Chương 7
Access Control List

- GV : ThS.Nguyễn Duy
- Email : duyn@uit.edu.vn

Nội Dung

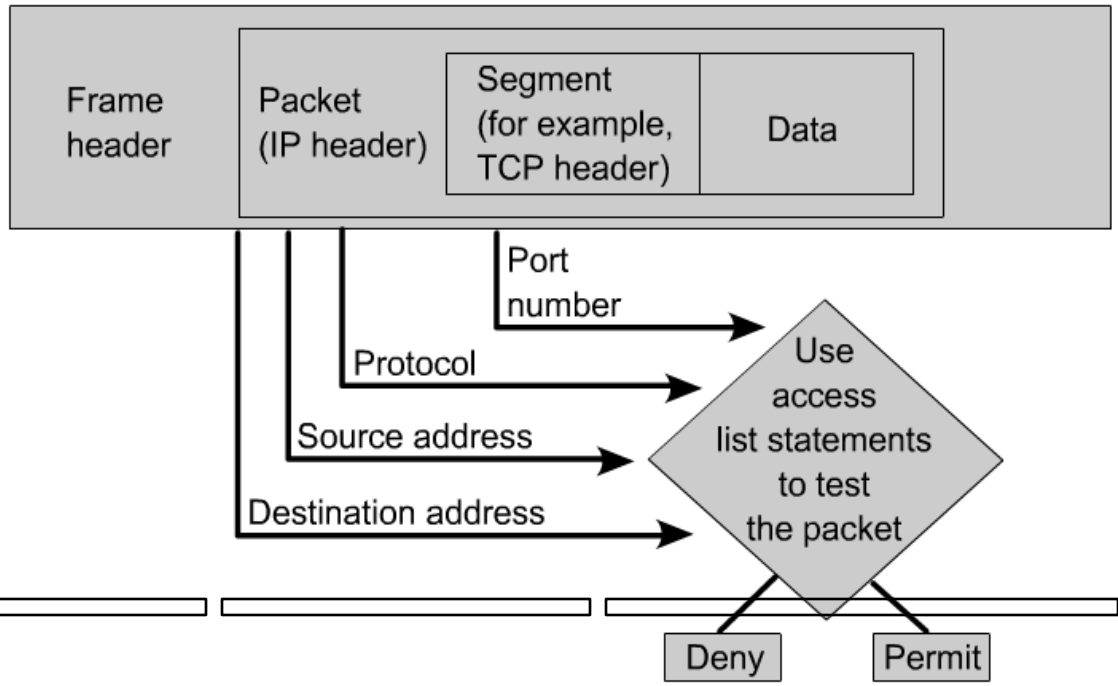
- Access Control List (ACL) là gì ?
- Nguyên nhân tạo ra ACL
- Cơ chế hoạt động của ACL
- Phân loại ACL
  - Standard ACLs
  - Extended ACLs
  - Named ACLs
- Nguyên tắc khi tạo ACL
- Vị trí đặt ACLs

Nội Dung

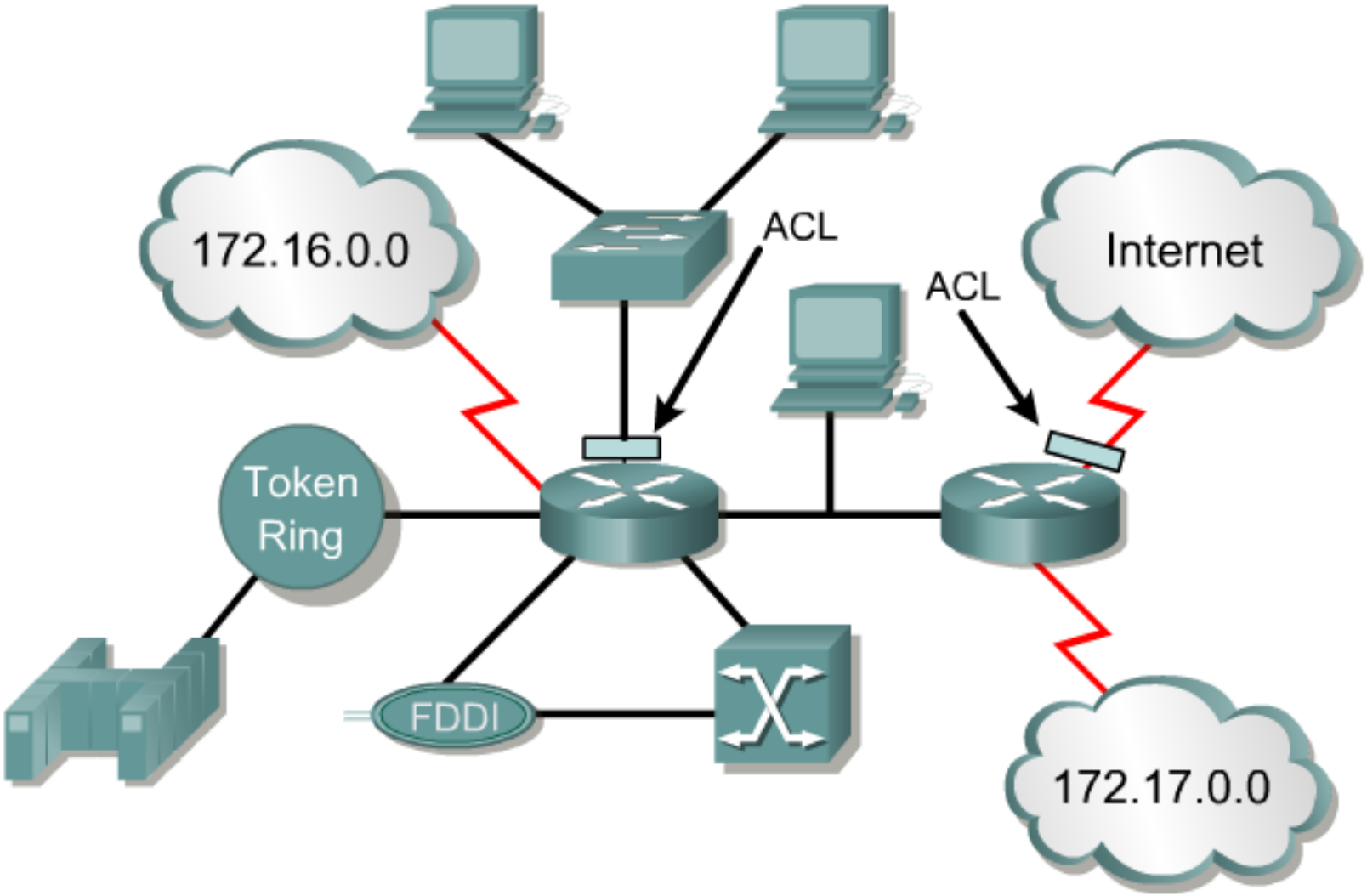
- **Access Control List (ACL) là gì ?**
- Nguyên nhân tạo ra ACL
- Cơ chế hoạt động của ACL
- Phân loại ACL
  - Standard ACLs
  - Extended ACLs
  - Named ACLs
- Nguyên tắc khi tạo ACL
- Vị trí đặt ACLs

Access Control List (ACL) là gì ?

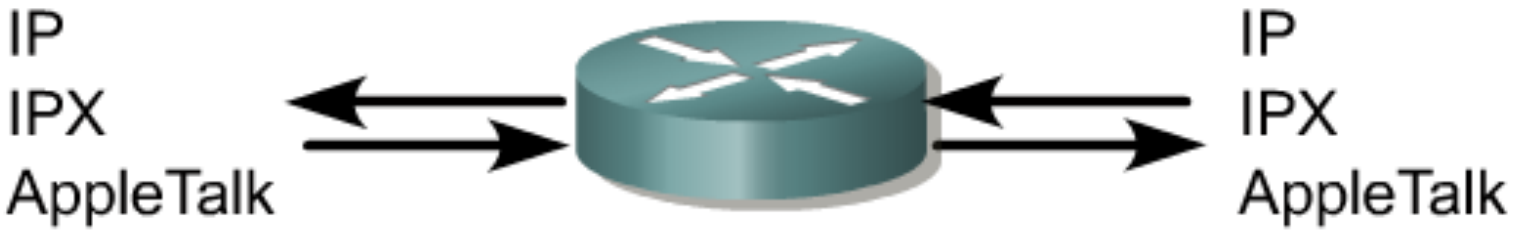
- ACL là một danh sách các điều kiện mà Router/Switch L3 dùng để kiểm tra khi gói tin đi qua một cổng của Router/Switch L3. ACL áp lên interface của thiết bị.
- Danh sách các điều kiện này cho Router biết loại gói tin nào được chấp nhận hay từ chối dựa trên các điều kiện cụ thể
- Các điều kiện của ACL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



Access Control List (ACL) là gì ?



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.

Nội Dung

- Access Control List (ACL) là gì ?
- **Nguyên nhân tạo ra ACL**
- Cơ chế hoạt động của ACL
- Phân loại ACL
  - Standard ACLs
  - Extended ACLs
  - Named ACLs
- Nguyên tắc khi tạo ACL
- Vị trí đặt ACLs

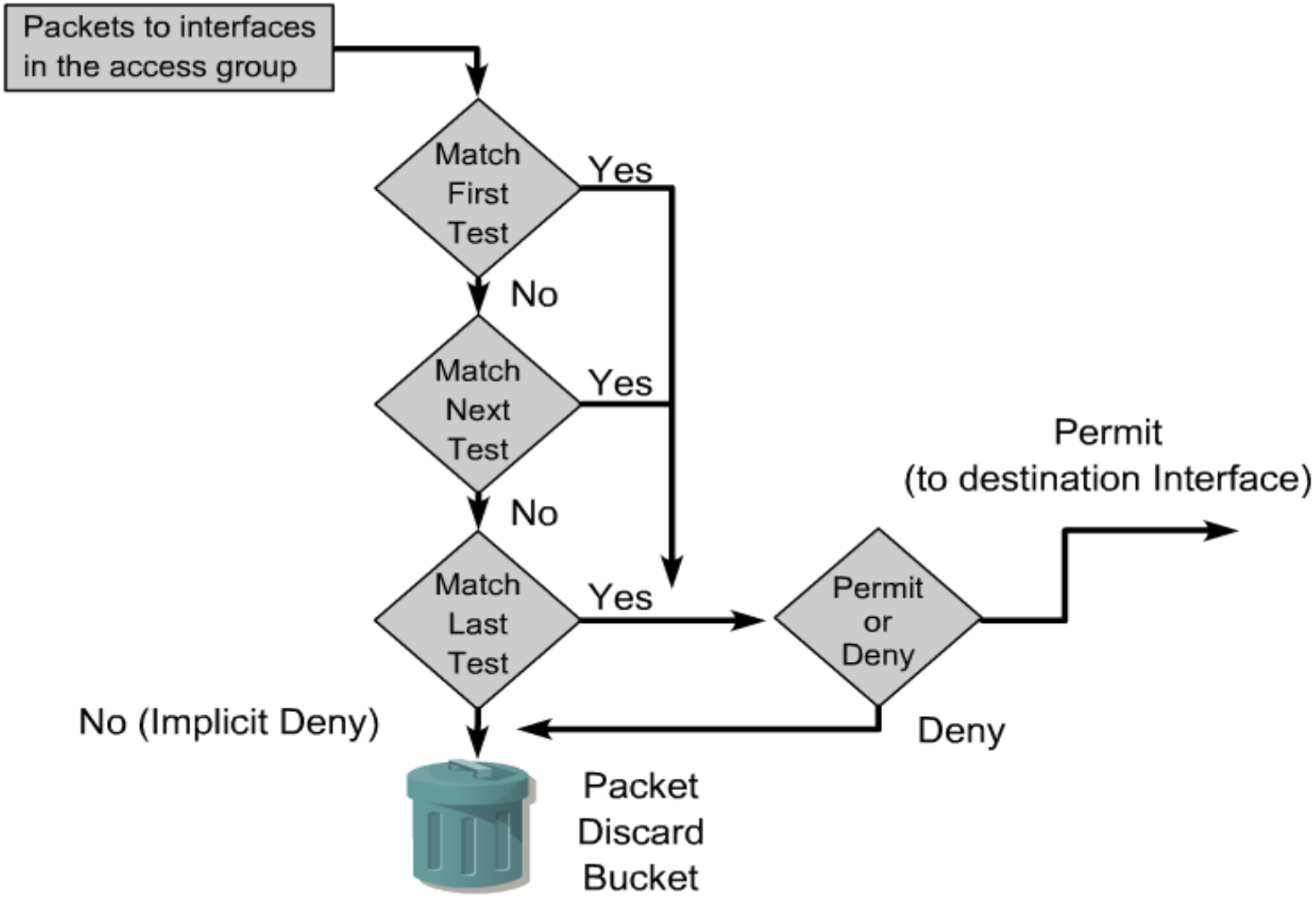
Nguyên nhân tạo ra ACL

- 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
  - …..

Nội Dung

- Access Control List (ACL) là gì ?
- Nguyên nhân tạo ra ACL
- **Cơ chế hoạt động của ACL**
- Phân loại ACL
  - Standard ACLs
  - Extended ACLs
  - Named ACLs
- Nguyên tắc khi tạo ACL
- Vị trí đặt ACLs

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

Nội Dung

- Access Control List (ACL) là gì ?
- Nguyên nhân tạo ra ACL
- Cơ chế hoạt động của ACL
- **Phân loại ACL**
  - Standard ACLs
  - Extended ACLs
  - Named ACLs
- Nguyên tắc khi tạo ACL
- Vị trí đặt ACLs

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*

Practice – wildcard mask

```
RouterB(config)#access-list 10 permit _____ _____
```

Permit the following networks:

	Network/Subnet Mask	Address/Wildcard Mask
A.	172.16.0.0 255.255.0.0	
B.	172.16.1.0 255.255.255.0	
C.	192.168.1.0 255.255.255.0	
D.	172.16.16.0 255.255.240.0	(hmmm . . .?)
E.	172.16.128.0 255.255.192.0	(hmmm . . .?)

Permit the following hosts:

	Network/Subnet Mask	Address/Wildcard Mask
A.	172.16.10.100	
B.	192.168.1.100	
C.	All hosts	

Practice – Do you see a relationship?

```
RouterB(config)#access-list 10 permit _____ _____
```

Permit the following networks:

	Network/Subnet Mask	Address/Wildcard Mask
A.	172.16.0.0 255.255.0.0	172.16.0.0 0.0.255.255
B.	172.16.1.0 255.255.255.0	172.16.1.0 0.0.0.255
C.	192.168.1.0 255.255.255.0	192.168.1.0 0.0.0.255
D.	172.16.32.0 255.255.240.0	172.16.32.0 0.0.15.255
E.	172.16.128.0 255.255.192.0	172.16.128 0.0.63.255

Permit the following hosts:

	Network/Subnet Mask	Address/Wildcard Mask
A.	172.16.10.100	172.16.10.100 0.0.0.0
B.	192.168.1.100	192.168.1.100 0.0.0.0
C.	All hosts	0.0.0.0 255.255.255.255

Answers Explained

A. 172.16.0.0 0.0.255.255

RouterB(config)#**access-list 10 permit 172.16.0.0 0.0.255.255**

0 = check, we want this to match

1 = don't check, this can be any value, does not need to match

Test Conditon

172.16.0.0	10101100 . 00010000	. 00000000 . 00000000
0.0.255.255	00000000 . 00000000	. 11111111 . 11111111

172.16.0.0	10101100 . 00010000	. 00000000 . 00000000
172.16.0.1	10101100 . 00010000	. 00000000 . 00000001
172.16.0.2	10101100 . 00010000	. 00000000 . 00000010
		... (through)
172.16.255.255	10101100 . 00010000	. 11111111 . 11111111

Matching packets will look like this.

The packet(s)

Answers Explained

D. 172.16.32.0 255.255.240.0

RouterB(config)#**access-list 10 permit 172.16.32.0 0.0.15.255**

0 = check, we want this to match

1 = don't check, this can be any value, does not need to match

Test Conditon

```
172.16.16.0     10101100 . 00010000 . 00100000 . 00000000
0.0.15.255      00000000 . 00000000 . 00001111 . 11111111
                ---------------------------------------

172.16.16.0     10101100 . 00010000 . 00100000 . 00000000
172.16.16.1     10101100 . 00010000 . 00100000 . 00000001
172.16.16.2     10101100 . 00010000 . 00100000 . 00000010
                                          ... (through)
172.16.16.255   10101100 . 00010000 . 00101111 . 11111111
```

The packet(s)

Packets belonging to the 172.16.32.0/20 network will match this condition because they have the same 20 bits in common.

G

There is a relationship!
Bitwise-not on the Subnet Mask

D. 172.16.32.0 255.255.240.0

RouterB(config)#**access-list 10 permit 172.16.32.0 0.0.15.255**

```
Subnet Mask:          255 . 255 . 240 .   0
Wildcard Mask:   +      0 .   0 .  15 . 255
                      -----------------------
                      255 . 255 . 255 . 255
```

So, we could calculate the Wildcard Mask by:

```
                      255 . 255 . 255 . 255
Subnet Mask:      -   255 . 255 . 240 .   0
                      ---------------------
Wildcard Mask:         0 .   0 .  15 .  255
```

255.255.255.255 – Subnet = Wildcard

```
RouterB(config)#access-list 10 permit __________ __________
```

Permit the following networks:

	255.255.255.255. - Subnet Mask	=	Wildcard Mask
A.	255.255.255.255 - 255.255.0.0	=	0.0.255.255
B.	255.255.255.255 - 255.255.255.0	=	0.0.0.255
C.	255.255.255.255 - 255.255.255.0	=	0.0.0.255
D.	255.255.255.255 - 255.255.240.0	=	0.0.15.255
E.	255.255.255.255 - 255.255.192.0	=	0.0.63.255

Permit the following hosts: (host routes have a /32 mask)

	255.255.255.255. - /32 Mask	=	Wildcard Mask
A.	255.255.255.255 – 255.255.255.255	=	0.0.0.0
B.	255.255.255.255 – 255.255.255.255	=	0.0.0.0

255.255.255.255 – Subnet = Wildcard

```
RouterB(config)#access-list 10 permit _____ _____
```

Permit the following networks:

	Network/Subnet Mask	Address/Wildcard Mask
A.	172.16.0.0 255.255.0.0	172.16.0.0 0.0.255.255
B.	172.16.1.0 255.255.255.0	172.16.1.0 0.0.0.255
C.	192.168.1.0 255.255.255.0	192.168.1.0 0.0.0.255
D.	172.16.32.0 255.255.240.0	172.16.32.0 0.0.15.255
E.	172.16.128.0 255.255.192.0	172.16.128 0.0.63.255

Permit the following hosts:

	Network/Subnet Mask	Address/Wildcard Mask
A.	172.16.10.100	172.16.10.100 0.0.0.0
B.	192.168.1.100	192.168.1.100 0.0.0.0
C.	All hosts or “any”	0.0.0.0 255.255.255.255

“host” option

```
RouterB(config)#access-list 10 permit 192.168.1.100 0.0.0.0
RouterB(config)#access-list 10 permit host 192.168.1.100
```

Permit the following hosts:

	Network/Subnet Mask	Address/Wildcard Mask
A.	172.16.10.100	172.16.10.100 0.0.0.0
B.	192.168.1.100	192.168.1.100 0.0.0.0

The **host** option substitutes for the 0.0.0.0 mask.

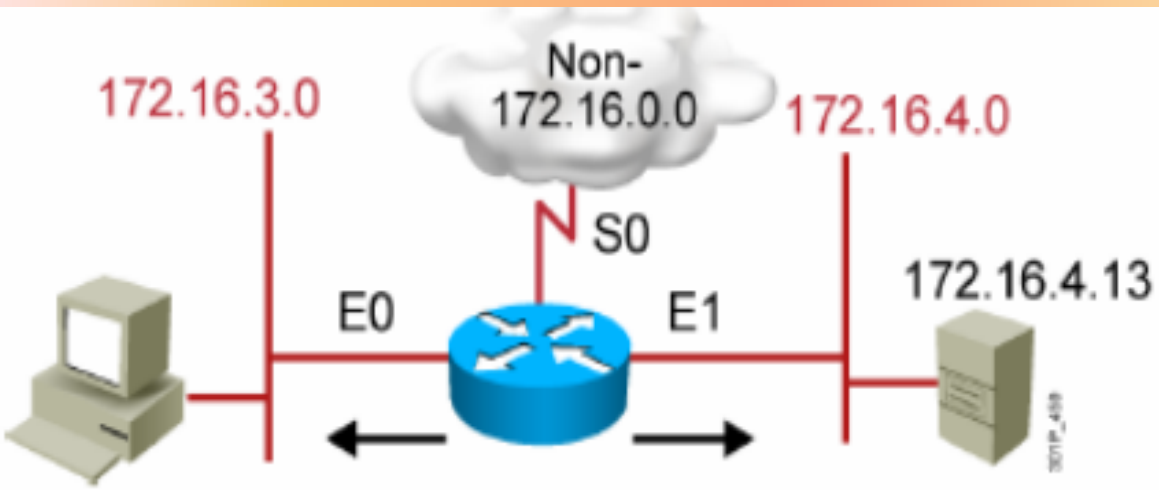
This mask requires that all bits of the ACL address and the packet address match.

The host keyword precedes the IP address.

This option will match just one address.

172.16.10.100 0.0.0.0	***replaced by***	host 172.16.10.100
192.168.1.100 0.0.0.0	***replaced by***	host 192.168.1.100

Standard ACL – Tạo

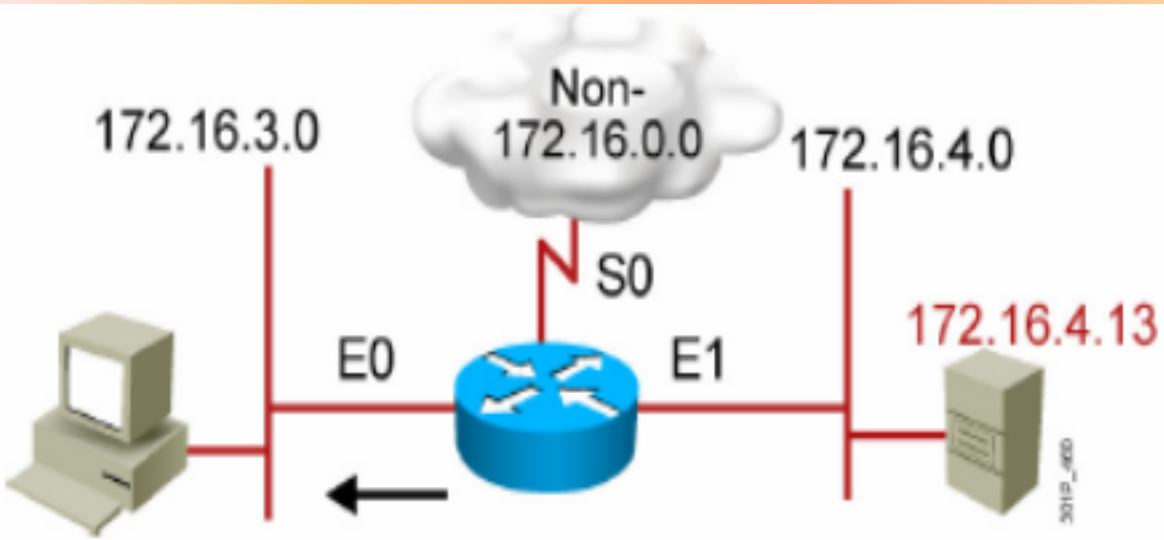



```
RouterX(config)# access-list 1 permit 172.16.0.0  0.0.255.255
(implicit deny all - not visible in the list)
(access-list 1 deny 0.0.0.0   255.255.255.255)

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

Chỉ cho phép các mạng nội bộ

Standard ACL – Tạo

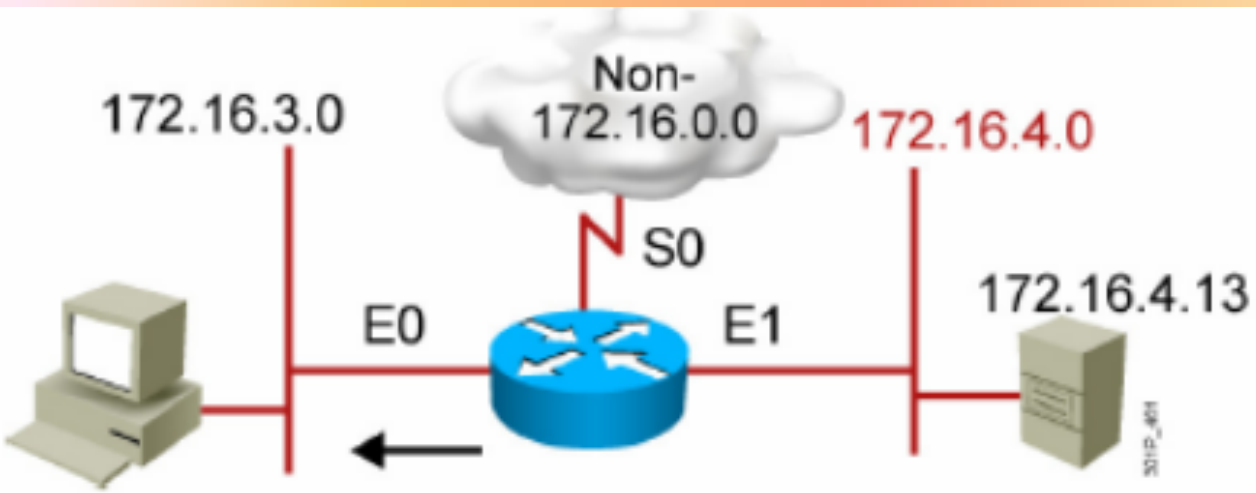



```
RouterX(config)# access-list 1 deny 172.16.4.13 0.0.0.0
RouterX(config)# access-list 1 permit 0.0.0.0  255.255.255.255
(implicit deny all)
(access-list 1 deny 0.0.0.0   255.255.255.255)

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

Cấm một host truy cập

Standard ACL – Tạo



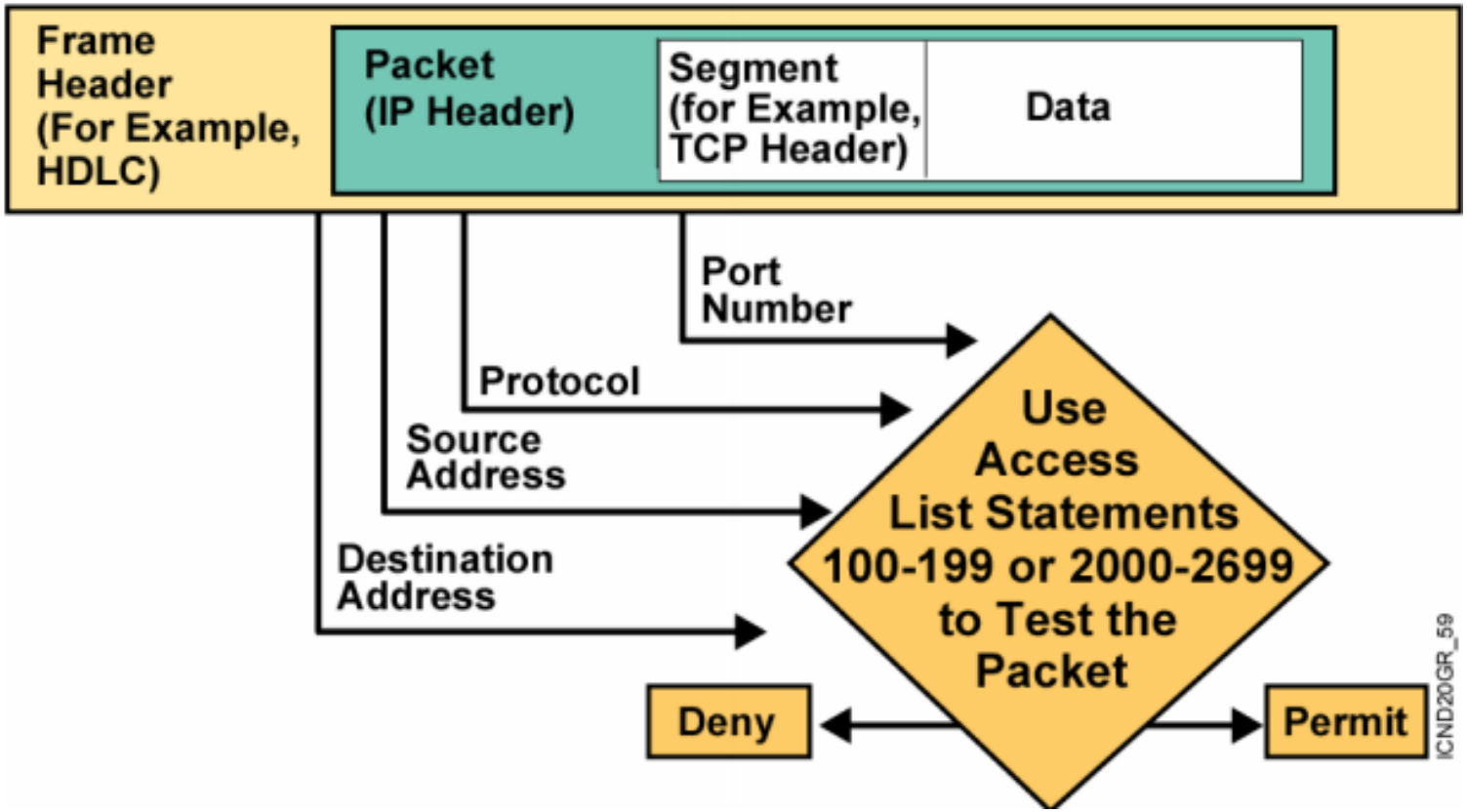

```
RouterX(config)# access-list 1 deny 172.16.4.0  0.0.0.255
RouterX(config)# access-list 1 permit any
(implicit deny all)
(access-list 1 deny 0.0.0.0   255.255.255.255)

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

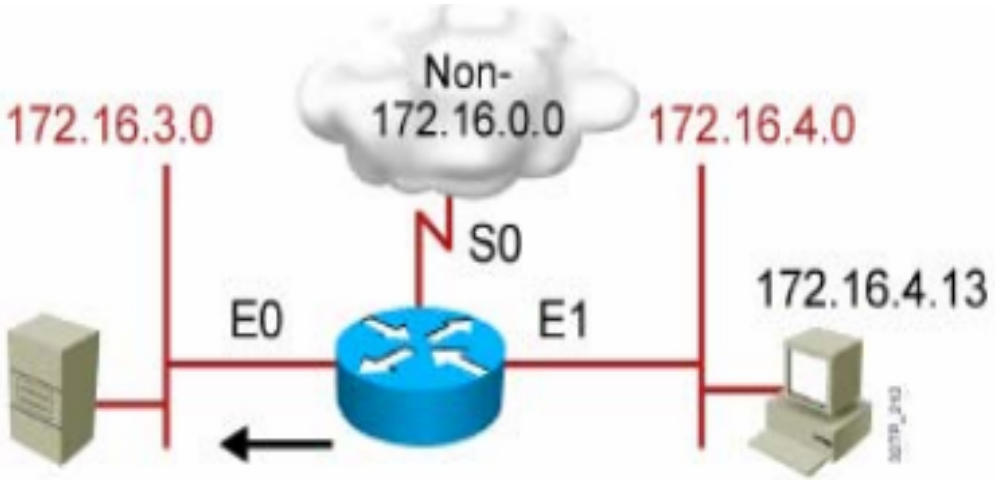
Source-wildcard and destination-wildcard : Mặt nạ wildcard ; 0 chỉ ra phần địa chỉ phải kiểm tra sự phù hợp , 1 chỉ ra phần không cần phải kiểm tra

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

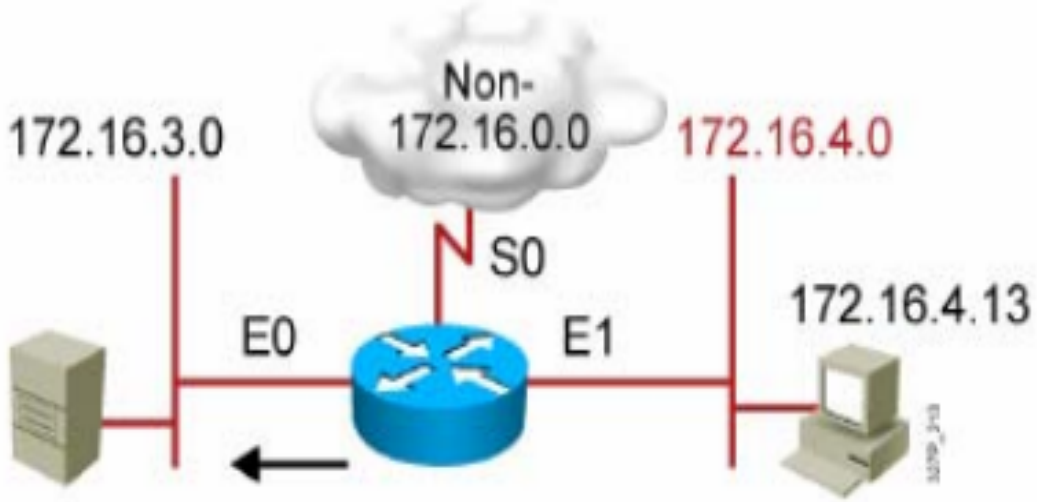



```
RouterX(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
RouterX(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
RouterX(config)# access-list 101 permit ip any any
(implicit deny all)
(access-list 101 deny ip 0.0.0.0 255.255.255.255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

Named ACL

- Tự nghiên cứu

Nội Dung

- Access Control List (ACL) là gì ?
- Nguyên nhân tạo ra ACL
- Cơ chế hoạt động của ACL
- Phân loại ACL
  - Standard ACLs
  - Extended ACLs
  - Named ACLs
- **Nguyên tắc khi tạo ACL**
- Vị trí đặt ACLs

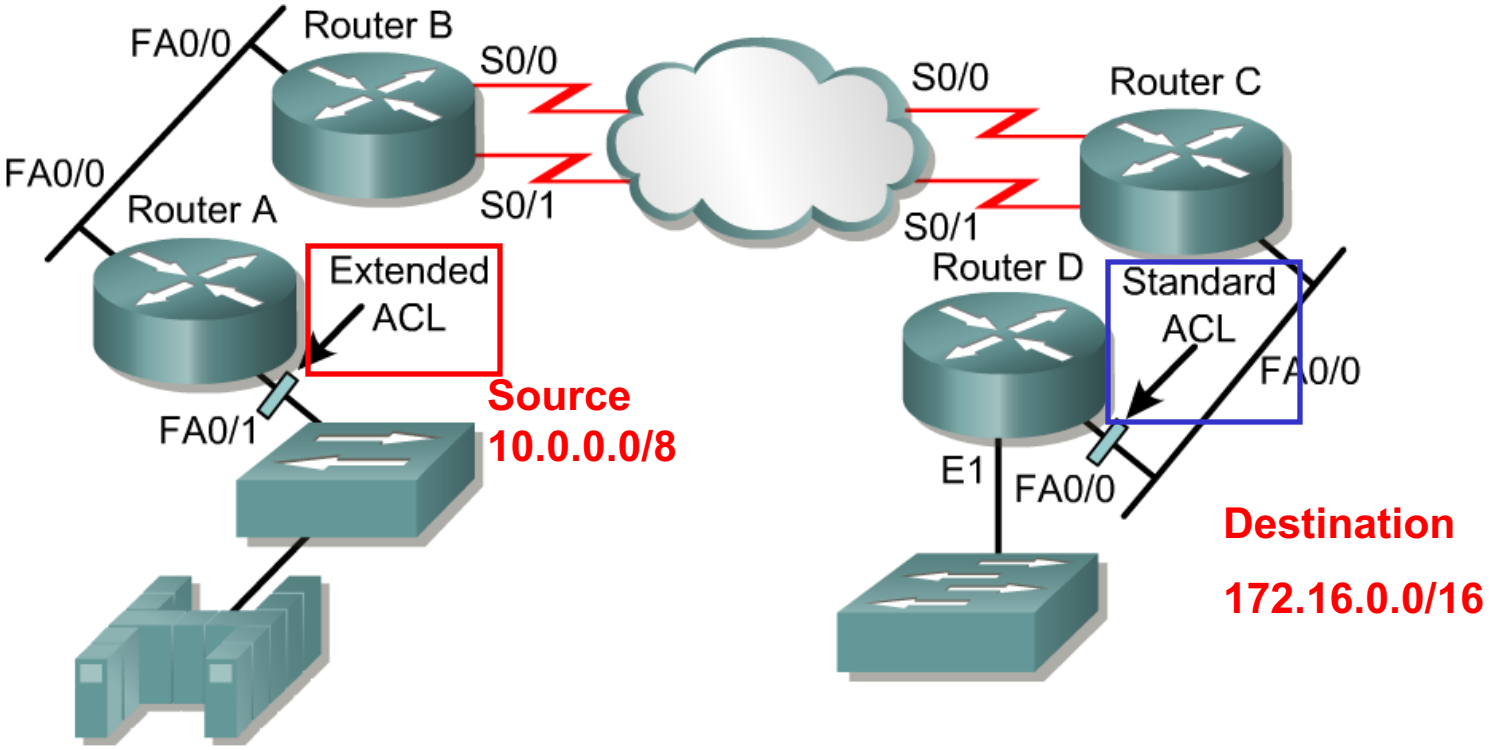
Nguyên tắc khi tạo ACL

- **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 thi 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

Nội Dung

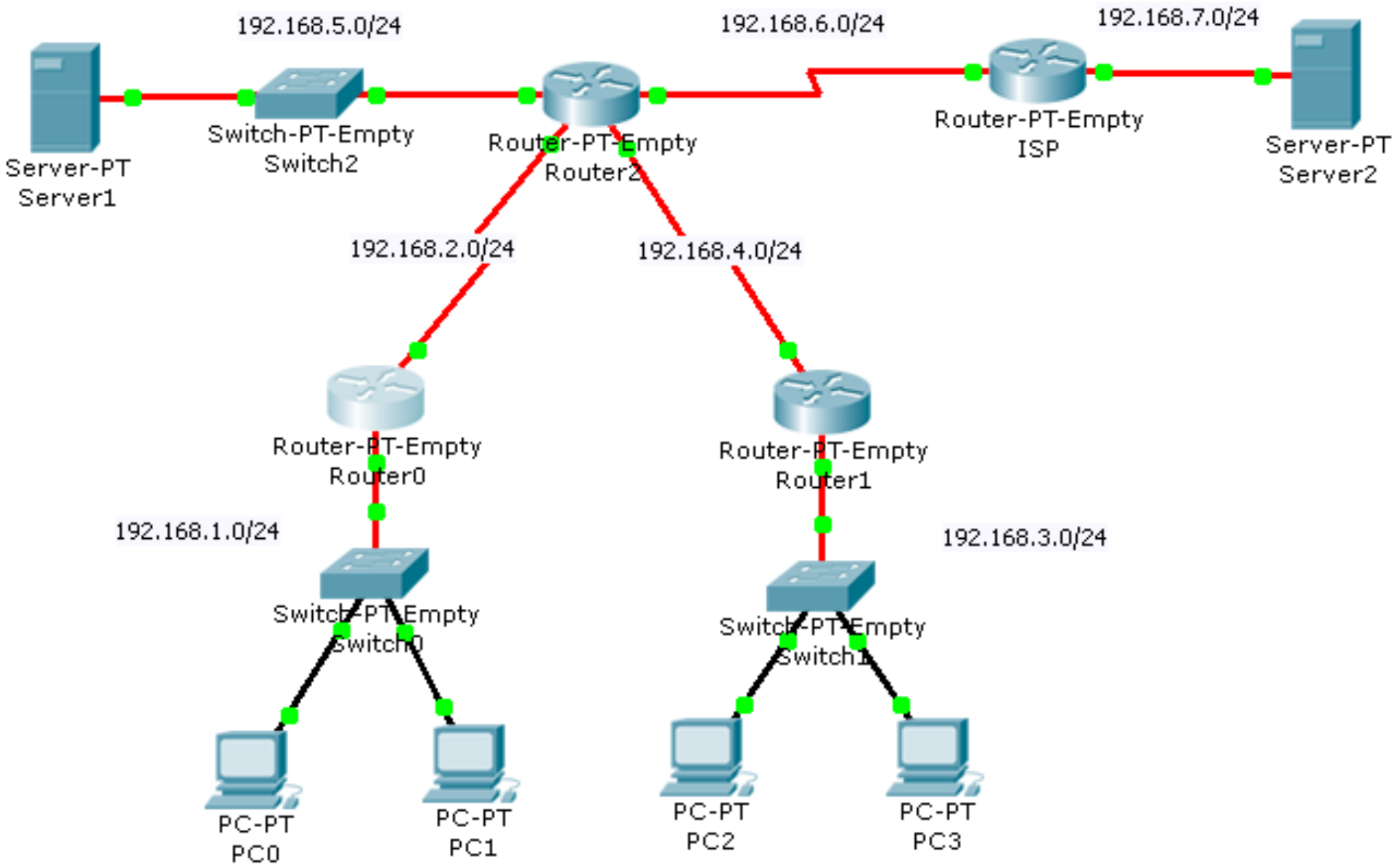
- Access Control List (ACL) là gì ?
- Nguyên nhân tạo ra ACL
- Cơ chế hoạt động của ACL
- Phân loại ACL
  - Standard ACLs
  - Extended ACLs
  - Named ACLs
- Nguyên tắc khi tạo ACL
- **Vị trí đặt ACLs**

Vị trí đặt ACLs



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

Bài tập


192.168.5.0/24
192.168.6.0/24
192.168.7.0/24
Server-PT
Server1
Switch-PT-Empty
Switch2
Router-PT-Empty
Router2
Router-PT-Empty
ISP
Server-PT
Server2
192.168.2.0/24
192.168.4.0/24
Router-PT-Empty
Router0
Router-PT-Empty
Router1
192.168.1.0/24
192.168.3.0/24
Switch-PT-Empty
Switch0
Switch-PT-Empty
Switch1
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3

Bài tập

1) PC0 không thể truy xuất bất cứ dịch vụ gì từ Server2
2) PC0 không được ping Server1, nhưng được truy cập dịch vụ Web trên Server1
3) Cấm tất cả các máy trong mạng 192.168.3.0/24 sử dụng dịch vụ web từ Server1 ngoại trừ PC2
4) Các máy trong mạng 192.168.1.0/24 không thể truy cập qua mạng 192.168.3.0/24

Câu hỏi ôn tập

1) ACL là gì ?
2) Nguyên tắc hoạt động của ACL ?
3) Phân biệt được Standard ACL và Extented ACL