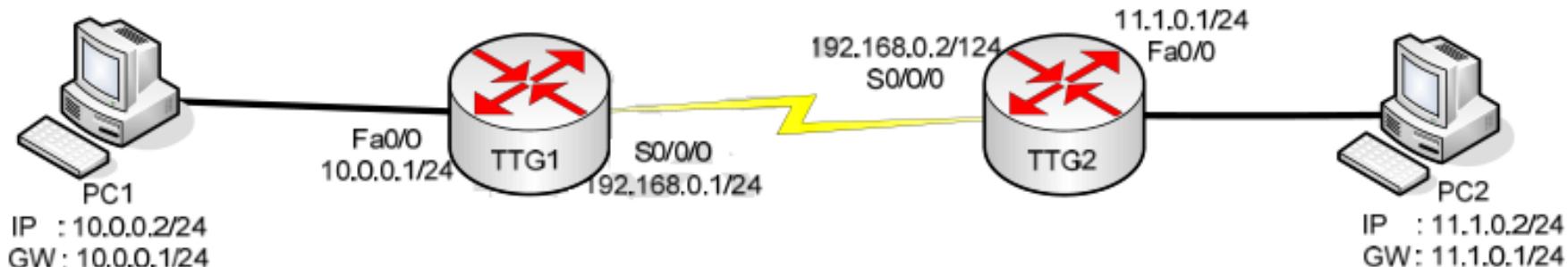
```
R3(config-router)#neighbor 2.2.2.2 remote-as 123
```

```
R3(config-router)#neighbor 2.2.2.2 update-source loopback 0
```

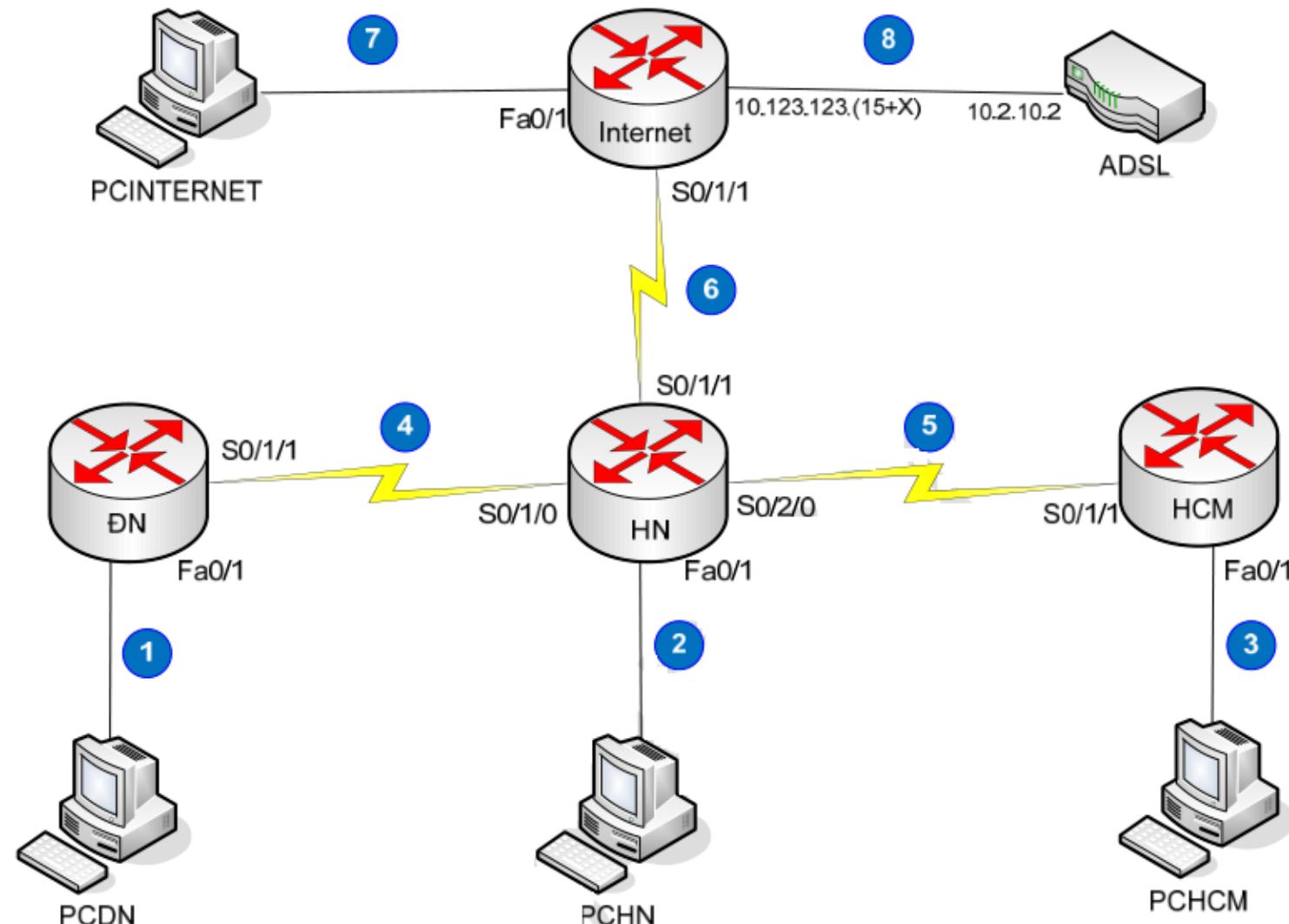
Lab 1: Cấu hình định tuyến tĩnh

1. Sử dụng Static Route để định tuyến
2. Kiểm tra lại thông tin định tuyến bằng các lệnh

- + Show ip route
- + Từ PC dùng lệnh tracert ra internet để liệt kê đường đi



LAB 2: ĐỊNH TUYỀN RIPv2

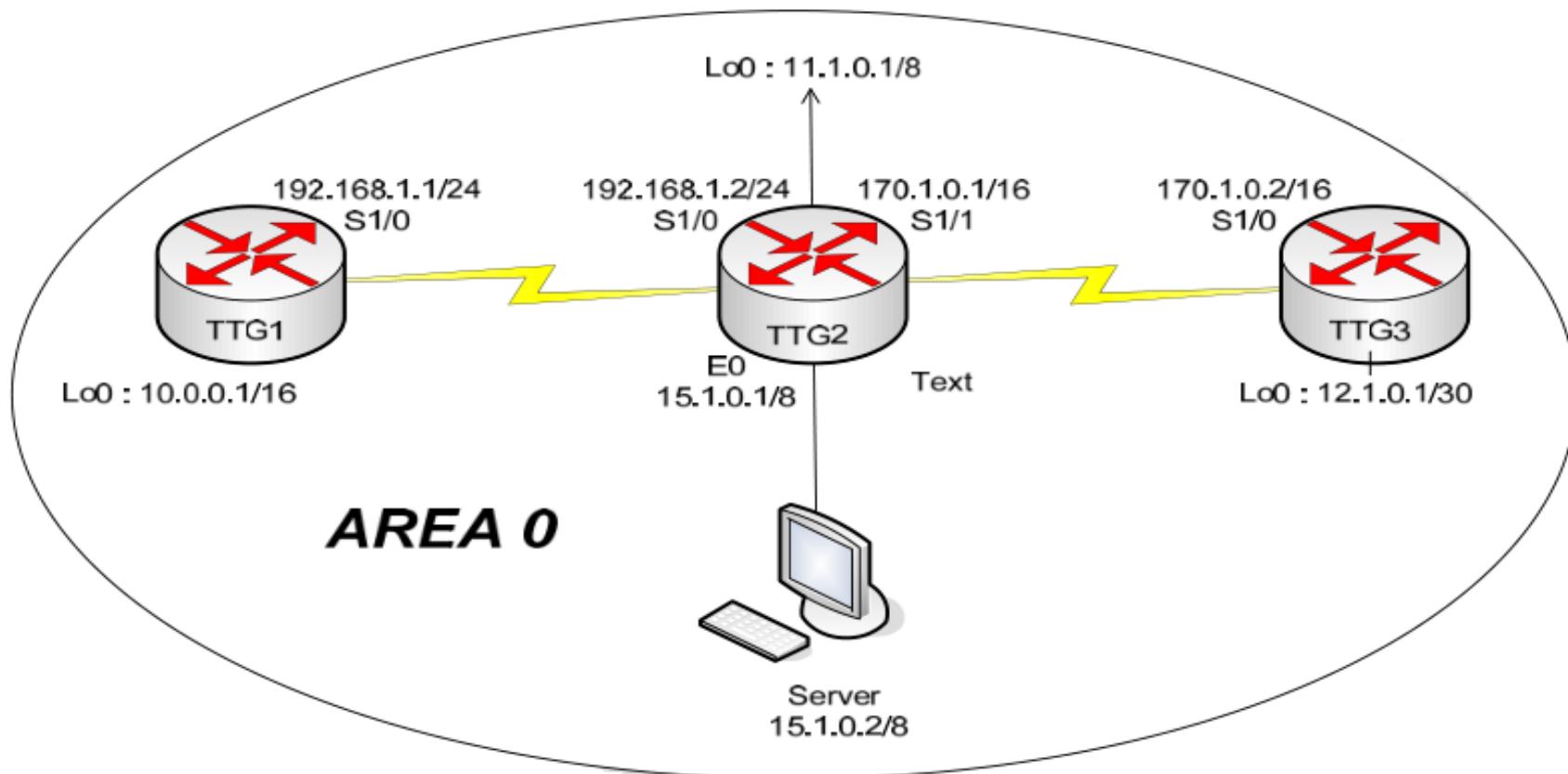


YÊU CẦU

1. Học viên sẽ thực hành trên thiết bị Cisco 2801
2. Sử dụng mạng 172.(15+X).0.0/16 để chia subnet với X là số thứ tự của nhóm
3. Sử dụng RIPv2 để định tuyến
4. Các PC phải đi được internet
5. Sau khi định tuyến xong, kiểm tra lại thông tin định tuyến bằng các lệnh :
 - + Show ip route
 - + Ping ra internet từ PC và router
 - + Từ PC dùng lệnh tracert ra internet để liệt kê đường đi từ nguồn đến đích

LAB 3: ĐỊNH TUYẾN OSPF

Các router được cấu hình các interface loopback 0. Địa chỉ IP của các interface được ghi trên hình. Lưu ý ở đây chúng ta sử dụng subnetmask của các mạng khác nhau.





TRƯỜNG ĐẠI HỌC THỦY LỢI

KHOA CÔNG NGHỆ THÔNG TIN
Bộ môn: Kỹ thuật máy tính và mạng

QUẢN TRỊ MẠNG

Giảng viên: Trần Văn Hội

Email: hoitv@tlu.edu.vn

Điện thoại: 0944.736.007

NỘI DUNG MÔN HỌC



Chương 1: Tổng quan về mạng



Chương 2: Các kỹ thuật định tuyến



Chương 3: Chuyển mạch trong mạng LAN



Chương 4: Công nghệ mạng WAN



Chương 5: Bảo mật mạng

CHƯƠNG 3: CHUYỂN MẠCH TRONG MẠNG LAN

1

- Khái niệm về chuyển mạch

2

- Mạng VLAN

3

- Trunking

4

- Giao thức VTP

5

- Định tuyến giữa các VLAN

6

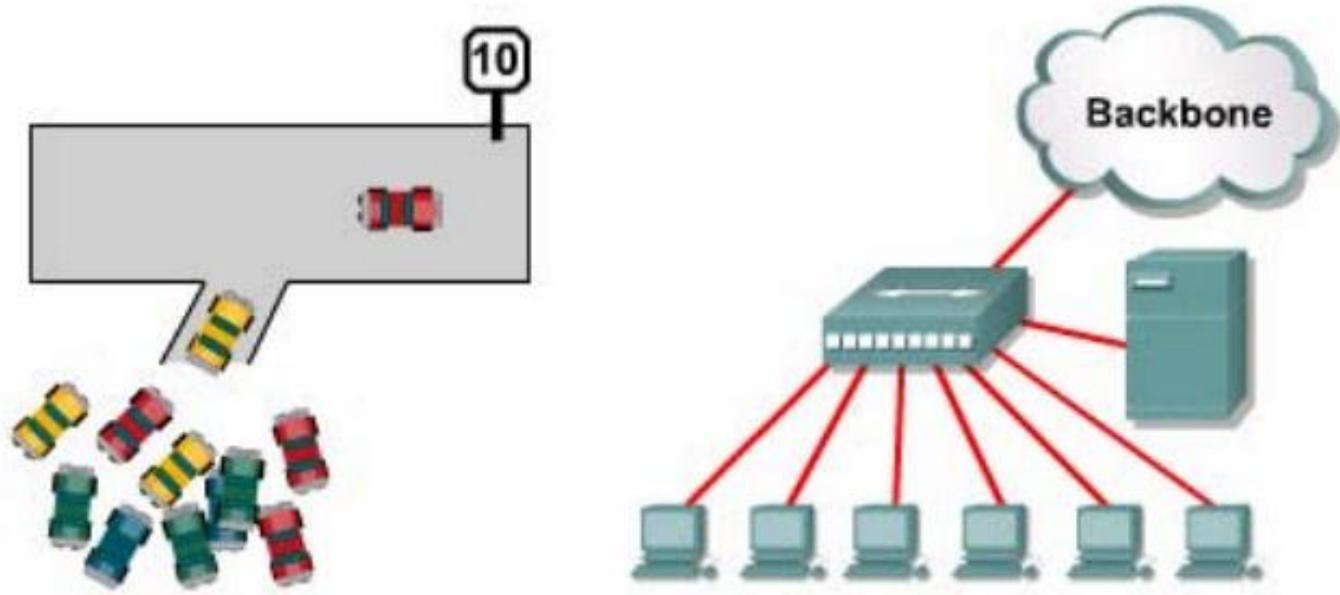
- Giao thức STP

BÀI 1: KHÁI NIỆM VỀ CHUYỂN MẠCH

1. GIỚI THIỆU VỀ HUB VÀ BRIDGE

- ❖ Ethernet cơ bản là kỹ thuật chia sẻ cùng 1 băng thông cho mọi người dùng trong 1 phân đoạn LAN.
- ❖ Các user kết nối và cùng một Hub hay Switch chia sẻ băng thông trên cùng một đường truyền.
- ❖ Hub là thiết bị lớp 1 và đôi khi được coi là một bộ tập trung Ethernet hay Repeater đa port. Sử dụng Hub trong mạng cho phép kết nối được nhiều user hơn.
- ❖ Loại Hub chủ động còn cho phép mở rộng khoảng cách của mạng vì nó thực hiện tái tạo lại tín hiệu dữ liệu.
- ❖ Hub ko hề có quyết định gì đối với tín hiệu dữ liệu mà nó nhận được. Nó chỉ đơn giản là khuếch đại và tái tạo lại tín hiệu mà nó nhận được và chuyển ra cho tất cả các thiết bị nối vào nó.

Collision domain: miền đụng độ



- ❖ Đụng độ là một hậu quả tất yếu của mạng Ethernet. Nếu có hai hay nhiều thiết bị cùng truyền cùng một lúc thì đụng độ sẽ xảy ra.

Collision domain: miền đụng độ

- ❖ Khi đụng độ xảy ra, các gói tin đang được truyền đều bị phá hủy, các máy đang truyền sẽ ngưng việc truyền dữ liệu và chờ một khoảng thời gian ngẫu nhiên theo quy luật của CSMA/CD.
- ❖ Nếu đụng độ xảy ra quá nhiều mạng có thể không hoạt động được.
- ❖ Miền đụng độ là khu vực mà dữ liệu được phát ra có thể bị đụng độ.
- ❖ Tất cả các môi trường mạng chia sẻ là các miền đụng độ.

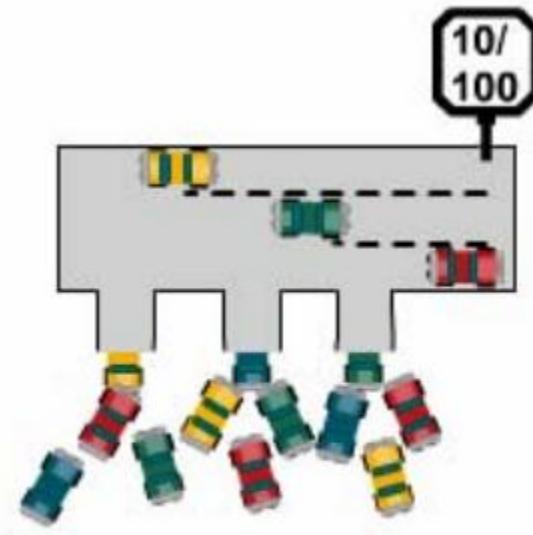
BRIDGE

- ❖ Bridge là 1 thiết bị lớp 2 được sử dụng để phân đoạn mạng. Bridge thu thập và chọn lựa dữ liệu để chuyển mạch giữa hai đoạn mạng bằng cách học địa chỉ MAC của tất cả các thiết bị nằm trong từng đoạn mạng kết nối vào nó.
- ❖ Dựa vào các địa chỉ MAC, Bridge xây dựng thành bảng chuyển mạch và theo đó để chuyển hoặc chặn gói lại. Nhờ vậy Bridge tách 1 mạng thành nhiều miền dung độ nhỏ hơn, làm tăng hiệu quả hoạt động của mạng.
- ❖ Bridge ko chặn các lưu lượng quảng bá nhưng dù sao thì Bridge cũng điều khiển lưu lượng mạng tốt hơn Hub.

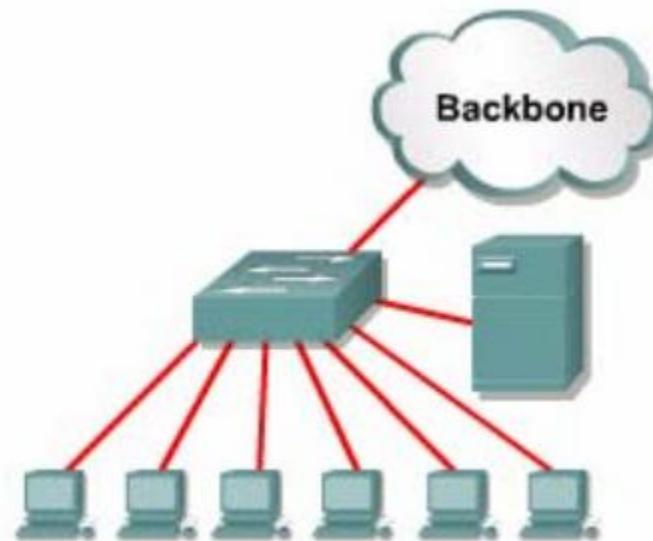
2. CHUYỂN MẠCH SWITCH

- ❖ Switch là 1 thiết bị lớp 2, Switch có thể quyết định chuyển 1 gói dựa trên địa chỉ MAC được ghi trong gói đó. Switch học địa chỉ MAC của các thiết bị kết nối trên từng port của nó và xây dựng thành bảng chuyển mạch.
- ❖ Khi hai thiết bị kết nối vào Switch thực hiện trao đổi với nhau, Switch sẽ thiết lập một mạch ảo cung cấp một đường liên lạc riêng giữa hai thiết bị này.
- ❖ Switch có khả năng phân đoạn mạng cực nhỏ, nghĩa là tạo ra môi trường ko đụng độ giữa nguồn và đích.
- ❖ Switch có thể tạo nhiều mạch ảo đồng thời giữa các cặp thiết bị khác nhau.

CHUYỀN MẠCH SWITCH



Multiple devices sending
at the same time



Each node has 10/100 Mbps

- ❖ Switch nhận được gói quảng bá thì nó sẽ gửi ra tất cả các cổng của nó trừ cổng nhận gói tin vào. Mỗi thiết bị nhận được gói quảng bá đều phải xử lý thông tin nằm trong đó.
- ❖ Khi số lượng quảng bá quá nhiều sẽ làm cho thời của mạng rất chậm.

Broadcast domain: miền quảng bá

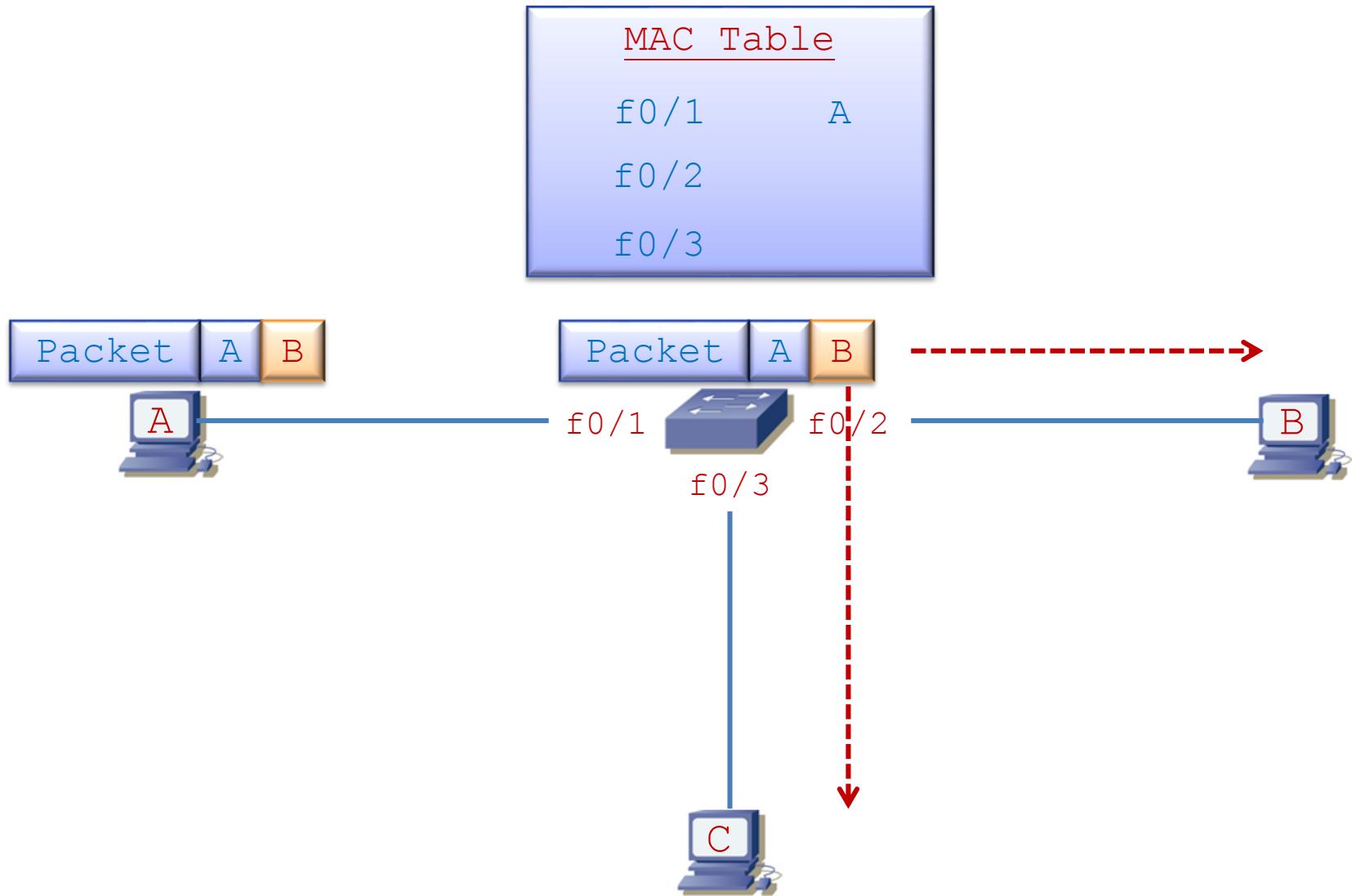
Các thông tin liên lạc trong mạng được thực hiện theo ba cách: unicast, multicast và broadcast.

- Unicast: gửi trực tiếp từ một máy đến một máy.
- Multicast: được thực hiện khi một máy muốn gửi gói tin cho một nhóm máy.
- Broadcast: được thực hiện khi một máy muốn gửi cho tất cả các máy khác trong mạng.

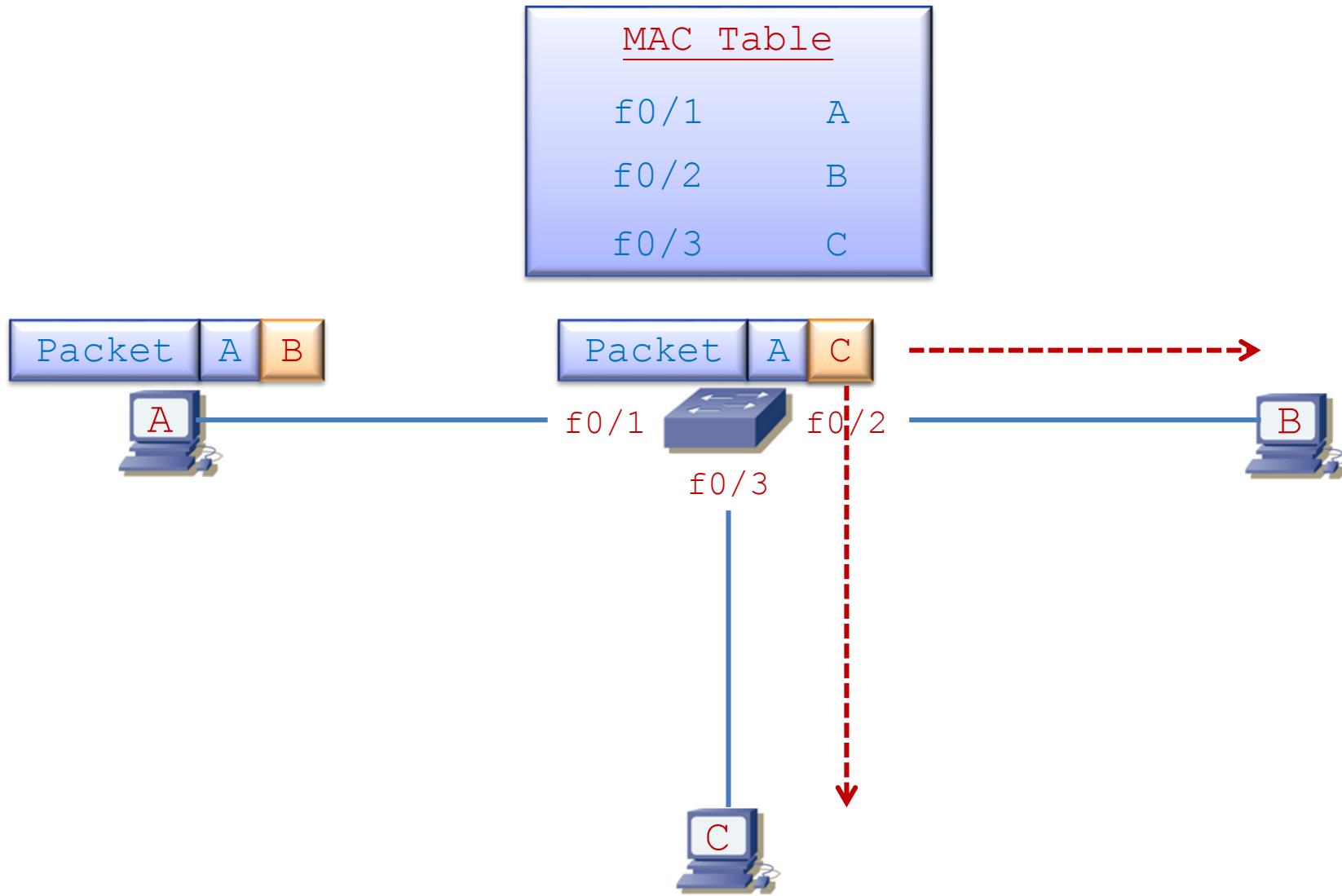
Khi một thiết bị muốn gửi một gói quảng bá thì địa chỉ MAC đích của gói tin đó sẽ là

FF:FF:FF:FF:FF:FF. Với địa chỉ như vậy, mọi thiết bị đều nhận và xử lý gói quảng bá. Miền quảng bá là miền bao gồm tất cả các thiết bị có thể nhận được gói tin quảng bá từ một thiết bị nào đó trong LAN.

SWITCHING



SWITCHING



CHƯƠNG 3: CHUYỂN MẠCH TRONG MẠNG LAN

1

- Khái niệm về chuyển mạch

2

- Mạng VLAN

3

- Trunking

4

- Giao thức VTP

5

- Định tuyến giữa các VLAN

6

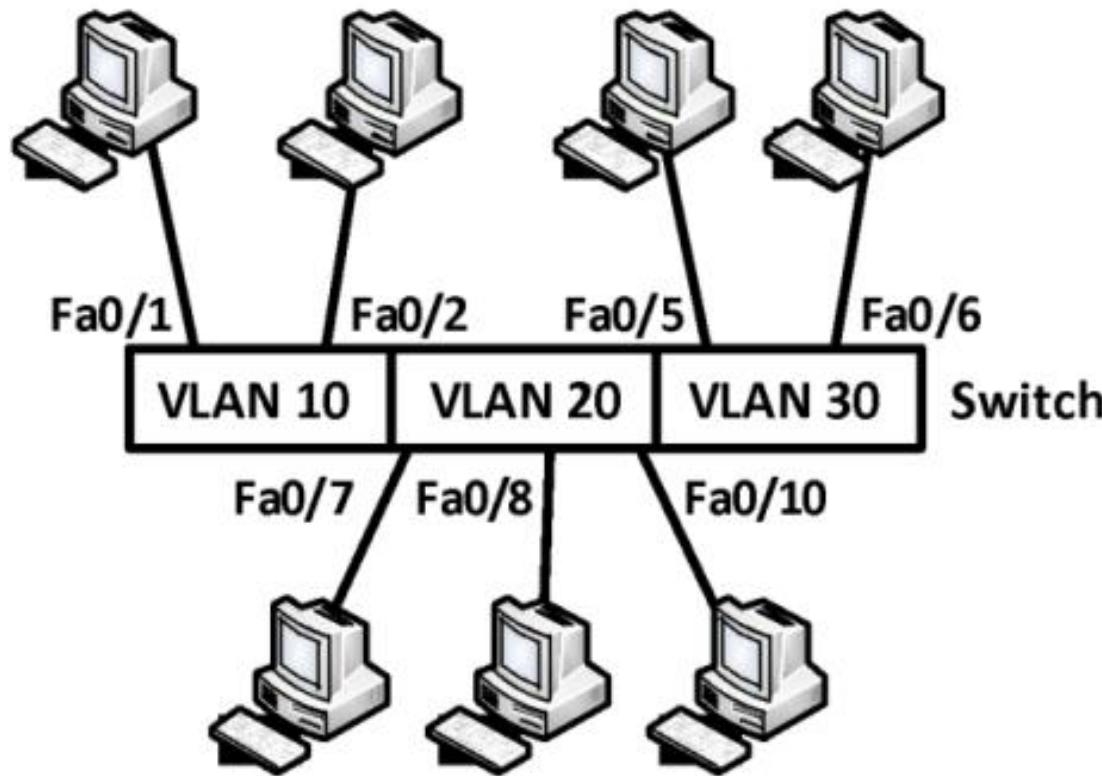
- Giao thức STP

BÀI 2: MẠNG VLAN

1. Khái niệm VLAN

- ❖ VLAN (Virtual LAN) là kỹ thuật được sử dụng trên Switch, dùng để chia một Switch vật lý thành nhiều Switch luận lý.
- ❖ Mỗi một Switch luận lý gọi là một VLAN hoặc có thể hiểu VLAN là một tập hợp của các cổng trên Switch nằm trong cùng một miền quảng bá.
- ❖ Các cổng trên Switch có thể được nhóm vào các VLAN khác nhau trên một Switch hoặc được triển khai trên nhiều Switch.

VLAN = broadcast domain = logical network



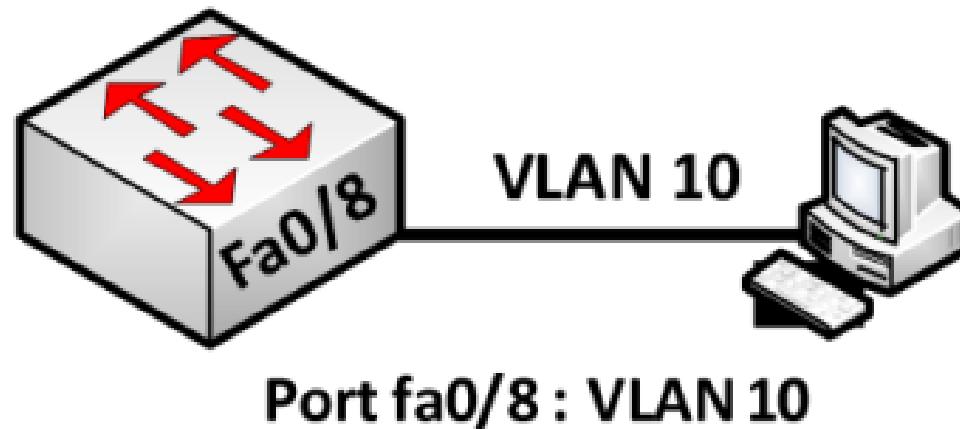
Một VLAN là một tập hợp của các switchport nằm trong cùng một broadcast domain. Các cổng trên switch có thể được nhóm vào các VLAN khác nhau trên từng switch hoặc trên nhiều switch.

VLAN

- ❖ Khi có một gói tin quảng bá được gửi bởi một thiết bị nằm trong một VLAN sẽ được chuyển đến các thiết bị khác nằm trong cùng VLAN đó, gói tin quảng bá sẽ không được chuyển tiếp đến các thiết bị thuộc VLAN khác.
- ❖ VLAN cho phép người quản trị tổ chức mạng theo luận lý chứ không theo vật lý. Sử dụng VLAN có ưu điểm là:
 - ✓ Tăng khả năng bảo mật
 - ✓ Thay đổi cấu hình LAN dễ dàng
 - ✓ Di chuyển máy trạm trong LAN dễ dàng
 - ✓ Thêm máy trạm vào LAN dễ dàng.

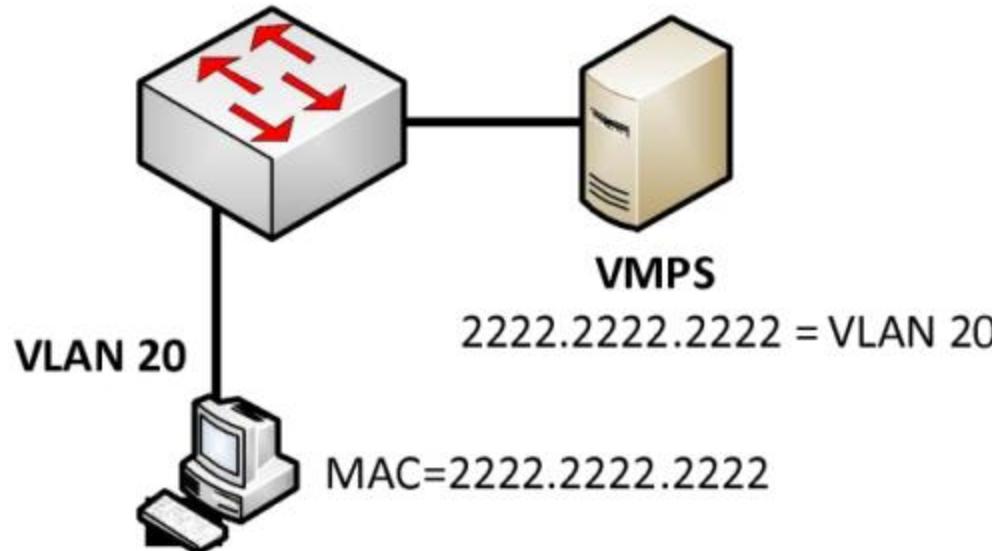
2. PHÂN LOẠI VLAN

- ❖ VLAN tĩnh (Static VLAN): Đối với loại này, các cổng của Switch được cấu hình thuộc về một VLAN nào đó, các thiết bị gắn vào cổng đó sẽ thuộc về VLAN đã định trước. Đây là loại VLAN dùng phổ biến.



2. PHÂN LOẠI VLAN

- ❖ VLAN động (dynamic VLAN): Loại VLAN này sử dụng một server lưu trữ địa chỉ MAC của các thiết bị và qui định VLAN mà thiết bị đó thuộc về, khi một thiết bị gắn vào Switch, Switch sẽ lấy địa chỉ MAC của thiết bị và gửi cho server kiểm tra và cho vào VLAN định trước.



3. CẤU HÌNH VLAN

❖ Bước 1: Tạo VLAN

Switch(config)#vlan <vlan-id>

Switch(config-vlan)#name <vlan-name>

Ví dụ: Switch(config)#vlan 10

 Switch(config-if)#name P.KyThuat

3. CẤU HÌNH VLAN

❖ Bước 2: Gán các cổng cho VLAN

Switch(config)#interface <interface>

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan <vlan-id>

Ví dụ: Switch(config)#interface fa0/5

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10

GÁN 1 DÃY CÁC CÔNG

❖ Gán nhiều cổng liên tiếp

Switch(config)#interface range <start>-<end-intf>

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan <vlan-id>

❖ Ví dụ: Switch(config)#interface fa0/10 - 20

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 10

GÁN 1 DÃY CÁC CÔNG

❖ Gán nhiều cổng không liên tiếp

Switch(config)#interface range <interface1,
interface2,...>

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan <vlan-id>

❖ Ví dụ: Switch(config)#interface fa0/7, fa0/9, fa0/2

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 10

LỆNH XÓA VÀ KIỂM TRA

- ❖ Xóa VLAN: Xóa một VLAN trên switch bằng cách sử dụng lệnh “no” trước câu lệnh tạo VLAN.

- ❖ Lệnh kiểm tra cấu hình VLAN

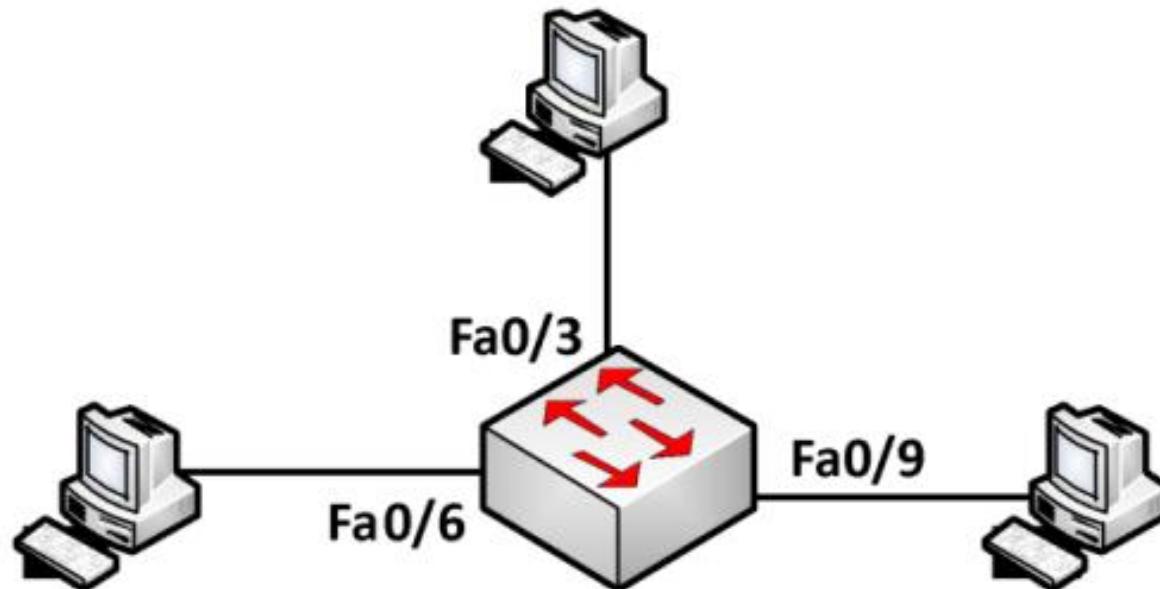
Switch#show vlan

- ❖ Lệnh này cho phép hiển thị các VLAN-ID (số hiệu VLAN), tên VLAN, trạng thái VLAN và các cổng được gán cho VLAN trên switch.

BÀI TẬP

Mô tả yêu cầu:

- ❖ Cấu hình VLAN trên Switch Tạo 3 VLAN: VLAN 10, VLAN 20, VLAN 30
- ❖ Fa0/1 –Fa0/6: VLAN 10, Fa0/7 – Fa0/9: VLAN 20, Fa0/10 – Fa0/12: VLAN 30



CHƯƠNG 3: CHUYỂN MẠCH TRONG MẠNG LAN

1

- Khái niệm về chuyển mạch

2

- Mạng VLAN

3

- Trunking

4

- Giao thức VTP

5

- Định tuyến giữa các VLAN

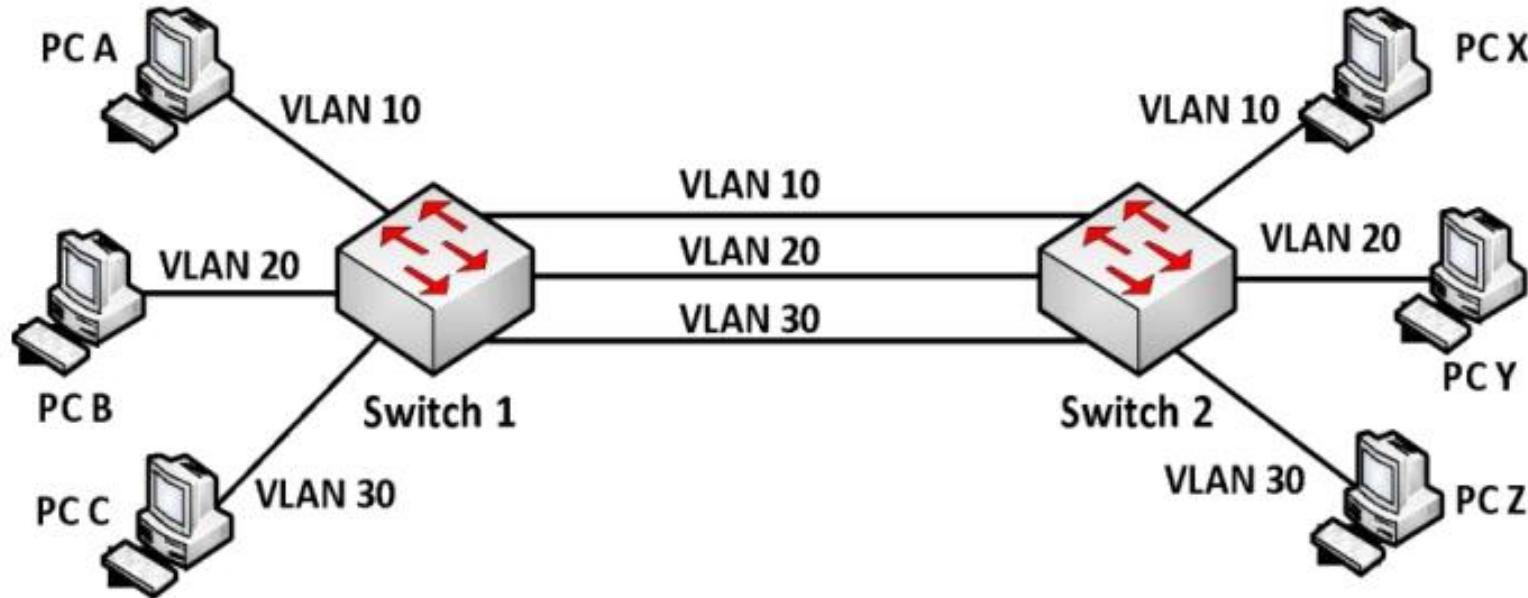
6

- Giao thức STP

BÀI 3: ĐƯỜNG TRUNKING

Cách tổ chức để các thiết bị cùng VLAN nhưng ở trên nhiều switch khác nhau có thể liên lạc với nhau?

❖ Dùng mỗi kết nối cho từng VLAN

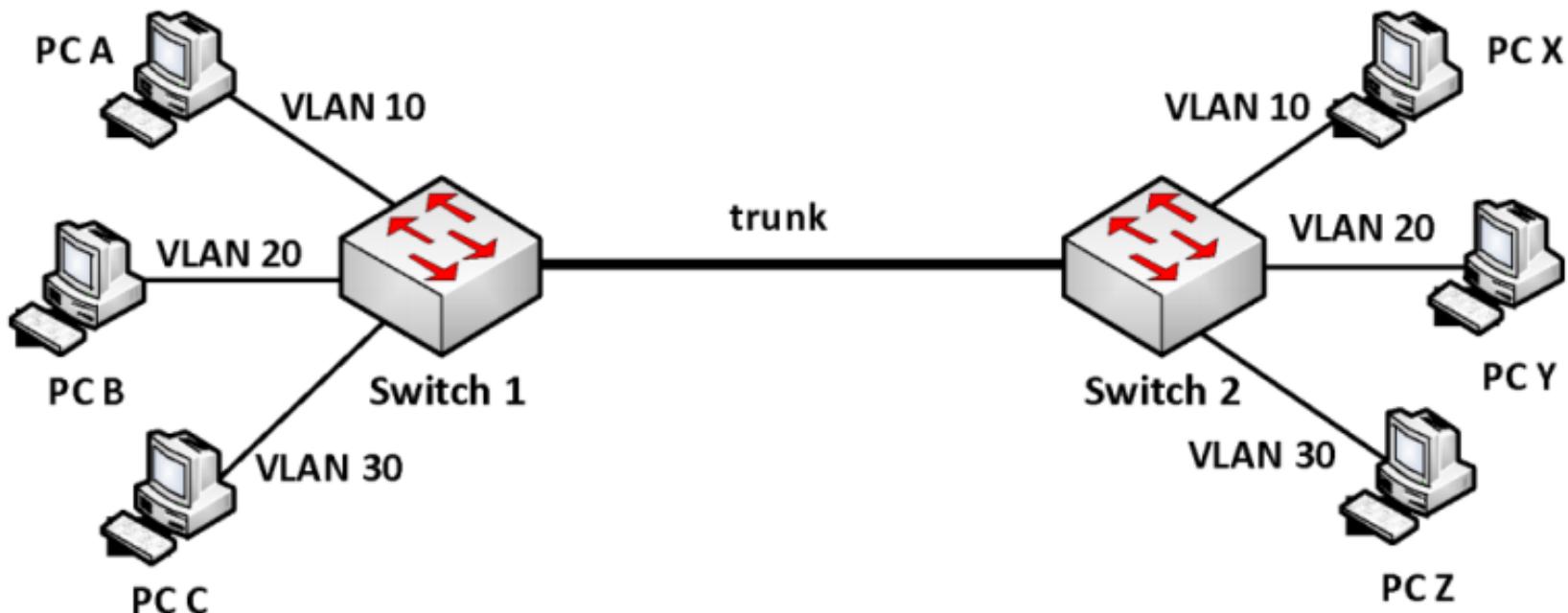


Điều này gây ra lãng phí.

ĐƯỜNG TRUNK

❖ Kết nối trunk (đường trunk)

Một kỹ thuật khác để giải quyết vấn đề trên là dùng chỉ một kết nối cho phép dữ liệu của các VLAN có thể cùng lưu thông qua đường này. Người ta gọi kết nối này là đường trunk.



Đường dây như thế gọi là liên kết trunk lớp 2.

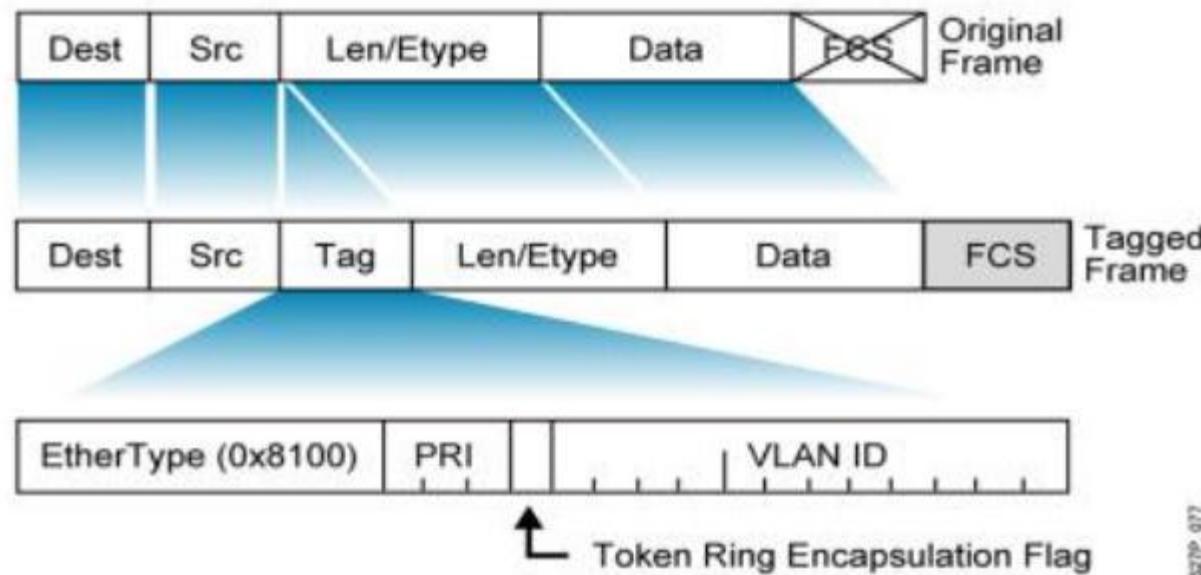
ĐƯỜNG TRUNK

- ❖ Kết nối “trunk” là liên kết Point-to-Point giữa các cổng trên switch với router hoặc với switch khác. Kết nối “trunk” sẽ vận chuyển dữ liệu của nhiều VLAN thông qua một liên kết đơn và cho phép mở rộng VLAN trên hệ thống mạng.
- ❖ Vì kỹ thuật này cho phép dùng chung một kết nối vật lý cho dữ liệu của các VLAN đi qua nên để phân biệt được chúng là dữ liệu của VLAN nào, người ta gắn vào các gói tin một dấu hiệu gọi là “tagging”. Hay nói cách khác là dùng một kiểu đóng gói riêng cho các gói tin di chuyển qua đường “trunk” này. Giao thức được sử dụng là 802.1Q (dot1q).

GIAO THỨC 802.1Q

Đây là giao thức chuẩn của IEEE để dành cho việc nhận dạng các VLAN bằng cách thêm vào “frame header” đặc điểm của một VLAN. Phương thức này còn được gọi là gắn thẻ cho VLAN (frame tagging).

802.1Q Frame



CẤU HÌNH VLAN TRUNKING

- ❖ Để cấu hình đường “trunk”, chúng ta cấu hình 2 cổng “trunk” như sau:

```
switch(config)#interface <interface>
```

```
switch(config-if)#switchport mode trunk
```

```
switch(config-if)#switchport trunk encapsulation
```

```
dot1q
```

- ❖ Lệnh cuối cùng là mặc định ở một số dòng switch

CHƯƠNG 3: CHUYỂN MẠCH TRONG MẠNG LAN

1

- Khái niệm về chuyển mạch

2

- Mạng VLAN

3

- Trunking

4

- Giao thức VTP

5

- Định tuyến giữa các VLAN

6

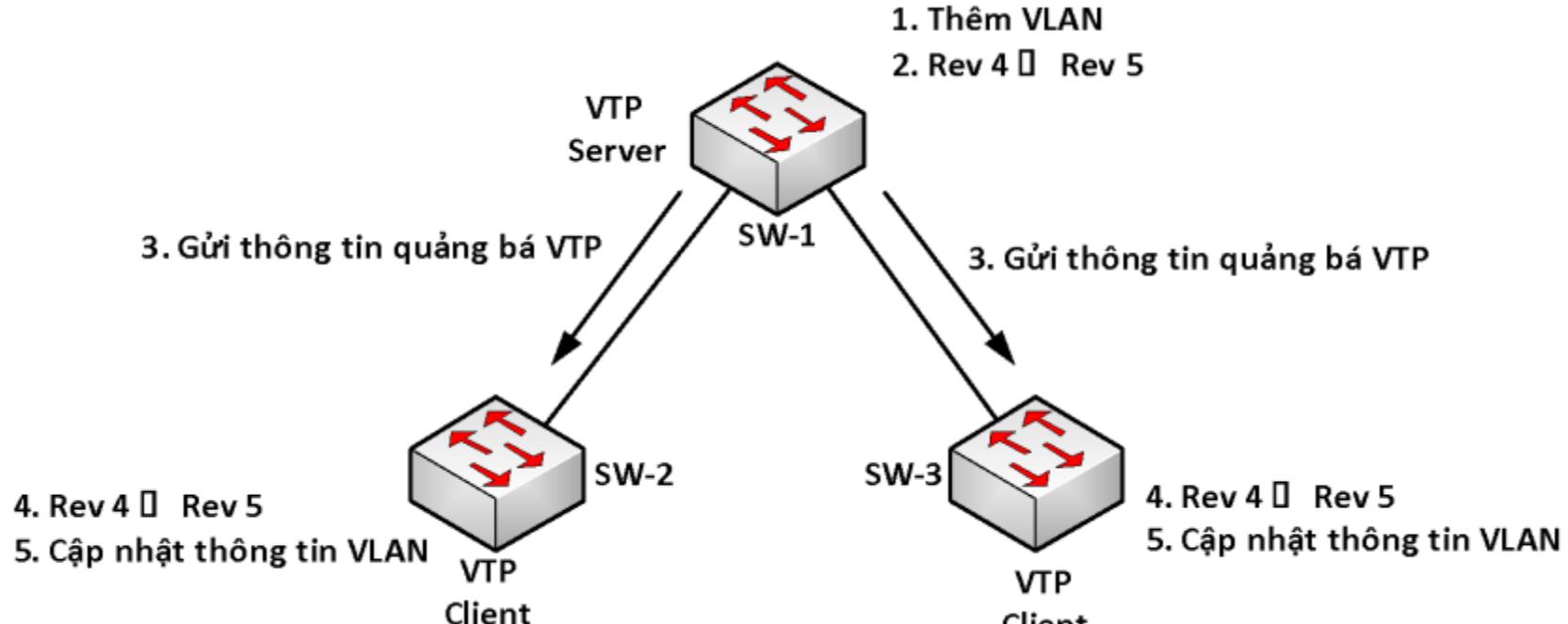
- Giao thức STP

BÀI 4: GIAO THỨC VTP

- ❖ VTP (VLAN Trunking Protocol) là giao thức hoạt động ở tầng liên kết dữ liệu trong mô hình OSI. VTP giúp cho việc cấu hình VLAN luôn đồng nhất khi thêm, xóa, sửa thông tin về VLAN trong hệ thống mạng.
- ❖ Hoạt động của VTP
 - VTP gửi thông điệp quảng bá qua “VTP domain” mỗi 5 phút một lần, hoặc khi có sự thay đổi xảy ra trong cấu hình VLAN.
 - Một thông điệp VTP bao gồm “revision-number”, tên VLAN (VLAN name), số hiệu VLAN (VLAN number), và thông tin về các switch có cổng gắn với mỗi VLAN.
 - Bằng sự cấu hình VTP Server và việc quảng bá thông tin VTP, tất cả các switch đều đồng bộ về tên VLAN và số hiệu VLAN của tất cả các VLAN.

GIAO THÚC VTP

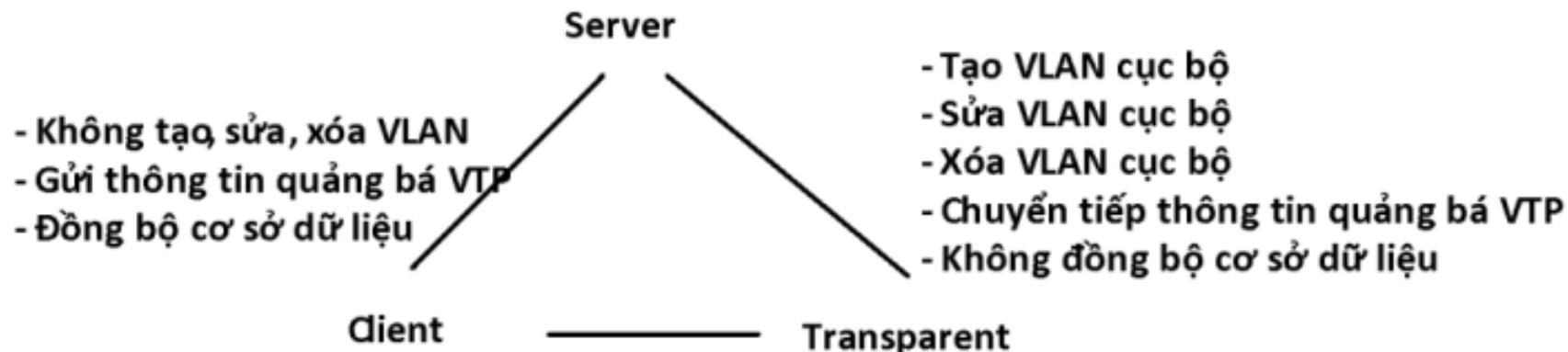
- ❖ Một trong những thành phần quan trọng trong các thông tin quảng bá VTP là tham số “revision number”.
- ❖ Mỗi lần VTP server điều chỉnh thông tin VLAN, nó tăng “revisionnumber” lên 1, rồi sau đó VTP Server mới gửi thông tin quảng bá VTP đi.
- ❖ Khi một switch nhận một thông điệp VTP với “revision-number” lớn hơn, nó sẽ cập nhật cấu hình VLAN.



CHẾ ĐỘ HOẠT ĐỘNG CỦA VTP

❖ **Switch ở chế độ VTP server:** Có thể tạo, chỉnh sửa và xóa VLAN. VTP server lưu cấu hình VLAN trong NVRAM của nó. VTP Server gửi thông điệp ra tất cả các cổng “trunk”.

- Tạo VLAN
- Sửa VLAN
- Xóa VLAN
- Gửi thông tin quảng bá VTP
- Đồng bộ cơ sở dữ liệu



CHẾ ĐỘ HOẠT ĐỘNG CỦA VTP

❖ Switch ở chế độ VTP client:

- ✓ Không tạo, sửa và xóa thông tin VLAN. VTP Client có chức năng đáp ứng theo mọi sự thay đổi của VLAN từ Server và gửi thông điệp ra tất cả các cổng “trunk” của nó.

- ✓ VTP Client đồng bộ cấu hình VLAN trong hệ thống.

❖ Switch ở chế độ transparent: Sẽ nhận và chuyển tiếp các thông điệp quảng bá VTP do các switch khác gửi đến mà không quan tâm đến nội dung của các thông điệp này.

- ✓ Không cập nhật vào cơ sở dữ liệu của nó; đồng thời nếu cấu hình VLAN của nó có gì thay đổi, nó cũng không gửi thông tin cập nhật cho các switch khác.

- ✓ Switch hoạt động ở “transparent-mode” chỉ có thể tạo ra các VLAN cục bộ. Các VLAN này sẽ không được quảng bá đến các switch khác.

CẤU HÌNH VTP

- ❖ Cấu hình VTP domain

Switch(config)#vtp domain <domain_name>

- ❖ Cấu hình VTP mode

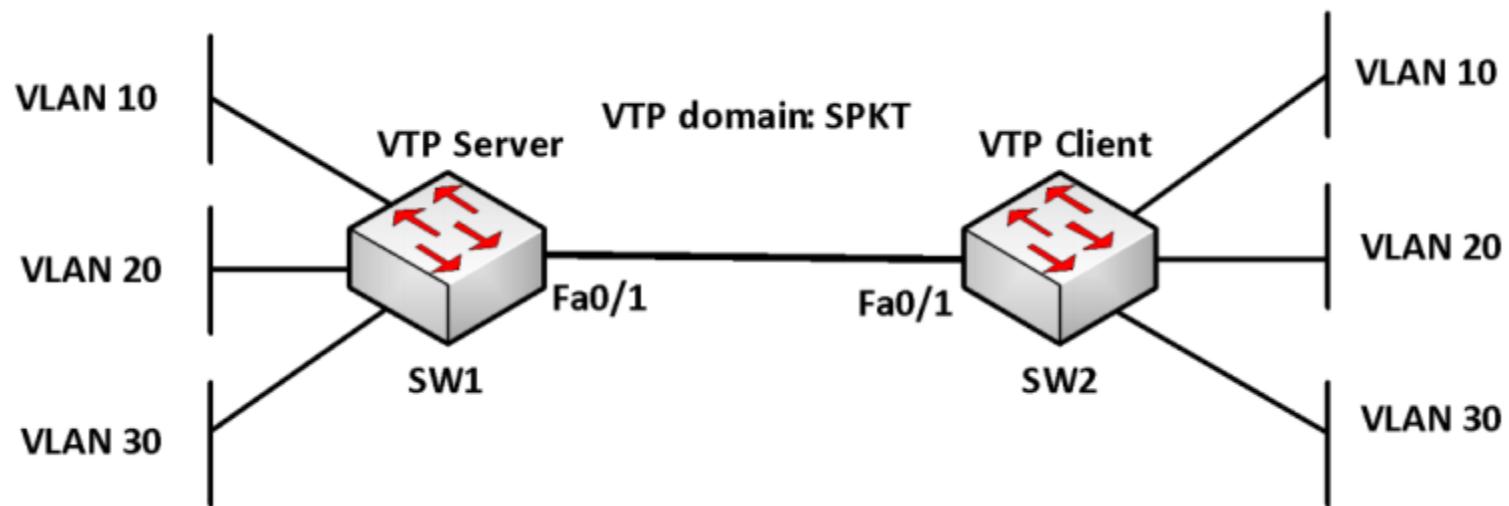
Switch(config)#vtp mode [client| transparent| server]

- ❖ Lệnh xem cấu hình VTP

Switch#show vtp status

BÀI TẬP

- ❖ Hai switch kết nối với nhau qua đường “trunk”.
- ❖ Tạo 3 vlan: VLAN 10, VLAN 20, VLAN 30 trên SW1
- ❖ Cấu hình VTP để các thông tin các VLAN trên SW1 cập nhật cho SW2
- ❖ Trên SW1: VLAN 10 (Fa0/2 – Fa0/4), VLAN 20 (Fa0/5 – Fa0/7), VLAN 30 (Fa0/8 – Fa0/10)
- ❖ Trên SW2: VLAN 10 (Fa0/4 – Fa0/6), VLAN 20 (Fa0/7 – Fa0/9), VLAN 30 (Fa0/10 – Fa0/12)



CẤU HÌNH SW1 LÀM VTP SERVER

- Thiết lập VTP domain: SPKT, VTP mode Server, và tạo các VLAN
 - sw1#config terminal
 - sw1(config)#vtp mode server
 - sw1(config)#vtp domain SPKT
 - sw1(config)#vlan 10 name CNTT
 - sw1(config)#vlan 20 name TTTH
 - sw1(config)#vlan 30 name TTCLC

GÁN CÁC PORT VÀO CÁC VLAN

- ❖ sw1(config)#int range f0/2 - 4
- ❖ sw1(config-if-range)#switchport mode access
- ❖ sw1(config-if-range)#switchport access vlan 10
- ❖ sw1(config-if)#int range f0/5 - 7
- ❖ sw1(config-if-range)#switchport mode access
- ❖ sw1(config-if-range)#switchport access vlan 20
- ❖ sw1(config-if)#int range f0/8 - 10
- ❖ sw1(config-if-range)#switchport mode access
- ❖ sw1(config-if-range)#switchport access vlan 30

CẤU HÌNH ĐƯỜNG TRUNK

- ❖ Cấu hình đường trunk và cho phép tất cả các VLAN qua đường trunk

```
sw1(config)#interface f0/1
```

```
sw1(config-if)#switchport mode trunk
```

```
sw1(config-if)#switchport trunk encapsulation dot1q
```

- ❖ Kiểm tra cấu hình

```
switch#show vlan
```

```
switch# show vtp status
```

```
switch#show vtp counters:
```

(kiểm tra số lần gửi và nhận thông tin trunking)

CẤU HÌNH SW2 LÀM VTP CLIENT

- ❖ Cấu hình vtp domain: SPKT, vtp mode: client

SW2(config)#vtp domain SPKT

SW2(config)#vtp mode client

- ❖ Cấu hình trunking trên cổng f0/1 của SW2

SW2(config)#int f0/1

SW2(config-if)#switchport mode trunk

SW2(config-if)#switchport trunk encapsulation dot1q

GÁN CÁC PORT VÀO CÁC VLAN

- ❖ sw2(config)#int range f0/4 - 6
- ❖ sw2(config-if-range)#switchport mode access
- ❖ sw2(config-if-range)#switchport access vlan 10
- ❖ sw2(config)#int range f0/7 - 9
- ❖ sw2(config-if-range)#switchport mode access
- ❖ sw2(config-if-range)#switchport access vlan 20
- ❖ sw2(config)#int range f0/10 - 12
- ❖ sw2(config-if-range)#switchport mode access
- ❖ sw2(config-if-range)#switchport access vlan 30

CHƯƠNG 3: CHUYỂN MẠCH TRONG MẠNG LAN

1

- Khái niệm về chuyển mạch

2

- Mạng VLAN

3

- Trunking

4

- Giao thức VTP

5

- Định tuyến giữa các VLAN

6

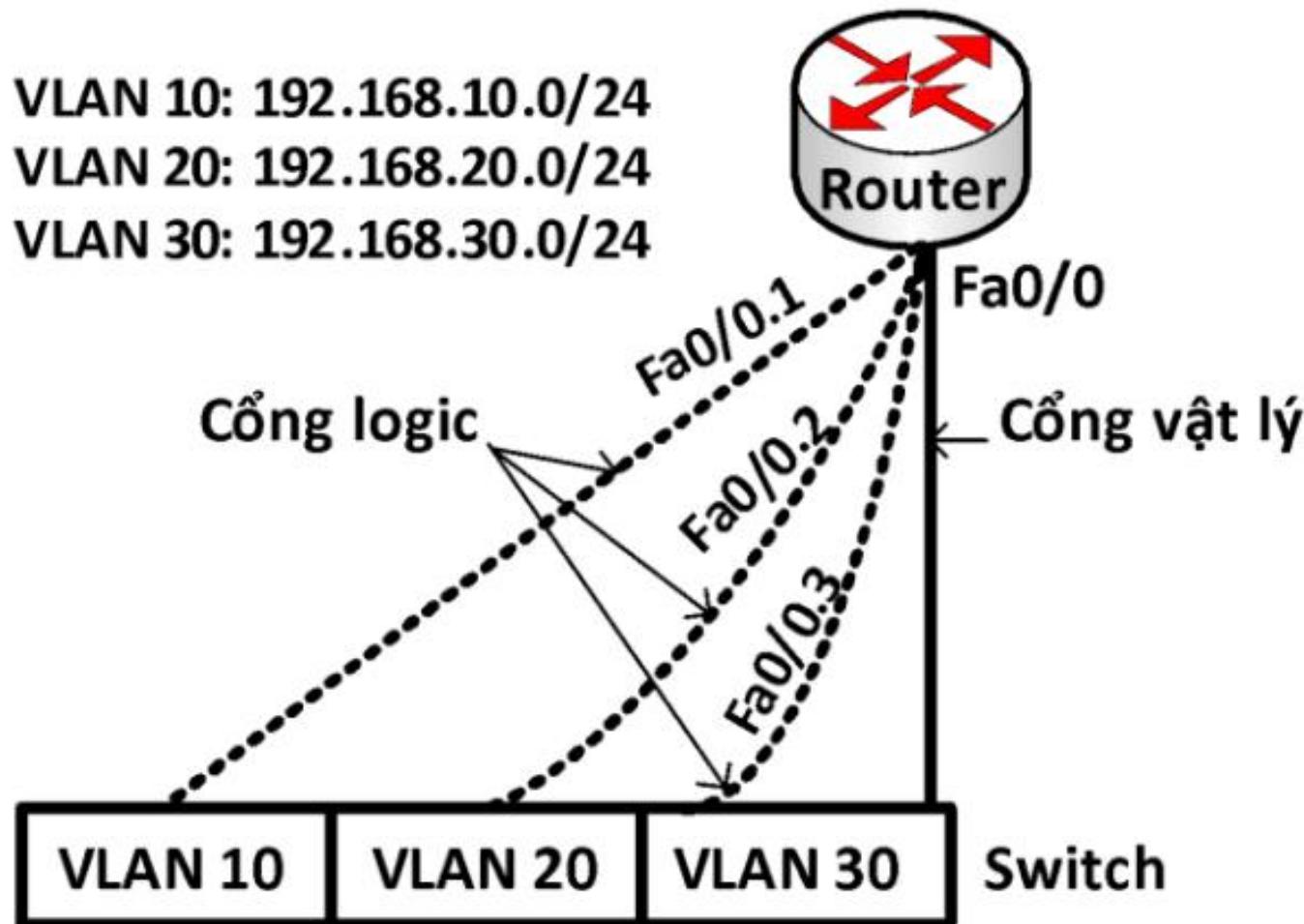
- Giao thức STP

BÀI 5: ĐỊNH TUYẾN GIỮA CÁC VLAN

- ❖ Nếu một máy tính trong một VLAN muốn liên lạc với một máy tính thuộc một VLAN khác thì nó phải thông qua thiết bị định tuyến như là router.
- ❖ Router trong cấu trúc VLAN thực hiện ngăn chặn quảng bá, bảo mật và quản lý các lưu lượng mạng.
- ❖ Switch layer 2 không thể chuyển dữ liệu giữa các VLAN với nhau. Dữ liệu trao đổi giữa các VLAN phải được định tuyến qua thiết bị hoạt động ở tầng mạng như router.
- ❖ Giả sử trên switch tạo 3 VLAN, nếu ta dùng 3 cổng của router để định tuyến cho 3 VLAN này thì quá cồng kềnh và không tiết kiệm. Ta chỉ cần sử dụng 1 cổng trên router kết nối với một cổng trên switch và cấu hình đường này làm đường trunk (trunk layer 3) để định tuyến cho các VLAN.

CÔNG VẬT LÝ VÀ CÔNG LOGIC

VLAN 10: 192.168.10.0/24
VLAN 20: 192.168.20.0/24
VLAN 30: 192.168.30.0/24

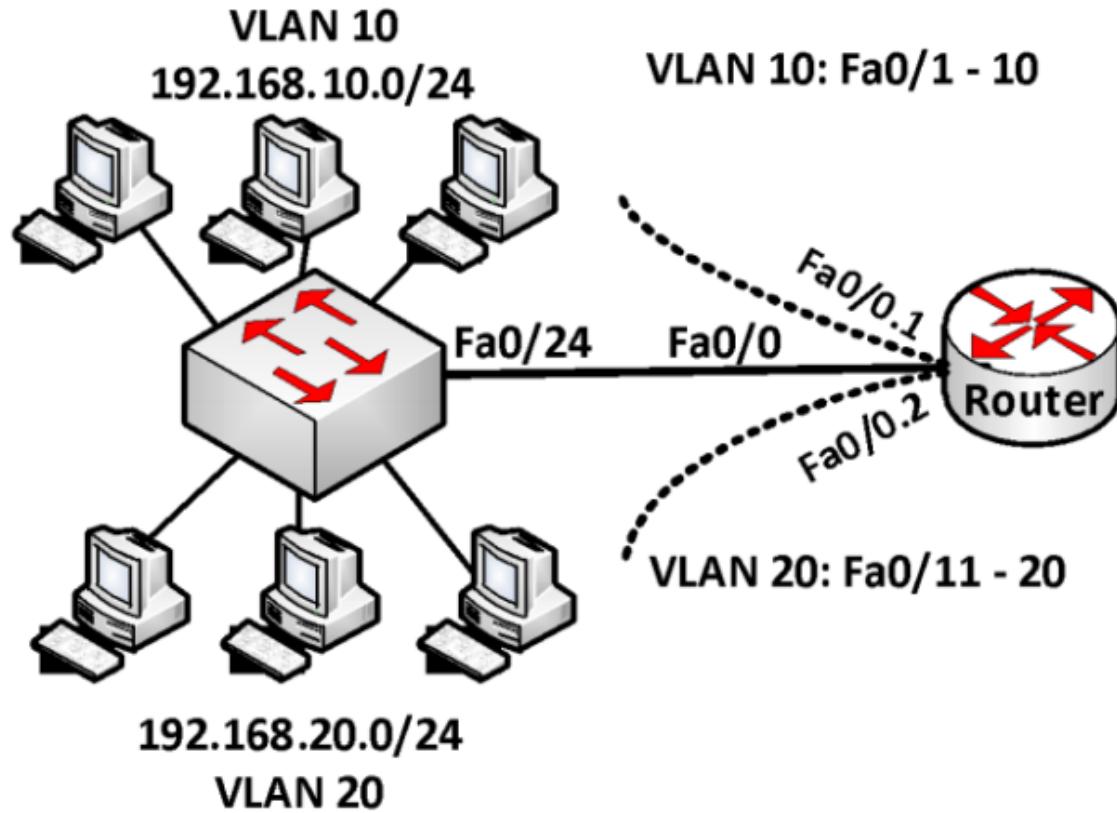


CẤU HÌNH ĐỊNH TUYẾN CHO CÁC VLAN DÙNG ROUTER

- ❖ R(config)#interface <interface.subintf-number>
- ❖ R(config-if)#encapsulation dot1q <vlan-id>
- ❖ R(config-if)#ip address <address> <subnet-mask>

BÀI TẬP

- ❖ Yêu cầu: Tạo 2 vlan: VLAN 10 (P.KinhDoanh) có cổng Fa0/1–Fa0/10 và VLAN 20 (P.KeToan) có cổng Fa0/11–Fa0/20.
- ❖ Cấu hình định tuyến cho phép hai VLAN này có thể liên lạc được với nhau.



CẤU HÌNH TRÊN SWITCH

❖ Tạo VLAN

```
switch(config)#vlan 10
```

```
switch(config-vlan)#name P.KinhDoanh
```

```
switch(vlan)#vlan 20
```

```
switch(config-vlan)#name P.KeToan
```

❖ Gán các port vào VLAN

```
switch(config)#interface range fa0/1 - 10
```

```
switch(config-if-range)#switchport mode access
```

```
switch(config-if-range)#switchport access vlan 10
```

```
switch(config)#int fa0/11 - 20
```

```
switch(config-if-range)#switchport mode access
```

```
switch(config-if-range)#switchport access vlan 20
```

CẤU HÌNH TRÊN SWITCH

❖ Cấu hình đường trunk

```
switch(config)#int fa0/24
```

```
switch(config-if)#switchport mode trunk
```

```
switch(config-if)#switchport trunk encapsulation dot1q
```

CẤU HÌNH TRÊN ROUTER

- ❖ Chọn cổng fa0/0 để cấu hình trunk

```
router(config)#interface fa0/0
```

```
router(config-if)#no shutdown
```

- ❖ Kích hoạt trunk trên subinterface fa0/0.1 và đóng gói dot1q

```
router(config)#int fa0/0.1
```

```
router(config-if)#encapsulation dot1q 10
```

- ❖ Cấu hình thông tin lớp 3 cho sub-interface fa0/0.1

```
router(config-subif)#ip address 192.168.1.1 255.255.255.0
```

CẤU HÌNH TRÊN ROUTER

- ❖ Kích hoạt “trunk” trên sub-interface fa0/0.2 và đóng gói bằng dot1q

```
router(config)#int fa0/0.2
```

```
router(config-subif)#encapsulation dot1q 20
```

- ❖ Cấu hình thông tin lớp 3 cho sub-interface fa0/0.2

```
router(config-subif)#ip address 192.168.2.1 255.255.255.0
```

- ❖ Lưu cấu hình

```
router#copy run start
```

- ❖ Kiểm tra cấu hình

```
Switch#show interface <interface>
```

```
Switch#show vlan ; Router#show vlan
```

```
Switch#show vtp status
```

CHƯƠNG 3: CHUYỂN MẠCH TRONG MẠNG LAN

1

- Khái niệm về chuyển mạch

2

- Mạng VLAN

3

- Trunking

4

- Giao thức VTP

5

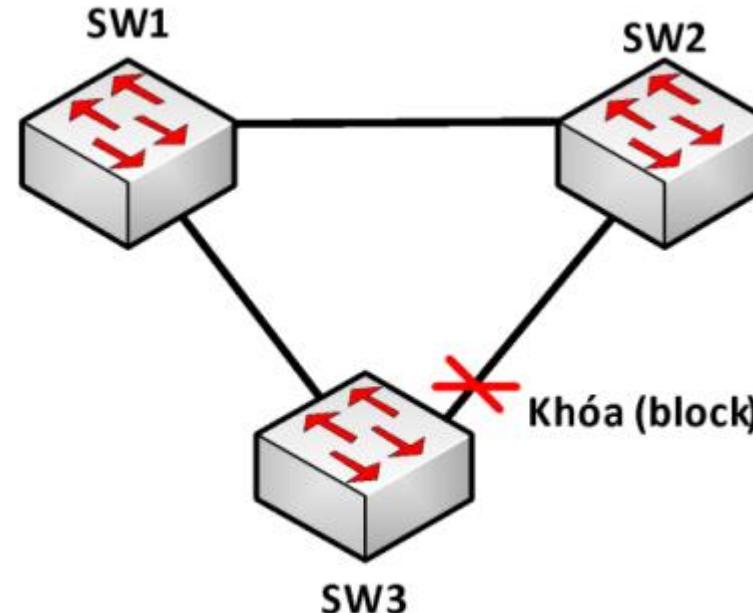
- Định tuyến giữa các VLAN

6

- Giao thức STP

BÀI 6: GIAO THỨC STP

- ❖ Việc thiết kế đường link dự phòng sẽ có 3 vấn đề cần xem xét là: bão quảng bá, nhiều gói tin được nhận giống nhau và bảng địa chỉ MAC trên các Switch không ổn định. Gọi chung là “switching loop”.
- ❖ Giao thức STP được sử dụng để giải quyết vấn đề này bằng cách khóa tạm thời một hoặc một số cổng để tránh tình trạng như trên.



Hoạt động của STP

Hoạt động của STP qua các bước sau:

- ❖ Bầu chọn 1 switch làm “Root switch” còn gọi là “Root bridge”
- ❖ Chọn “Root port” trên các switch còn lại
- ❖ Chọn “Designated port” trên mỗi phân đoạn (segment) mạng
- ❖ Cổng còn lại gọi là “Nondesignated port” sẽ bị khóa

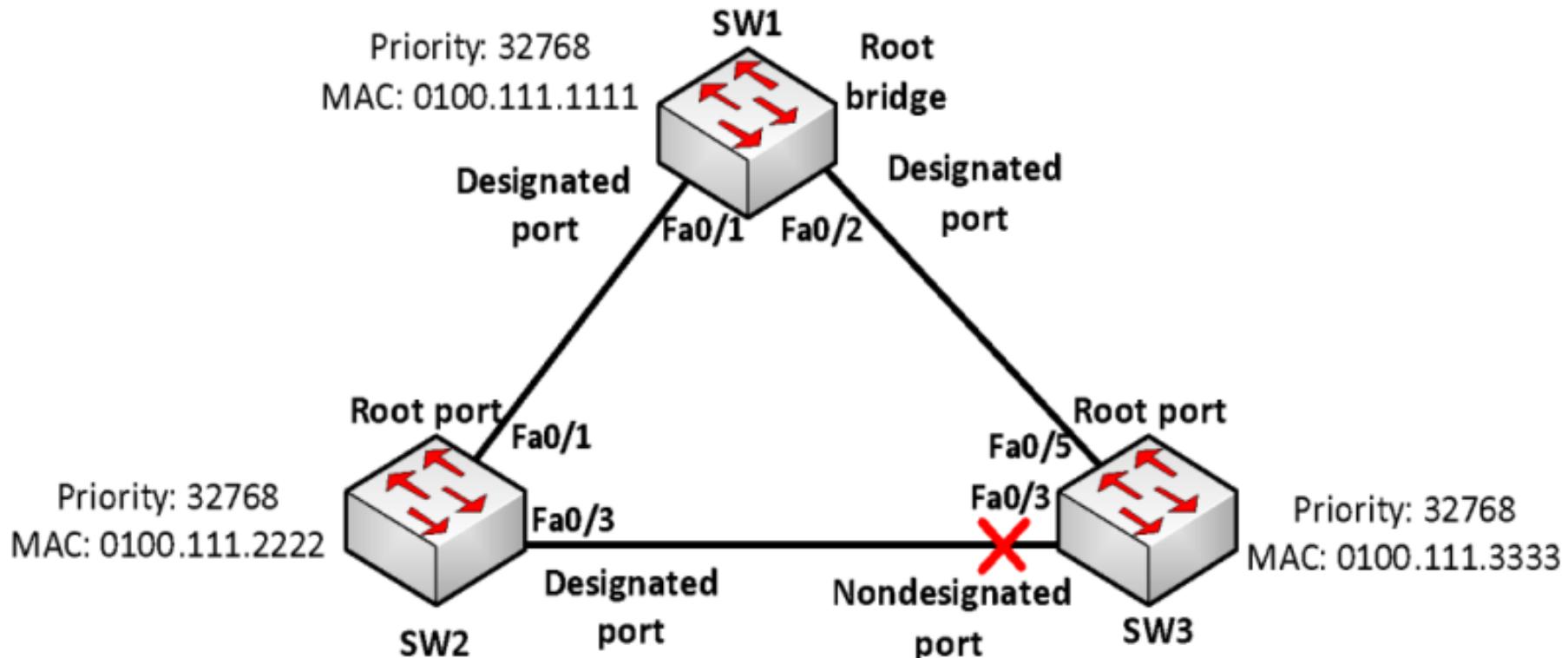
Quá trình bầu chọn “root switch”

- ❖ Mỗi switch có một giá trị “Bridge-ID” gồm 2 trường là “Bridge priority” và “MAC address” và được đặt vào trong BPDU và gửi quảng bá cho các switch khác mỗi 2 giây.
- ❖ Switch được chọn làm “root switch” là switch có giá trị “Bridge-ID” nhỏ nhất. Để so sánh, giá trị “Bridge priority” được dùng để so sánh trước, nếu tất cả các switch đều có giá trị này bằng nhau thì tham số thứ 2 là “MAC address” sẽ được dùng để so sánh.
- ❖ Các loại cổng khác “root port”, “designated port” sẽ lần lượt được bầu chọn dựa vào chi phí nhỏ nhất tính từ nó đến “root switch”.

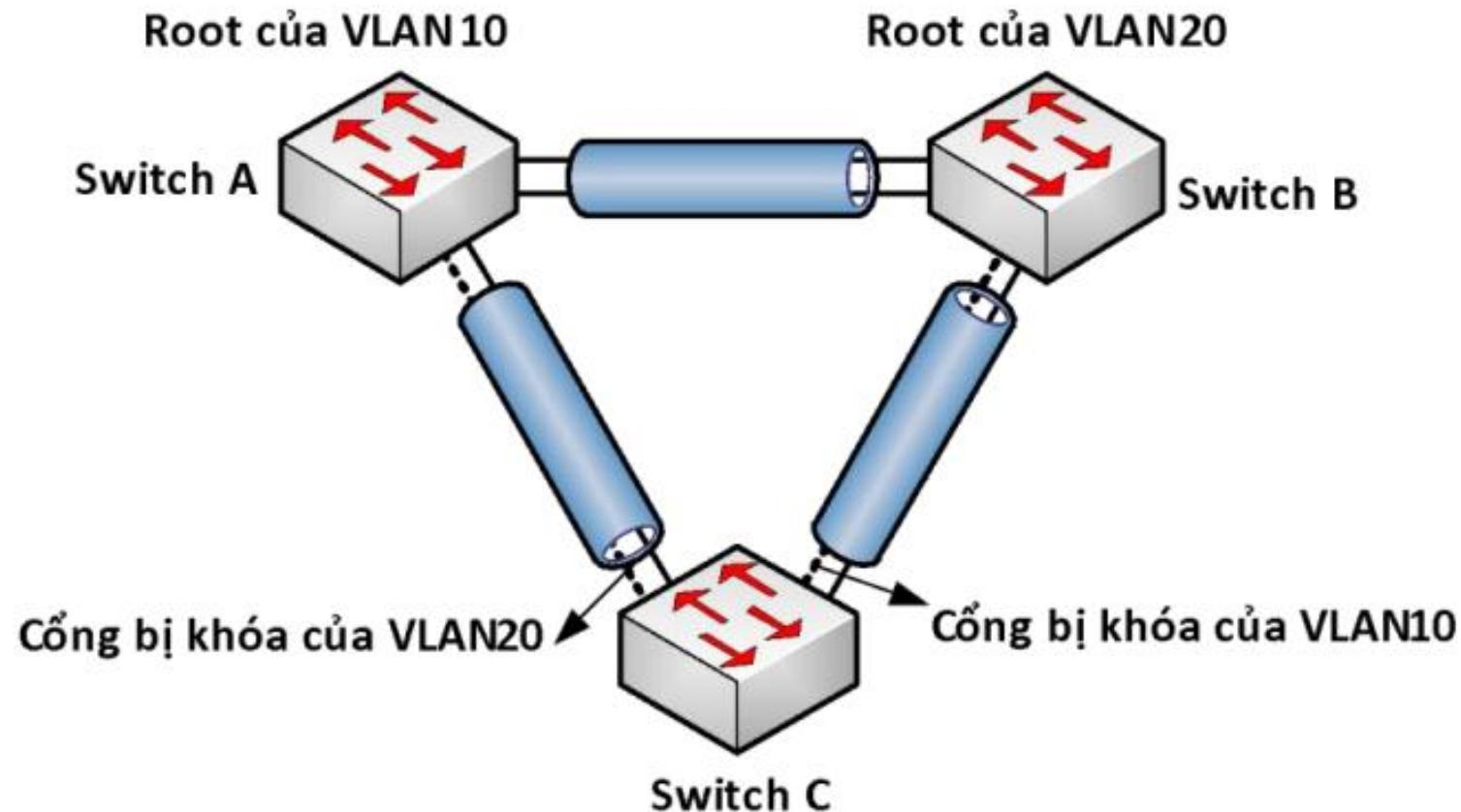
- ❖ Dựa vào bảng sau để tính chi phí cho mỗi chặng.

Tốc độ kết nối	Chi phí (Cost)
10 Gb/s	2
1 Gb/s	4
100 Mb/s	19
10 Mb/s	100

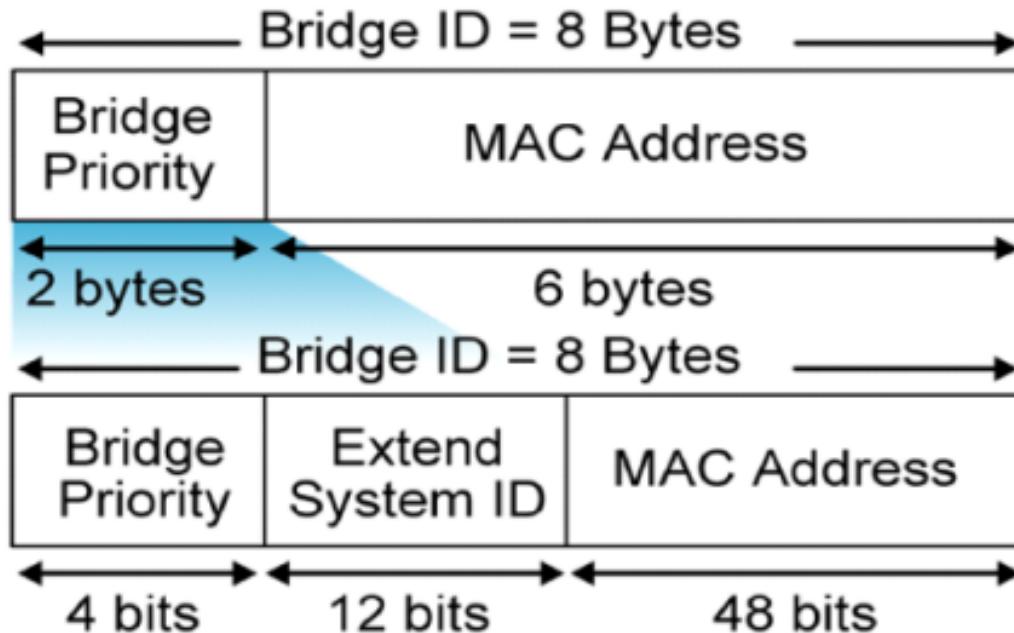
VÍ DỤ



- ❖ Một số dạng STP được cải tiến như: PVSTP+ (Per VLAN Spanning Tree Plus) dùng tạo cho mỗi VLAN một STP riêng.



- ❖ Trong PVSTP+, Bridge-ID có thêm trường System-ID (VLAN-ID) để phân biệt cho từng VLAN.



- ❖ Một số cải tiến khác như RSTP (Rapid Spanning Tree Protocol), MSTP.

- ❖ Một số lệnh cấu hình để điều chỉnh giá trị “Bridge priority” mặc định của switch.
- ❖ Chọn switch làm “root switch” bằng lệnh sau:
`Switch(config)#spanning-tree vlan <vlan-id> root primary`
- ❖ Hoặc
`Switch(config)#spanning-tree vlan <vlan-id> priority <priority>`



TRƯỜNG ĐẠI HỌC THỦY LỢI

KHOA CÔNG NGHỆ THÔNG TIN
Bộ môn: Kỹ thuật máy tính và mạng

QUẢN TRỊ MẠNG

Giảng viên: Trần Văn Hội

Email: hoitv@tlu.edu.vn

Điện thoại: 0944.736.007

NỘI DUNG MÔN HỌC



Chương 1: Tổng quan về mạng



Chương 2: Các kỹ thuật định tuyến



Chương 3: Chuyển mạch trong mạng LAN



Chương 4: Công nghệ mạng WAN



Chương 5: Bảo mật mạng

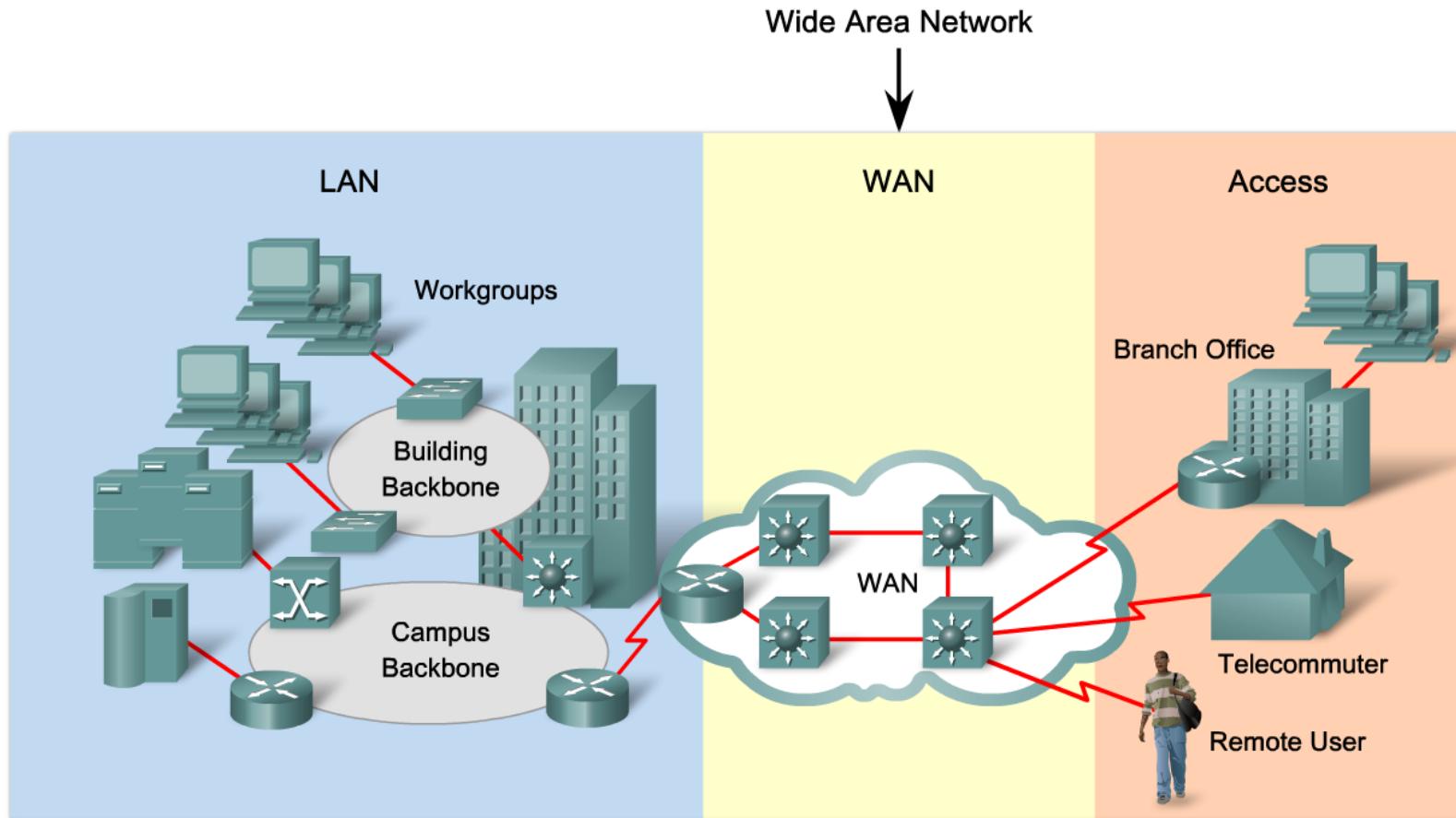
CHƯƠNG 4: CÔNG NGHỆ MẠNG WAN

- 1. Công nghệ mạng WAN
- 2. Leased-line điểm nối điểm
- 3. Giao thức PPPoE
- 4. Mạng VPN

BÀI 1. CÔNG NGHỆ MẠNG WAN

Mạng WAN (Wide Area Network) – Mạng diện rộng

What is a WAN?



MẠNG WAN (WIDE AREA NETWORK)

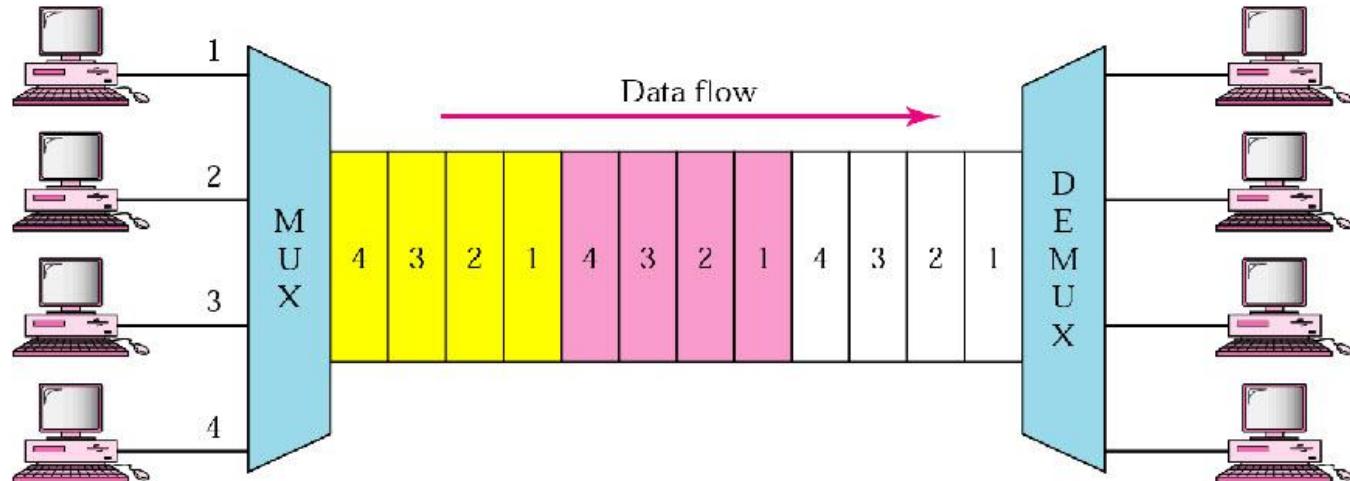
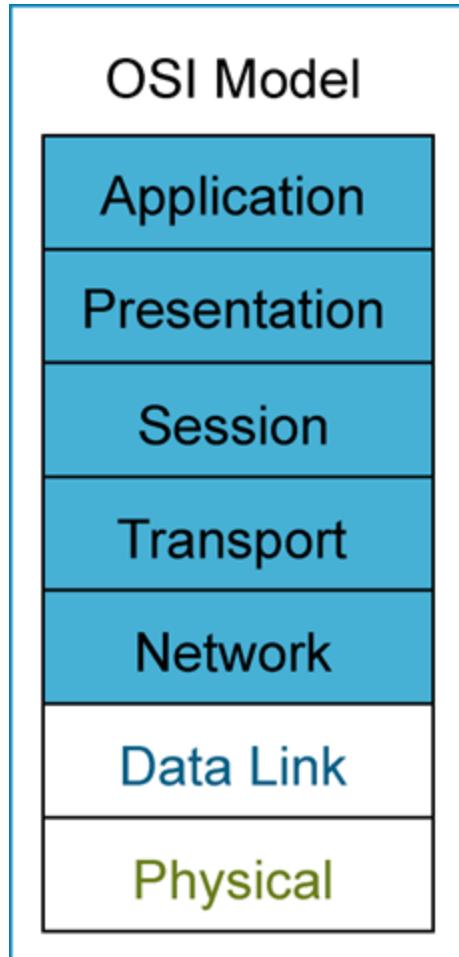
- ❖ Mạng WAN là mạng điện rộng kết nối các máy tính trong phạm vi giữa các tòa nhà, các thành phố hay một quốc gia, một vùng lãnh thổ hoặc giữa các vùng lãnh thổ trong một châu lục bằng đường viễn thông hoặc tín hiệu vệ tinh.
- ❖ WAN sử dụng các kỹ thuật chuyển mạch Frame Relay, ATM, MPLS hỗ trợ các dịch vụ để truy cập băng thông vượt qua vùng địa lý rộng lớn.

SO SÁNH CÔNG NGHỆ MẠNG LAN VÀ WAN

So sánh	WANs	LANs
Mô hình vật lý	Khu vực có vị trí địa lý rộng	Trong tòa nhà, trong công ty
Quyền hạn sử dụng	Phải đi thuê đường truyền của nhà cung cấp dịch vụ để đấu nối các hệ thống mạng lại với nhau	Sở hữu riêng trong công ty

DỊCH VỤ SỬ DỤNG TRONG WAN

- ❖ Dịch vụ của WAN nó nằm từ tầng Network trở lên



MPLS VPN

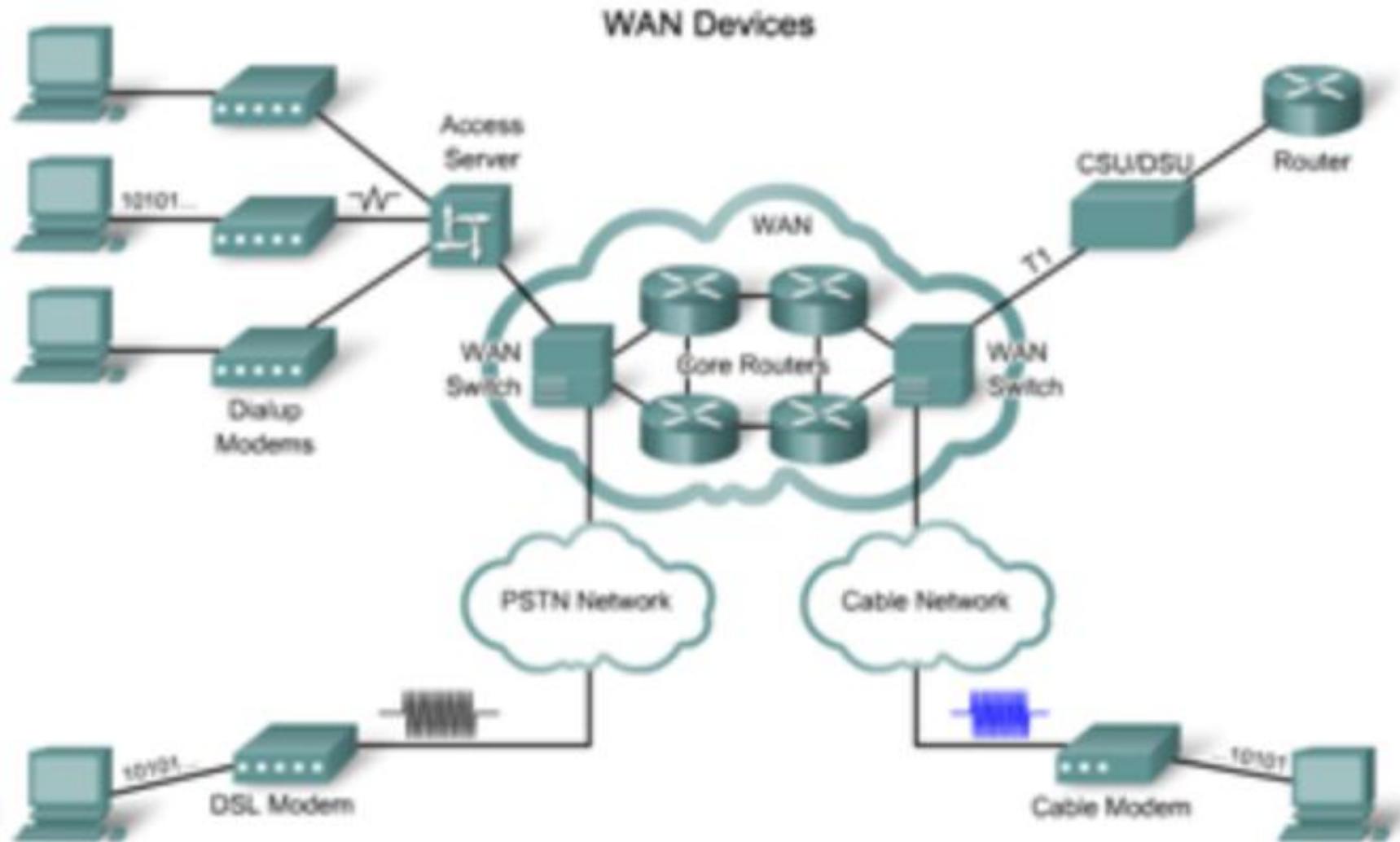
Frame Relay & ATM, HDLC & PPP, AToM & VPLS

TDM, E1, E3, SONET, SDH

HỆ THỐNG TRUY NHẬP MẠNG WAN

- ❖ Layer 1: là nó đến thiết bị vật lý, đường truyền tín hiệu, các kiểu kết nối WAN gồm đường thuê riêng (leased line), chuyển mạch kênh (circuit switched), chuyển mạch gói (packet-switched).
- ❖ Layer 2: Data link nói đến các giao thức đóng gói WAN như: HDLC, PPP, ATM, Frame Relay, Metro Ethernet, AToM
- ❖ Layer 3: Các giao thức MPLS VPN, IP Sec VPN, GRE VPN, DMVPN

THIẾT BỊ SỬ DỤNG TRONG MẠNG WAN



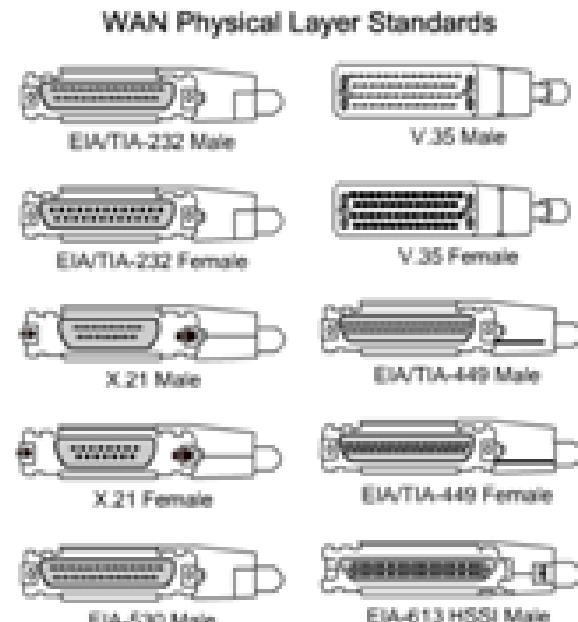
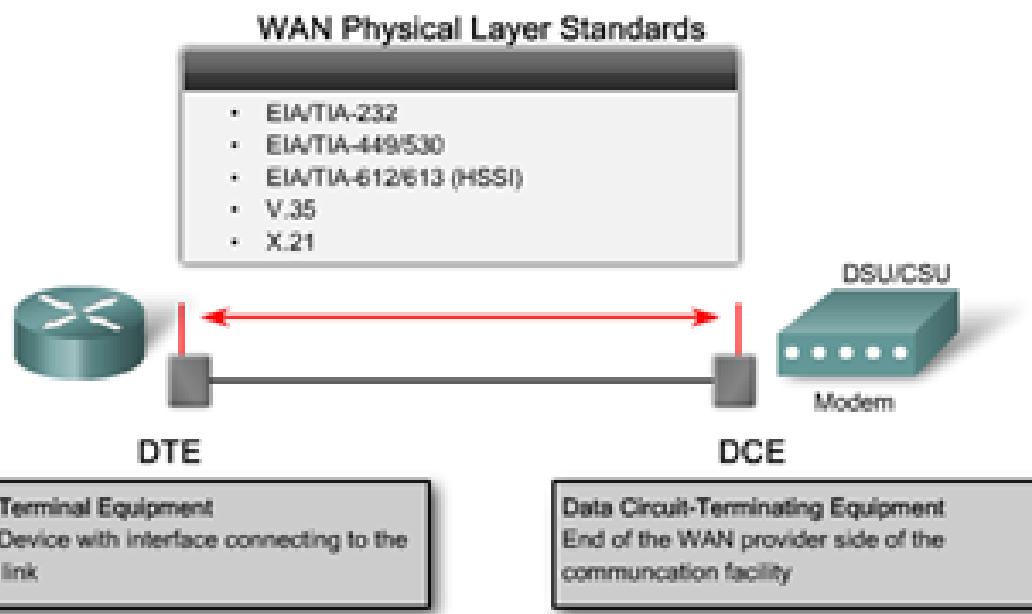
THIẾT BỊ SỬ DỤNG TRONG MẠNG WAN

- ❖ **Router:** có cổng đầu nối WAN như cổng Serial, hay cổng nghệ đường truyền quang FTTH sử dụng cổng fastethernet'
- ❖ **Terminal Server:** cho phép truy nhập vào để cấu hình nhiều Router ở đầu xa cùng lúc
- ❖ **Modem:** Là các bộ điều chế tín hiệu dùng cho các đường ADSL
- ❖ **DSU/CSU:** (Data Service Unit và Channel Service Unit) dùng chuyển đổi định dạng vật lý từ đường truyền này sang đường kia

THIẾT BỊ SỬ DỤNG TRONG MẠNG WAN

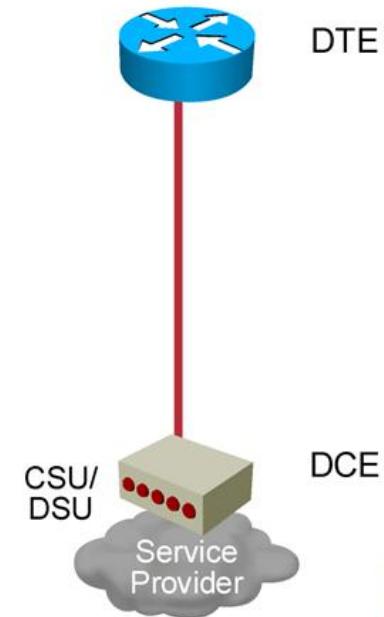
- ❖ Trong WAN có sử dụng thêm những con Switch, Router Core:
 - ATM Switch (Asynchronous Transfer Mode), Chuyển mạch truyền dẫn không đồng bộ ATM.
 - Frame Relay Switch: Là những thiết bị chuyển mạch khung Frame Relay.
 - MPLS: Multi-Protocol Label Switching là thiết bị chuyển mạch nhãn đa giao thức.

TẦNG VẬT LÝ MẠNG WAN

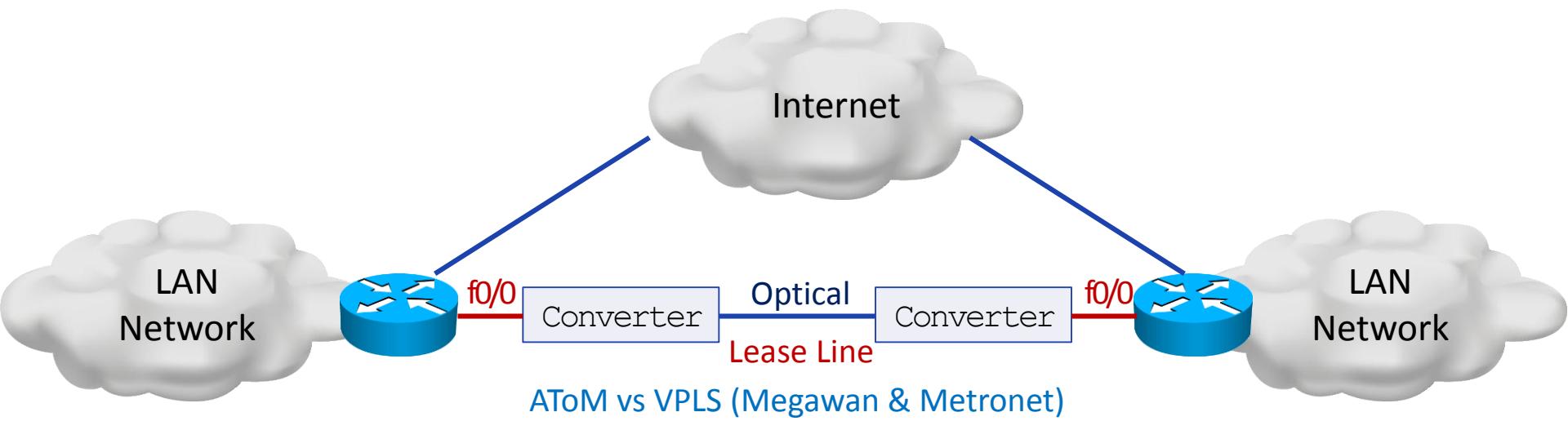


TẦNG VẬT LÝ MẠNG WAN

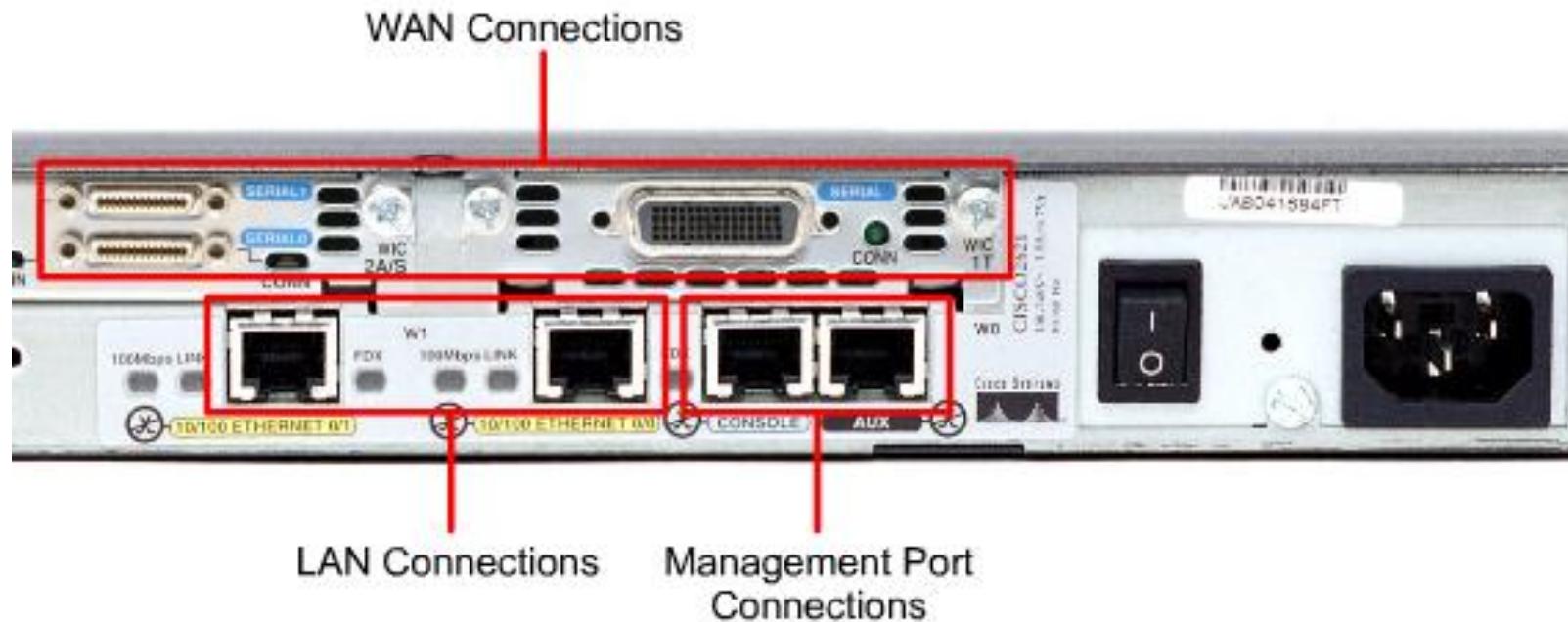
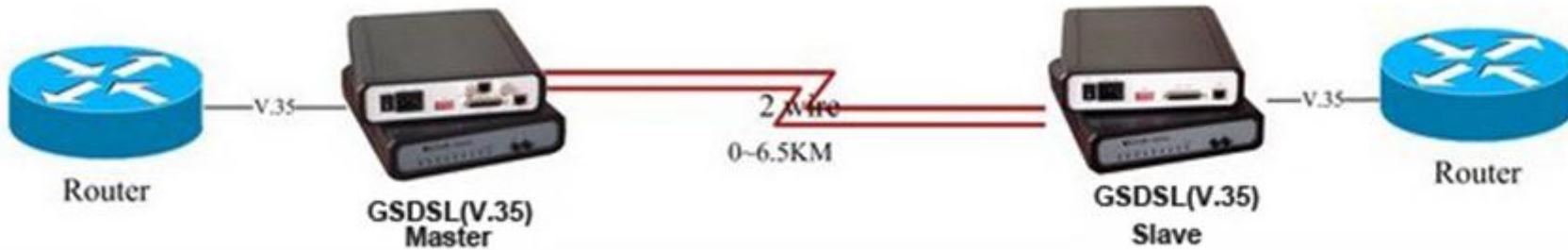
- ❖ DSU/CSU là khối thiết bị do nhà cung cấp dịch vụ lắp đặt.
- ❖ Kết nối Router của khách hàng với nhà cung cấp dịch vụ có thể dùng cáp V35 hoặc RJ45.
- ❖ DTE (Data Terminal Equipment) là phía người sử dụng.
- ❖ DCE (Data Circuit Terminating Equipment) là phía cuối của nhà cung cấp dịch vụ.
- ❖ Cổng cáp WIC-1T:
 - Các đầu nối về Router đều là Serial.
 - Đầu nối về nhà cung cấp dịch vụ hay sử dụng là đầu nối V.35 (tùy vào nhà cung cấp).



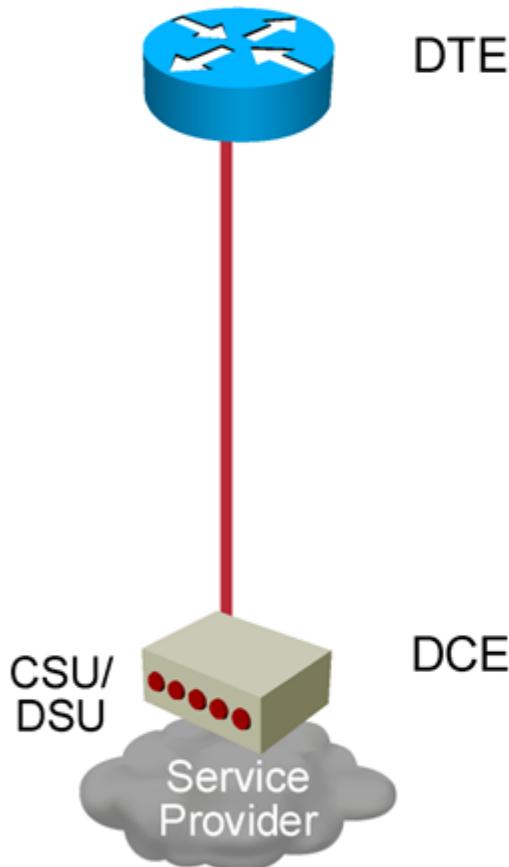
TẦNG VẬT LÝ MẠNG WAN



TẦNG VẬT LÝ MẠNG WAN



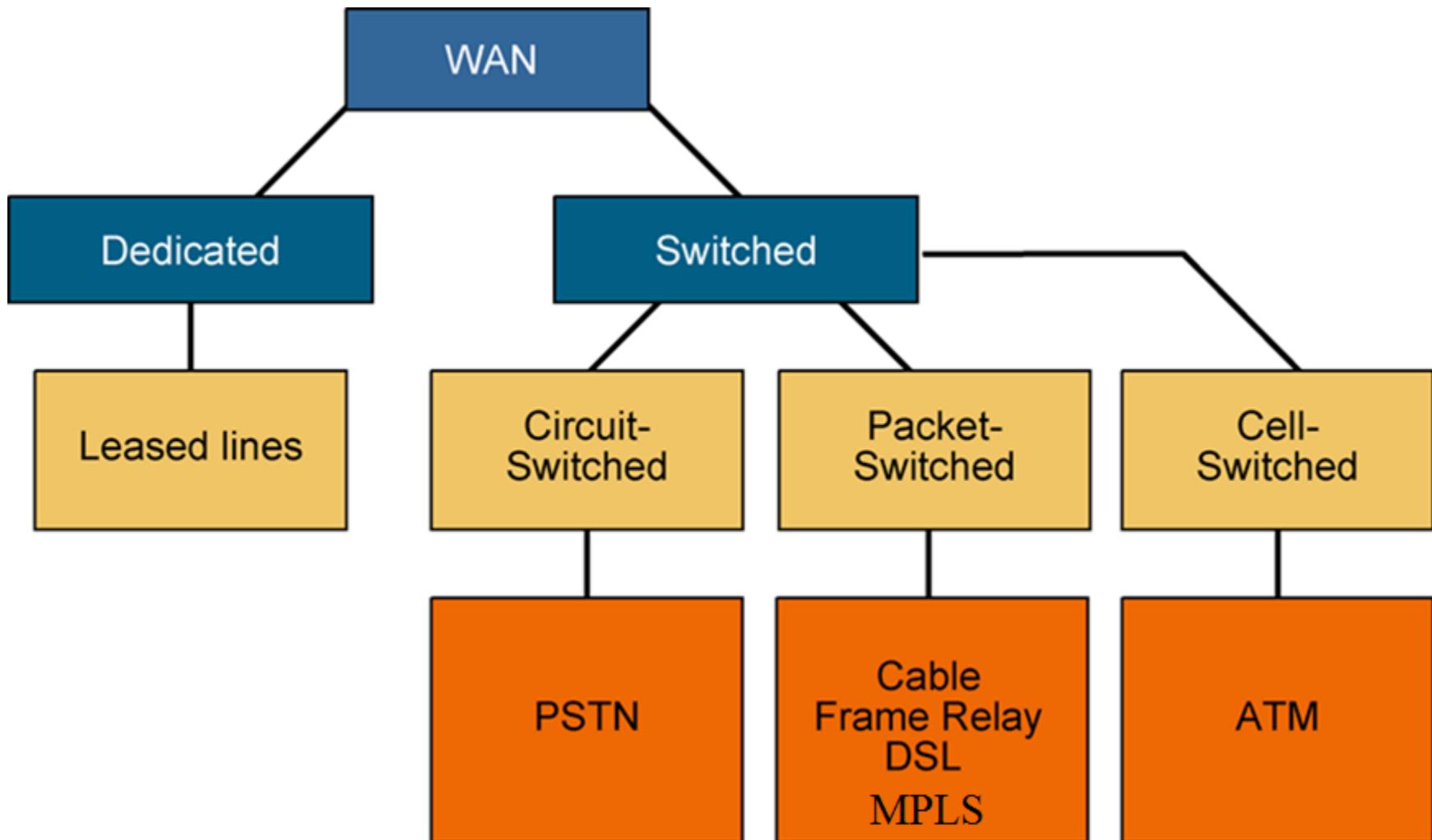
TẦNG VẬT LÝ MẠNG WAN



GIAO THỨC DATA LINK CHẠY TRÊN MẠNG WAN

- ❖ HDLC hay sử dụng dạng kết nối kênh trăng điểm tới điểm (Leased lines)
- ❖ PPP hay sử dụng dạng kết nối kênh trăng (Leased lines)
- ❖ PPPoE Giao thức PPP over Ethernet
- ❖ Frame Relay
- ❖ ATM: Asynchronous Transfer Mode
- ❖ AToM: Anny Transport over MPLS

LỰA CHỌN KẾT NỐI WAN



CHƯƠNG 4: CÔNG NGHỆ MẠNG WAN

- 1. Công nghệ mạng WAN
- 2. Leased-line điểm nối điểm
- 3. Giao thức PPPoE
- 4. Mạng VPN

BÀI 2. LEASED-LINE ĐIỂM NỐI ĐIỂM

- ❖ Giao thức liên kết dữ liệu sử dụng trong mạng WAN:
 - Kết nối Serial Point-to-Point được dùng phổ biến là HDLC (High-level Data Link Control) và PPP (Point to Point Protocol).
 - Giao thức PPPoE (Point-to-Point Protocol over Ethernet) dựa trên giao thức PPP.

HDLC

Flag	Address	Control	Data	FCS	Flag
------	---------	---------	------	-----	------

PPP

Flag	Address	Control	Protocol	Data	FCS	Flag
------	---------	---------	----------	------	-----	------

GIAO THÚC PPP

- ❖ PPP có thể được sử dụng trên cáp xoắn (twisted pair), đường cáp quang (fiber-optic lines) và truyền dẫn vệ tinh (satellite transmission).
- ❖ PPP cung cấp vận chuyển qua ATM, Frame Relay, ISDN và các liên kết quang.
- ❖ Để bảo mật, PPP cho phép bạn xác thực hoặc bảo mật các kết nối bằng Giao thức xác thực mật khẩu (Password Authentication Protocol - PAP) hoặc giao thức xác thực bắt tay thử thách (Challenge Handshake Authentication Protocol - CHAP) hiệu quả hơn.

QUÁ TRÌNH THIẾT LẬP KẾT NỐI PPP

- ❖ Pha đầu tiên là thiết lập đường Link giữa 2 Router
- ❖ Pha thứ 2 là xác thực lẫn nhau giữa 2 Router này thông qua giao thức xác thực PAP, CHAP.
- ❖ Pha thứ 3 là triển khai giao thức PPP sau khi thiết lập

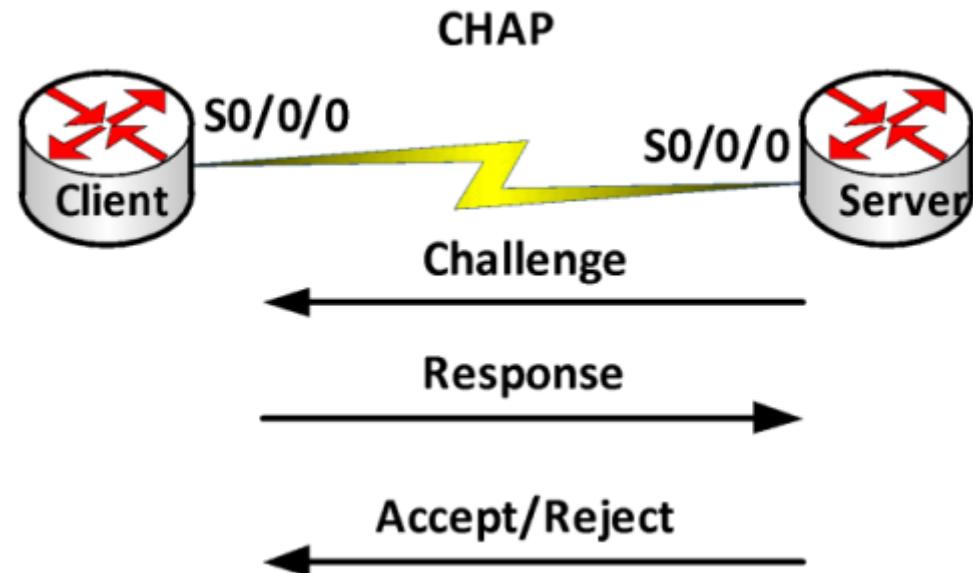
CHỨNG THỰC PPP BẰNG PAP

- ❖ PAP sử dụng cơ chế bắt tay 2 bước.
- Bước 1: Client sẽ gửi username và password cho Server để xác thực.
- Bước 2: Server sẽ tiến hành kiểm tra, nếu thành công thì sẽ thiết lập kết nối; ngược lại sẽ không thiết lập kết nối với Client.
- ❖ Password được gửi dưới dạng không được mã hóa (clear – text) và username/password được gửi đi kiểm tra một lần khi thiết lập kết nối.



CHỨNG THỰC PPP BẰNG CHAP

- ❖ Sử dụng bắt tay 3 bước:
- ❖ Bước 1: Router A bên server gửi sang Router kia một mẫu tin Challenge
- ❖ Bước 2: Router B bên client sử dụng hàm băm để băm mẫu tin và User name, Password của mình rồi gửi lại thông tin là Response
- ❖ Bước 3: Router server kiểm tra thông tin. Nếu thấy phù hợp nó sẽ gửi đáp trả là xác nhận.
- ❖ Gói tin Response gửi sang đã được băm ra nên nó bảo mật được User name, Password.



CẤU HÌNH PPP

Cấu hình PPP trên Client

Bước 1: Router(config)#**interface <interface>**

Bước 2: Enable PPP

➤ Router(config-if)#**encapsulation ppp**

Bước 3: PAP phải được enable trên interface bằng lệnh

Router(config-if)#**ppp pap sent-username <username> password <password>**

CẤU HÌNH PPP

Cấu hình chứng thực PPP PAP trên Server

❖ Bước 1: Tạo username và password trên Server

➤ Router(config)#**username <username> password <password>**

❖ Bước 2: Enable PPP

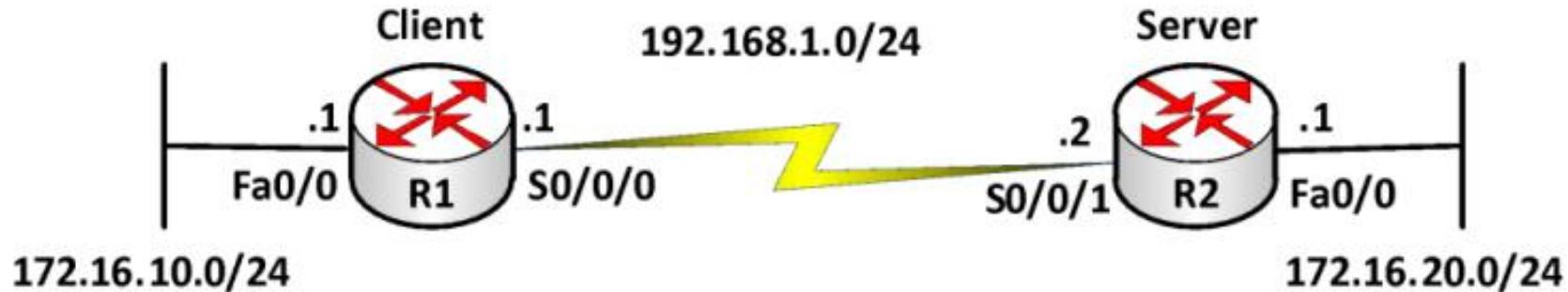
➤ Router(config-if)#**encapsulation ppp**

❖ Bước 3: Cấu hình xác thực

➤ Router(config-if)#**ppp authentication {pap|chap|pap-chap|chappap}**

VÍ DỤ

- ❖ Cấu hình PPP chứng thực bằng PAP



- ❖ Router R2 sẽ chứng thực cho router R1 bằng giao thức PAP
- ❖ Cấu hình định tuyến: tùy chọn giao thức

BÀI GIẢI

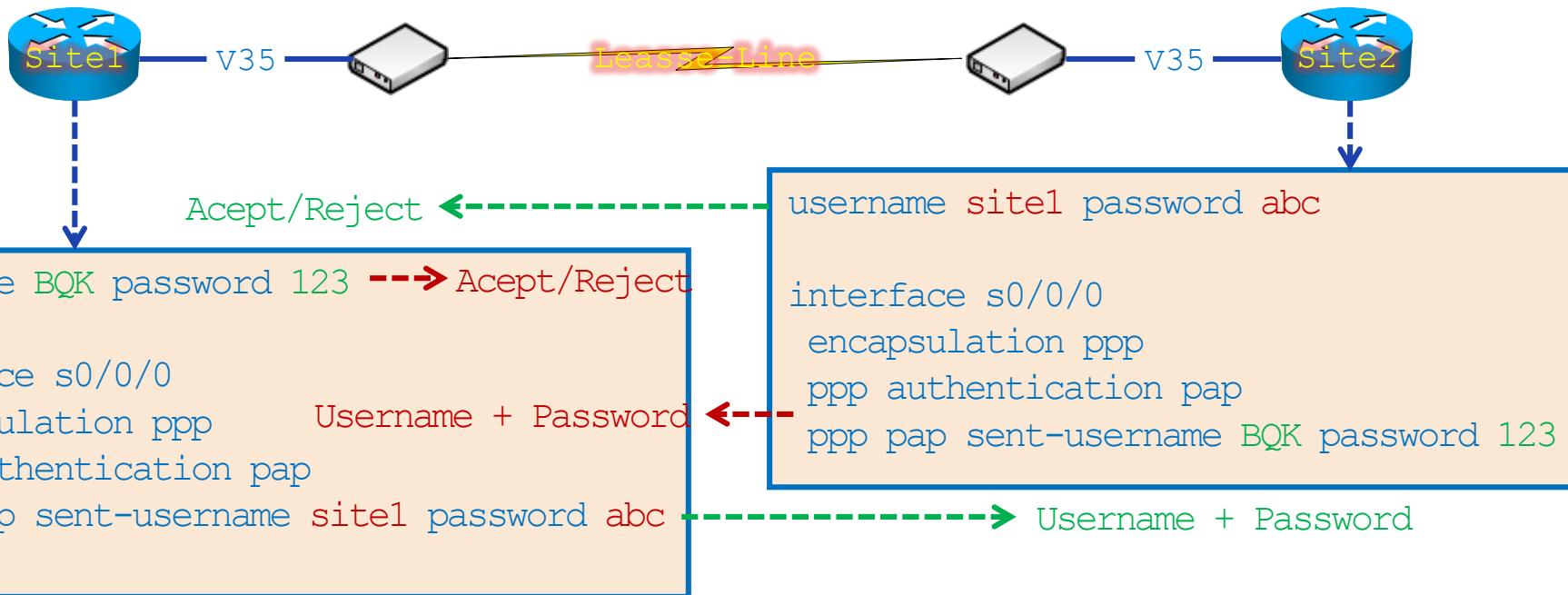
❖ Cấu hình trên R1

- R1(config)#int S0/0/0
- R1(config-if)#encapsulation ppp
- R1(config-if)#ppp pap sent-username cisco password cisco

❖ Cấu hình trên server R2

- R2(config)#username cisco password cisco
- R2(config)#int S0/0/1
- R2(config-if)#encapsulation ppp
- R2(config-if)#ppp authentication pap

PPP: PAP (Password Authentication Protocol)

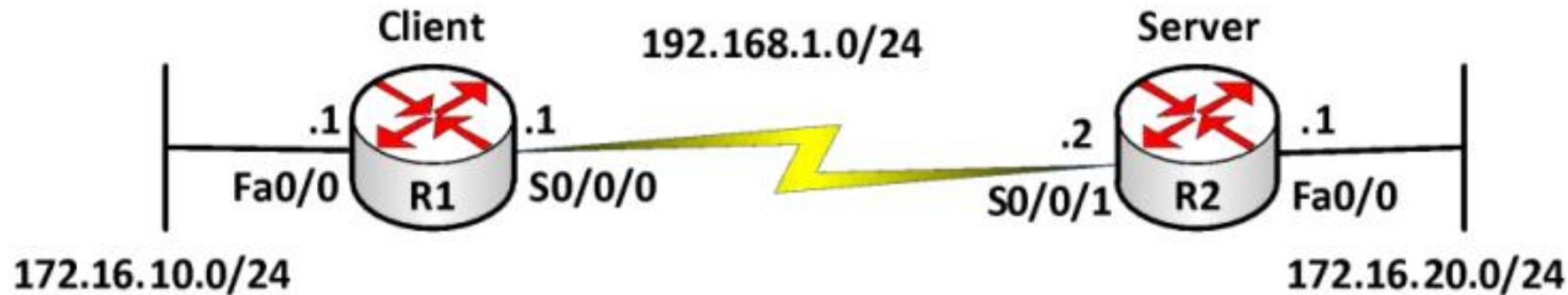


KIỂM TRA CẤU HÌNH

- ❖ Sử dụng các lệnh sau
 - Router#show interfaces serial
 - Router#ping
 - Router#debug ppp authentication

CẤU HÌNH CHỨNG THỰC PPP CHAP

- ❖ Trường hợp 1: Các router dùng hostname để chứng thực.

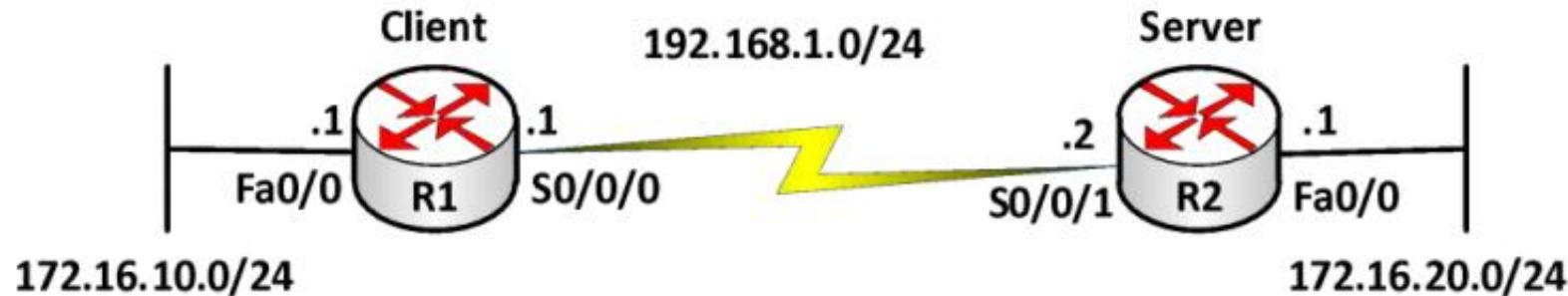


CẤU HÌNH CHỨNG THỰC CHAP

- ❖ R1(config)#username R2 password cisco
- ❖ R1(config)#int S0/0/0
- ❖ R1(config-if)#encapsulation ppp
- ❖ R2(config)#username R1 password cisco
- ❖ R2(config)#interface serial 0/0/1
- ❖ R2(config-if)#encapsulation ppp
- ❖ R2(config-if)#ppp authentication chap

CẤU HÌNH CHỨNG THỰC PPP CHAP

- ❖ Trường hợp 2: Các router gửi username và password bất kỳ.



CẤU HÌNH CHỨNG THỰC CHẠP

- ❖ R1(config)#int S0/0/0
- ❖ R1(config-if)#encapsulation ppp
- ❖ R1(config-if)#ppp chap hostname abc
- ❖ R1(config-if)#ppp chap password cisco
- ❖ R2(config)#username abc password cisco
- ❖ R2(config)#int S0/0/1
- ❖ R2(config-if)#encapsulation ppp
- ❖ R2(config-if)#ppp authentication chap

CHƯƠNG 4: CÔNG NGHỆ MẠNG WAN

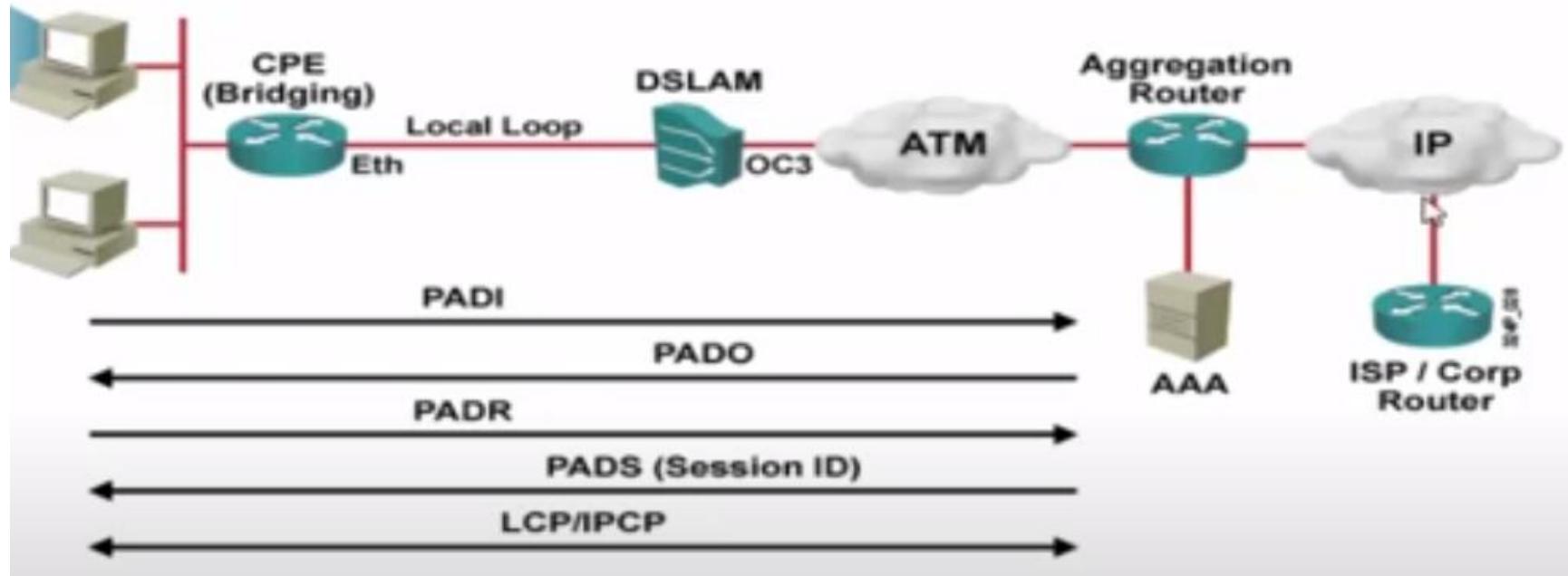
- 1. Công nghệ mạng WAN
- 2. Leased-line điểm nối điểm
- 3. Giao thức PPPoE
- 4. Mạng VPN

BÀI 3. GIAO THÚC PPPoE

- ❖ PPPoE (Point-to-Point Protocol over Ethernet) là giao thức Point-to-Point trên Ethernet, cho phép nhiều người dùng có thể sử dụng đường truyền.
- ❖ PPPoE được sử dụng chủ yếu với các dịch vụ DSL nơi người dùng cá nhân kết nối với modem DSL qua Ethernet với được hình thành bởi sự đóng gói dữ liệu của gói tin PPP trong gói tin Ethernet

GIAO THÚC PPPoE

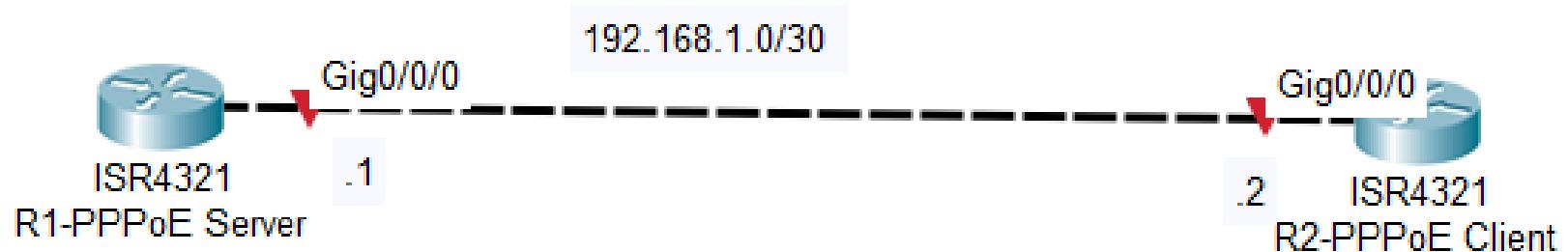
❖ Quá trình thiết lập phiên PPPoE



- ❖ PADI - PPPoE Active Discovery Initiation
- ❖ PADO - PPPoE Active Discovery Offer
- ❖ PADR – PPPoE Active DiscoveryRequest
- ❖ PADS – PPPoE Active Discovery Session Conformation

VÍ DỤ

❖ Cấu hình PPPoE Server



- R1(config)#bba-group pppoe example
- R1(config-bba-group)#virtual-template 1
- R1(config-bba-group)#exit

Cấu hình PPPoE Server

- R1(config)#interface virtual-template 1
- R1(config-if)#encapsulation ppp
- R1(config-if)#ip address 192.168.1.1 255.255.255.252
- R1(config-if)#ppp authentication chap
- R1(config-if)#exit
- R1(config)#username R2 password cisco
- R1(config)#interface gig0/0/0
- R1(config-if)#no shutdown
- R1(config-if)#pppoe enable group example
- R1(config-if)#exit

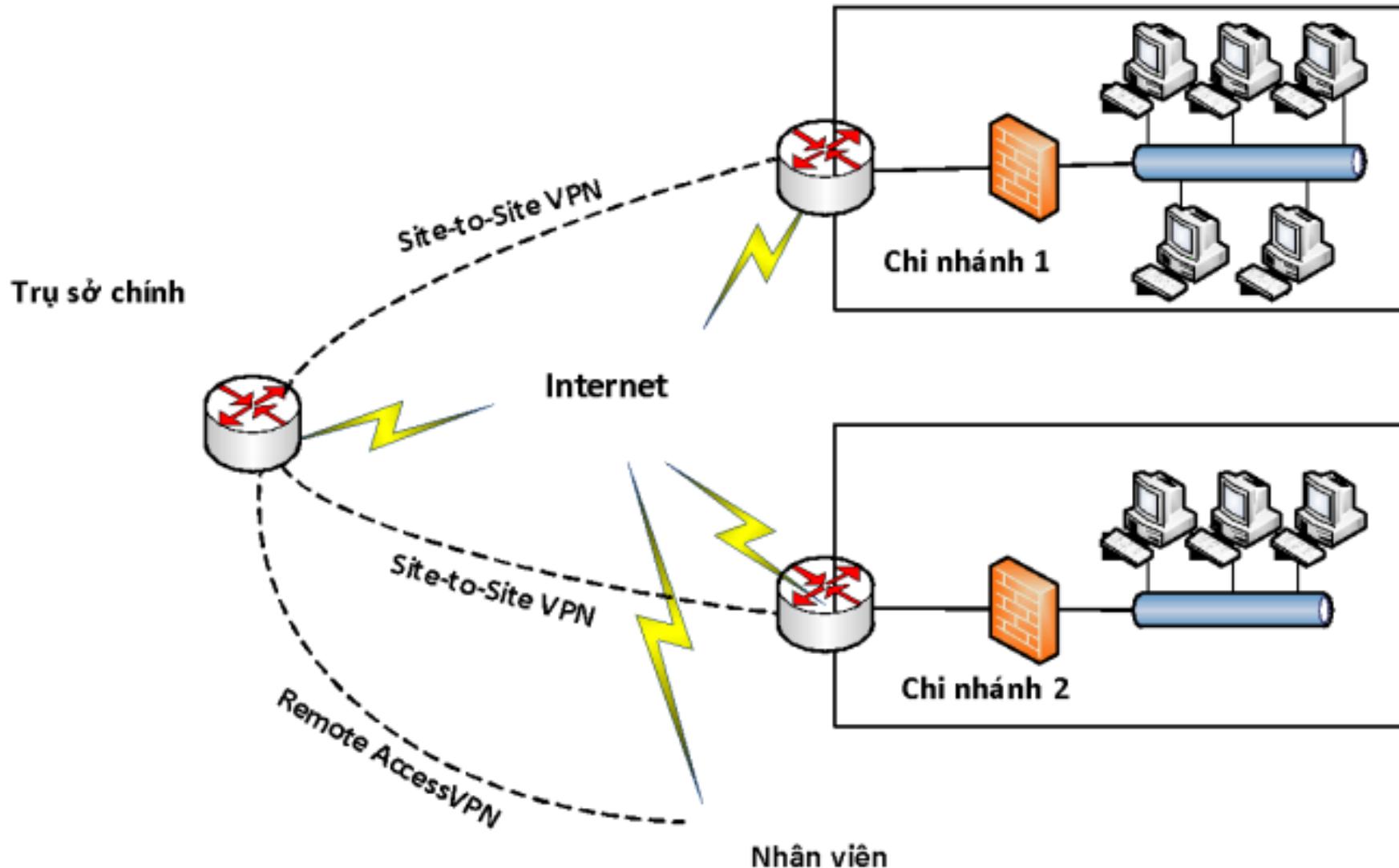
Cấu hình PPPoE Client

- ❖ R2(config)#interface gig0/0/0
- ❖ R2(config-if)#no shutdown
- ❖ R2(config-if)#pppoe-client dial-pool-number 1
- ❖ R2(config-if)#exit
- ❖ R2(config)#interface dialer 0
- ❖ R2(config-if)#dialer pool 1
- ❖ R2(config-if)#encapsulation ppp
- ❖ R2(config-if)#ip address 192.168.1.2 255.255.255.252
- ❖ R2(config-if)#exit
- ❖ R2(config)# username R1 password cisco

CHƯƠNG 4: CÔNG NGHỆ MẠNG WAN

- 1. Công nghệ mạng WAN
- 2. Leased-line điểm nối điểm
- 3. Giao thức PPPoE
- 4. Mạng VPN

BÀI 4. MẠNG VPN – VIRTUAL PRIVATE NETWORK



MẠNG VPN

- ❖ VPN là sự mở rộng của một mạng riêng (private network) thông qua mạng công cộng (internet), được dùng để kết nối các văn phòng chi nhánh, người từ xa kết nối về văn phòng chính.
- ❖ VPN có thể được tạo ra bằng cách sử dụng phần cứng, phần mềm hay kết hợp cả hai để tạo ra một kết nối ảo bảo mật giữa hai mạng riêng thông qua mạng công cộng.
- ❖ Lợi ích của công nghệ VPN là đáp ứng nhu cầu trao đổi thông tin, truy cập từ xa và tiết kiệm chi phí.

CÁC MODE KẾT NỐI VPN

- ❖ Transport mode: Một kết nối ở mode transport được sử dụng địa chỉ IP nguồn và đích thật sự của các thiết bị trong các gói tin để truyền dữ liệu. Hạn chế của transport mode là không có khả năng mở rộng
- ❖ Tunnel mode: Các thiết bị nguồn-đích thực thông thường sẽ không bảo vệ dữ liệu, thay vào đó các thiết bị trung gian được sử dụng để bảo vệ luồng dữ liệu. Các thiết bị này được gọi là các VPN gateway.

ƯU ĐIỂM CỦA TUNNEL MODE

- ❖ Tính mở rộng: ta có thể chọn một thiết bị phù hợp để thực hiện việc xử lý bảo vệ.
- ❖ Tính linh động: không cần phải thay đổi gì trong cấu hình VPN khi thêm vào một thiết bị mới sau VPN Gateway.
- ❖ Tính ẩn của các giao tiếp: các lưu lượng được các VPN Gateway đại diện trao đổi với nhau, vì vậy sẽ che dấu nguồn và đích thật sự của kết nối.
- ❖ Sử dụng địa chỉ cục bộ: các thiết bị đích và nguồn thực có thể sử dụng địa chỉ được đăng ký (public) hay cục bộ bởi vì các gói tin được đóng gói bởi các VPN Gateway.
- ❖ Sử dụng các chính sách bảo mật hiện có: các chính sách bảo mật được thực hiện trên các thiết bị tường lửa và bộ lọc gói tin.

PHÂN LOẠI VPN

❖ Remote Access VPN:

- Sử dụng cho các kết nối có băng thông thấp giữa một thiết bị của người dùng như là PC, Ipad,... và một thiết bị Gateway VPN.
- Người dùng ở xa sử dụng các phần mềm VPN để truy cập vào mạng của công ty thông qua Gateway hoặc VPN concentrator (bản chất là một server), giải pháp này thường được gọi là client/server.
- Trong Remote Access VPN có nhiều kỹ thuật được sử dụng để bảo mật trong việc trao đổi dữ liệu: IPSec, SSL,...

PHÂN LOẠI VPN

- ❖ Site-to-Site VPN (LAN-to-LAN)
 - Là kỹ thuật kết nối các hệ thống mạng (site) của cùng một công ty ở các nơi khác nhau tạo thành một hệ thống mạng thống nhất thông qua môi trường mạng công cộng.
 - Quá trình xác thực ban đầu cho những người dùng cần phải được kiểm soát chặt chẽ bởi các thiết bị ở các site tương ứng. Các thiết bị này hoạt động như Gateway, truyền lưu lượng một cách an toàn cho đầu bên kia.

CÁC GIAO THỨC VPN PHỔ BIẾN

- ❖ **OpenVPN**: Giao thức nguồn mở có tốc độ trung bình nhưng vẫn hỗ trợ mã hóa mạnh mẽ.
- ❖ **L2TP/IPSec** (Layer 2 Tunneling Protocol): Điều này khá phổ biến và cung cấp tốc độ khá nhưng dễ bị chặn bởi một số trang web không có lợi cho người dùng VPN.
- ❖ **SSTP** (Secure Socket Tunneling Protocol): Không phổ biến như vậy và ngoài việc mã hóa tốt không có nhiều để tự giới thiệu.
- ❖ **IKEv2** (Internet Key Exchange): Kết nối rất nhanh và đặc biệt tốt cho các thiết bị di động mặc dù cung cấp các tiêu chuẩn mã hóa yếu hơn.
- ❖ **PPTP**: Rất nhanh nhưng đã bị chọc thủng đầy đủ các lỗ hổng bảo mật qua nhiều năm.

SO SÁNH GIAO THỨC VPN

VPN Protocols	Encryption	Security	Speed
OpenVPN	256-bit	Highest encryption	Fast on high latency connections
L2TP	256-bit	Highest encryption	Slow and highly processor dependant
SSTP	256-bit	Highest encryption	Slow
IKEv2	256-bit	Highest encryption	Fast
PPTP	128-bit	Minimum security	Fast



TRƯỜNG ĐẠI HỌC THỦY LỢI

KHOA CÔNG NGHỆ THÔNG TIN
Bộ môn: Kỹ thuật máy tính và mạng

QUẢN TRỊ MẠNG

Giảng viên: Trần Văn Hội

Email: hoitv@tlu.edu.vn

Điện thoại: 0944.736.007

NỘI DUNG MÔN HỌC



Chương 1: Tổng quan về mạng



Chương 2: Các kỹ thuật định tuyến



Chương 3: Chuyển mạch trong mạng LAN



Chương 4: Công nghệ mạng WAN



Chương 5: Bảo mật mạng

CHƯƠNG 5: BẢO MẬT MẠNG

- 1. Giới thiệu chung
- 2. Điều khiển truy cập ACL
- 3. Xác thực người dùng
- 4. Tường lửa

BÀI 1: GIỚI THIỆU CHUNG

- ❖ Hệ thống mạng là một tập hợp các máy tính gồm thành phần phần cứng, phần mềm và dữ liệu.
- ❖ Tài nguyên thông tin:
 - ✓ Phần cứng.
 - ✓ Phần mềm.
 - ✓ Dữ liệu.
 - ✓ Môi trường truyền thông giữa các máy tính.
 - ✓ Môi trường làm việc.
 - ✓ Con người.

Các mối đe doạ đối với một hệ thống thông tin

❖ Phá hoại: Phá hỏng thiết bị phần cứng hoặc phần mềm trên hệ thống. Sửa đổi tài nguyên của hệ thống trái phép.

❖ Tấn công kiểu do thám (Bắt gói, dò port, ping quét thông tin).

❖ Tấn công kiểu truy xuất

Tìm mật khẩu, lỗ hổng...

❖ Can thiệp: Bị truy cập bởi những người không có thẩm quyền

❖ Từ chối dịch vụ DoS.

❖ Sử dụng Worm, Virus,

Trojan horse.

Types of Network Attacks



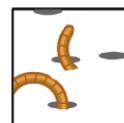
Reconnaissance



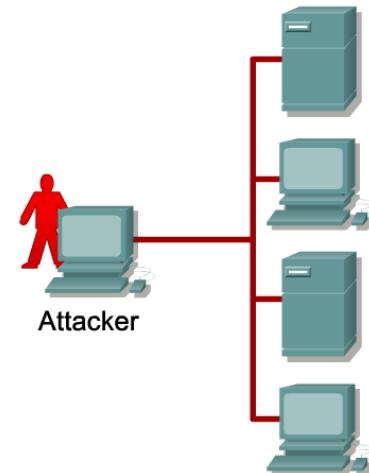
Access



Denial of Services

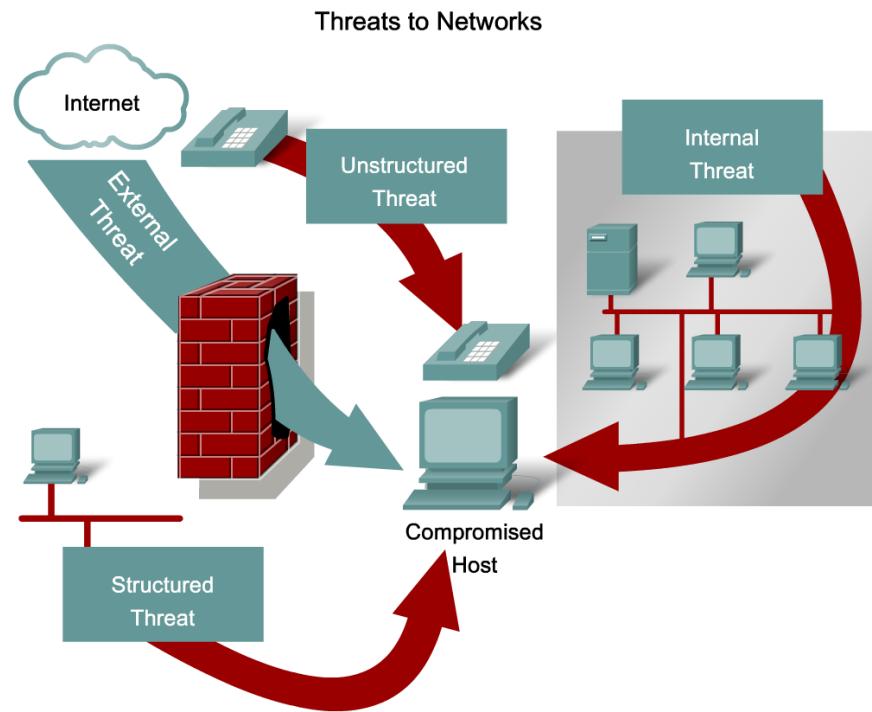


Worms, Viruses, and Trojan Horses



Có ba loại đối tượng chính khai thác

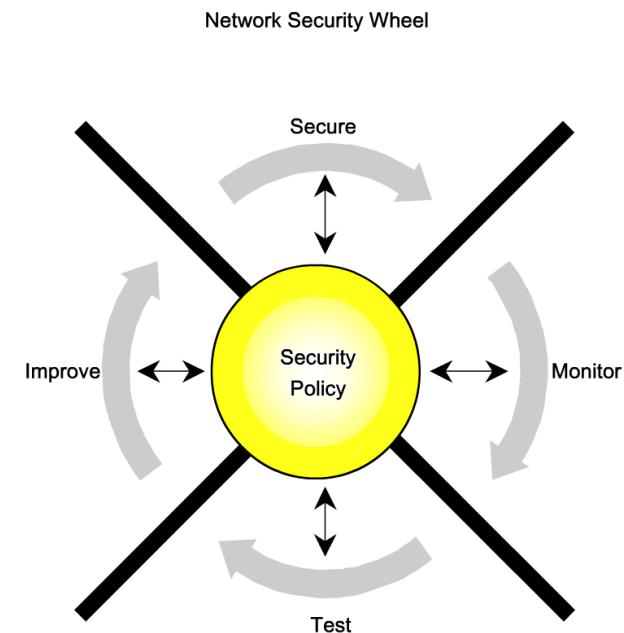
- ❖ Inside: Các đối tượng từ bên trong hệ thống, đây là những người có quyền truy cập hợp pháp đối với hệ thống.
- ❖ Outside: hacker, cracker....
- ❖ Phần mềm: Virut, spyware, mainware và các lỗ hổng phần mềm: SQL injection ...



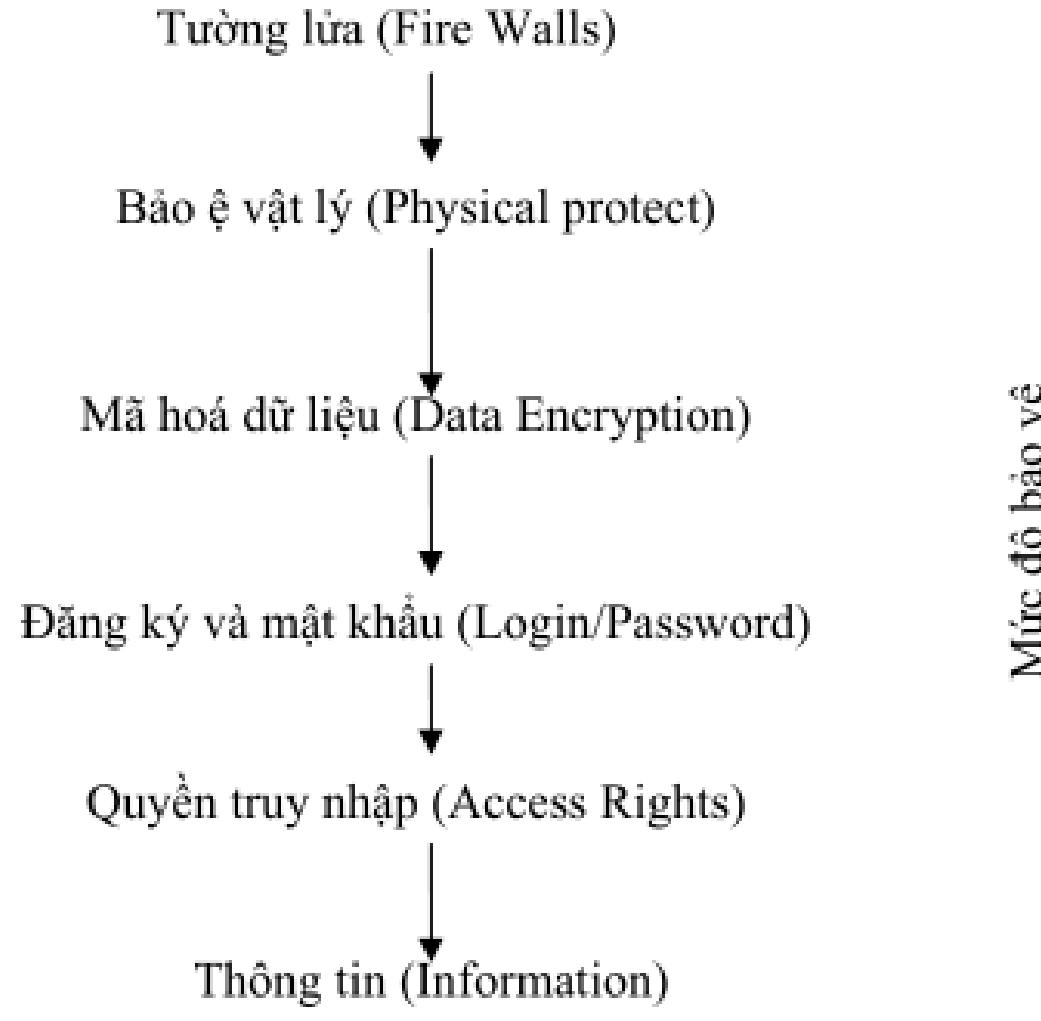
Các biện pháp ngăn chặn

Thường có 3 biện pháp ngăn chặn:

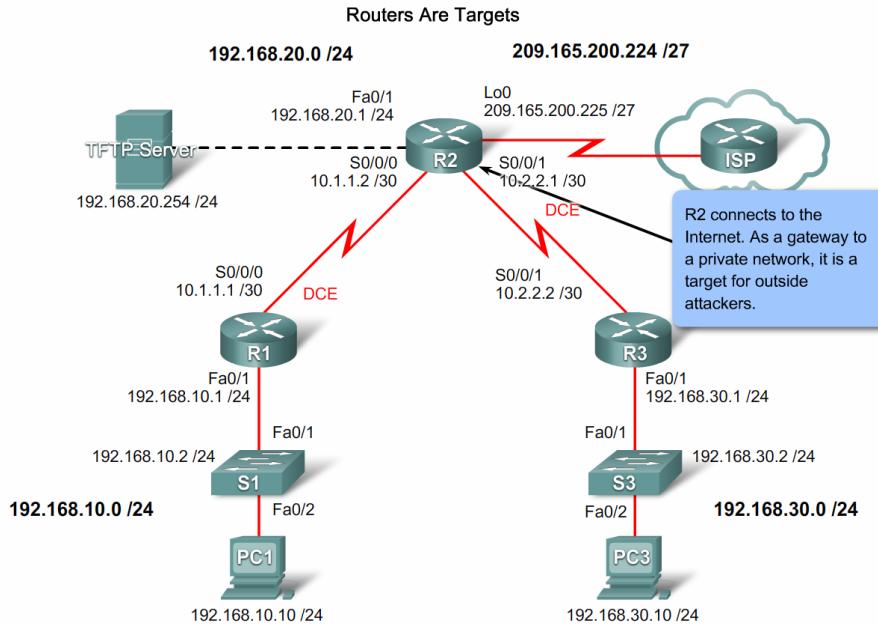
- ❖ Thông qua phần mềm: Sử dụng các thuật toán mật mã học tại các cơ chế an toàn bảo mật của hệ thống mức hệ điều hành.
- ❖ Thông qua phần cứng: Sử dụng các hệ thống đã được cứng hóa.
- ❖ Thông qua các chính sách AT& BM
Thông tin do tổ chức ban hành nhằm đảm bảo an toàn bảo mật của hệ thống.



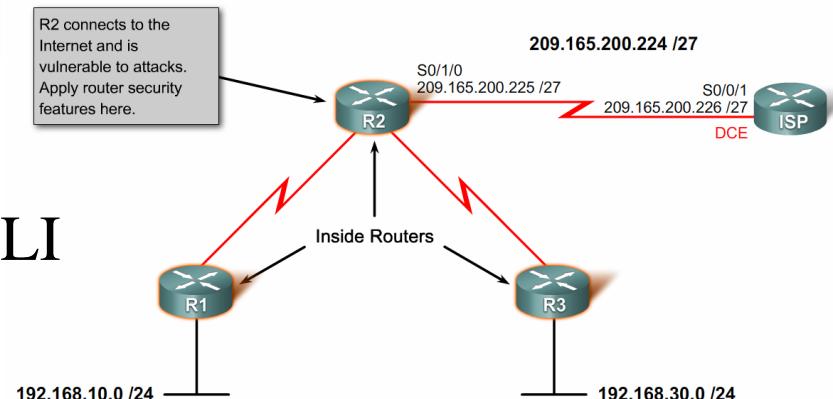
CÁC MỨC BẢO VỆ TRÊN MẠNG



BẢO MẬT ROUTER



Securing Your Network



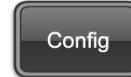
1. Sử dụng giao diện dòng lệnh CLI
2. Sử dụng phần mềm SDM
(Security Device Manager)

BẢO MẬT ROUTER

- ❖ Bảo mật quyền truy nhập vào router, switch:
- ❖ Mật khẩu quy định của Cisco:
 - Có thể có độ dài từ 1- 25 ký tự (Nên từ 10 ký tự).
 - Có ký tự, số kết hợp ký tự viết hoa.

ĐẶT PASSWORD CÔNG CONSOLE

Press RETURN to get started.



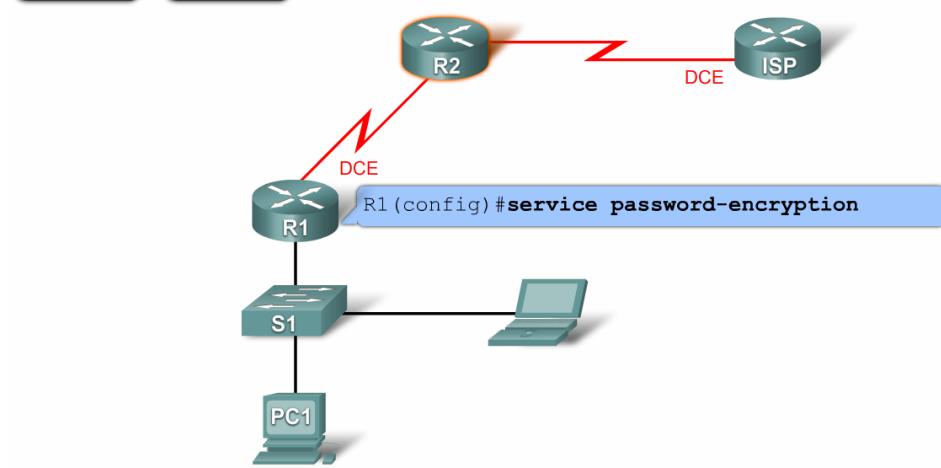
Configuring Router Passwords

Password:

Router> enable

Password:

Router#



Router(config)# line console 0

Router(config-line)# password cisco

Router(config-line)# login // Bật chế độ kiểm tra mật khẩu

Bỏ mật khẩu

Router(config-line)# no password

ĐẶT PASSWORD CHO MỨC PRIVILEGED

Router> **enable**

Password:

Router# **Configure terminal**

Router(config)# **enable password cisco1**

//Hoặc mật khẩu được mã hóa

Router(config)# **enable secret cisco2**

Router(config)# **exit**

Xem mật khẩu được mã hóa MD5

Router(config)# **Show running-config**

ĐẶT PASSWORD TRUY NHẬP TỪ XA

Router# **Configure terminal**

Router(config)# **line vty 0 4**

Router(config-line)# **password cisco**

Router(config-line)# **login**

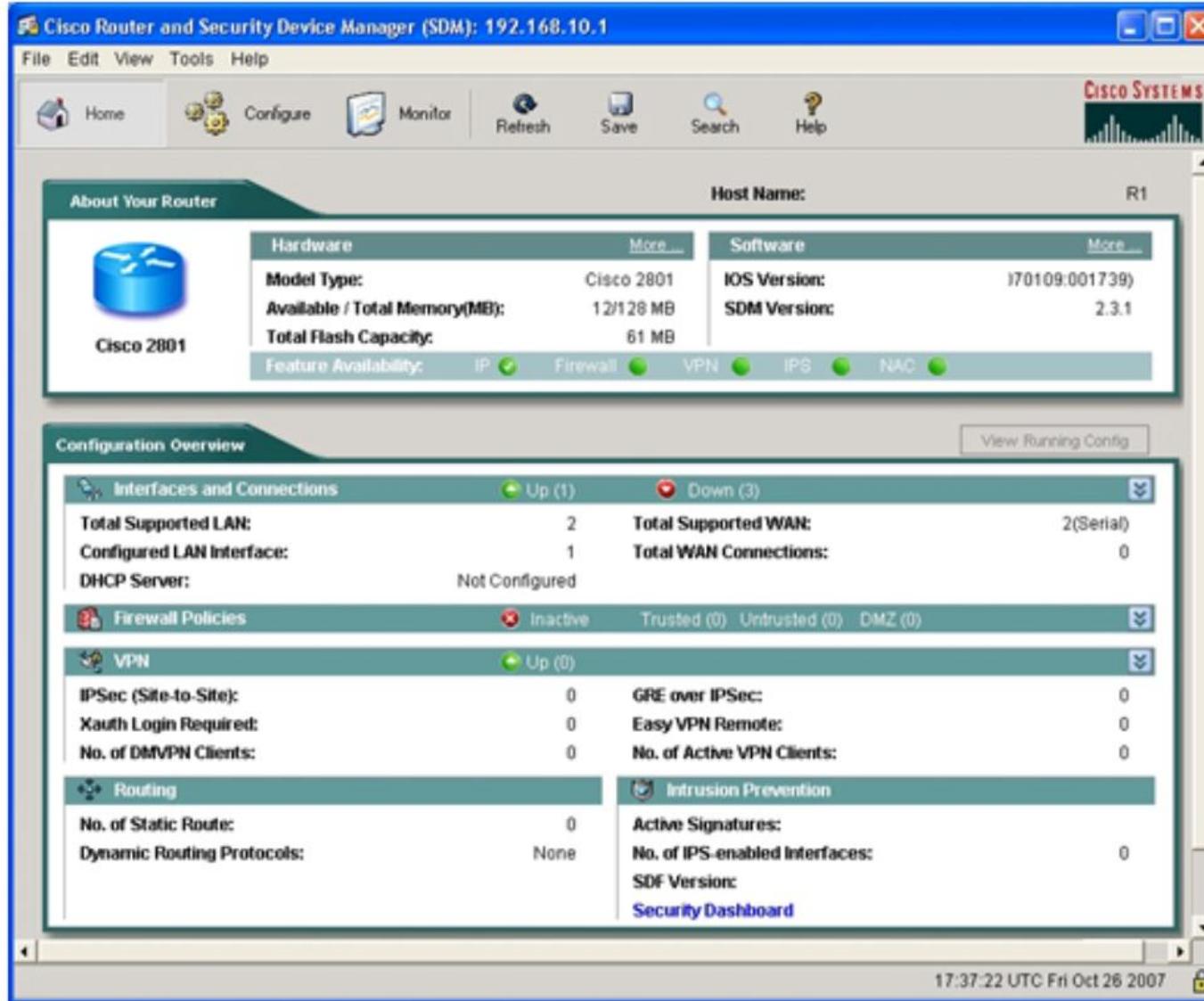
Thoát ra để thử mật khẩu

Mã hóa tất cả các mật khẩu

Router(config)# **Service password-encryption**

GIAO DIỆN SDM

What Is Cisco SDM?



CHƯƠNG 5: BẢO MẬT MẠNG

- 1. Giới thiệu chung
- 2. Điều khiển truy cập ACL
- 3. Xác thực người dùng
- 4. Tường lửa

BÀI 2: ĐIỀU KHIỂN TRUY CẬP

- ❖ Điều khiển truy cập (Access Control) là sự hạn chế về quyền tiếp cận, truy cập, xâm nhập vào mạng, tác dụng chính của Access Control là để phân quyền người dùng (chỉ cho phép những người nào được truy cập vào tài nguyên mạng).
- ❖ Điều khiển truy cập trong an ninh máy tính (computer security access control) bao gồm các nhiệm vụ: xác thực (Authentication), phân quyền (Authorization), ghi nhận thông tin và đánh giá (Accounting and Auditing)

ĐIỀU KHIỂN TRUY CẬP

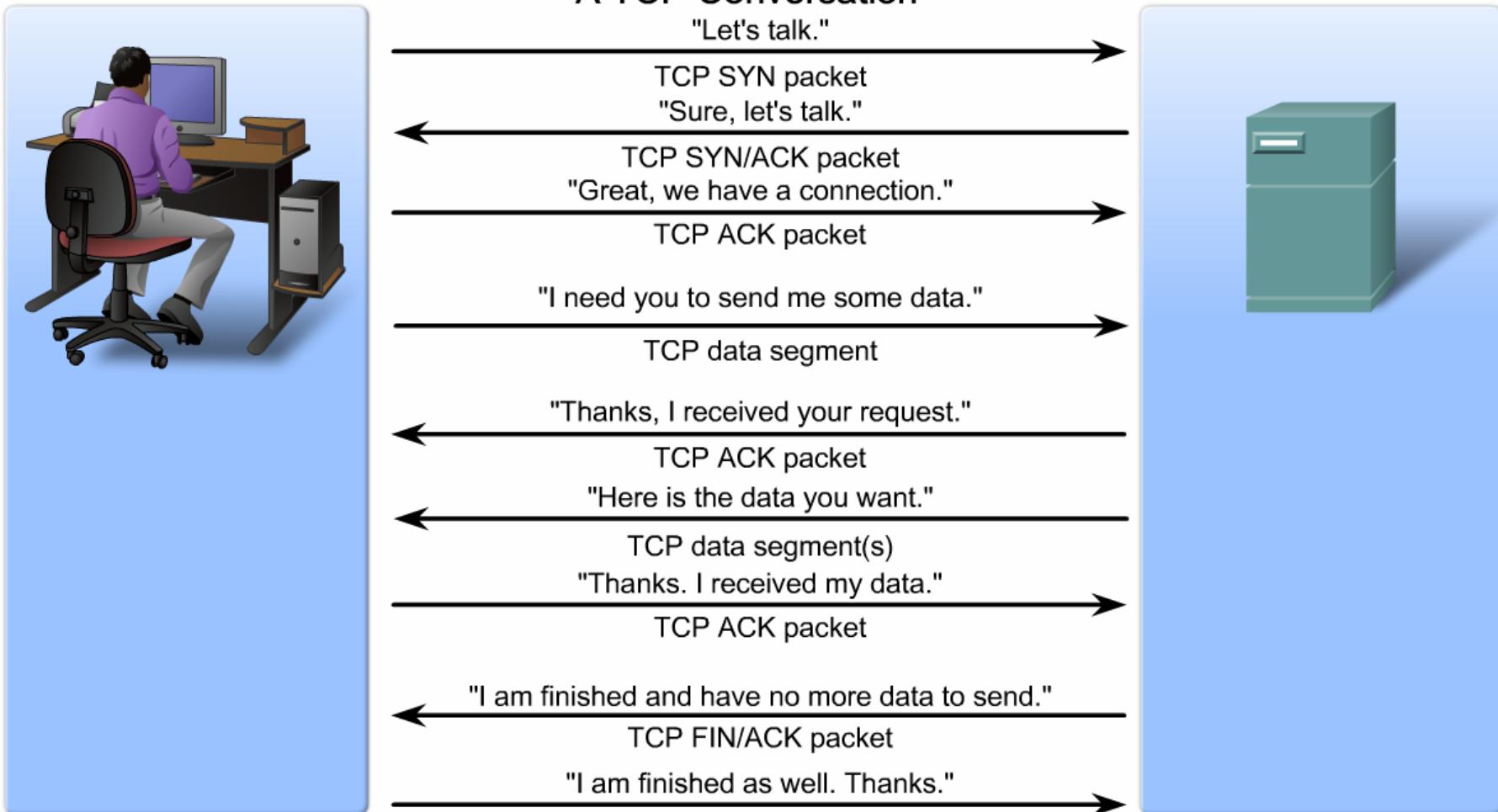
- ❖ Xác thực (Authentication): Đòi hỏi người sử dụng chứng minh được họ thực sự là ai, thông qua yêu cầu như username, password, các yêu cầu challenge và response...
- ❖ Phân quyền (Authorization): Sau khi xác thực thành công, các dịch vụ Authorization sẽ quyết định người sử dụng này được thao tác gì trên hệ thống và được sử dụng những tài nguyên nào.
- ❖ Ghi nhận thông tin và đánh giá (Accounting and Auditing): Ghi nhận lại những thao tác mà người sử dụng này đã thực hiện trên thiết bị, những tài nguyên mà họ đã sử dụng và thời gian sử dụng bao lâu. Các thông tin này được đánh giá định kỳ hay khi có sự cố về bảo mật xảy ra.

ĐIỀU KHIỂN TRUY CẬP

Điều khiển truy cập nói chung được chia ra làm hai loại, hoặc là tùy quyền (discretionary), hoặc là bắt buộc (mandatory).

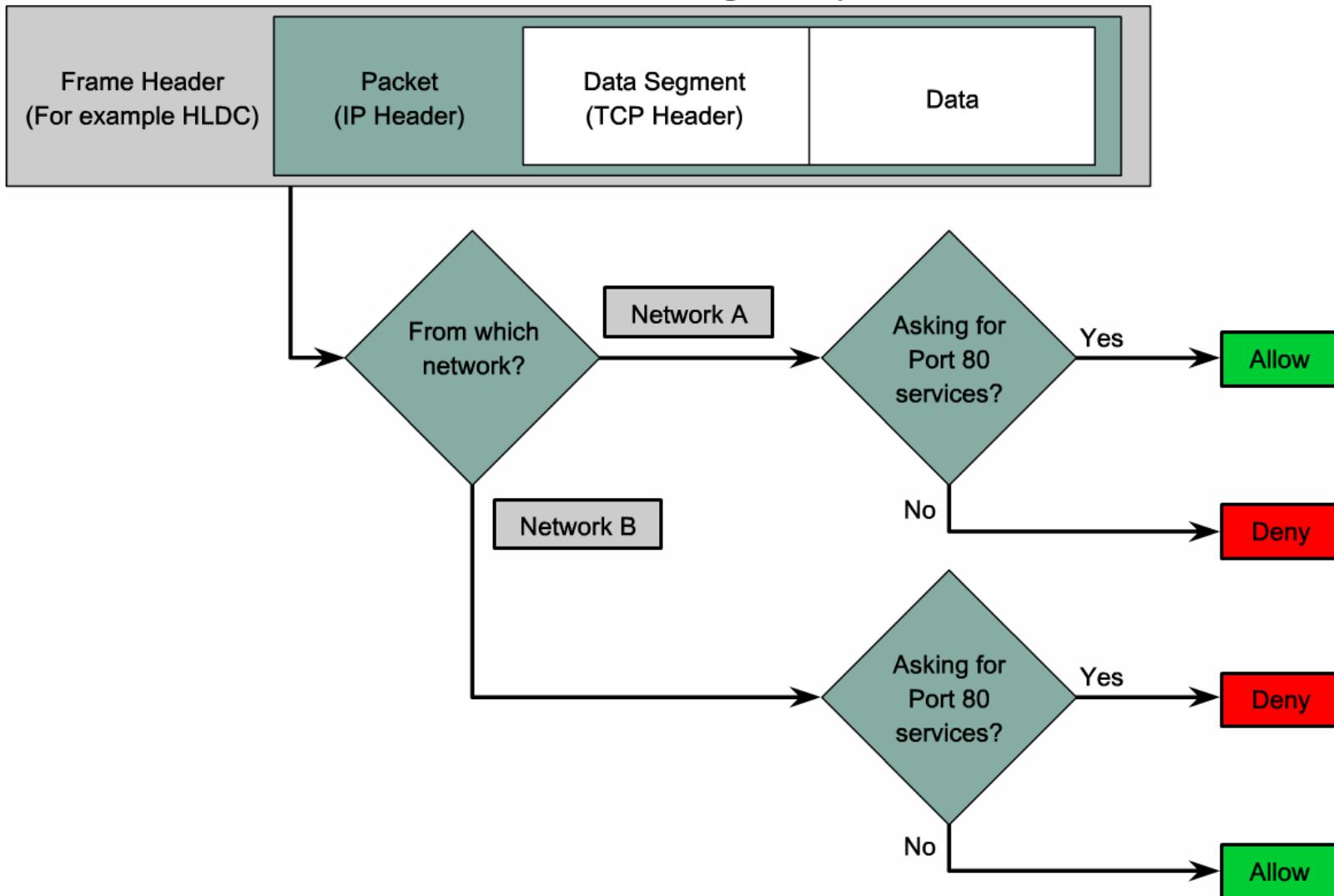
- ❖ Điều khiển truy cập tùy quyền (DAC – Discretionary Access Control): Do chủ tài nguyên cấp quyền thiết lập một danh sách kiểm soát truy cập (ACL – Access Control List) hoặc kiểm tra truy cập trên cơ sở vai trò (role-based access control) chỉ định tư cách nhóm hội viên dựa trên vai trò của tổ chức hoặc chức năng của các vai trò.
- ❖ Điều khiển truy cập bắt buộc (MAC – Mandatory Access Control): Cách truy cập tĩnh, sử dụng một tập các quyền truy cập được định nghĩa trước đối với các file trong hệ thống.

CÁC BƯỚC TRONG PHIÊN TCP



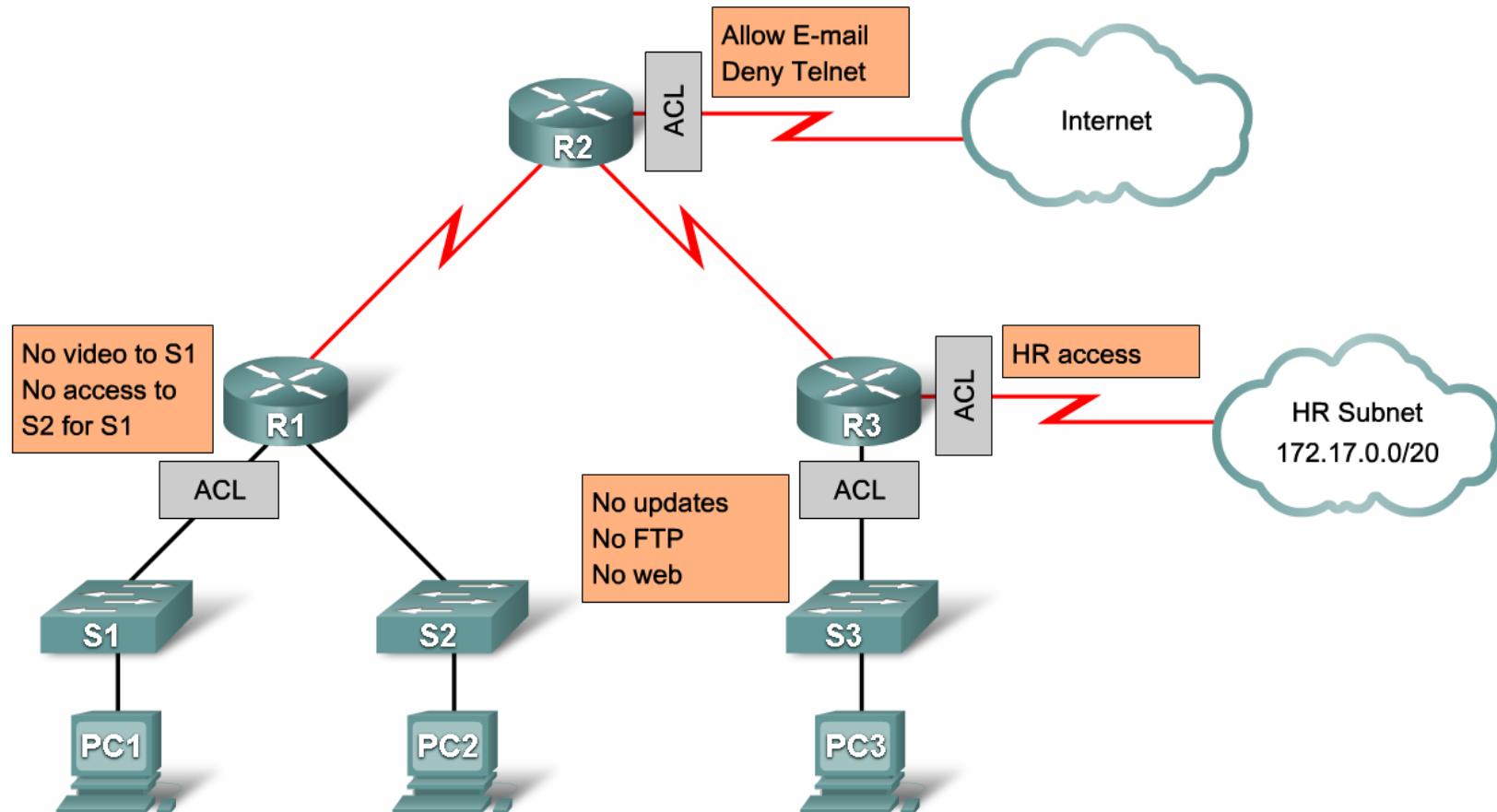
VÍ DỤ LỌC GÓI TIN

Packet Filtering Example



ĐIỀU KHIỂN TRUY CẤP ACL

What Is an ACL?

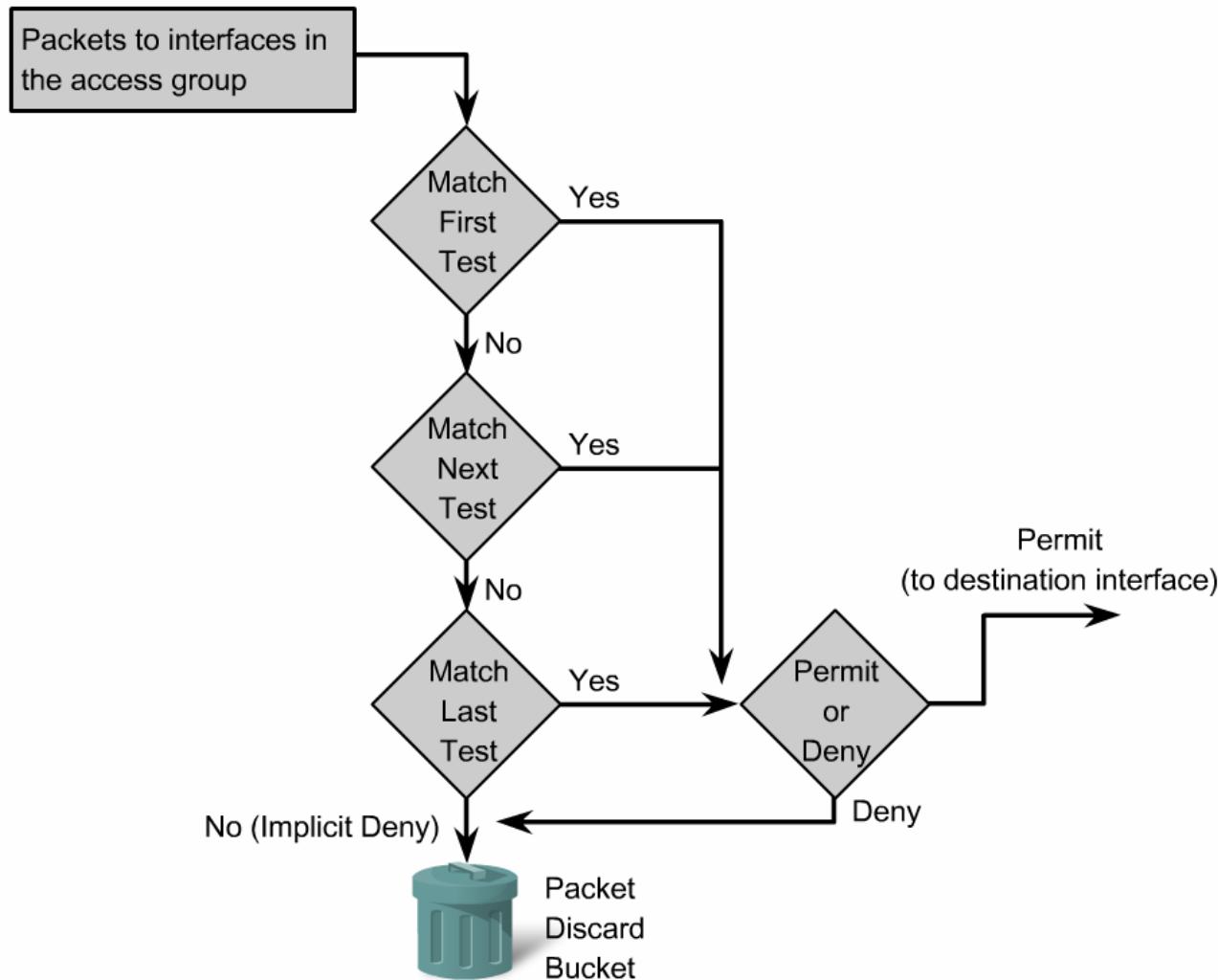


What Is an ACL?

ACLs on a Router

HOẠT ĐỘNG CỦA ACLs

How ACLs Work

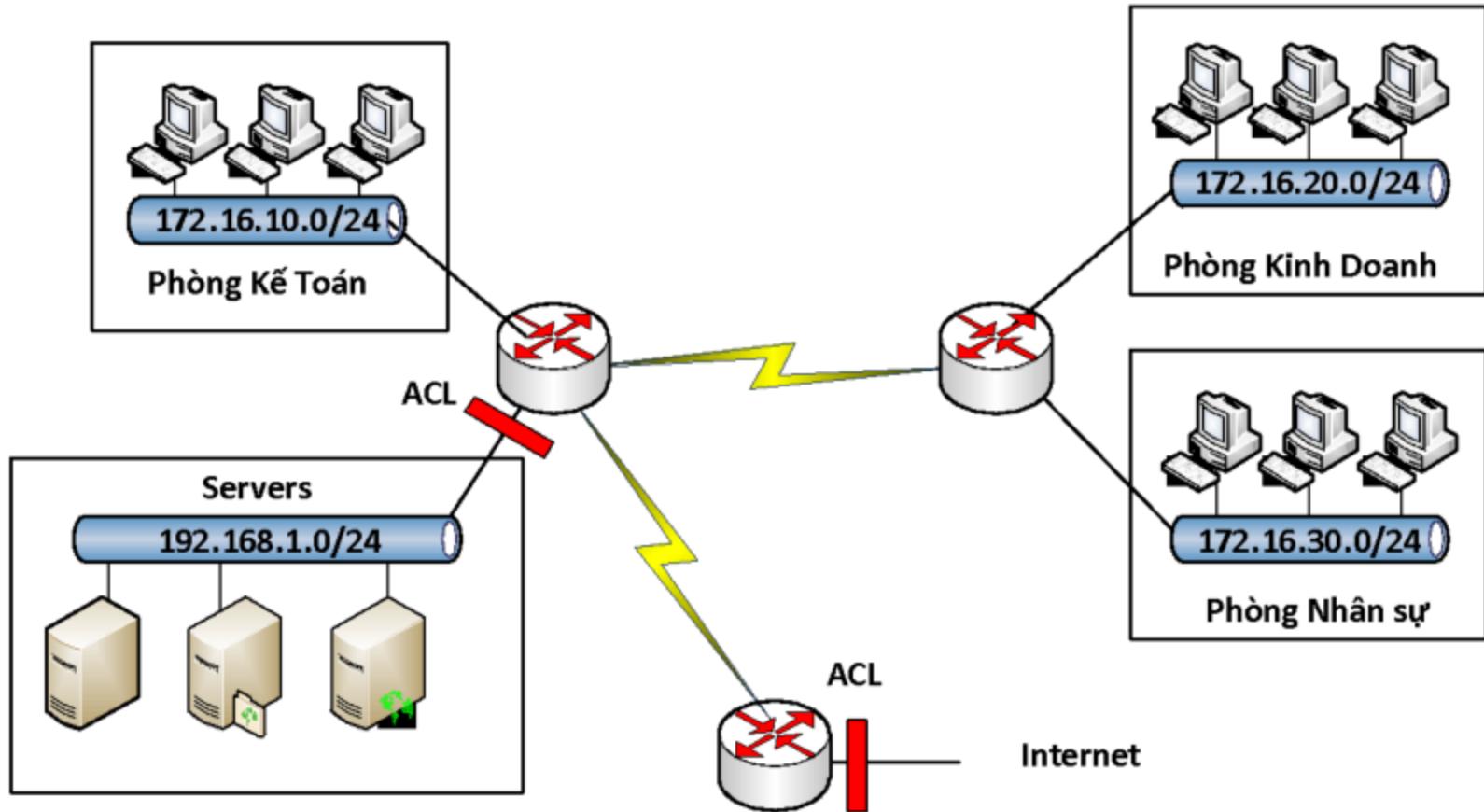


ACL TRÊN ROUTER CISCO

❖ Cấu hình ACL – Access Control List trên router Cisco

- ACL là một danh sách các điều kiện được áp đặt vào các cổng của router để lọc các gói tin đi qua nó.
- Danh sách này chỉ ra cho router biết loại dữ liệu nào được cho phép (allow) và loại dữ liệu nào bị hủy bỏ (deny).
- Sự cho phép và huỷ bỏ này có thể được kiểm tra dựa vào địa chỉ nguồn, địa chỉ đích, giao thức hoặc chỉ số cổng.
- Sử dụng ACL để quản lý các lưu lượng mạng, hỗ trợ ở mức độ cơ bản về bảo mật cho các truy cập mạng, thể hiện ở tính năng lọc các gói tin qua router.

ACCESS CONTROL LIST



PHÂN LOẠI VÀ HOẠT ĐỘNG ACL

❖ ACL được chia thành 2 loại:

- Standard ACL
- Extended ACL

❖ Hoạt động của ACL

- ACL thực hiện việc kiểm tra theo trình tự của các điều kiện trong danh sách cấu hình. Nếu có một điều kiện được khớp trong danh sách thì nó sẽ thực hiện hành động tương ứng trong điều kiện đó, và các điều kiện còn lại sẽ không được kiểm tra nữa.
- Trường hợp tất cả các điều kiện trong danh sách đều không khớp thì một câu lệnh mặc định “deny any” được thực hiện, có nghĩa là điều kiện cuối cùng ngầm định trong một ACL mặc định sẽ là cấm tất cả.

PHÂN LOẠI VÀ HOẠT ĐỘNG ACL

- Trong cấu hình ACL cần phải có ít nhất một câu lệnh có hành động là “permit”.
- Khi gói tin đi vào một cổng, router sẽ kiểm tra xem có ACL nào được đặt trên cổng để kiểm tra hay không, nếu có thì các gói tin sẽ được kiểm tra với những điều kiện trong danh sách.
- Nếu gói tin đó được cho phép bởi ACL, nó sẽ tiếp tục được kiểm tra trong bảng định tuyến để quyết định chọn cổng ra để đi đến đích.
- Tiếp đó, router sẽ kiểm tra xem trên cổng dữ liệu chuyển ra có đặt ACL hay không. Nếu không thì gói tin đó có thể sẽ được gửi tới mạng đích. Nếu có ACL thì nó sẽ kiểm tra với những điều kiện trong danh sách ACL đó.

CẤU HÌNH ACL

- ❖ Có 2 phương pháp cấu hình ACL:
 - Dựa vào số (numbered ACL)
 - Dựa vào tên (named ACL)
- ❖ Để cài đặt một ACL, ta thực hiện các bước sau:

Bước 1: Tạo ACL

- ✓ Xác định loại ACL dựa vào số hiệu ACL (numbered ACL) hoặc tên (named ACL)
- ✓ Lựa chọn hành động cho từng điều kiện “permit” hay “deny” theo yêu cầu cụ thể.

CẤU HÌNH ACL

Bước 2: Gán ACL vào cổng của router

- ✓ Các ACL được gán vào một hoặc nhiều cổng và có thể được lọc theo chiều các gói tin đi vào hay đi ra.
- ✓ Một router với một ACL được đặt ở cổng dữ liệu vào phải kiểm tra mỗi gói tin để tìm xem nó có khớp các điều kiện trong danh sách ACL trước khi chuyển gói tin đó đến một cổng ra.

MỘT SỐ THUẬT NGỮ

❖ Wildcard-mask:

Với Standard ACL, nếu không thêm “wildcard-mask” trong câu lệnh tạo ACL thì mặc định “wildcard-mask” sẽ là 0.0.0.0

❖ Wildcard “host”

“Wildcard mask” dùng cho một thiết bị hay còn gọi là “wildcard-host” Ví dụ: host 172.30.26.29

Câu lệnh ACL cho phép một thiết bị như sau:

R(config)#**access-list 1 permit 172.30.16.29 0.0.0.0**

hoặc: R(config)#**access-list 1 permit host 172.30.16.29**

MỘT SỐ THUẬT NGỮ

❖ Wildcard “any”

Wildcard mask cho tất cả các thiết bị được gọi là wildcard “any” có dạng: 255.255.255.255 (không kiểm tra tất cả các bit)

- Ý nghĩa: chấp nhận tất cả các địa chỉ
- “Wildcard mask” dùng cho tất cả các thiết bị có thể đại diện bằng từ khoá “any”
- Ví dụ:

R(config)#**access-list 1 permit 0.0.0.0 255.255.255.255**

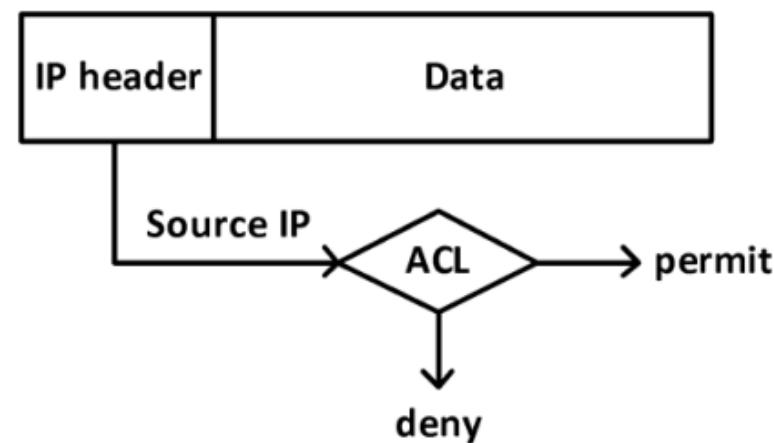
hoặc: R(config)#**access-list 1 permit any**

❖ Inbound và outbound

Khi áp dụng ACL trên một cổng, phải xác định ACL đó được dùng cho luồng dữ liệu vào (inbound) hay ra (outbound). Chiều của luồng dữ liệu được xác định trên cổng của router.

STANDARD ACL

- ❖ Sử dụng “Standard CL” khi ta muốn cấm hay cho phép tất cả các luồng dữ liệu từ một thiết bị hay một mạng xác định trên toàn bộ giao thức.
- ❖ “Standard CL” kiểm tra điều kiện dựa vào địa chỉ nguồn trong các gói tin và thực hiện hành động cấm hoặc cho phép tất cả các lưu lượng từ một thiết bị hay một mạng xác định nào đó.
- ❖ Kiểm tra gói tin với “Standard ACL”:



CẤU HÌNH STANDARD ACL

❖ Cấu hình Standard ACL

Router(config)# access-list <ACL-number> {permit|deny} source [wildcast-mask]

❖ Trong đó:

- ACL-number: có giá trị từ 1 đến 99, hoặc 1300-1999
- Wildcast-mask: nếu không được cấu hình sẽ lấy giá trị mặc định là: 0.0.0.0

❖ Gán ACL vào một cổng và đặt chế độ kiểm tra cho luồng dữ liệu đi vào hay đi ra khỏi cổng của router.

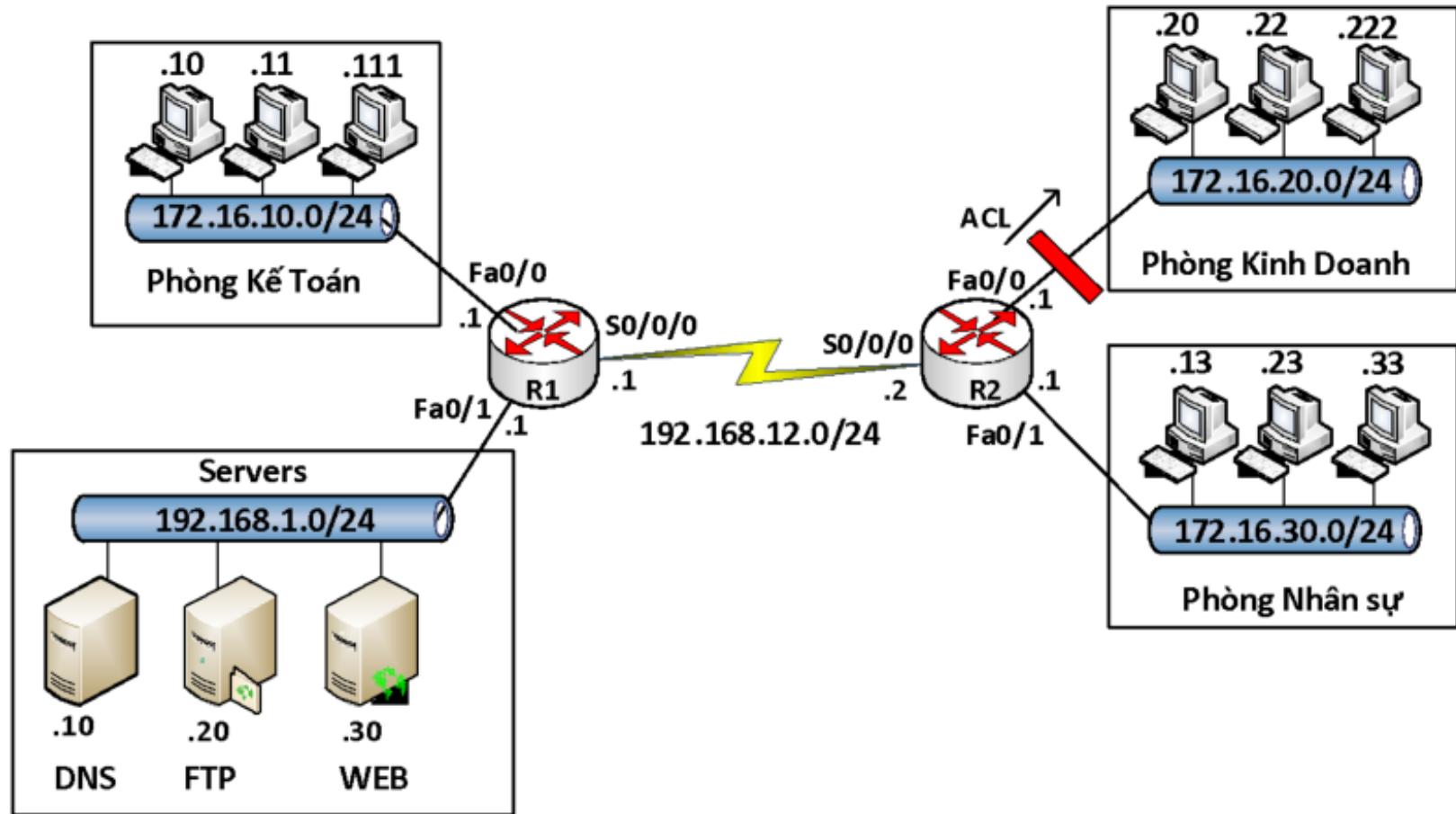
Router(config-if)# ip access-group <ACL-number> {in|out}

❖ Huỷ bỏ câu lệnh áp đặt ACL vào cổng

Router(config-if)# no ip access-group <ACL-number> {in|out}

VÍ DỤ

- ❖ Cấm các máy tính thuộc mạng 172.16.10.0/24 truy nhập tới mạng 172.16.20.0/24



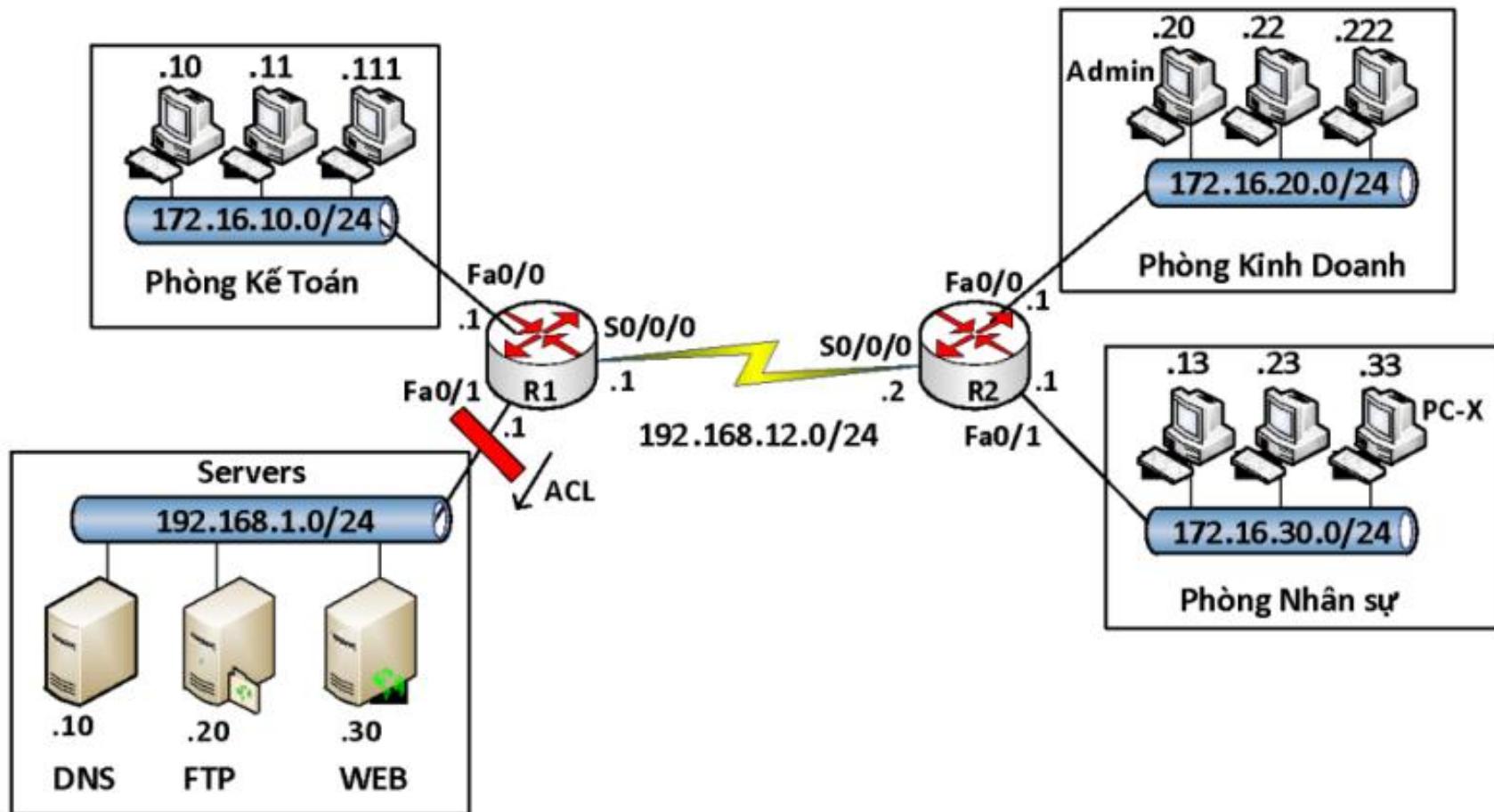
CẤU HÌNH TRÊN ROUTER R2

- ❖ R2(config)#access-list 1 deny 172.16.10.0 0.0.0.255
- ❖ R2(config)#access-list 1 permit any
- ❖ R2(config)#interface fa0/0
- ❖ R2(config-if)#ip access-group 1 out

- ❖ R2(config)#Ip access-list standard cam10
- ❖ R2(config)# deny 172.16.10.0 0.0.0.255
- ❖ R2(config)#permit any
- ❖ R2(config)#interface fa0/0
- ❖ R2(config-if)#ip access-group cam10 out

BÀI TẬP

- ❖ Cốm PC-X có địa chỉ 172.16.30.33/24 truy cập vào mạng 192.168.1.0/24



- ❖ R1(config)# access-list 10 deny host 172.16.30.33
- ❖ R1(config)# access-list 10 permit any
- ❖ R1(config)#interface fa0/1
- ❖ R1(config-if)#ip access-group 10 out

DÙNG STANDARD ACL ĐIỀU KHIỂN TELNET

- ❖ Trên router có các “virtual terminal port” được dùng để cấu hình cho mục đích cho phép telnet vào router.
- ❖ Cấu hình: thực hiện hai bước chính sau
 - Chọn các thiết bị hoặc mạng được phép telnet vào các thiết bị dùng Standard ACL
 - Gán ACL đã được cài đặt ở trên vào cổng telnet.
- ❖ Các câu lệnh cấu hình:
 - Router(config)#**line vty { vty-number|vty-range}**
 - Router(config-line)#**access-class <access-list-number> {in|out}**
 - ✓ vty-number: có giá trị 0 đến 4 (Router), 0 đến 15 (Switch)
 - ✓ vty-range: là một dãy liên tiếp các port vty được sử dụng
 - ✓ access-list-number: ACL gán vào các cổng vty để điều khiển truy cập

VÍ DỤ

- ❖ Viết ACL chỉ cho phép Admin có IP 172.16.20.20 telnet vào các router R1, R2 trong mô hình bài tập trên.
- ❖ Trước tiên, cấu hình mở telnet trên R1 và R2.
- ❖ ACL thực hiện yêu cầu đầu bài: trên R1 và R2 sử dụng ACL:

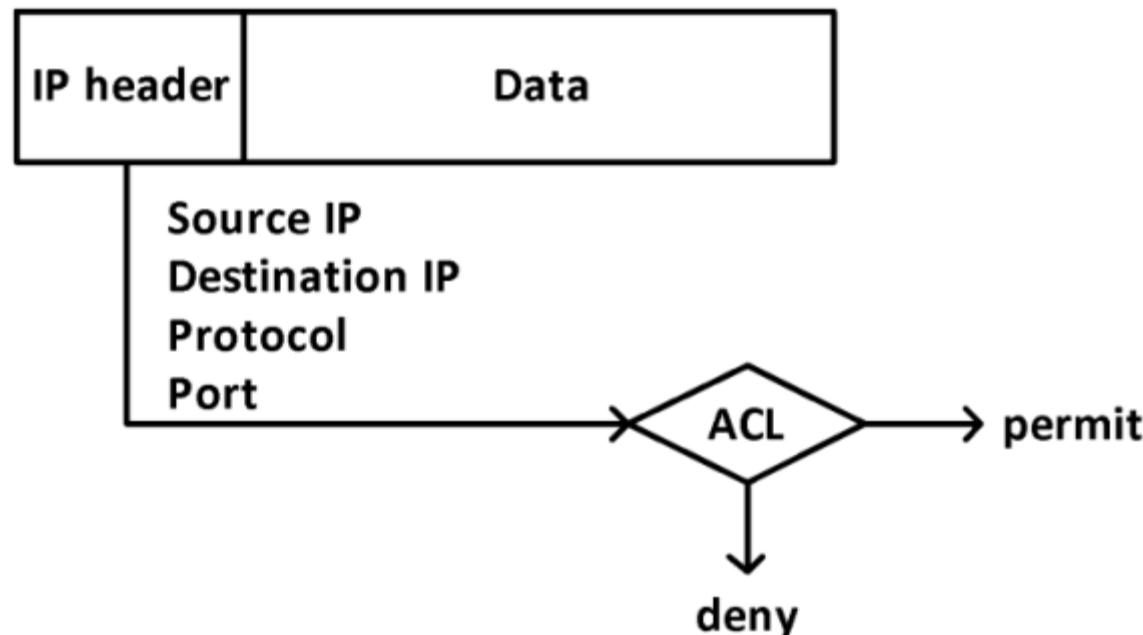
R(config)#**access-list 20 permit host 172.16.20.20**

R(config)#**line vty 0 4**

R(config-line)#**access-class 20 in**

EXTENDED ACL

- ❖ “Extended ACL” cung cấp sự điều khiển linh hoạt hơn “Standard ACL”. Nó kiểm tra cả địa chỉ nguồn, địa chỉ đích, giao thức, chỉ số cổng ứng dụng. “Extended ACL” thực hiện hành động cấm hay cho phép ở một số ứng dụng xác định.
- ❖ Kiểm tra các gói tin với “Extended ACL”:



CẤU HÌNH EXTENDED ACL

- ❖ Lệnh tạo một điều kiện (ACL entry) trong một ACL access-list-number

Router(config)#**access-list <access-list-number> {permit|deny}**
<protocol> <source-address> <source-wildcard> <destination-address> <destination-wildcard> <operation> <operand>

- ❖ Trong đó:
 - access-list-number: có giá trị từ 100 – 199 hoặc 2000 - 2699
 - protocol: là ip, udp, tcp, icmp,...
 - operation: thường dùng là eq
 - operand: là chỉ số port của dịch vụ hay tên của dịch vụ.

Ví dụ: ta có thể dùng chỉ số port 23 hay có thể dùng tên dịch vụ là telnet

CÂU HÌNH EXTENDED ACL

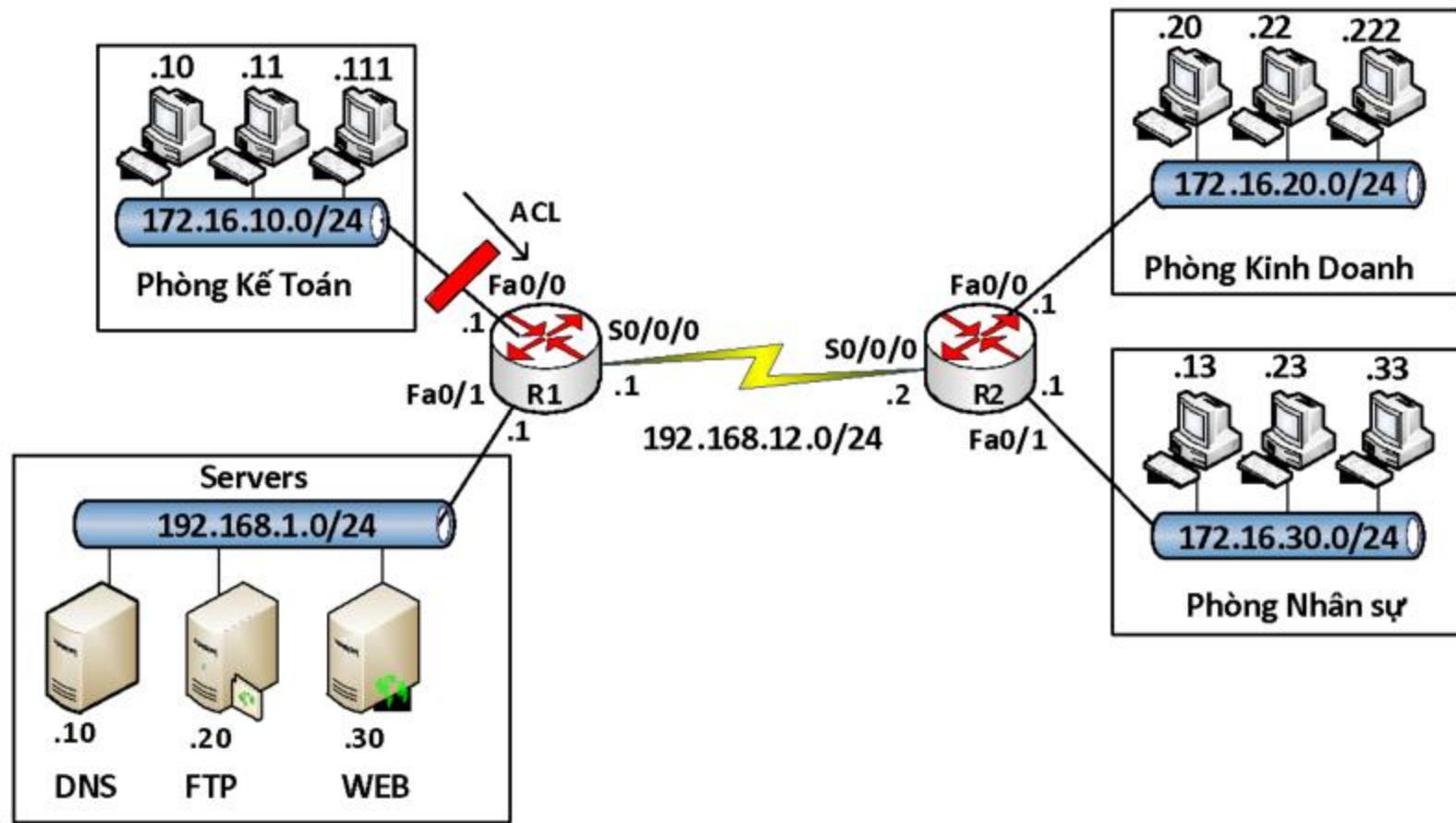
- ❖ Gán danh sách ACL vào interface và chọn hướng (inbound hoặc outbound) các traffic sẽ được kiểm tra.

Router(config-if)#**ip access-group <access-list-number> {in|out}**

- ❖ Trong đó, access-list-number là số hiệu (có giá trị 100 – 199 hoặc 2000 - 2699) chỉ danh sách ACL ta đã tạo.

VÍ DỤ

- ❖ Cấu hình trên router trong mô hình mạng dưới đây để cấm các FTP traffic từ các host thuộc subnet 172.16.10.0 đến FTP server có IP 192.168.1.20/24, cho phép tất cả các traffic còn lại hoạt động bình thường.



```
R1(config)#access-list 100 deny tcp 172.16.10.0 0.0.0.255 host  
192.168.1.20 eq 20
```

```
R1(config)#access-list 100 deny tcp 172.16.10.0 0.0.0.255 host  
192.168.1.20 eq 21
```

```
R1(config)#access-list 100 permit ip any any
```

```
R1(config)#interface fa0/0
```

```
R1(config-if)#ip access-group 100 in
```

- ❖ Vị trí đặt ACL: Nên đặt extended ACL gần nguồn của traffic muốn cấm và nên đặt Standard ACL gần đích đến của traffic.

```
R1(config)#access-list 100 deny icmp 172.16.10.0 0.0.0.255 host  
172.16.20.20
```

```
R1(config)#access-list 100 permit ip any any
```

```
R1(config)#interface fa0/0
```

```
R1(config-if)#ip access-group 100 in
```

- ❖ Vị trí đặt ACL: Nên đặt extended ACL gần nguồn của traffic muốn cấm và nên đặt Standard ACL gần đích đến của traffic.

NAMED ACL

- ❖ Named-ACL cho phép Standard và Extended ACL được định danh bởi một tên thay vì đại diện bởi một con số. Loại ACL này có thể cho phép xóa một số dòng (điều kiện) trong một danh sách đã được cấu hình.
- ❖ Named-ACL không tương thích với các Cisco IOS phiên bản trước 11.2 và không thể sử dụng cùng một tên cho nhiều ACL. ACL của các loại giao thức khác nhau không thể có cùng một tên.

CÁC CÂU LỆNH CẤU HÌNH NAME ACL

- ❖ Router(config)#**ip access-list { standard | extended } name**
- ❖ Router(config{ std|ext- }nacl)#[sequence-number]
 {permit|deny} {ip access list test conditions}
- ❖ Router(config-if)#**ip access-group name {in | out}**
- ❖ Trong đó: sequence-number là dòng chèn vào danh sách.

MỘT SỐ LỆNH KIỂM TRA CẤU HÌNH ACL

Router# show access-list {access-list-number | name }

Ví dụ: Router# show access-lists

Standard IP access list 1

 permit 10.2.2.1

 permit 10.3.3.1

 permit 10.4.4.1

 permit 10.5.5.1

Extended IP access list 101

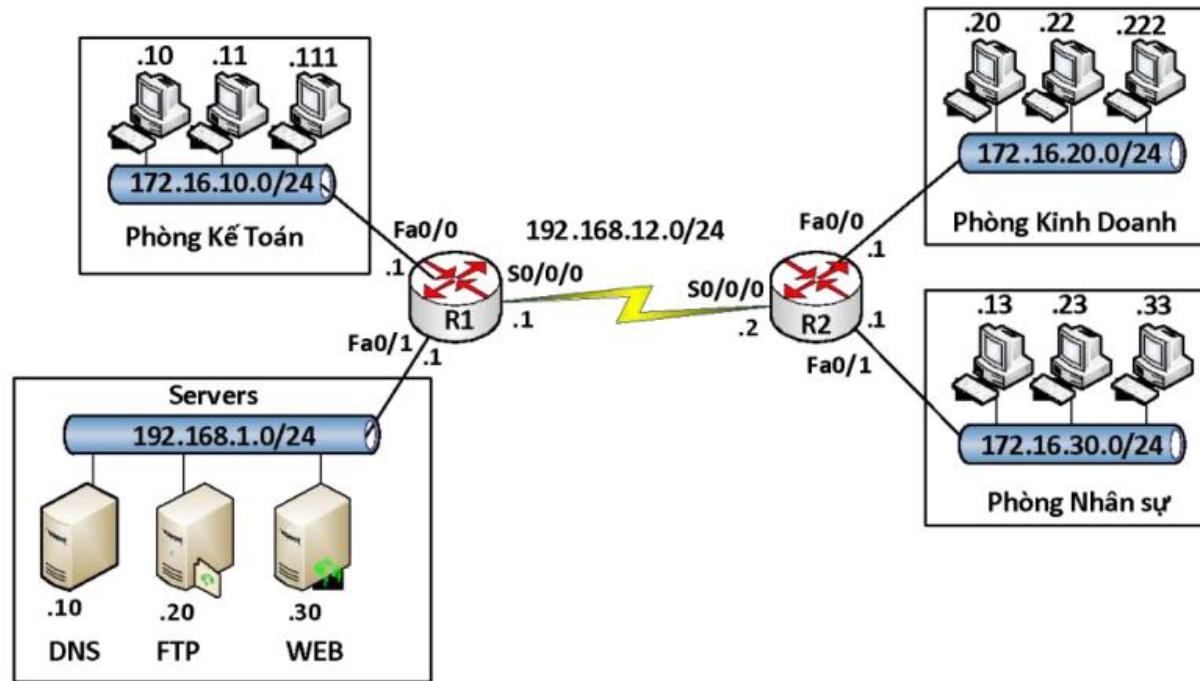
 permit tcp host 10.22.22.1 any eq telnet

 permit tcp host 10.33.33.1 any eq ftp

 permit tcp host 10.44.44.1 any eq ftp-data

VÍ DỤ

1. Cấu hình Extended ACL cấm các máy tính thuộc phòng Kinh doanh truy cập tới phòng Kế toán
2. Cấm các máy tính thuộc phòng Kế toán truy cập tới Web server bằng dịch vụ www
3. Cấm các máy tính thuộc phòng Nhân sự ping tới DNS server



HƯỚNG DẪN CẤU HÌNH

- ❖ Bước 1: Cấu hình hostname, địa chỉ IP cho các cổng trên các thiết bị, cấu hình định tuyến cho hệ thống mạng trên với giao thức định tuyến tùy chọn.
- ❖ Bước 2: Cấu hình ACL theo yêu cầu
 - (1) Có thể dùng standard ACL và extended ACL cho yêu cầu này
 - Dùng “Standard ACL”

R1(config)# **ip access-list standard abc**

R1(config-std-nacl)# **deny 172.16.20.0 0.0.0.255**

R1(config-std-nacl)# **permit any**

R1(config)# **interface fa0/0**

R1(config-if)# **ip access-group abc out**

HƯỚNG DẪN CẤU HÌNH

- ❖ Dùng “Extended ACL” (có thể cấu hình trên R1 hoặc R2)

```
R2(config)# ip access-list extended xyz
```

```
R2(config-ext-nacl)# deny ip 172.16.20.0 0.0.0.255 172.16.10.0  
0.0.0.255
```

```
R2(config-ext-nacl)# permit ip any any
```

```
R2(config)# interface fa0/0
```

```
R2(config-if)# ip access-group xyz in
```

HƯỚNG DẪN CẤU HÌNH

(2) Cấm các máy tính thuộc phòng Kế toán truy cập tới Web server bằng dịch vụ www

R1(config)# ip access-list extended tlu

R1(config-ext-nacl)# deny tcp 172.16.10.0 0.0.0.255 host
192.168.1.30 eq 80

R1(config-ext-nacl)# permit ip any any

R1(config)# interface fa0/1

R1(config-if)# ip access-group tlu out

HƯỚNG DẪN CẤU HÌNH

(3) Cấm các máy tính thuộc phòng Nhân sự ping tới DNS server

```
R2(config)# ip access-list extended cntt
```

```
R2(config-ext-nacl)#deny icmp 172.16.30.0 0.0.0.255 host
```

```
192.168.1.10
```

```
R2(config-ext-nacl)# permit ip any any
```

```
R2(config)# interface fa0/1
```

```
R2(config-if)# ip access-group cntt in
```

❖ Kiểm tra

Dùng lệnh ping, trình duyệt Web để kiểm tra kết quả, dùng các câu lệnh show trên router để kiểm tra cấu hình

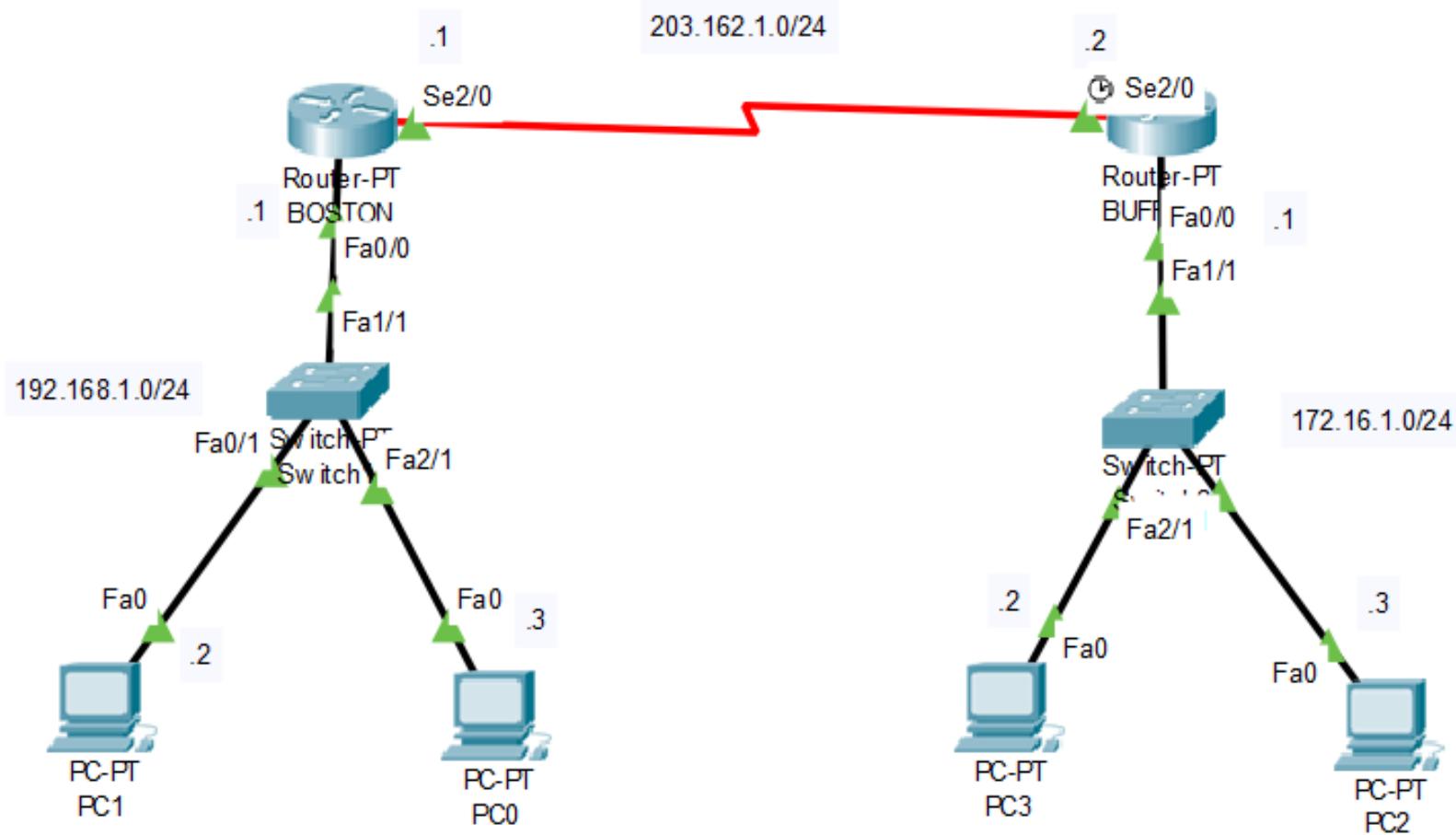
R# show run

R# show ip route

R# show access-lists

BÀI TẬP 1: STANDARD ACL

- Lọc các packet sử dụng standard ACL, thực hiện cấm tất cả các traffic từ PC1 đến các PC trong mạng 172.16.1.0/24



CẤU HÌNH TRÊN ROUTER BUFFALO

Buffalo(config)#**access-list 1 deny 192.168.1.2 0.0.0.0**

(hoặc Buffalo (config)#**access-list 1 deny host 192.168.1.2**)

Buffalo(config)#**access-list 1 permit ip any**

Buffalo(config)#**interface f0/0**

Buffalo(config-if)#**ip add 172.16.1.1 255.255.255.0**

Buffalo(config-if)#**ip access-group 1 out**

Buffalo(config-if)#**no shut**

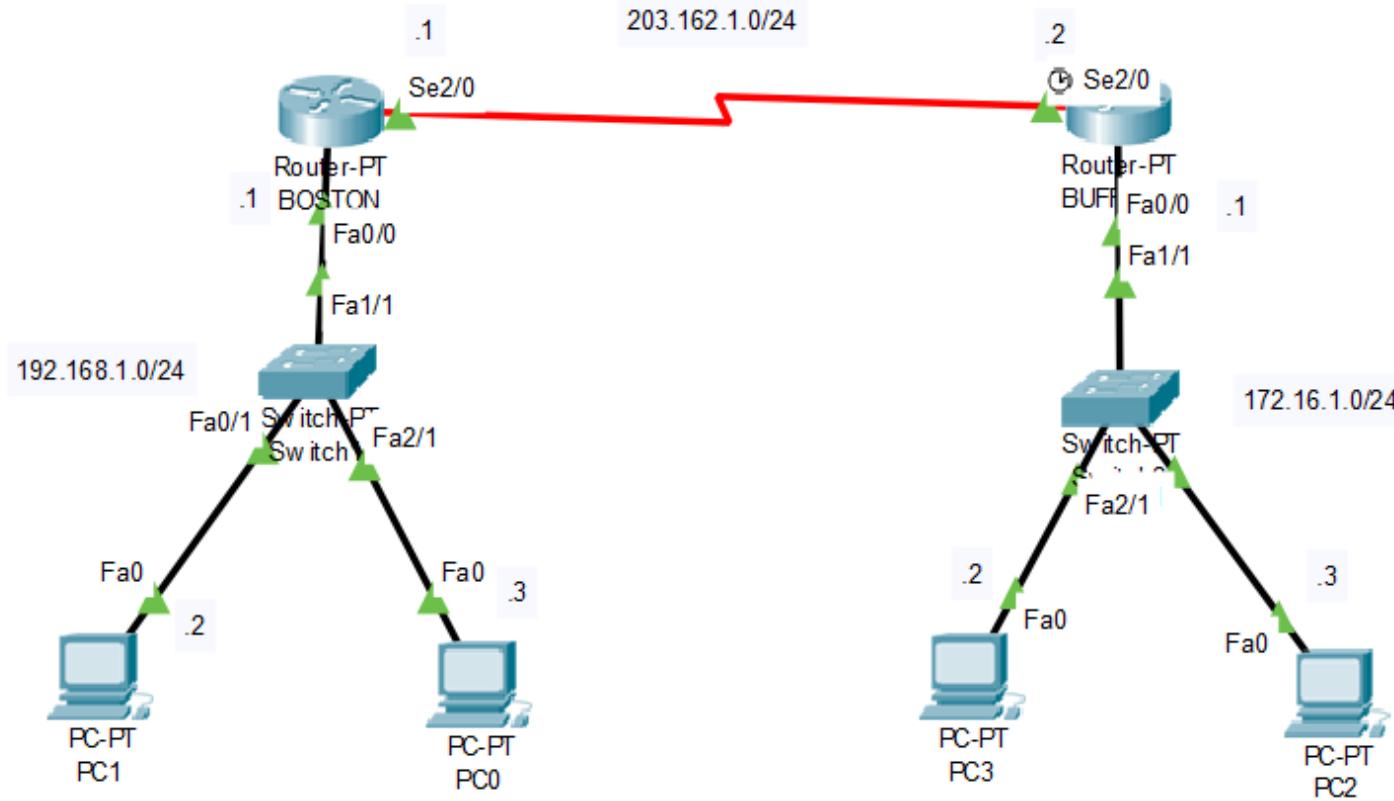
Buffalo(config-if)#**exit**

KIỂM TRA

- ❖ Dùng lệnh ping để theo dõi kết quả hiển thị
 - Ping từ PC1 đến PC2, PC3
 - Ping từ PC3 đến PC1, PC2
 - Ping từ PC2 đến PC1, PC3
- ❖ Dùng các câu lệnh show trên router để kiểm tra cấu hình
 - Router#show run
 - Router#show ip route
 - Router#show access-lists

BÀI TẬP 2: EXTENDED ACL

Yêu cầu: Sử dụng Access-list để lọc ngõ vào trên cổng serial của Router Boston cho phép tất cả các lưu lượng từ PC3 tới PC0 và từ chối tất cả các lưu lượng từ PC3 tới PC1.



CẤU HÌNH TRÊN ROUTER BOSTON

❖ Cấu hình ACL

Boston(config)#**access-list 100 permit ip host 172.16.1.2 host 192.168.1.3**

Boston(config)#**access-list 100 deny ip host 172.16.1.2 host 192.168.1.2**

❖ Gán ACL vào cổng serial của RouterA

Boston(config)#**interface Serial 2/0**

Boston(config-if)#**ip access-group 100 in**

❖ Kiểm tra cấu hình

Từ PC3 ping PC2

Từ PC3 ping PC1

CHƯƠNG 5: BẢO MẬT MẠNG

- 1. Giới thiệu chung
- 2. Điều khiển truy cập ACL
- 3. Xác thực người dùng
- 4. Tường lửa

BÀI 3. XÁC THỰC NGƯỜI DÙNG

- ❖ Nhận dạng và chứng thực (Identification and authentication - I&A) là một quy trình gồm hai bước nhằm xác minh người truy nhập vào hệ thống.
- ❖ Nhận dạng là phương pháp người dùng báo cho hệ thống biết họ là ai (chẳng hạn như username hoặc chỉ danh của người dùng userID).
- ❖ Trong trường hợp đối với một hệ thống hoặc một quy trình (process), việc nhận dạng thường dựa vào:
 - Tên máy tính (computer name)
 - Địa chỉ truy cập thiết bị (Media Access Control - MAC - address)
 - Địa chỉ giao thức mạng (Internet Protocol - IP - address)
 - Chỉ danh của quy trình (Process ID - PID)

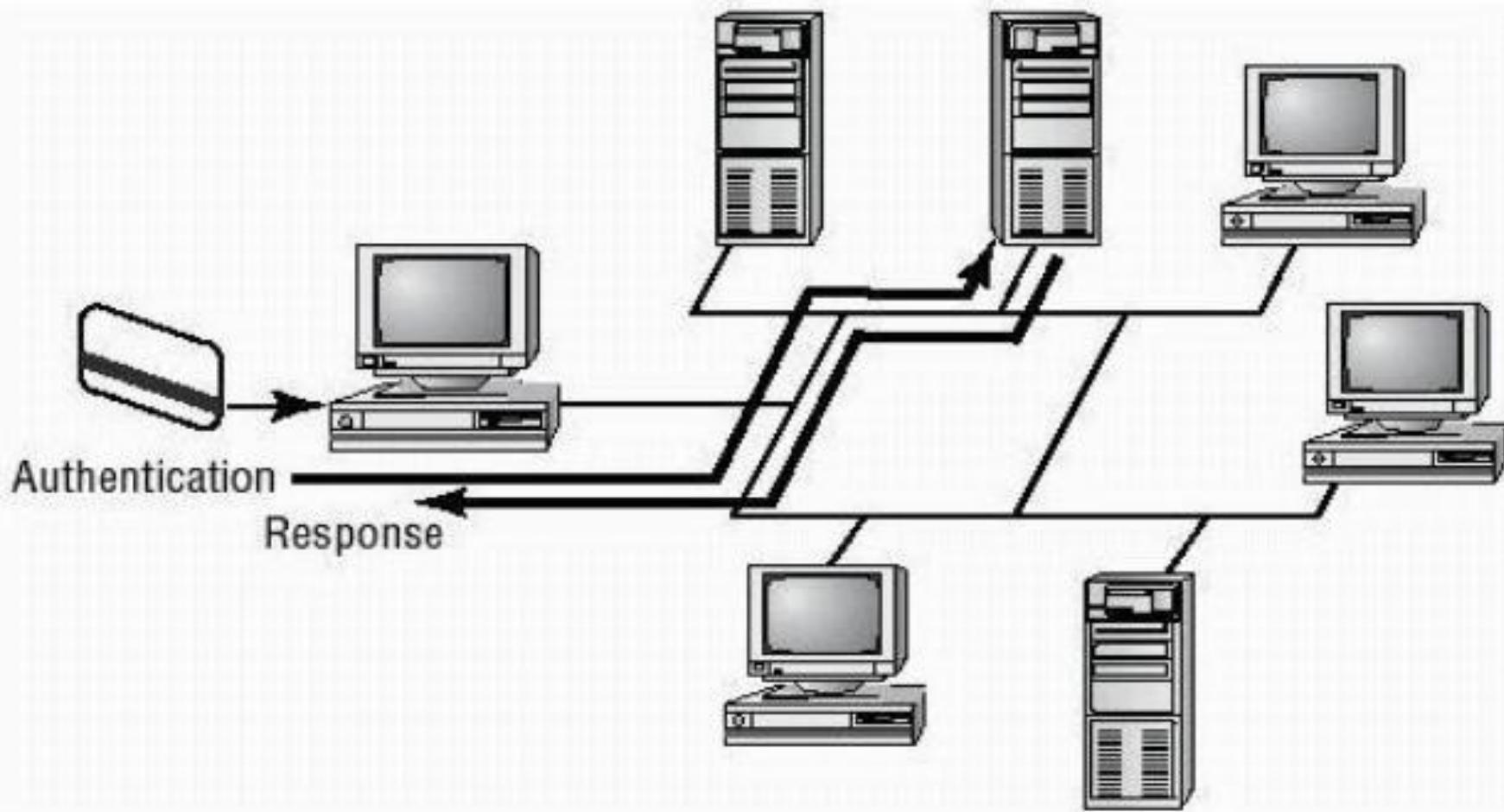
XÁC THỰC NGƯỜI DÙNG

- ❖ Xác thực là một quy trình xác minh danh hiệu của một người dùng (Chẳng hạn bằng cách so sánh mật khẩu mà người dùng đăng nhập với mật khẩu được lưu trữ trong hệ thống đối với một tên người dùng cho trước nào đó).
- ❖ Quy trình xác thực phải dựa vào một trong ba yếu tố sau đây:
 - ✓ Cái bạn biết (Something you know) – Mật mã hay số PIN.
 - ✓ Cái bạn có (Something you have) – Một card thông minh hay một thiết bị chứng thực.
 - ✓ Cái bạn sở hữu (Something you are) – dấu vân tay hay võng mạc mắt của bạn.

Những phương thức chứng thực thông dụng

- ❖ Dùng username/Password:
 - ✓ Một tên truy cập và một mật khẩu là định danh duy nhất để đăng nhập. Bạn là chính bạn chứ không phải là người giả mạo.
 - ✓ Thiết bị hoặc Server sẽ so sánh những thông tin này với những thông tin lưu trữ trong máy bằng các phương pháp xử lý bảo mật và sau đó quyết định chấp nhận hay từ chối sự đăng nhập.

Chứng thực bằng thẻ thông minh (Smart card)



Chứng thực bằng sinh trắc học

- ❖ Nhận dạng cá nhân bằng các đặc điểm riêng biệt của từng cá thể.
- ❖ Hệ thống sinh trắc học gồm các thiết bị quét tay, quét võng mạc mắt, và sắp tới sẽ có thiết bị quét DNA
- ❖ Để có thể truy cập vào tài nguyên thì bạn phải trải qua quá trình nhận dạng vật lý

CẤU HÌNH CHỨNG THỰC RIPv2

- ❖ Chứng thực trong định tuyến là cách thức bảo mật trong việc trao đổi thông tin định tuyến giữa các router.
- ❖ Nếu có cấu hình chứng thực thì các router phải vượt qua quá trình này trước khi các thông tin trao đổi định tuyến được thực hiện.
- ❖ RIPv2 hỗ trợ hai kiểu chứng thực là: “Plain text” và “MD5”

CẤU HÌNH CHỨNG THỰC PLAIN TEXT

Chứng thực dạng “Plain Text” hay còn gọi là “Clear text”

❖ Các router được cấu hình một khóa (password) và trao đổi chúng để so khớp. Các khóa này được gửi dưới dạng không mã hóa trên đường truyền.

❖ Các bước cấu hình:

❖ Bước 1. Tạo bộ khóa: Router(config)#**key chain <name>**

❖ Bước 2. Tạo các khóa

Router(config-keychain)#**key <key-id>**

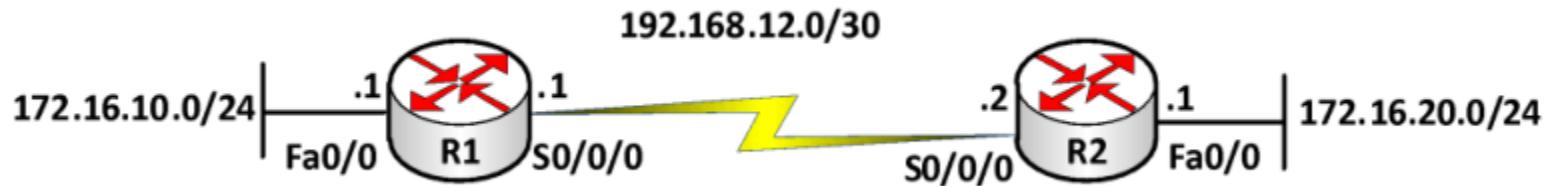
Router(config-keychain-key)#**key-string <password>**

❖ Bước 3. Áp đặt vào cổng gửi chứng thực

Router(config)#**interface <interface>**

Router(config-if)#**ip rip authentication key-chain <name>**

VÍ DỤ



```
R1(config)#key chain TLU1
```

```
R1(config-keychain)#key 1
```

```
R1(config-keychain-key)#key-string 123456
```

```
R1(config)#interface S0/0/0
```

```
R1(config-if)#ip rip authentication key-chain TLU1
```

```
R2(config)#key chain TLU2
```

```
R2(config-keychain)#key 1
```

```
R2(config-keychain-key)#key-string 123456
```

```
R2(config)#interface S0/0/0
```

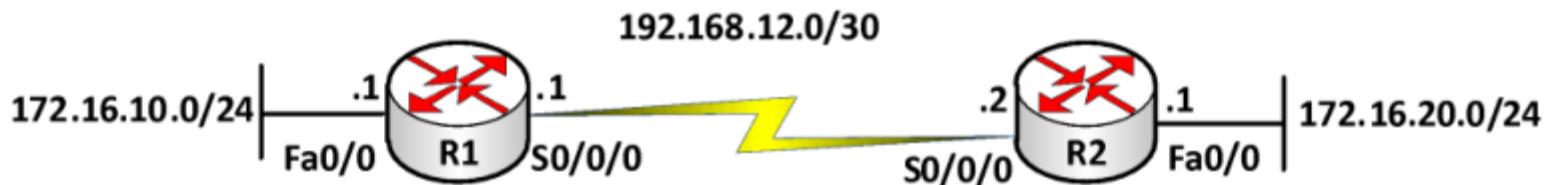
```
R2(config-if)#ip rip authentication key-chain TLU2
```

CẤU HÌNH CHỨNG THỰC MD5

- ❖ Dạng chứng thực này sẽ gửi thông tin về khóa đã được mã hóa giúp các thông tin trao đổi được an toàn hơn.
- ❖ Các bước cấu hình tương tự như dạng “Plain Text”, chỉ có khác ở bước 3 phải thêm 1 lệnh sau:

Router(config-if)#**ip rip authentication mode md5**

VÍ DỤ: Cấu hình chứng thực định tuyến RIPv2 bằng MD5 với tên bộ khóa là “tlu” và mật khẩu là “123456” trên R1 và tên bộ khóa là “cntt” và mật khẩu là “123456” trên R2



VÍ DỤ

```
R1(config)#key chain tlu
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string 123456
R1(config)#interface S0/0/0
R1(config-if)#ip rip authentication mode md5
R1(config-if)#ip rip authentication key-chain tlu
R2(config)#key chain cntt
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string 123456
R2(config)#interface S0/0/0
R2(config-if)#ip rip authentication mode md5
R2(config-if)#ip rip authentication key-chain cntt
```

CẤU HÌNH CHỨNG THỰC OSPF

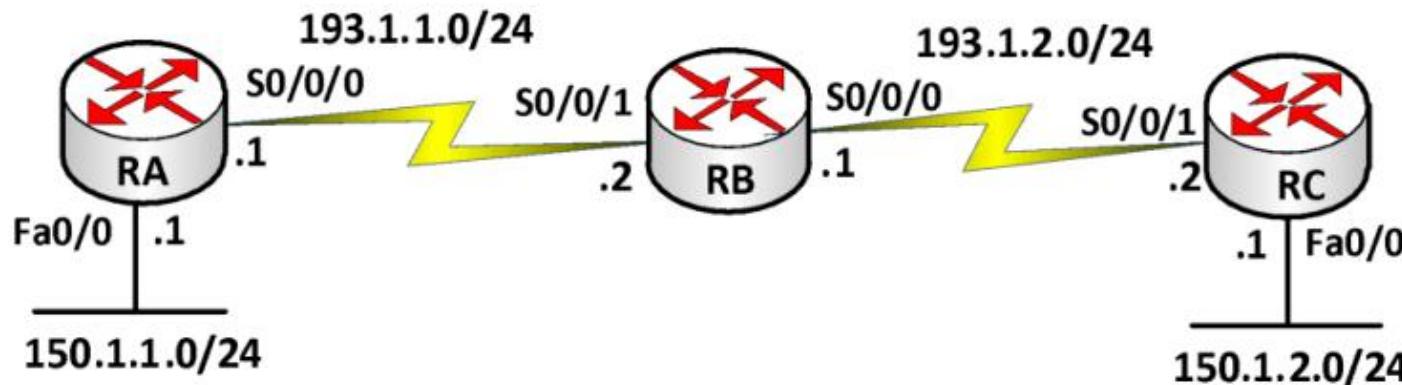
❖ Chứng thực Plain Text

- R(config)# **interface <interface>**
- R(config-if)# **ip ospf authentication**
- R(config-if)# **ip ospf authentication-key <password>**

❖ Chứng thực Bằng MD5

- R(config)# **interface <interface>**
- R(config-if)# **ip ospf authentication message-digest**
- R(config-if)# **ip ospf messages-digest-key 1 md5 <password>**

VÍ DỤ



Chứng thực dạng “Plain Text” giữa 2 router: RA và RB với mật khẩu là cisco

```
RA(config)# interface S0/0/0
```

```
RA(config-if)# ip ospf authentication
```

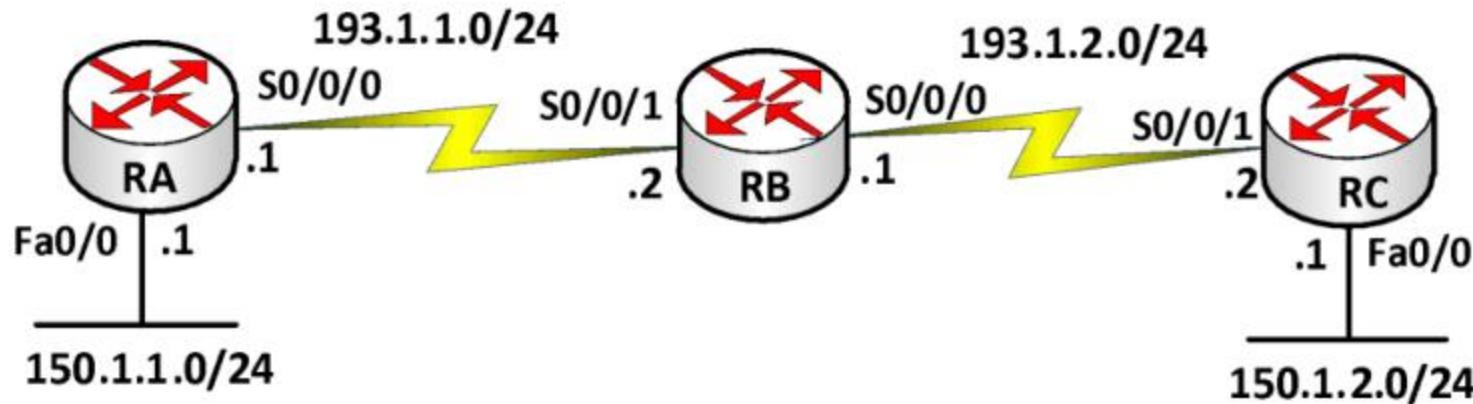
```
RA(config-if)# ip ospf authentication-key cisco
```

```
RB(config)# interface S0/0/1
```

```
RB(config-if)# ip ospf authentication
```

```
RB(config-if)# ip ospf authentication-key cisco
```

VÍ DỤ



Cấu hình chứng thực dạng MD5 giữa 2 router: RA và RB

```
RA(config)# interface S0/0/0
```

```
RA(config-if)# ip ospf authentication message-digest
```

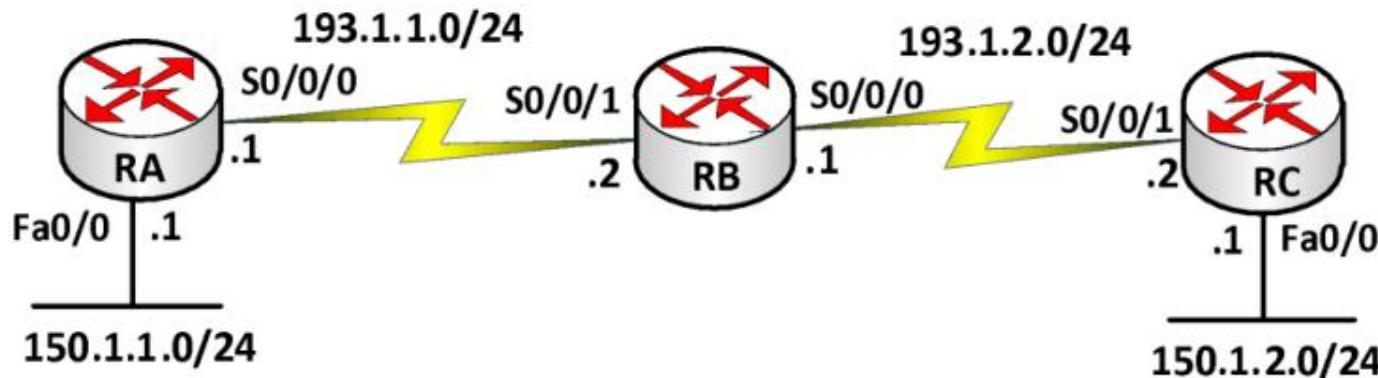
```
RA(config-if)# ip ospf message-digest-key 1 md5 cisco
```

```
RB(config)# interface S0/0/1
```

```
RB(config-if)# ip ospf authentication message-digest
```

```
RB(config-if)# ip ospf message-digest-key 1 md5 cisco
```

BÀI ÔN TẬP



Cho mạng như hình vẽ:

1. Cấu hình cơ bản các Router, cấu hình password cho các cổng và privileged với mật khẩu 123456.
2. Cấu hình giao thức (Static, RIPv2, OSPF).
3. Cấu hình ACL để thực hiện cấm mạng 150.1.2.0/24 truy cập vào mạng 150.1.1.0/24.
4. Cấu hình chứng thực (Plain text, MD5) giữa các router: với mật khẩu 123a@.

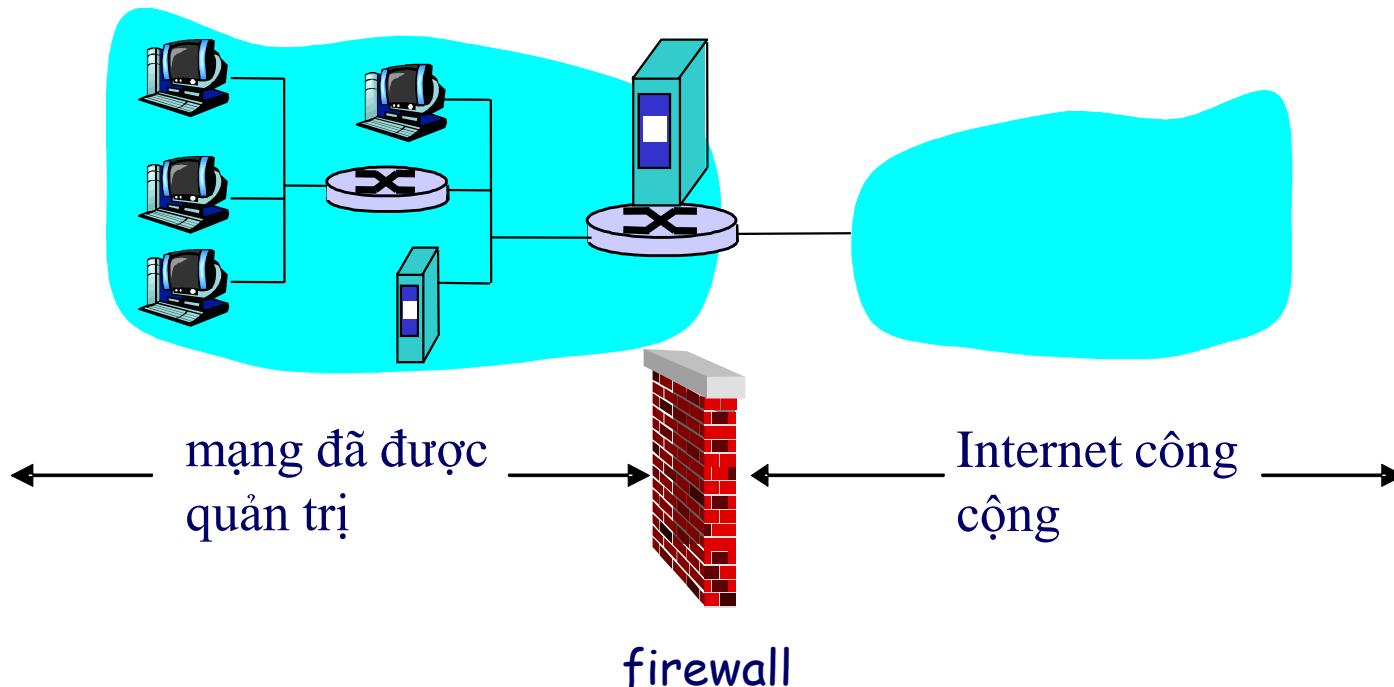
CHƯƠNG 5: BẢO MẬT MẠNG

- 1. Giới thiệu chung
- 2. Điều khiển truy cập ACL
- 3. Xác thực người dùng
- 4. Tường lửa

BÀI 4. TƯỜNG LỬA - FIREWALL

firewall

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

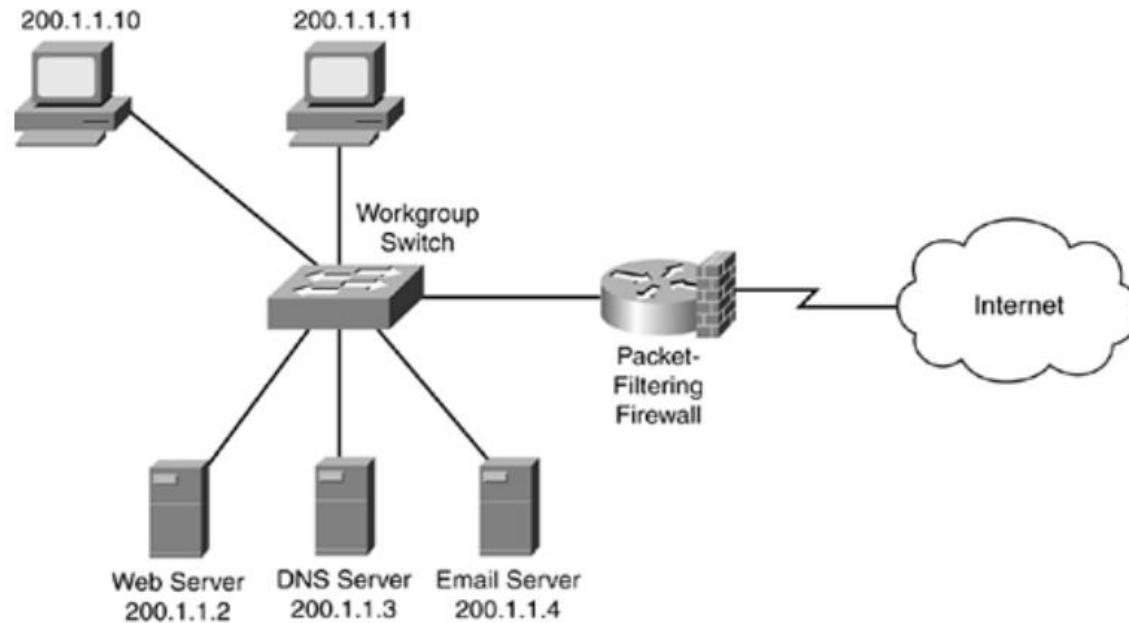


Firewall: Tại sao phải dùng?

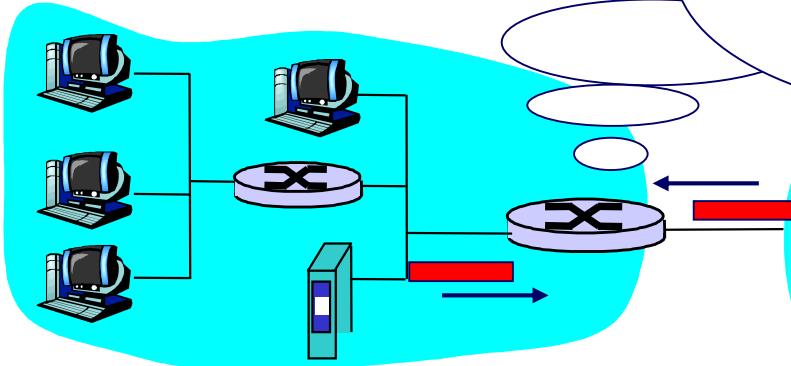
- ❖ Kiểm soát luồng thông tin từ giữa Intranet và Internet, ngăn chặn việc sửa đổi/truy cập bất hợp pháp các dữ liệu nội bộ.
- ❖ Ngăn chặn các cuộc tấn công từ bên ngoài vào mạng nội bộ: Như tấn công chối dịch vụ Denial Of Service (DoS) (SYN flooding: kẻ tấn công thiết lập nhiều kết nối TCP “ảo”, không còn tài nguyên cho các kết nối “thật”)
- ❖ 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 (application-level gateway hay proxy server)
 - Lọc gói tin (packet-filtering)

Firewall kiểu lọc gói tin

- ❖ Packet filtering “không trạng thái”: được sử dụng trên các router hoặc các OS.
- ❖ Stateful inspection packet filtering “có trạng thái”: được sử dụng trên các firewall hiện đại.



Lọc gói tin không trạng thái



Các gói đến sẽ được phép vào? Các gói chuẩn bị ra có được phép không?

- ❖ **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 không trạng thái

❖ **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.

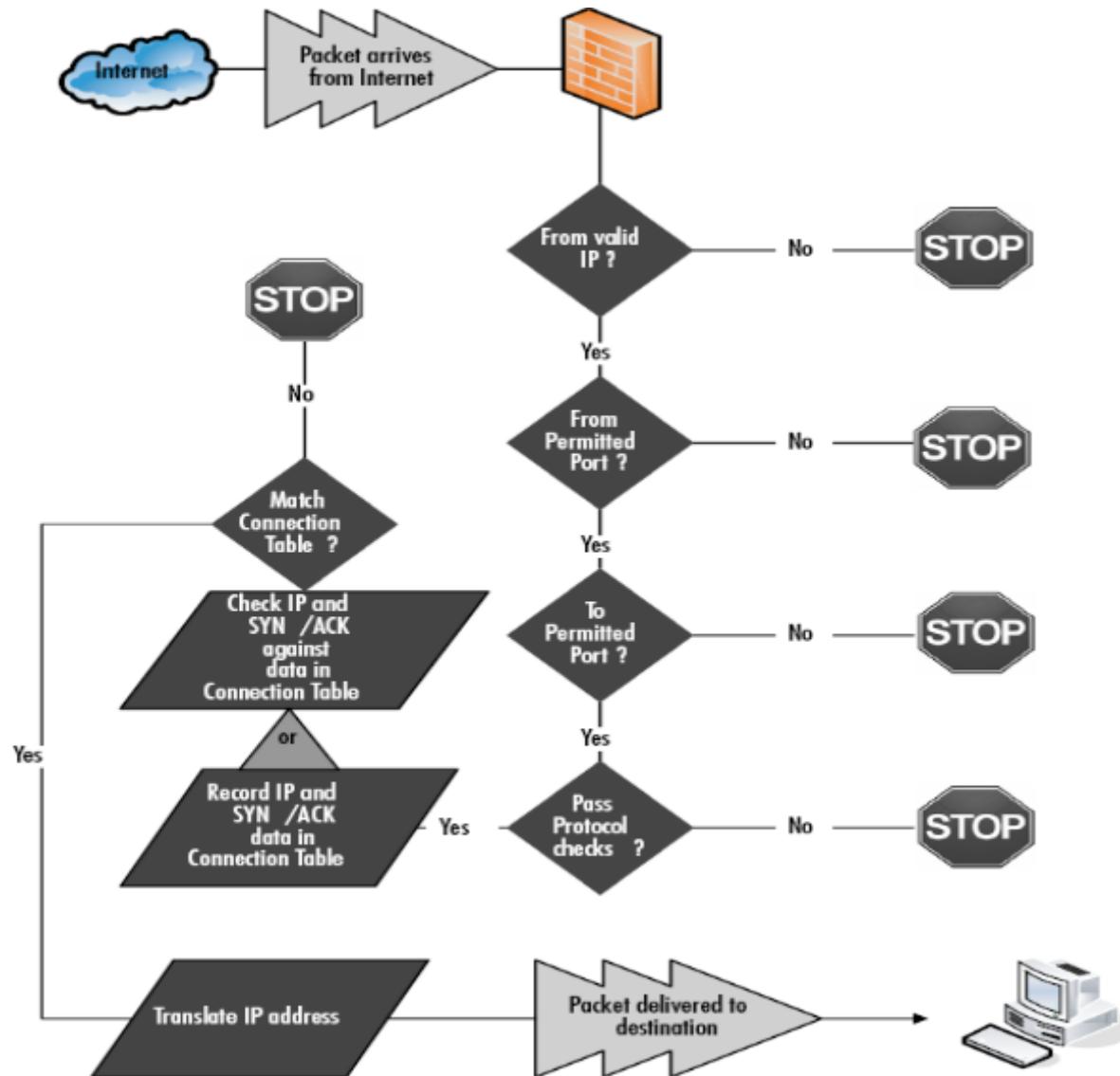
❖ **Ví dụ 2: Chặn các đoạn Block TCP với ACK=0.**

- ✓ 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.

Firewall lọc gói tin “có trạng thái”

- ❖ Firewall có trạng thái nhớ trạng thái của các kết nối tại mức mạng và phiên nhò ghi lại các thông tin thiết lập phiên mà được pass thông qua Firewall.
- ❖ Firewall có trạng thái không cho phép bất cứ dịch vụ nào thông qua firewall, ngoại trừ các dịch vụ này đã được cấu hình để cho phép và các nối đã sẵn sàng trong bảng trạng thái của chúng.

Firewall lọc gói tin “có trạng thái”



Firewall mức ứng dụng (Application level gateway)

- ❖ Kiểu firewall này hoạt động dựa trên phần mềm.
- ❖ Đây là loại Firewall được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ, giao thức được cho phép truy cập vào hệ thống mạng.
- ❖ Cơ chế hoạt động của nó dựa trên cách thức gọi là Proxy Service (dịch vụ đại diện).
- ❖ Proxy Service là các bộ mã đặc biệt được cài đặt trên cổng ứng dụng cho từng ứng dụng khác nhau.

PHÂN LOẠI FIREWALL

Có hai loại: Firewall phần cứng và Firewall phần mềm.

- ❖ ***Firewall phần cứng:*** Cung cấp mức độ bảo vệ cao hơn so với Firewall phần mềm và dễ bảo trì hơn.
 - Firewall phần cứng cũng có một ưu điểm khác là không chiếm dụng tài nguyên hệ thống trên máy tính như Firewall phần mềm.
- ❖ Ví dụ: Firewall 501, Firewall 506E, 515E, 525, 535... (Cisco)

PHÂN LOẠI FIREWALL

Có hai loại: Firewall phần cứng và Firewall phần mềm.

❖ *Firewall phần mềm*

So với Firewall phần cứng, Firewall phần mềm cho phép linh động hơn, nhất là khi cần đặt lại các thiết lập cho phù hợp hơn với nhu cầu riêng của từng công ty.

Ví dụ: ISA 2004, 2006, Comodo (client), Econpro (client)...