

❖ IPv4

## Phân loại địa chỉ IP

### ☐ Phân loại theo phạm vi hoạt động :

#### ➤ Private IP : LAN

- 10.0.0.0 → 10.255.255.254
- 172.16.0.0 → 172.31.255.254
- 192.168.0.0 → 192.168.255.254

#### ➤ Public IP : WAN

### ☐ Phân loại trong quá trình truyền thông :

#### ➤ Host

#### ➤ Network

## Địa chỉ Host

- ☐ Là địa chỉ IP có thể dùng để đặt cho các Interface
- ☐ Hai máy nằm thuộc cùng một mạng thì có **Network\_ID** giống nhau nhưng có **Host\_ID** khác nhau

## Địa chỉ Network

- ☐ Là địa chỉ IP triển khai cho các mạng, địa chỉ này không dùng để đặt cho các Card mạng
- ☐ Phần Host\_ID của địa chỉ chỉ chứa các bit 0
- ☐ Địa chỉ này không thể đặt cho các Interface

## Địa chỉ Broadcast

- ☐ Là địa chỉ IP được dùng để đại diện cho tất cả các Host trong cùng 1 Mạng
- ☐ Phần Host\_ID chỉ chứa các bit 1
- ☐ Địa chỉ này không thể đặt cho các Interface

- Phân lớp địa chỉ IP

## **Class A**

❑ Dãy địa chỉ IP hợp lệ của Class A là :

➤ **1.0.0.1 -> 126.255.255.254**

## **Class B**

❑ Dãy địa chỉ IP hợp lệ của Class B :

➤ **128.0.0.1 → 191.255.255.254**

## **Class C**

❑ Dãy địa chỉ IP hợp lệ của Class C :

➤ **192.0.0.1 → 223.255.255.254**

- Subnet

## Subnet

- ❑ Khi ta chia mạng thành các mạng nhỏ hơn, các mạng nhỏ hơn này được gọi là subnet
- ❑ Hình thức chia : Network mượn bit của Host làm Subnet

## Mặt nạ mạng (subnet mask)

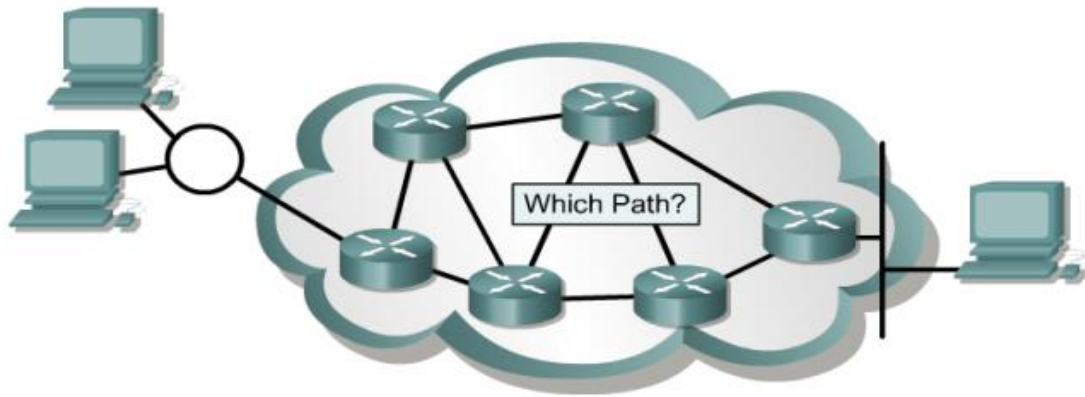
- ❑ Là 1 con số dài 32bit , là phương tiện giúp máy tính xác định được địa chỉ mạng
- ❑ Mặt nạ mạng mặc định của các lớp:
  - Lớp A: 255.0.0.0
  - Lớp B: 255.255.0.0
  - Lớp C: 255.255.255.0

## ❖ Router

### Router là gì ?

- ❑ Router là thiết bị phần cứng chuyên dụng và có các thành phần gần giống như máy tính. Nhưng Router có tính năng chuyên biệt đó là định tuyến
- ❑ Router được sử dụng để kết nối các đường mạng khác nhau.
- ❑ Router có thể phá vỡ được Broadcast Domain
- ❑ Router hoạt động ở Layer 3 và dựa vào IP Address để định tuyến gói tin
- ❑ Router là thiết bị thiết yếu trong môi trường mạng WAN

## Vai trò của Router trong mạng WAN ?



- ❑ Hai chức năng chính của Router là :
  - ❑ *Chọn lựa đường đi tốt nhất tới mạng đích*
  - ❑ *Chuyển tiếp gói tin tới Interface tương ứng với đường đi ngắn nhất*
- ❑ Router có thể làm được tốt công việc định tuyến là do sử dụng **Routing Protocol** để xây dựng **Routing Table**. Và dựa vào Routing Table để định tuyến gói tin

❖ Routing Protocol

## Định tuyến là gì ?

- ❑ Định tuyến là qui trình Router giúp vận chuyển gói tin từ Mạng Nguồn đến Mạng Đích theo ***đường đi tốt nhất***

❑ Router dựa vào đâu để chọn đường đi ?

❑ Routing Table

❑ Router dựa vào đâu để chọn đường đi tốt nhất ?

❑ Metric

- Hop Count
- Bandwidth
- Load
- Delay
- Cost
- Reliability



## Phân tích Routing Table

- ❑ **Administrative Distance** : Độ tin cậy của giao thức định tuyến

Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

Note: Administrative Distance càng nhỏ thì độ ưu tiên càng lớn

## Phân loại Định Tuyến

### ❑ Static Routing

- ❑ Người quản trị mạng phải cấu hình trên từng Router để tạo và cập nhật Routing Table

### ❑ Dynamic Routing

- ❑ Routing Table tự động tạo và cập nhật
- ❑ Cách tạo và cập nhật bảng định tuyến như thế nào là tùy thuộc từng giao thức định tuyến.
- ❑ Các giao thức định tuyến thông dụng : RIPv1, RIPv2, IGRP, EIGRP, OSPF, IS-IS, BGP

## Static Routing

### Phân loại Định Tuyến

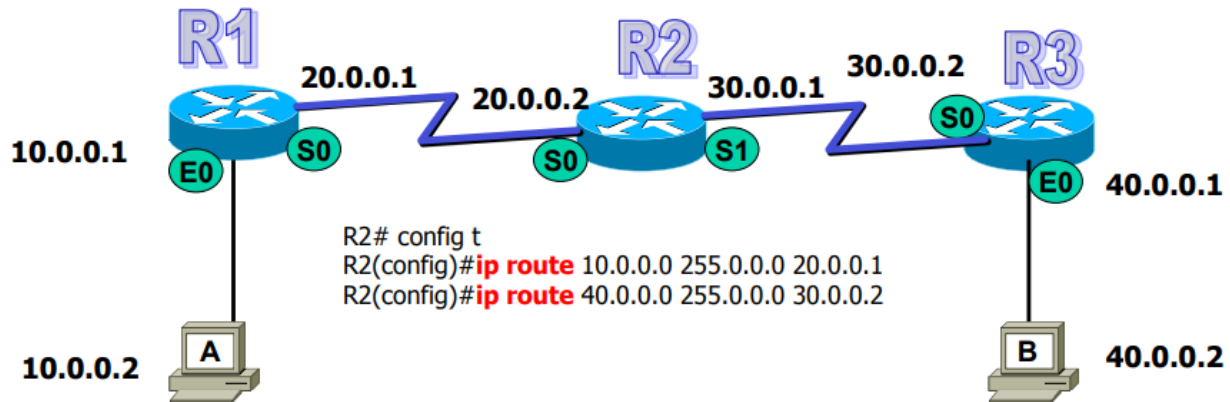
```
ip route [destination_network] [mask] [next-hop_address or exitinterface]  
[administrative_distance] [permanent]
```

- ❑ **ip route** : câu lệnh tạo ra static routing
- ❑ **Destination\_network** : mạng đích
- ❑ **Mask** : subnet mark của destination network
- ❑ **Next-hop\_address** : địa chỉ ip của next-hop Router
- ❑ **Exitinterface** : tên của Interface trên Router mà gói tin sẽ được chuyển ra interface này để tới destination network
- ❑ **Administrative\_distance** : mặc định

## Static Routing - LAB

### Phân loại Định Tuyến

- ❑ Cấu hình IP Route



R1# config t  
R1(config)#ip route 30.0.0.0 255.0.0.0 20.0.0.2  
R1(config)#ip route 40.0.0.0 255.0.0.0 20.0.0.2

R3# config t  
R3(config)#ip route 10.0.0.0 255.0.0.0 30.0.0.1  
R3(config)#ip route 20.0.0.0 255.0.0.0 30.0.0.1

## Default Routing

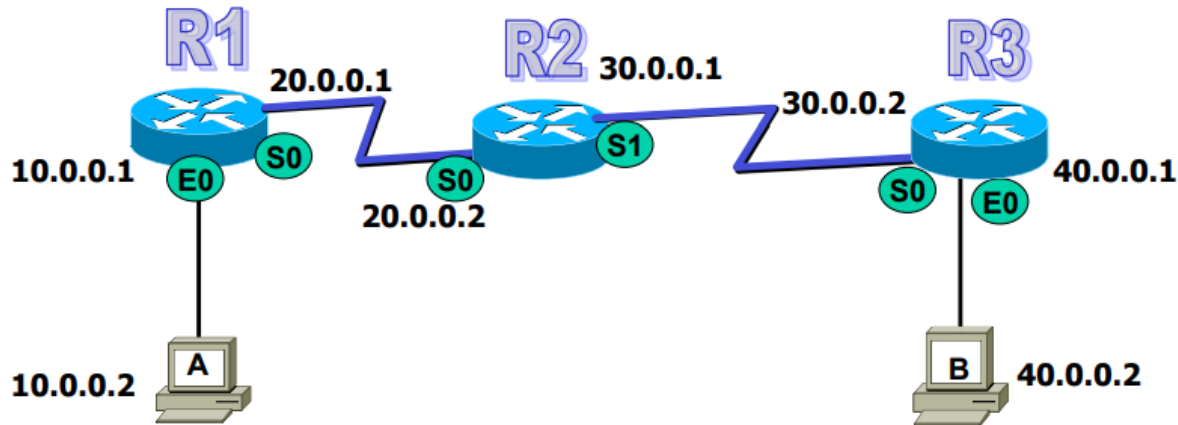
### Phân loại Định Tuyến

- ❑ Được sử dụng để định tuyến gói tin tới Destination Network, khi không có câu lệnh Route nào trong bảng Routing Table phù hợp với Destination Network
- ❑ Cấu trúc câu lệnh default route
  - ❑ **ip route 0.0.0.0 0.0.0.0** [*next-hop-address* | *outgoing interface*]
- ❑ Ví dụ sử dụng next-hop-address để cấu hình :
  - ❑ Router(config)#**ip route 0.0.0.0 0.0.0.0 172.16.4.1**
- ❑ Ví dụ sử dụng outgoing interface để cấu hình :
  - ❑ Router(config)#**ip route 0.0.0.0 0.0.0.0 s0/0**

# Default Routing

## Phân loại Định Tuyến

- Cấu hình Default Route



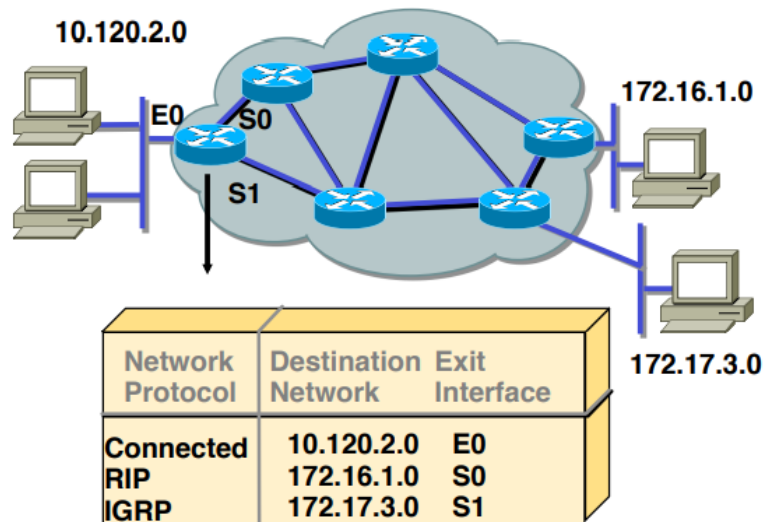
```
R2# config t
R2(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1
R2(config)#ip route 40.0.0.0 255.0.0.0 30.0.0.2
```

```
R1# config t
R1(config)#ip route 0.0.0.0 0.0.0.0 20.0.0.2
```

```
R3# config t
R3(config)#ip route 0.0.0.0 0.0.0.0 30.0.0.1
```

## Routing Protocol là gì ?

- **Routing Protocol** là giao thức được sử dụng để tạo và cập nhật bảng định tuyến một cách tự động.
- Hay nói cách khác, Routing Protocol là giao thức được sử dụng để tìm đường đi giữa các Router



## **Phân loại Routing Protocol**

### **❑ Distance Vector**

- ❖ RIP V1
- ❖ IGRP
- ❖ RIP V2

### **❑ Link state**

- ❖ OSPF

### **❑ Hybrid**

- ❖ EIGRP

## Phân loại Routing Protocol

- ❑ Classful Routing : không chứa subnet mark trong câu lệnh quảng bá định tuyến
  - ❑ RIPv1
  - ❑ IGRP
- ❑ Classless Routing : chứa subnet mark trong câu lệnh quảng bá định tuyến
  - ❑ RIPv2
  - ❑ EIGRP
  - ❑ OSPF
  - ❑ IS-IS
- ❑ Trong cùng 1 network, mặc định subnet mark sẽ bị summary

# Distance Vector Routing Protocol

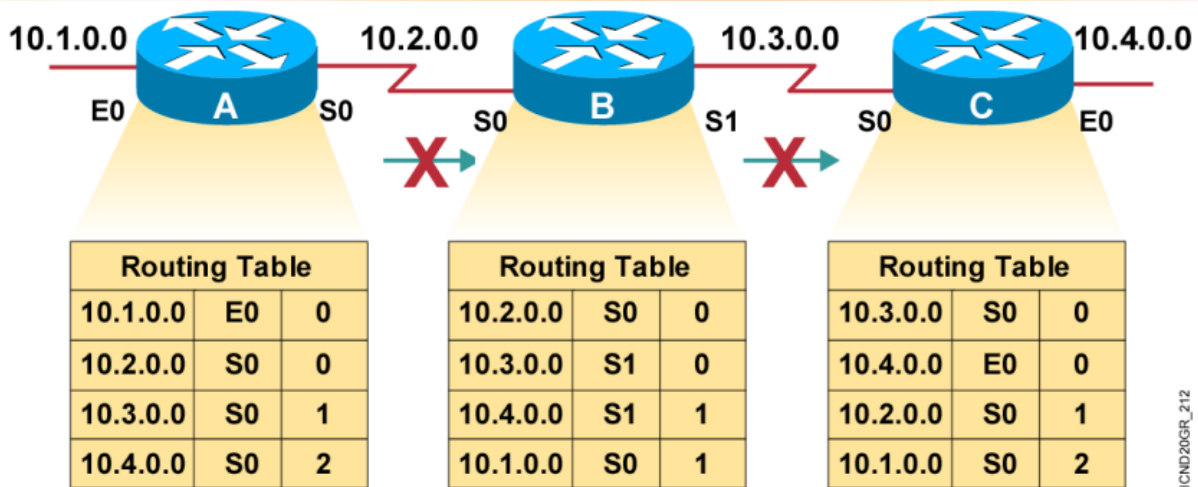
- ❑ Distance vector routing protocol là gì ?
- ❑ Quá trình cập nhật và trao đổi bảng định tuyến ?
- ❑ Routing loop
- ❑ Cách khắc phục loop :
  - ❑ Holddown
  - ❑ Split Horizone
  - ❑ Routing Poisoning
  - ❑ Trigged update

## Holddown Timer

- ❑ Khi có sự thay đổi về các Network mà Router quản lý, Router sẽ cập nhật thông tin này và gửi thông tin bảng định tuyến của nó cho Router lân cận, đồng thời bật **Timer**
- ❑ **Timer** là khoảng thời gian mà Router sẽ ko nhận thông tin định tuyến của các Router láng giềng của nó về Network mà nó vừa thông báo bị thay đổi

## Split Horzone

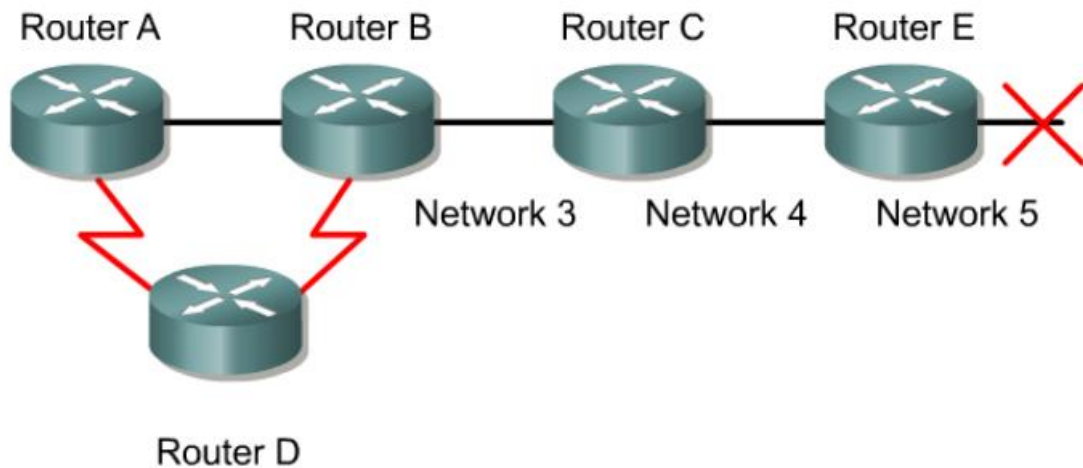
Distance Vector Routing Protocol / Routing Loop



ICND20GR\_212

- ❑ Router không được gửi thông tin định tuyến ra interface mà nó học thông tin định tuyến từ interface đó

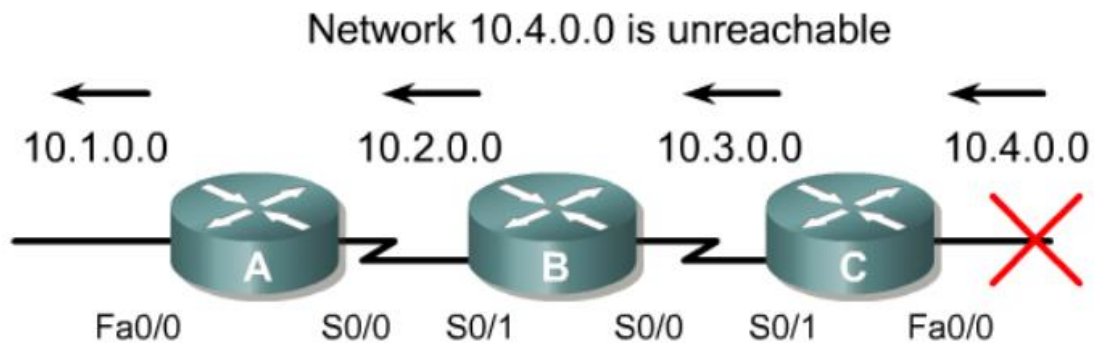
## Routing Poisoning



When Network 5 goes down, Router E initiates route poisoning by entering a table entry metric of 16 (unreachable).



## Triggered Update



## Distance Vector Routing Protocol

- ❑ Distance Vector Routing Protocol mô tả cách thức các Router
  - ❑ Tạo bảng định tuyến
  - ❑ Cập nhật bảng định tuyến
  - ❑ Trao đổi **bảng định tuyến** với các Router láng giềng
- ❑ Những đặc điểm chính :
  - ❑ Cập nhật thông tin định tuyến theo định kỳ
  - ❑ Trao đổi thông tin định tuyến với Router láng giềng
  - ❑ Toàn bộ bảng định tuyến được trao đổi với Router láng giềng

## **Quá trình cập nhật bảng định tuyến của Router**

### **Distance Vector Routing Protocol**

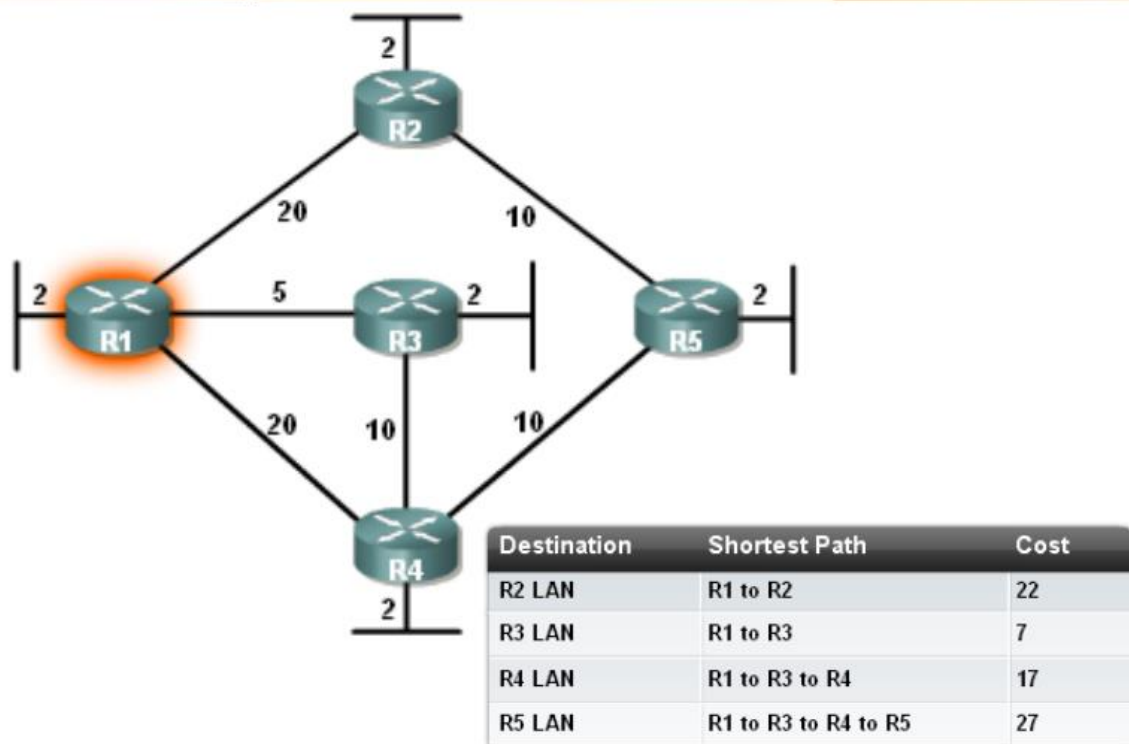
- ❑ Router cập nhật bảng định tuyến theo định kỳ hoặc khi cấu trúc mạng có sự thay đổi.
- ❑ Khi cập nhật bảng định tuyến của mình xong, Router sẽ gửi toàn bộ thông tin Bảng Định Tuyến của mình đến các Router lân cận.
- ❑ Các Router lân cận tiếp nhận và cập nhật thông tin Bảng Định Tuyến của mình và tiếp tục gửi cho các Router lân cận.
- ❑ Quá trình được tiếp tục .....

# Link-State Routing Protocol

- ❑ **Link-State Routing Protocol** mô tả cách thức các Router :
  - ❑ Tạo bảng định tuyến
  - ❑ Cập nhật bảng định tuyến
  - ❑ Trao đổi **thông tin định tuyến** với tất cả Router
- ❑ Những đặc điểm chính :
  - ❑ Cập nhật thông tin định tuyến khi có sự thay đổi về cấu trúc mạng
  - ❑ Trao đổi thông tin định tuyến với tất cả Router
  - ❑ Dựa vào Thuật toán Dijkstra và thông tin định tuyến để xác định đường đi ngắn nhất

## Shortest Path First (SPF)

### Link-State Routing Protocol



## Quy trình xử lý của Link-State Routing Protocol

### Link-State Routing Protocol

- 1) Mỗi Router sẽ “học” những Network kết nối trực tiếp với nó
- 2) Mỗi Router sẽ gửi gói tin “Hello” đến những Router kết nối trực tiếp với nó
- 3) Mỗi Router sẽ xây dựng Link-State Packet (LSP) chứa đựng trạng thái của mỗi Link kết nối trực tiếp với nó.
  - 1) Neighbor ID, Link Type và Bandwidth
- 4) Mỗi Router sẽ gửi LSP đến tất cả các Router
- 5) Mỗi Router dựa vào cơ sở dữ liệu nhận được từ Router lân cận để xây dựng cấu trúc của mạng và tìm đường đi ngắn nhất dựa trên cấu trúc mạng vừa xây dựng

## Link và Link-State

❑ **Link-State** : những thông tin trạng thái của Link

- ❑ IP Address của Interface và Subnet mask
- ❑ Loại Network : Ethernet , Serial
- ❑ Cost của Link
- ❑ Tên Router láng giềng kết nối thông qua Link này

## ❖ Routing Information Protocol

### Đặc điểm của RIPv1

#### RIPv1

- ❑ Distance Vector (DV) Routing Protocol
- ❑ Classful routing protocol
- ❑ Metric = Hop Count
  - ❑ Max = 15 Hops
- ❑ Không hỗ trợ VLSM
- ❑ Cập nhật và gửi thông tin định tuyến cho Router láng giềng theo chu kỳ 30s
- ❑ Administrative Distance of RIP is 120

# Cơ chế hoạt động của RIPv1

## RIPv1

❑ RIPv1 sử dụng 2 loại message :

❑ Request Message :

- Được gửi đi mỗi khi Router khởi động
- Chỉ được gửi trên interface bật RIP
- Gửi yêu cầu đến tất cả các Router láng giềng đang chạy giao thức RIP về thông tin định tuyến

❑ Response Message :

- Nội dung bảng định tuyến được gửi đến Requesting Router

## Passive Interface

❑ Khi Interface trên Router được bật tính năng Passive Interface thì Interface đó chỉ có **khả năng nhận thông tin định tuyến và không có khả năng gửi thông tin định tuyến**

## Đặc điểm của RIPv2

### RIPv2

- ❑ Distance Vector (DV) Routing Protocol
- ❑ Classless routing protocol
- ❑ Metric = Hop Count
  - ❑ Max = 15 Hops
- ❑ Hỗ trợ VLSM
- ❑ Cập nhật và gửi thông tin định tuyến cho Router láng giềng theo chu kỳ 30s
- ❑ Administrative Distance of RIP is 120

## Cơ chế hoạt động của RIPv2

### RIPv2

- ❑ RIPv2 sử dụng 2 loại message :
  - ❑ Request Message :
    - Được gửi đi mỗi khi Router khởi động
    - Chỉ được gửi trên interface bật RIP
    - Gửi yêu cầu đến tất cả các Router láng giềng đang chạy giao thức RIP về thông tin định tuyến
  - ❑ Response Message :
    - Nội dung bảng định tuyến được gửi đến Requesting Router

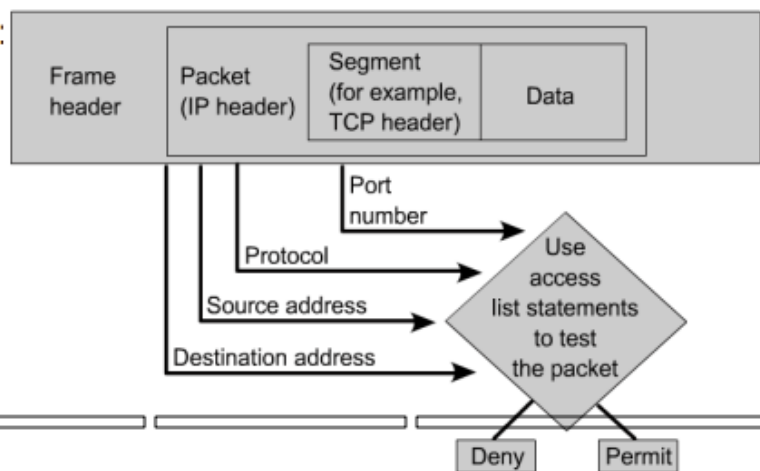
## ❖ Access Control List



## Access Control List (ACL) là gì ?

- ❑ ACL là một danh sách các điều kiện mà Router/Switch L3 dùng để kiểm tra khi gói tin đi qua một cổng của Router/Switch L3. ACL áp lên interface của thiết bị.
- ❑ Danh sách các điều kiện này cho Router biết loại gói tin nào được chấp nhận hay từ chối dựa trên các điều kiện cụ thể
- ❑ Các điều kiện của ACL :

- ❑ Địa chỉ Nguồn
- ❑ Địa chỉ Đích
- ❑ Giao thức
- ❑ Port



Nguyễn Duy

## Access Control List (ACL) là gì ?



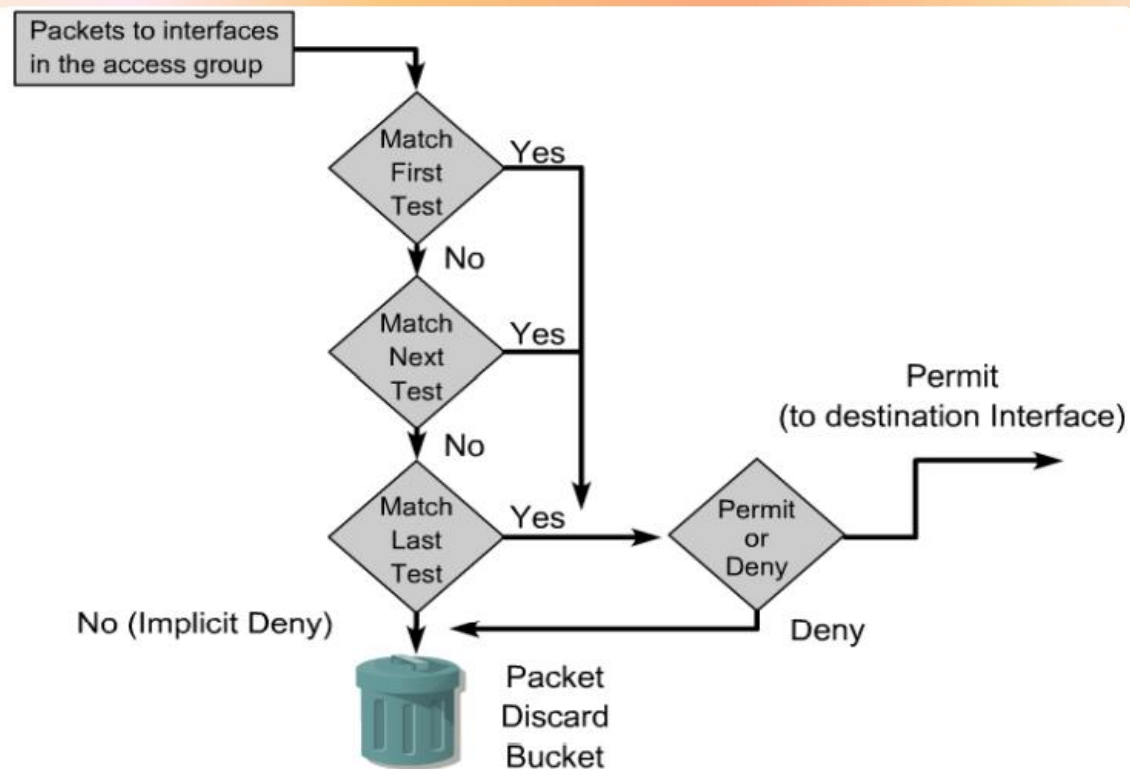
One list, per port, per direction, per protocol

With two interfaces and three protocols running, this router could have a total of 12 separate ACLs applied.

## Nguyên nhân tạo ra ACL

- ❑ Giới hạn lưu lượng mạng để tăng hiệu suất hoạt động của mạng
- ❑ Quyết định loại gói tin nào được phép cho qua hay chặn lại :
  - ❑ Host : Cho phép hay từ chối không cho truy cập vào một khu vực nào đó trong hệ thống mạng
  - ❑ Cho phép người quản trị điều khiển được phạm vi mà Host được quyền truy cập
  - ❑ .....

## Cơ chế hoạt động của ACL



## Cơ chế hoạt động của ACL

- ❑ Khi gói tin đi vào hay đi ra 1 cổng nào đó trên Router. Router sẽ dựa vào ACL để kiểm tra gói tin đó để quyết định cho qua hay drop gói tin.
- ❑ Gói tin sẽ được kiểm tra theo thứ tự của các điều kiện
- ❑ Khi kiểm tra phù hợp các thông số : Địa chỉ IP, Giao thức, Port sau đó Router kiểm tra tới điều kiện cho phép hay hủy bỏ gói tin
- ❑ Luôn luôn tồn tại 1 điều kiện cấm tất cả ở cuối danh sách điều kiện

## Phân loại ACL

❑ ACL chia thành 3 loại :

- ❑ Standard ACL
- ❑ Extended ACL
- ❑ Named ACL

Access List Type		Number Range/Identifier
IP	Standard	1-99, 1300-1999
	Extended	100-199, 2000-2699
	Named	Name

ICND20GR\_57

## Standard ACL

❑ Chỉ có thể lọc gói tin dựa vào địa chỉ nguồn của gói tin

```
Router(config)#access-list access-list-number {deny | permit}  
source [source-wildcard]
```

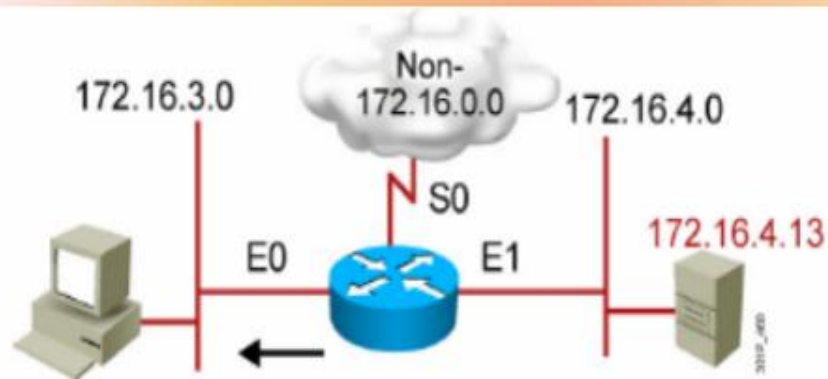
.....

```
Router(config-if)#{protocol} access-group access-list-number  
{in | out}
```

❑ Hủy một ACL:

```
Router(config)#no access-list access-list-number
```

## Standard ACL – Tạo

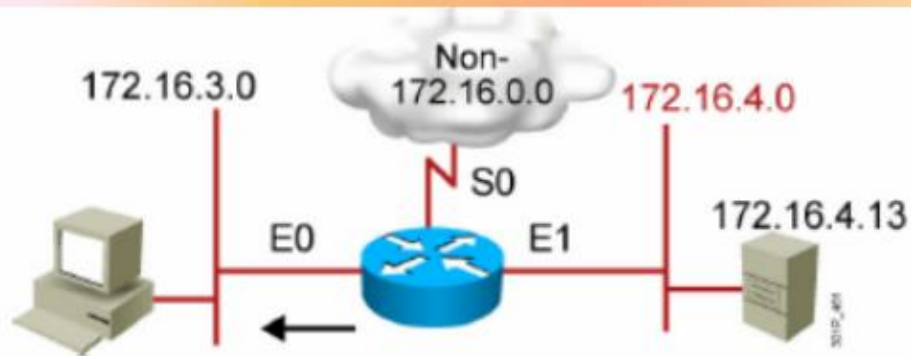


```
RouterX(config)# access-list 1 deny 172.16.4.13 0.0.0.0
RouterX(config)# access-list 1 permit 0.0.0.0 255.255.255.255
(implicit deny all)
(access-list 1 deny 0.0.0.0 255.255.255.255)

RouterX(config)# interface ethernet 0
RouterX(config-if)# ip access-group 1 out
```

Cấm một host truy cập

## Standard ACL – Tạo



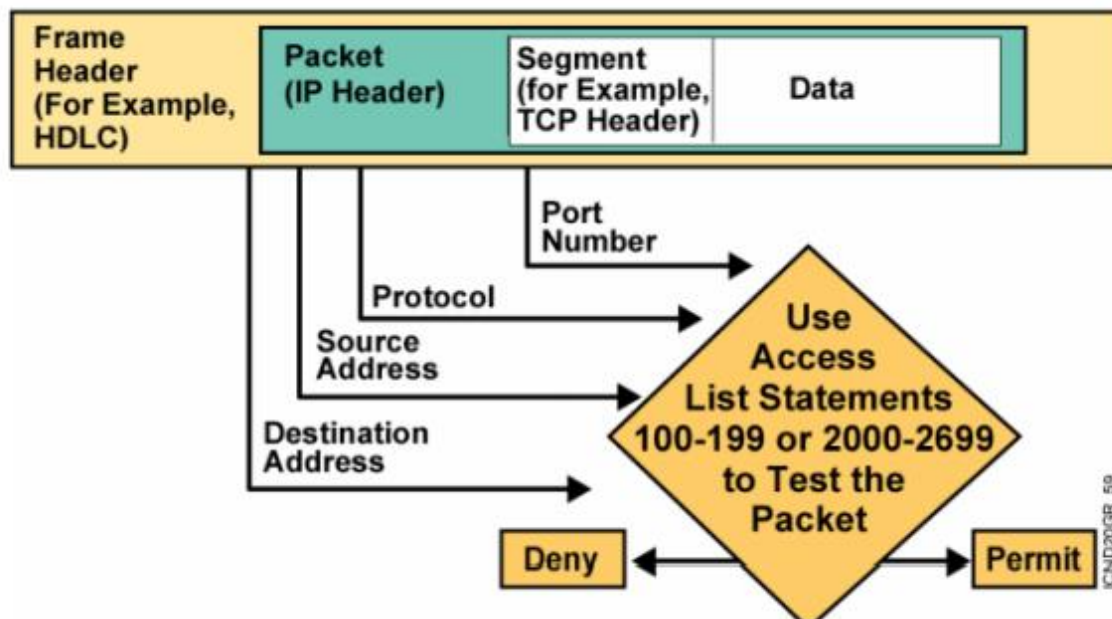
```
RouterX(config)# access-list 1 deny 172.16.4.0 0.0.0.255
RouterX(config)# access-list 1 permit any
(implicit deny all)
(access-list 1 deny 0.0.0.0 255.255.255.255)

RouterX(config)# interface ethernet 0
RouterX(config-if)# ip access-group 1 out
```

Cấm một mạng con truy cập

## Extended ACL

- Có thể lọc được : Địa chỉ nguồn, Địa chỉ đích, Giao thức và Port



## Extended ACL – Tạo

RouterX(config) #

```
access-list access-list-number {permit | deny}  
protocol source source-wildcard [operator port]  
destination destination-wildcard [operator port]  
[established] [log]
```

- Thiết lập các thông số cho dòng khai báo này

RouterX(config-if) #

```
ip access-group access-list-number {in | out}
```

- Kích hoạt ACL mở rộng trên cổng kết nối



## Extended ACL – Tạo

**Access-list-number** : Chỉ ra danh sách kiểm tra có số nằm trong khoảng từ 100 đến 199 hoặc từ 2000 đến 2699

**Permit | deny** : Chỉ ra dòng khai báo này cho phép hay từ chối gói tin

**Protocol** : IP, TCP, UDP, ICMP, GRE hoặc IGRP

**Source and destination**: Chỉ ra địa chỉ ip nguồn và đích

**Source-wildcard and destination-wildcard** : Mặt nạ wildcard ; 0 chỉ ra phần địa chỉ phải kiểm tra sự phù hợp , 1 chỉ ra phần không cần phải kiểm tra

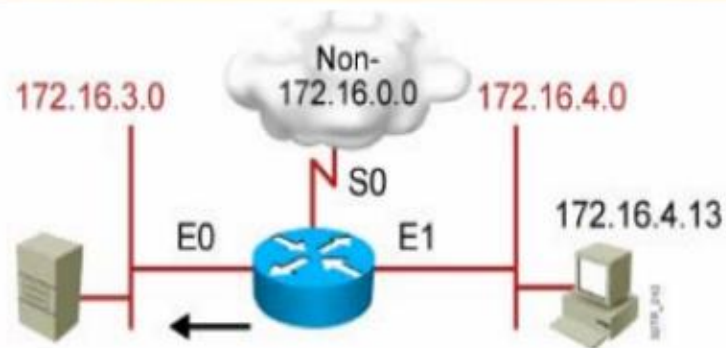
**Operator [ port | app-name ]** : thông số này có thể là Lt ( nhỏ hơn ) , gt ( lớn hơn ) và eq ( bằng ) , neq ( không bằng ) . Số cổng ứng dụng có thể là nguồn hoặc đích , tùy thuộc vào vị trí cấu hình trong ACL . Để thay thế cho số port ứng dụng , có thể sử dụng tên cho các ứng dụng quen thuộc như là Telnet , FTP , SMTP , vv

**Established** : Chỉ sử dụng cho giao thức TCP theo chiều vào . Cho phép các gói tin TCP đi qua khi gói tin này là gói trả lời phiên làm việc khởi tạo từ bên ngoài . Loại gói tin này có bit ACK ( xem phần ví dụ extended ACL với từ khóa Established )

**Log** : lưu lại nhật kí lên màn hình console



## Extended ACL – VD1

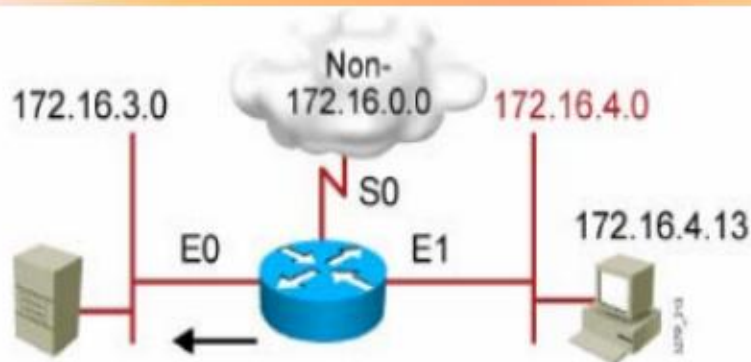


```
RouterX(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
RouterX(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
RouterX(config)# access-list 101 permit ip any any
(implicit deny all)
(access-list 101 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255)

RouterX(config)# interface ethernet 0
RouterX(config-if)# ip access-group 101 out
```

- Cấm dữ liệu FTP đi từ mạng 172.16.4.0 qua 172.16.3.0 ra khỏi E0
- Cho phép tất cả dữ liệu còn lại

## Extended ACL – VD2



```
RouterX(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 any eq 23
RouterX(config)# access-list 101 permit ip any any
(implicit deny all)

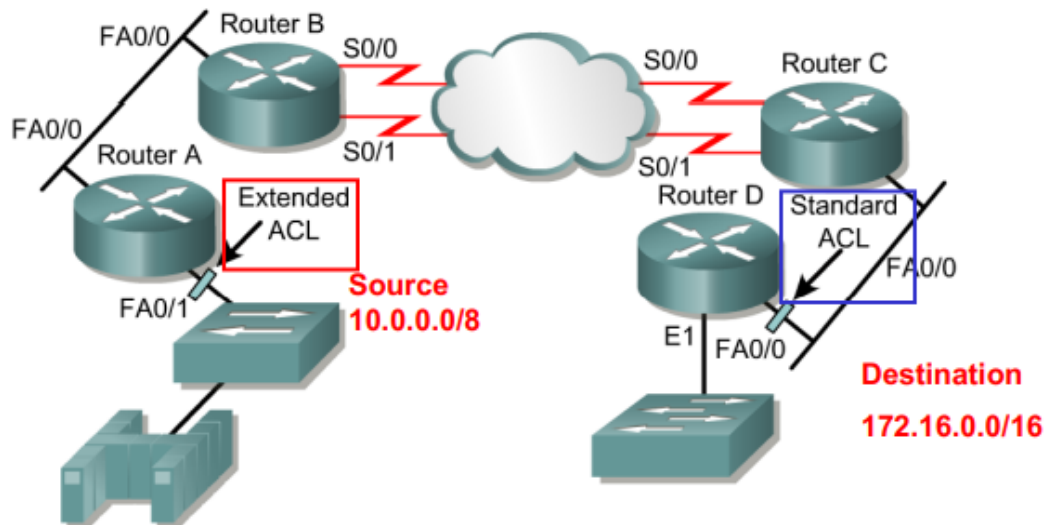
RouterX(config)# interface ethernet 0
RouterX(config-if)# ip access-group 101 out
```

- Cấm dữ liệu telnet từ mạng 172.16.4.0 ra E0
- Cho phép tất cả các dữ liệu còn lại

## Nguyên tắc khi tạo ACL

- ❑ **Một ACL** cho **một giao thức** trên **một chiều** của **một cổng**
- ❑ ACL cơ bản nên đặt ở vị trí gần mạng đích nhất có thể
- ❑ ACL nâng cao nên đặt ở vị trí gần mạng nguồn nhất có thể
- ❑ Đứng trong Router để xác định chiều ra hay chiều vào trên một cổng nào đó của gói tin
- ❑ Các câu lệnh ACL sẽ được kiểm tra từ trên xuống dưới cho tới khi một câu lệnh nào đó được thỏa
- ❑ Có một câu lệnh từ chối tất cả nằm ở cuối danh sách. Câu lệnh này không hiển thị trong danh sách
- ❑ Các câu lệnh nên được xếp theo thứ tự từ chi tiết tổng thể. Ví dụ : Host xét trước và Network xét sau

## Vị trí đặt ACLs



- ❑ Standard ACL : càng gần mạng đích càng tốt và theo chiều out
- ❑ Extended ACL : càng gần mạng nguồn càng tốt và theo chiều in

## ❖ Network Address Translation

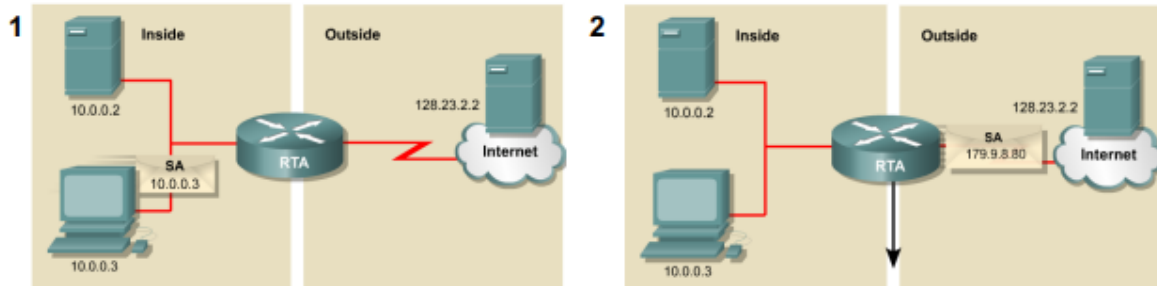
### Khái niệm về NAT

- ❑ Được thiết kế để tiết kiệm địa chỉ IP và cho phép mạng nội bộ sử dụng địa chỉ IP riêng
- ❑ Địa chỉ IP riêng sẽ được chuyển đổi thành địa chỉ công cộng và được định tuyến trên các thiết bị liên mạng
- ❑ Mạng riêng tách biệt và giấu địa chỉ IP nội bộ
- ❑ NAT thường được sử dụng trên Router biên

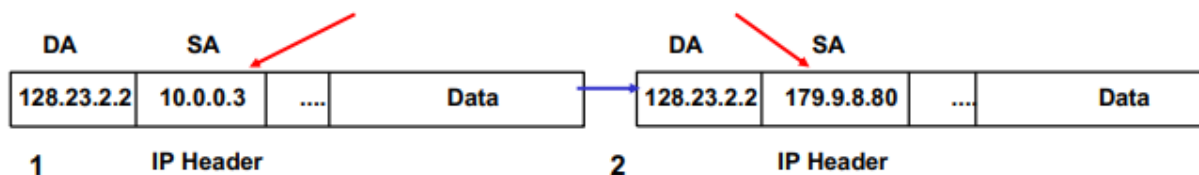
### Khái niệm về NAT

- ❑ Các thuật ngữ NAT được định nghĩa trong Cisco :
  - ❑ **Địa chỉ cục bộ bên trong (Inside local address)** : là địa chỉ IP của các Host trong mạng nội bộ
  - ❑ **Địa chỉ toàn cục bên trong (Inside global address)** : là địa chỉ IP của mặt ngoài Router ADSL được cấp bởi nhà cung cấp dịch vụ
  - ❑ **Địa chỉ cục bộ bên ngoài (Outside local address)** : là địa chỉ IP của các Host nằm ngoài mạng cục bộ
  - ❑ **Địa chỉ toàn cục bên ngoài (Outside global address)** : là địa chỉ IP công cộng của các Host nằm bên ngoài mạng cục bộ

## Khái niệm về NAT



NAT Table		
Inside Local IP Address	Inside Global IP Address	Outside Global IP Address
10.0.0.3	179.9.8.80	128.23.2.2



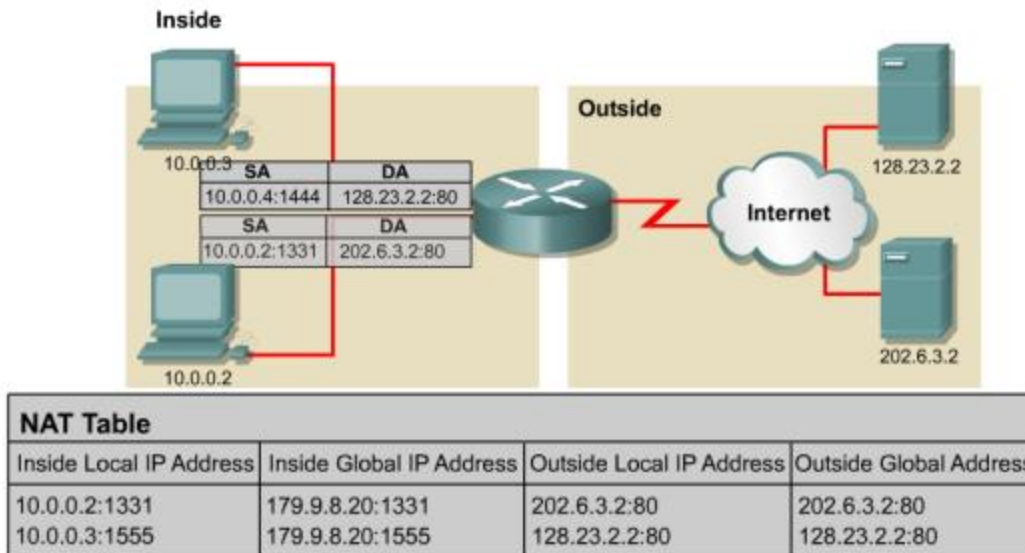
Chuyển đổi từ **Private source IP address** sang **Public source IP address**

## Dynamic NAT

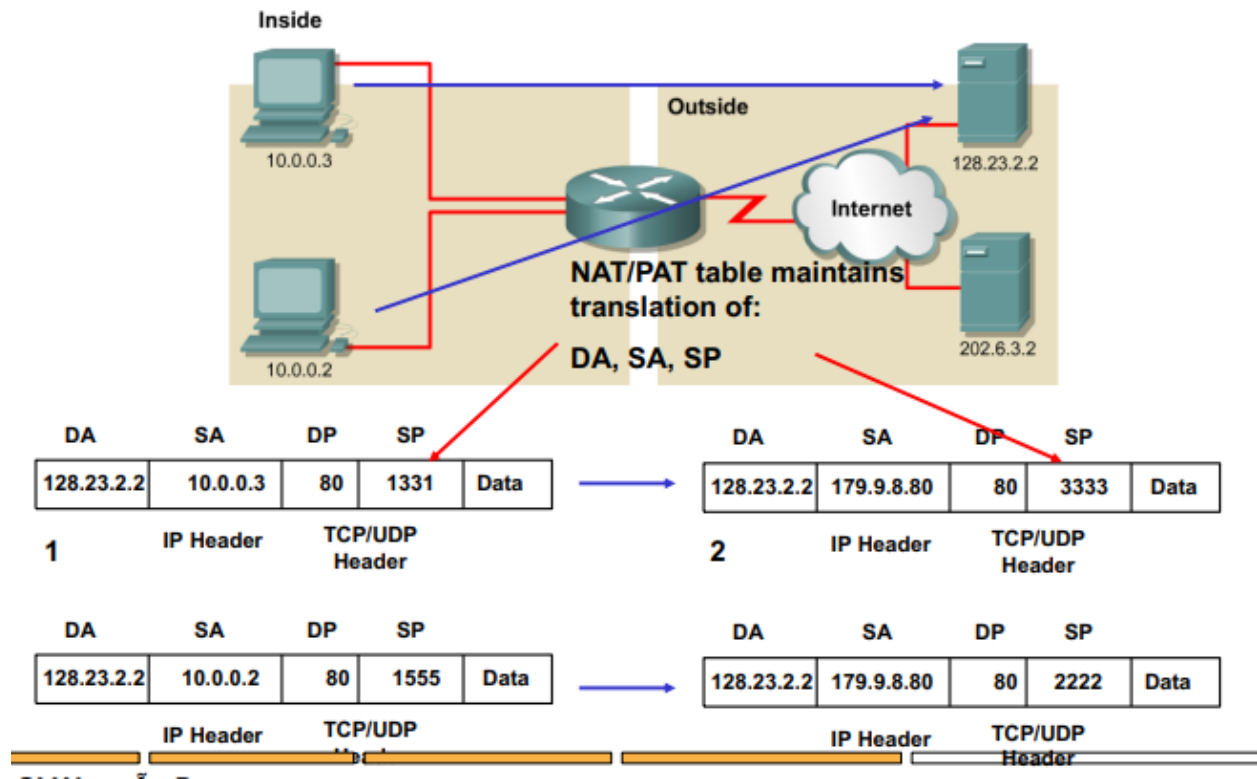
- ❑ **NAT động** được thiết kế để ánh xạ một địa chỉ IP riêng sang một địa chỉ công cộng một cách tự động. Bất kỳ địa chỉ IP nào nằm trong dải địa chỉ IP công cộng đã được định trước đều có thể được gán cho một host bên trong mạng

## Port Address Translation (PAT)

- ❑ Overloading hoặc PAT (Port Address Translation) có thể ánh xạ nhiều địa chỉ IP riêng sang **một địa chỉ IP công cộng**, mỗi địa chỉ riêng được phân biệt bằng số port.

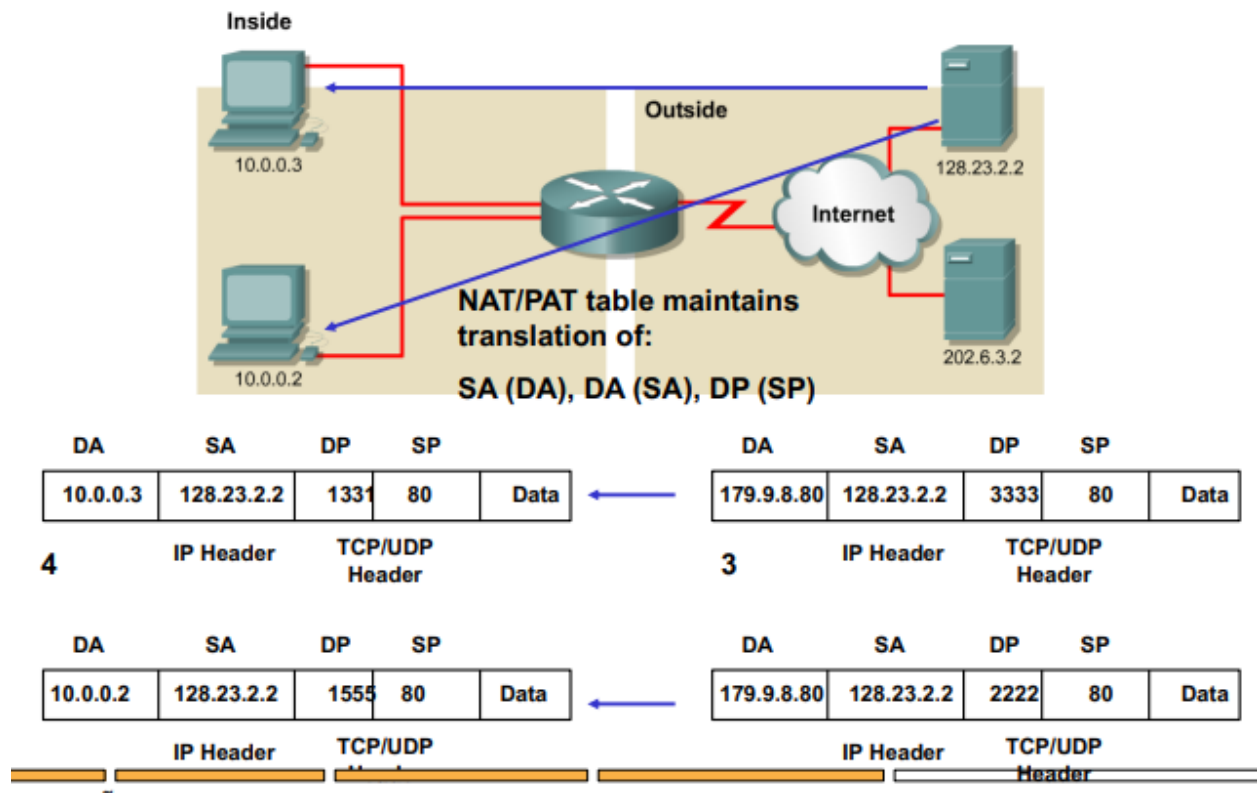


## Port Address Translation (PAT) \_ VD1



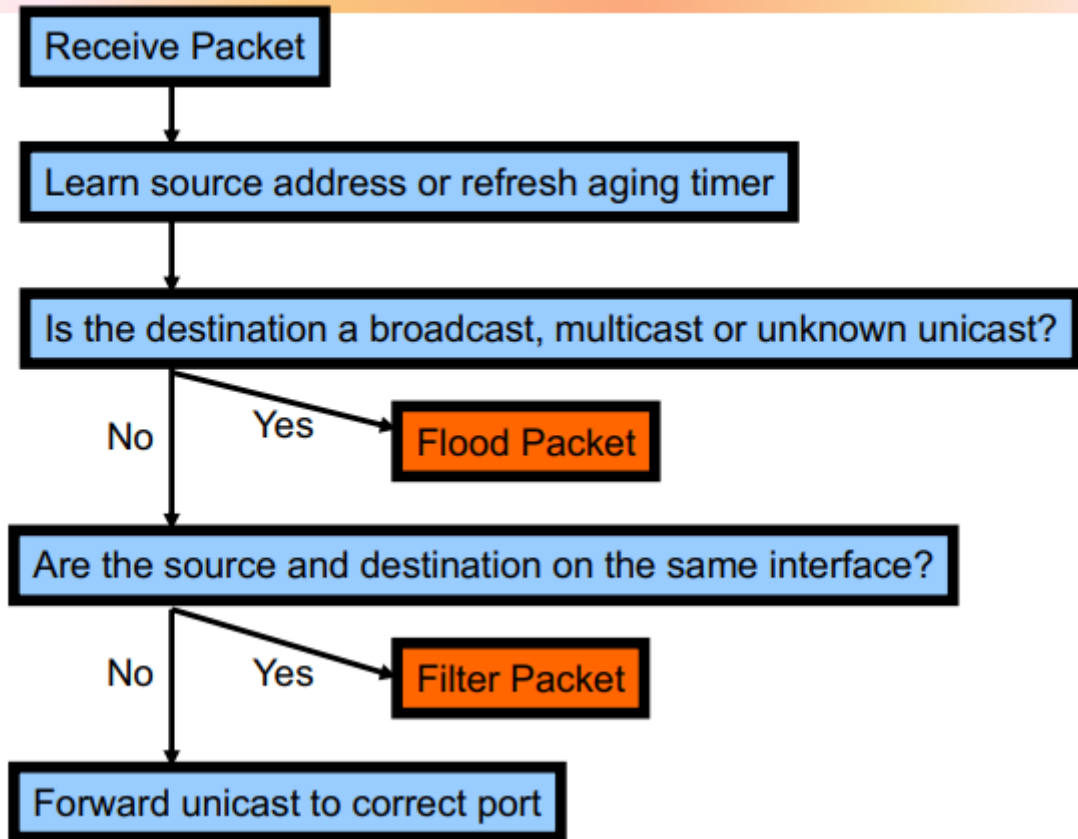


# Port Address Translation (PAT) \_ VD1



❖ **Switch**

## Quy trình xử lý gói tin của Switch



## Quy trình xử lý gói tin của Switch

- ❑ Quy trình xử lý Frame của Switch. Khi nhận Frame, Switch sẽ thực hiện 2 thao tác cơ bản :
  - ❑ **Learning** ( thêm mới hay cập nhật ) : **kiểm tra Source MAC Address**
    - Nếu Source MAC Address có trong bảng Source Address Table thì sẽ cập nhật Timer
    - Ngược lại sẽ thêm vào Source Address Table 1 entry : Source MAC Address và Port tương ứng
  - ❑ **Forwarding** (Filter hay Flood) : **kiểm tra Destination MAC Address**
    - Nếu Destination MAC Address có trong bảng Source Address Table thì Switch sẽ chuyển tiếp gói tin tới đúng port cần nhận
    - Ngược lại, Switch sẽ gởi frame ra tất cả các port

## Thiết kế mạng LAN

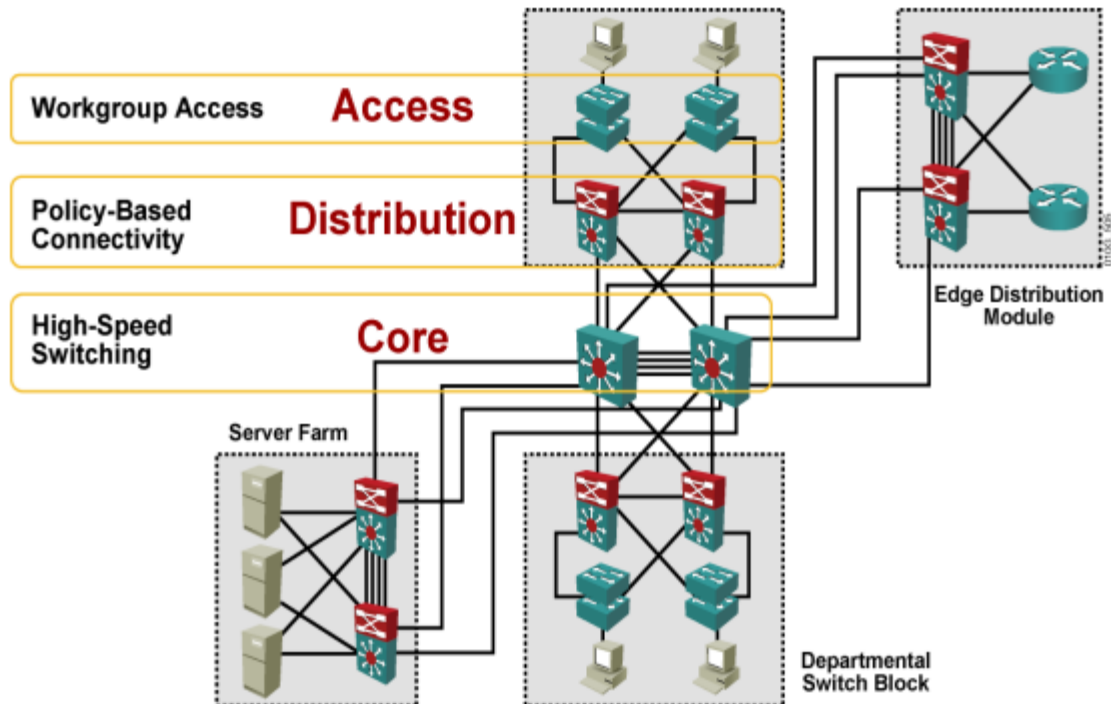
- ❑ Mục đích để thiết kế mạng LAN :

### Network design requirements:

- Functionality
- Scalability
- Adaptability
- Manageability

## Thiết kế mạng LAN

- ❑ Thiết kế mạng theo mô hình phân cấp :



## Distribution Layer

- ❑ Hoạt động ở Layer 2 và Layer 3
- ❑ Thiết lập những chính sách để lọc frame
- ❑ Những tính năng chính :
  - ❑ Chia Collision Domain và Broadcast Domain
  - ❑ VLAN
  - ❑ Security
  - ❑ .....