CANTHO UNIVERSITY

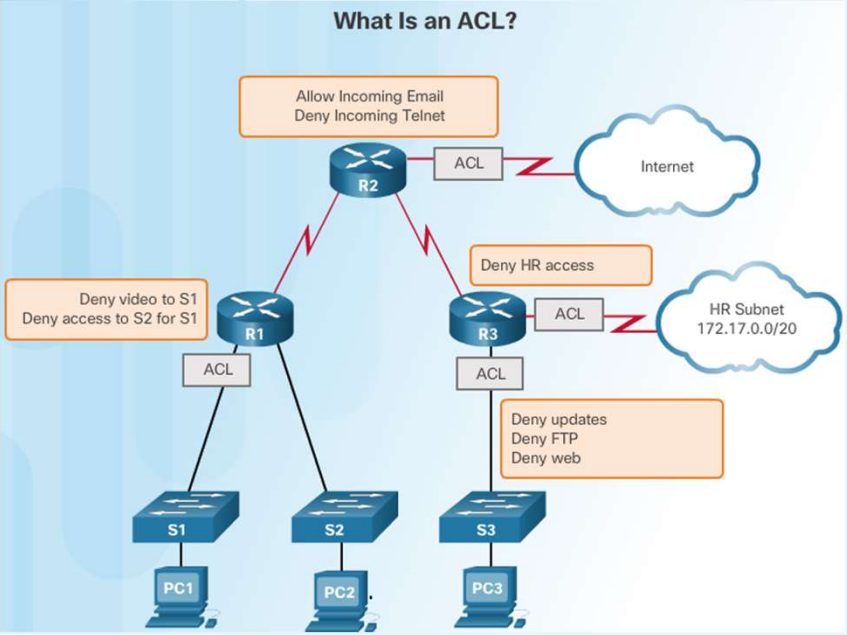
THIẾT KẾ CÀI ĐẶT MẠNG MÁY TÍNH

MÃ SỐ HỌC PHẦN: CT335

CHƯƠNG 9: DANH SÁCH ĐIỀU KHIỂN TRUY CẬP
ACCESS CONTROL LIST

CANTHO UNIVERSITY

GIỚI THIỆU ACL

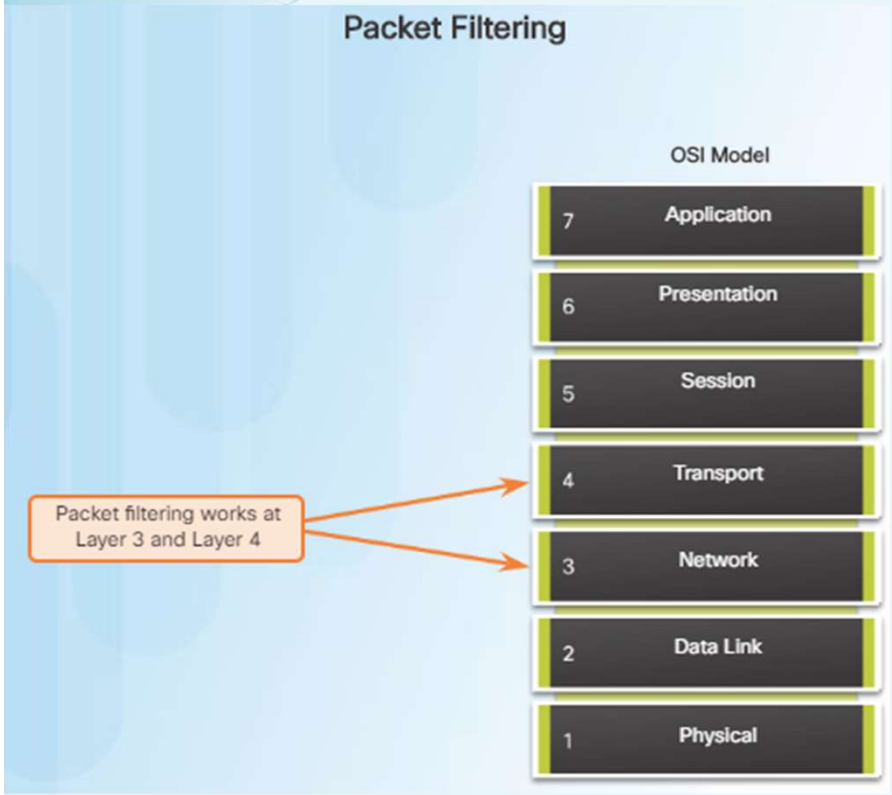


- ACL là một chuỗi có thứ tự các lệnh IOS trên router được định nghĩa để kiểm soát lưu thông qua đó cho phép chuyển tiếp hoặc chặn gói tin dựa trên thông tin trong header của gói tin. Mặc định thì ACL không được thiết lập trên router
- ACL có thể thực hiện các tác vụ:
  - Giới hạn một số kiểu lưu thông để tăng hiệu suất mạng (Ví dụ giảm kiểu lưu thông video)
  - Kiểm soát luồng lưu thông (ACL kiểm soát việc trao đổi thông tin từ một nguồn/ đích xác định)
  - ACL cung cấp cơ chế bảo mật cho việc truy cập mạng: có thể cho phép/ ngăn chặn một host/ một mạng truy cập đến một mạng hay một dịch vụ trên mạng khác (vd kiểm soát dịch vụ Telnet,FTP hoặc

```
R3(config)# access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.10.0 0.0.0.255
R3(config)# access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.11.0 0.0.0.255
R3(config)# access-list 130 permit tcp 192.168.30.128 0.0.0.127 any eq www
R3(config)# access-list 130 permit icmp 192.168.30.128 0.0.0.127 any
R3(config)# access-list 130 deny ip any any
```

CANTHO UNIVERSITY

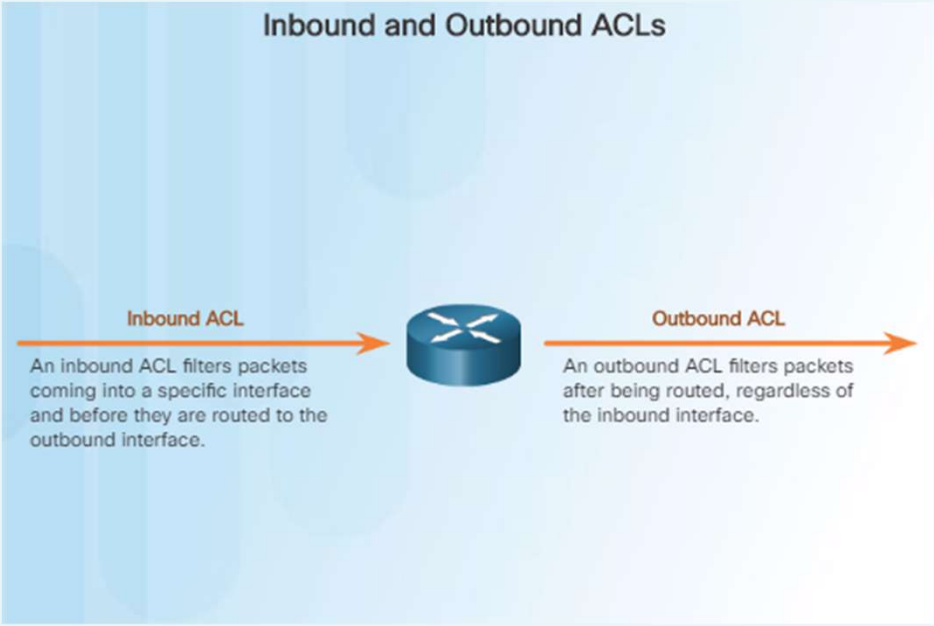
LỌC GÓI TIN [PACKET]



- ACL là một danh sách tuần tự các câu lệnh cho phép (permit) hoặc từ chối (deny), được gọi là câu lệnh ACL hay các phát biểu kiểm soát truy cập (ACE- access control entries)
- Khi lưu thông mạng đi qua giao diện được cấu hình với ACL, bộ định tuyến sẽ so sánh thông tin trong header gói tin với từng phát biểu, kiểm tra theo tuần tự từng phát biểu, để xác định xem gói có khớp [match] với một trong các phát biểu hay không. Điều này được gọi là lọc gói
- Lọc gói:
  - *Có thể phân tích các gói tin đi/ đến*
  - *Có thể xảy ra ở tầng 3 hoặc tầng 4*
- Phát biểu cuối cùng của ACL luôn là *từ chối ẩn (deny any)*. Phát biểu này được tự động chèn vào cuối mỗi ACL để ngăn chặn tất cả lưu lượng. Do đó, tất cả các ACL phải có ít nhất một câu lệnh cấp phép *(permit)*.

CANTHO UNIVERSITY

HOẠT ĐỘNG CỦA ACL

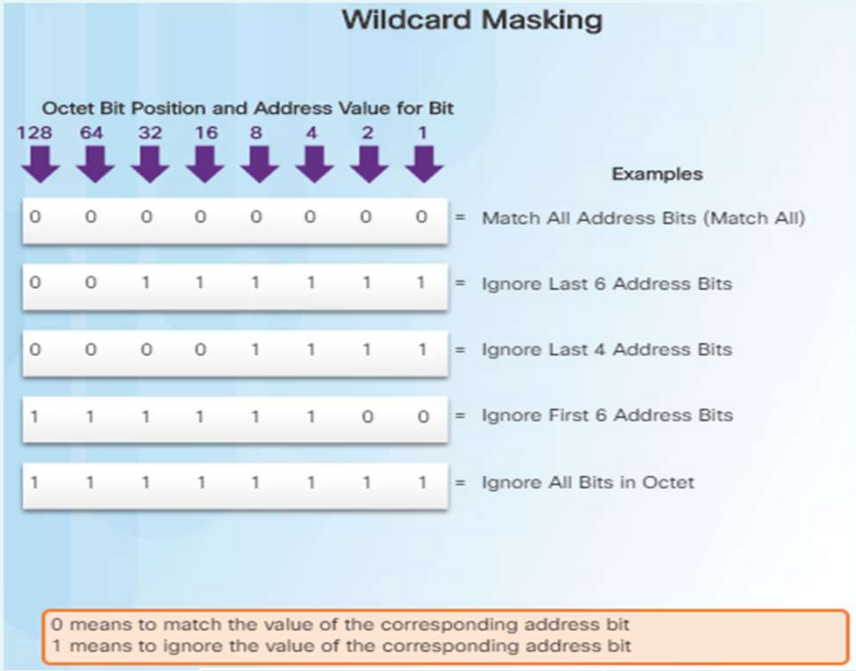


- ACL có thể được định cấu hình kiểm soát các lưu thông ***đến*** và ***đi*** qua giao diện của router
  - ***ACL ở giao diện đến:*** Các gói tin đến được xử lý trước khi chúng được vào router
  - ***ACL ở giao diện đi:*** Khi router xác định được đường đi, gói tin được chuyển đến giao diện ngõ ra, gói tin sẽ được xử lý qua ACL trước, nếu được phép mới gửi đi ra khỏi giao diện router

Chú ý: ACL *không kiểm soát* gói tin bắt nguồn từ chính router được đặt ACL

CANTHO UNIVERSITY

MẶT NẠ KÝ TỰ ĐẠI DIỆN WILDCARD MASK



- Các phát biểu ACL trong IPv4 sử dụng **mặt nạ ký tự đại diện (wildcard mask)**
- Mặt nạ wildcard là một dãy 32 bit được router sử dụng để xác định các bit của địa chỉ gói tin phù hợp với phát biểu
- Mặt nạ ký tự đại diện còn được gọi là *mặt nạ nghịch đảo* (không giống như mặt nạ mạng), trong đó:
  - Bit **1** trên mặt nạ: chỉ ra bit tương ứng trên địa chỉ của gói tin là giá trị bất kỳ
  - Bit **0** trên mặt nạ: yêu cầu kiểm tra bit tương ứng trên địa chỉ của gói tin phải trùng khớp với bit trên địa chỉ được khai báo trong phát biểu

	Địa chỉ dạng thập phân	Địa chỉ dạng nhị phân
Địa chỉ IP mẫu	192.168.10. 0	11000000.10101000.00001010.00000000
Mặt nạ wild card	0 . 0 .0 .255	00000000.00000000.00000000.11111111
Phần địa chỉ cần kiểm tra	192.168.10 . X	11000000.10101000.00001010.XXXXXXXX

CÁC VÍ DỤ VỀ MẶT NẠ KÝ TỰ ĐẠI DIỆN

CANTHO UNIVERSITY

Wildcard Masks to Match IPv4 Hosts and Subnets

Example 1

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.0	00000000.00000000.00000000.00000000
Result	192.168.1.1	11000000.10101000.00000001.00000001

Example 2

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	255.255.255.255	11111111.11111111.11111111.11111111
Result	0.0.0.0	00000000.00000000.00000000.00000000

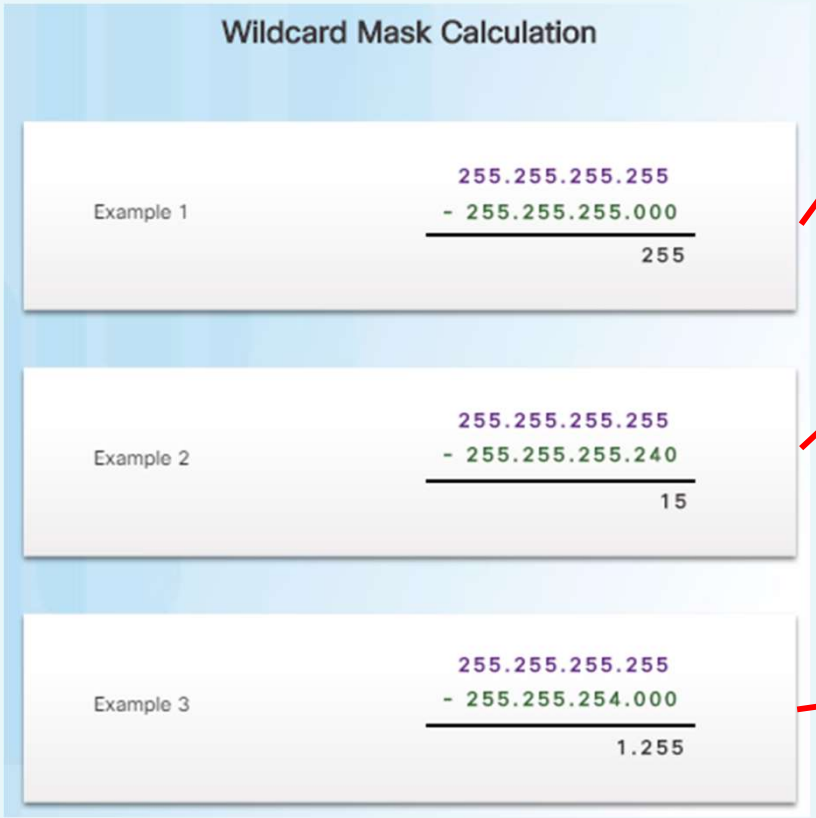
Example 3

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.255	00000000.00000000.00000000.11111111
Result	192.168.1.0	11000000.10101000.00000001.00000000

- Ví dụ 1: Mặt nạ ký tự đại diện 0.0.0.0 quy định rằng mọi bit trong địa chỉ IPv4 192.168.1.1 phải khớp chính xác
- Ví dụ 2: Mặt nạ ký tự đại diện 255.255.255.255 quy định rằng bất kỳ giá trị nào cũng khớp
- Ví dụ 3: Mặt nạ ký tự đại diện 0.0.0.255 quy định rằng *bất kỳ địa chỉ IP nào trong mạng* ***192.168.1****.0/24* sẽ khớp

CANTHO UNIVERSITY

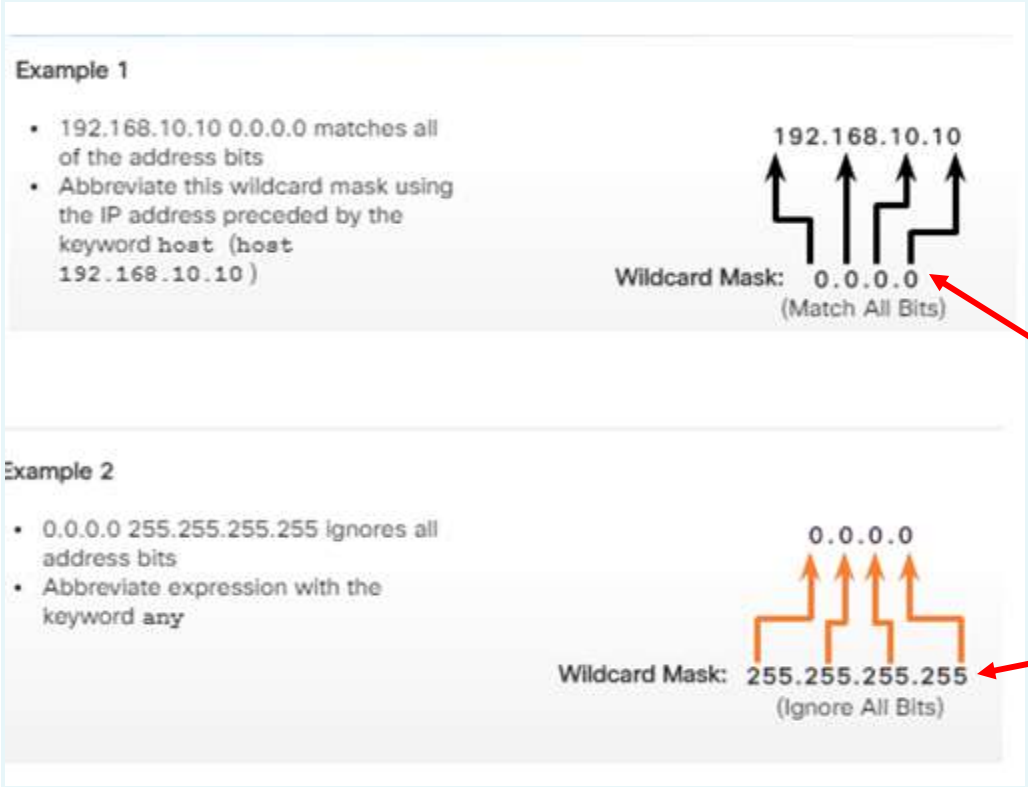
CÁCH TÍNH MẶT NẠ KÝ TỰ ĐẠI DIỆN



- *Các ví dụ:*
  - Ví dụ 1: Giả sử muốn cho phép tất cả các host trong mạng 192.168.3.0 với mặt nạ mạng con là 255.255.255.0. Lấy 255.255.255.255 ***trừ*** cho mặt nạ mạng con và kết quả là: 0.0.0.255
  - Ví dụ 2: Giả sử bạn muốn cho phép truy cập mạng cho 14 người dùng trong mạng con 192.168.3.32/28 với mặt nạ mạng con là 255.255.255.240. Sau khi 255.255.255.255 ***trừ*** cho mặt nạ mạng con, kết quả là 0.0.0.15
  - Ví dụ 3: Giả sử bạn chỉ muốn so khớp các mạng 192.168.10.0 và 192.168.11.0 với mặt nạ mạng con là 255.255.254.0. Sau khi 255.255.255.255 ***trừ*** cho mặt nạ mạng con, kết quả là 0.0.1.255

CÁC MẶT NẠ KÝ TỰ ĐẠI DIỆN ĐẶC BIỆT

CANTHO UNIVERSITY

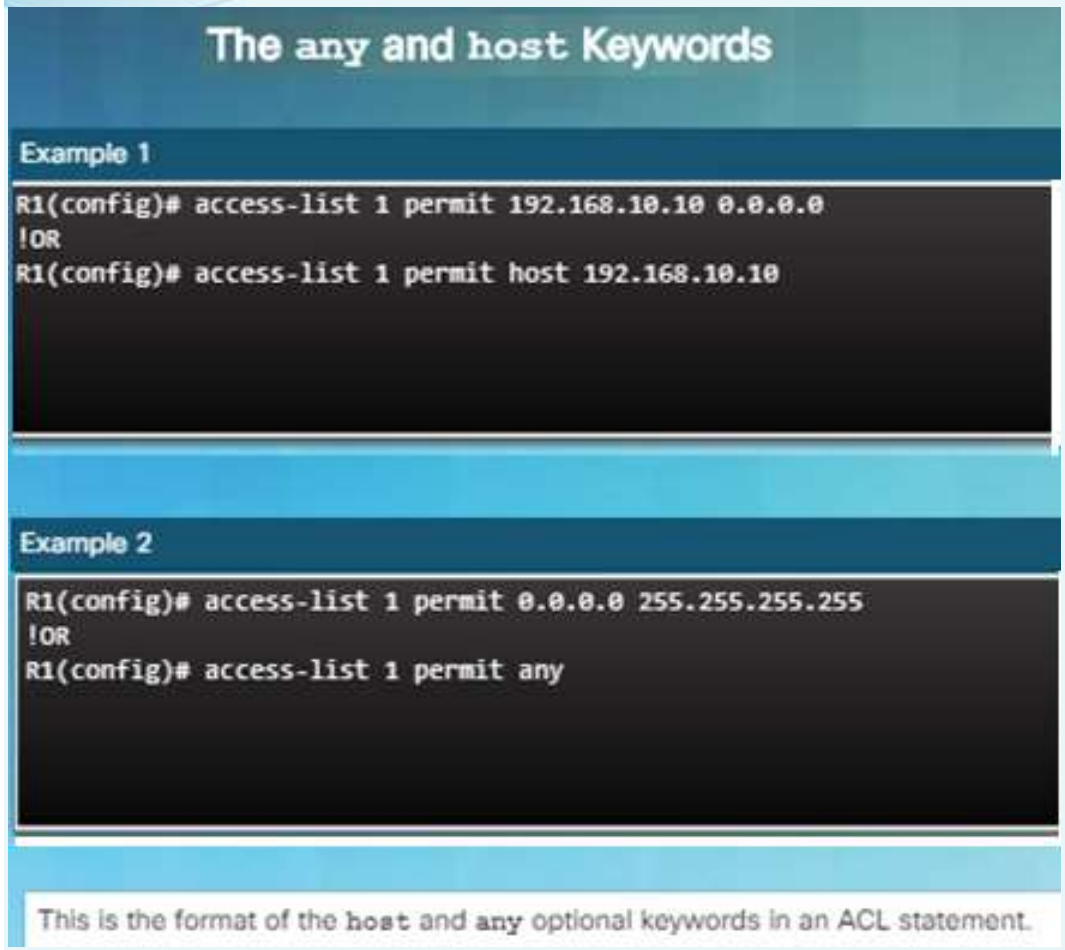


- Một số mặt nạ ký tự đại diện đặc biệt sẽ được thay thế bằng các từ khóa để dễ đọc hơn:
  - Từ ***host:*** được dùng thay cho mặt nạ **0.0.0.0**
  - Từ ***any***: được dùng thay cho mặt nạ **255.255.255.255**

- *Ví dụ 1:* Nếu muốn khớp với địa chỉ 192.169.10.10, có thể sử dụng ***192.168.10.10 0.0.0.0*** hoặc dùng ***host 192.168.10.10*** đều được

- *Ví dụ 2*: thay vì dùng mặt nạ ***0.0.0.0 255.255.255.255*** ta có thể sử dụng từ khóa ***any***

CÁC VÍ DỤ



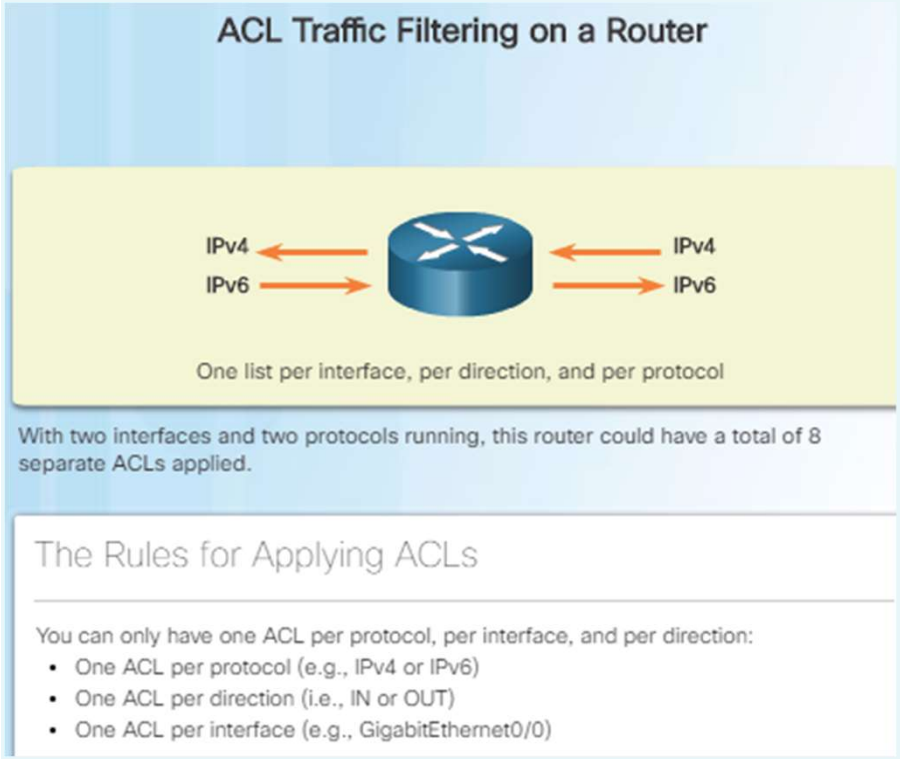
- Ví dụ 1: minh họa cách sử dụng từ khóa ***host*** để thay thế cho mặt nạ ký tự đại diện 0.0.0.0 khi xác định ***một*** địa chỉ IP duy nhất

- Ví dụ 2: minh họa cách sử dụng từ khóa ***any*** để thay thế địa chỉ IPv4 bất kỳ

  0.0.0.0 255.255.255.255

CANTHO UNIVERSITY

TẠO ACL



- ACL được tạo trên router hay tường lửa [firewall], ACL được đặt giữa các mạng khác nhau hay giữa mạng LAN hay Intranet và mạng bên ngoài (như Internet)

➢ Khi muốn kiểm soát lưu thông từ mạng bên ngoài đi vào mạng LAN, ACL sẽ được đặt trên router biên

➢ Khi muốn kiểm soát lưu thông từ mạng con này sang mạng con khác trong Intranet, ACL đặt trên giao diện các router liên mạng

➢ ACL có thể cấu hình cho từng giao thức riêng biệt trên cùng một giao diện của router (Vd: IPv4 & IPv6)

CANTHO UNIVERSITY

CÁC LOẠI ACL

- Có hai loại danh sách truy cập chính là:
  - ***Danh sách truy cập chuẩn*** (*Standard Access List*)
  - ***Danh sách truy cập mở rộng*** (*Extended Access List*)

➢ ***Danh sách truy cập chuẩn***: Mỗi phát biểu trong danh sách này được dùng để kiểm tra một thông số duy nhất là *địa chỉ nguồn* của các gói tin lưu thông.

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

➢ ***Danh sách truy cập mở rộng***: Mỗi phát biểu trong danh sách này kiểm tra nhiều thuộc tính: cả địa chỉ gởi và nhận của gói tin, kiểm tra trên từng giao thức cụ thể (IP, TCP, UDP, ICMP,…), số hiệu cổng (trên giao thức TCP, UDP và các tham số khác

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

Từ khóa *permit/ allow* (cho phép) hay *deny/ block* (từ chối) được dùng trong mỗi phát biểu của ACL để quyết định tác động với gói tin lưu thông

CANTHO UNIVERSITY

CÁC CÁCH KHAI BÁO ACL

Danh sách điều khiển truy cập dùng trong mạng TCP/IP có thể khai báo theo kiểu số hay kiểu tên

Với kiểu đánh số: tên của ACL được đặt bằng **kiểu số**, tùy theo số được đặt thì kiểu của danh sách có thể là khác nhau (do hãng sản xuất router qui định)

Ví dụ trên các router của Cisco:

- *Danh sách điều khiển chuẩn* được đánh số từ 1- 99 và từ 1,300 - 1,999
- *Danh sách điều khiển mở rộng* được đánh số từ 100 - 199 và từ 2,000 - 2,699

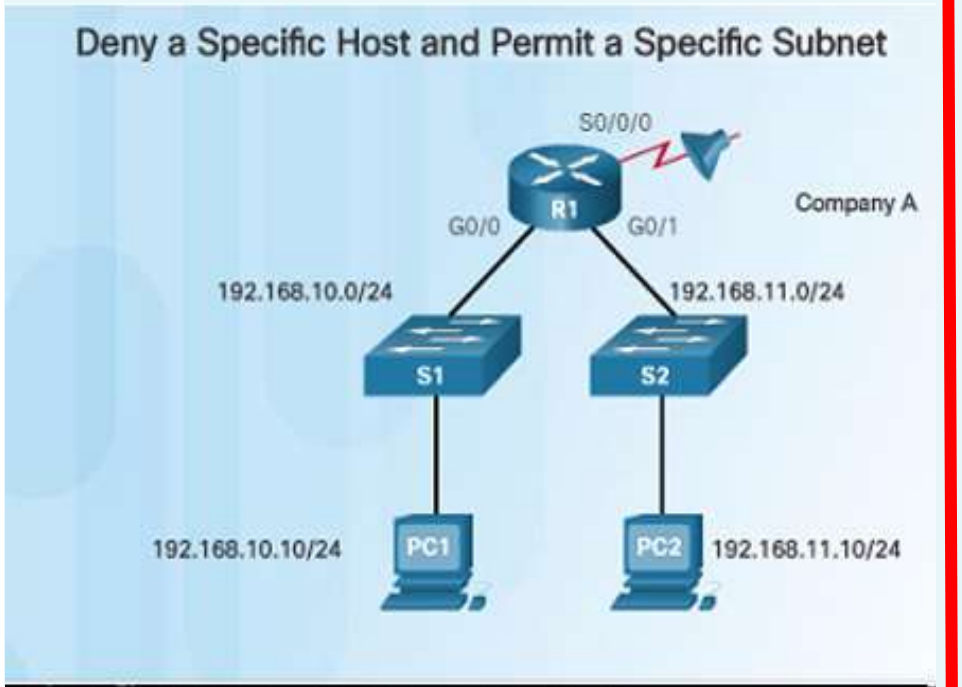
Với kiểu dùng tên: tên của ACL được đặt bằng **kiểu ký tự**, đặt theo qui cách xác định

- Tên chỉ chứa các ký tự Alphanumeric
- Tên nên viết bằng chữ IN HOA (để phân biệt với lệnh)
- Tên không được chứa khoảng trắng và dấu chấm

CANTHO UNIVERSITY

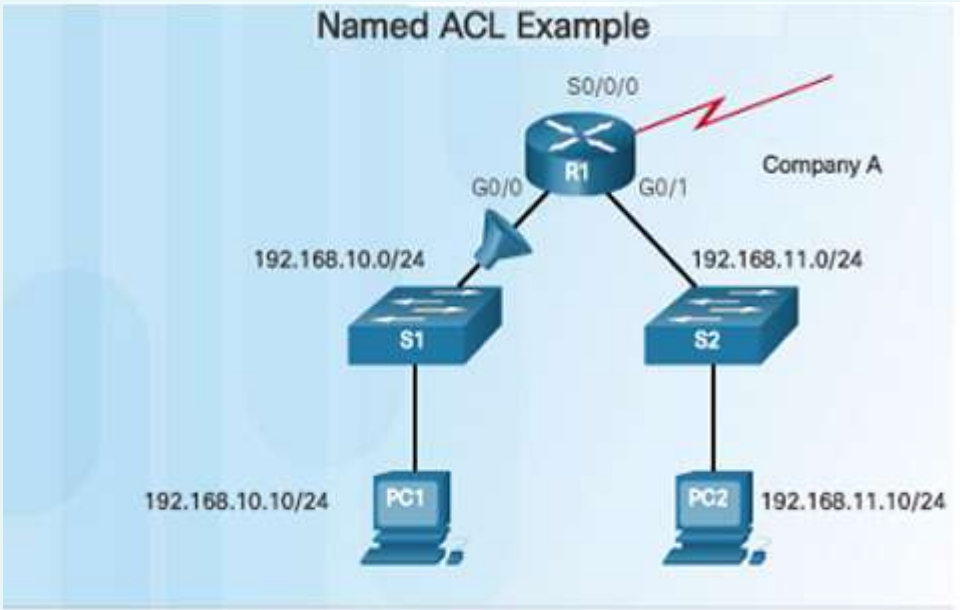
CÁC CÁCH KHAI BÁO ACL

Danh sách điều khiển truy cập kiểu số




```
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 1 out
```

Danh sách điều khiển truy cập kiểu tên




```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group NO_ACCESS out
```

CANTHO UNIVERSITY

ACL KIỂU SỐ

- Cú pháp cơ bản của ***danh sách điều khiển truy cập chuẩn*** kiểu số:

  Router(config)# **access-list** [*access-list-number]* [**deny** | **permit** | **remark**] *source* [*source-wildcard*]

- Cú pháp cơ bản của ***danh sách điều khiển truy cập mở rộng*** kiểu số:

Router(config)#**access-list** [*access-list-number*] [permit | deny] [protocol] [source address]

[wildcard mask] [source port] [destination address] [wildcard mask] [destination port]

- Để bỏ ACL khỏi router, dùng lệnh: Router(config)# **no access-list** *access-list-number*

- Để xem các ACL có trên router, dùng lệnh: Router# **show access-list**

CANTHO UNIVERSITY

ACL KIỂU TÊN

- Cú pháp cơ bản của ***danh sách điều khiển truy cập chuẩn*** kiểu tên:

Router(config)# **ip access-list standard** *ACL_NAME*

Router(config-std-nacl)# { **deny** | **permit** | **remark** } *source* [*source-wildcard*]

- Cú pháp cơ bản của ***danh sách điều khiển truy cập mở rộng*** kiểu tên:

Router(config)# **ip access-list extended** *ACL_NAME*

Router(config-ext-nacl)# [**{deny | permit** | **remark}** protocol source source-wildcard

destination destination-wildcard

CANTHO UNIVERSITY

TỔNG QUAN CÁC LOẠI LỆNH TRONG ACL

Hai loại tổng quát sau:

1.Lệnh loại 1: Bao gồm các lệnh cơ bản để xử lý các vấn đề tổng quát được mô tả ở phần trước (ACL kiểu số và kiểu tên)

(Vào giao diện cần gán ACL: Router(config)# interface {Name} {number})

2.Lệnh loại 2: danh sách truy cập được tạo bởi lệnh loại 1 sẽ được ***đặt vào giao diện của router, theo một hướng lưu thông cần kiểm soát***.

Cú pháp như sau:

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

CANTHO UNIVERSITY

TỔNG QUAN CÁC LOẠI LỆNH TRONG ACL

Loại 1: khai báo phát biểu của ACL

Loại 2: Gán ACL vào giao diện mạng + hướng kiểm soát

Step 1: Use the `access-list` global configuration command to create an entry in a standard IPv4 ACL.

```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
```

The example statement matches any address that starts with 192.168.10.x. Use the `remark` option to add a description to your ACL.

Step 2: Use the `interface` configuration command to select an inteface to which to apply the ACL.

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

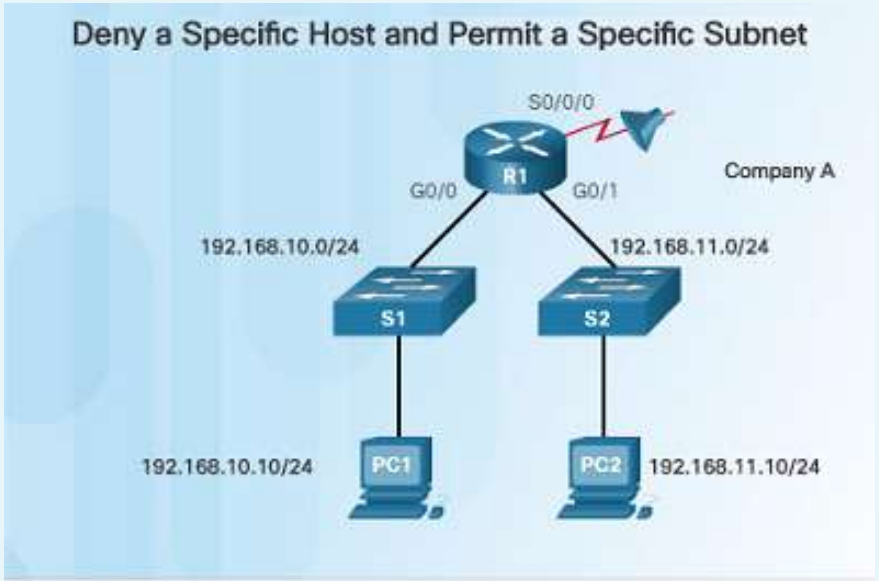
Step 3: Use the `ip access-group` interface configuration command to activate the existing ACL on an interface.

```
R1(config-if)# ip access-group 1 out
```

This example activates the standard IPv4 ACL 1 on the interface as an outbound filter.

CANTHO UNIVERSITY

VÍ DỤ VỀ KHAI BÁO ACL KIỂU SỐ

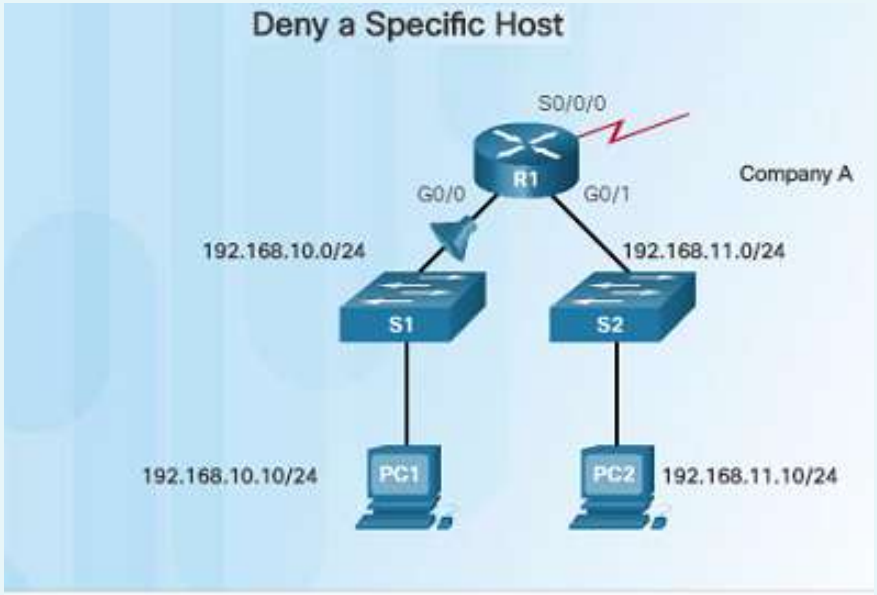



```
R1(config)# no access-list 1
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 1 out
```

- Hình bên trái là một ví dụ về ACL: cho phép lưu thông truy cập từ một nhánh mạng cụ thể (192.168.10.0/24) nhưng từ chối truy cập từ một máy (192.168.10.10/24) trong mạng đó .
- Lệnh *no access-list 1* sẽ xóa phiên bản trước của ACL 1
- Câu lệnh ACL tiếp theo từ chối máy có địa chỉ 192.168.10.10/24
- Câu lệnh kế tiếp, tất cả các máy chủ khác trên nhánh mạng 192.168.10.0/24 sau đó đều được phép
- Có một phát biểu ngầm (ẩn) từ chối tất cả các nhánh mạng khác
- Để ACL có hiệu lực, ACL 1 được áp dụng vào giao diện của router theo hướng ra ngoài trên giao diện S0/0/0

CANTHO UNIVERSITY

VÍ DỤ VỀ KHAI BÁO ACL KIỂU SỐ

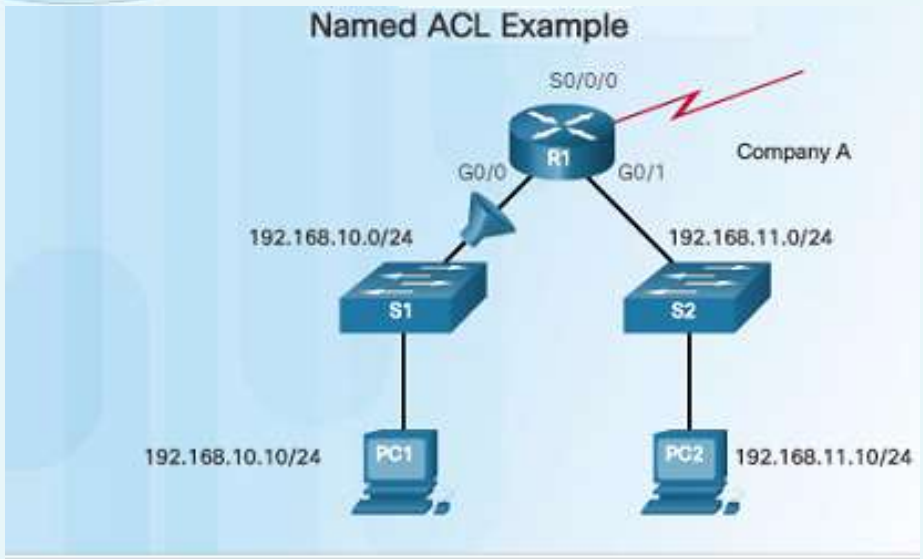



```
R1(config)# no access-list 1
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 permit any
R1(config)# interface g0/0
R1(config-if)# ip access-group 1 in
```

- Ví dụ tiếp theo này minh họa một ACL từ chối một máy chủ cụ thể nhưng sẽ cho phép tất cả các lưu lượng truy cập khác
- Câu lệnh ACL đầu tiên xóa phiên bản ACL 1 trước đó
- Lệnh tiếp theo, lưu thông truy cập từ máy PC1 có địa chỉ 192.168.10.10 sẽ bị ***từ chối***
- Lệnh tiếp theo ***cho phép tất cả*** các máy còn lại trong mạng
- ACL 1 này được áp dụng ***ngõ vào (in)*** giao diện G0/0 của router vì nó chỉ ảnh hưởng đến mạng LAN 192.168.10.0/24

CANTHO UNIVERSITY

VÍ DỤ VỀ KHAI BÁO ACL KIỂU TÊN

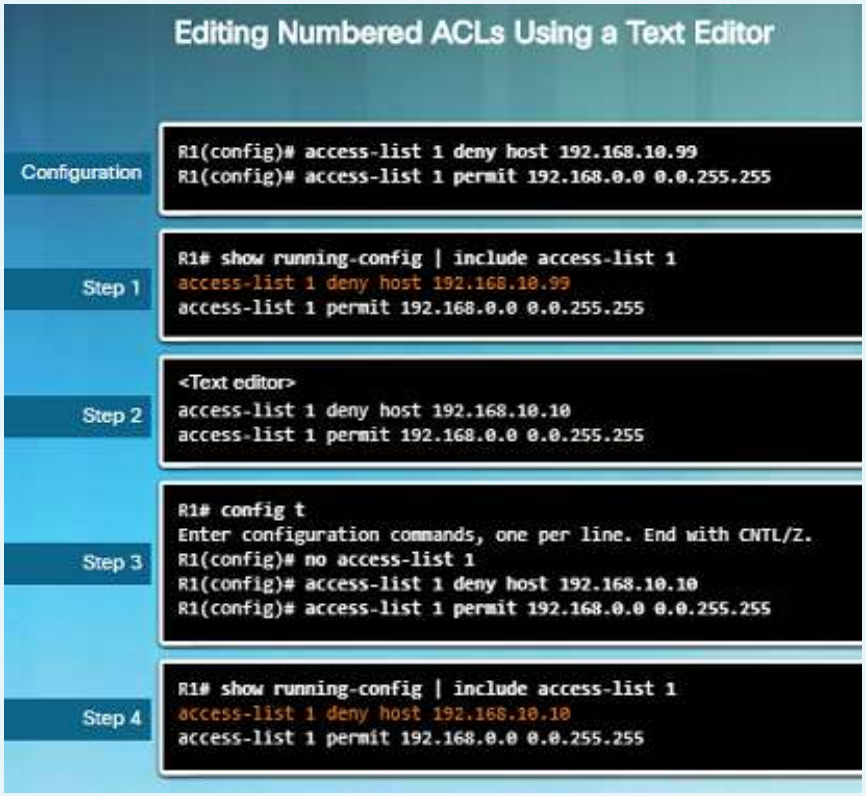



```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group NO_ACCESS out
```

- ACL được khai báo bằng tên thay vì một con số giúp người quản trị dễ hiểu chức năng của nó hơn
  Ví dụ bên trái cho thấy cách định cấu hình danh sách truy cập tiêu chuẩn kiểu tên
- Lưu ý cách các lệnh hơi khác một chút:
  - Sử dụng lệnh ***ip access-list*** để tạo ACL có tên
  - Tên dùng chữ và số, phân biệt chữ hoa chữ thường và phải là duy nhất
  - ACL được áp dụng trên giao diện bằng lệnh: ***ip access-group*** {name} {in/out}

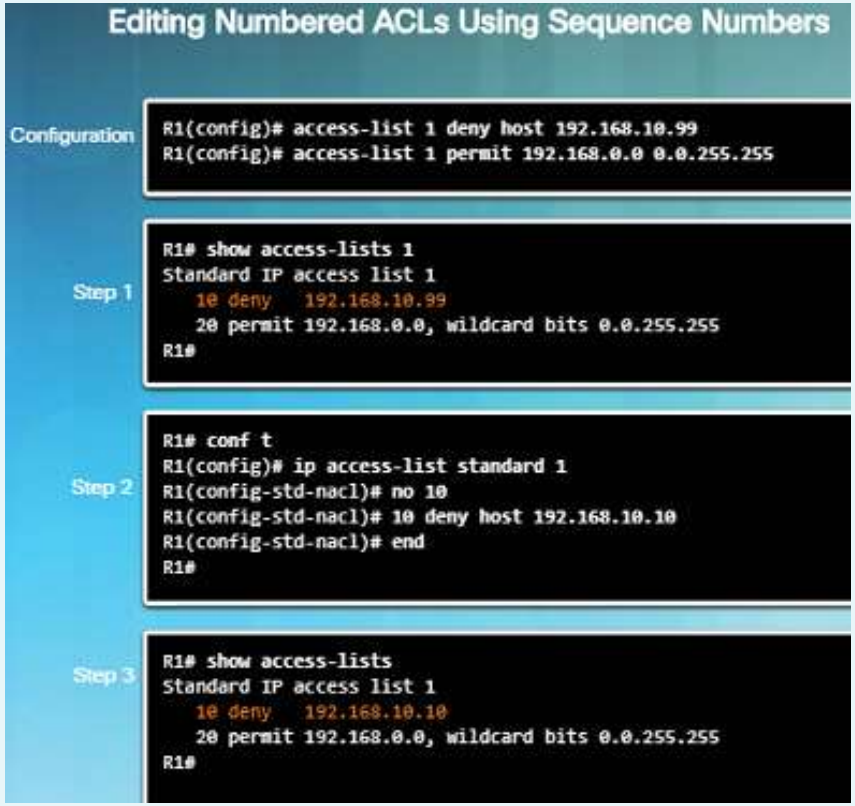
CANTHO UNIVERSITY

SOẠN THẢO ACL
CÁCH 1: SỬ DỤNG TEXT EDITOR



- Tạo và chỉnh sửa ACL trong một trình soạn thảo văn bản (Vd Microsoft Notepad) sẽ dễ dàng hơn thay vì thực hiện các thay đổi trực tiếp trên bộ định tuyến
- Đối với ACL hiện có, sử dụng lệnh ***show running-config*** để hiển thị ACL, sao chép và dán nó vào trình soạn thảo văn bản, thực hiện các thay đổi cần thiết, sau đó dán lại vào giao diện bộ định tuyến
- Điều quan trọng cần lưu ý là khi sử dụng lệnh ***no access-list***, các bản phát hành phần mềm IOS khác nhau sẽ hoạt động khác nhau

SOẠN THẢO ACL
CÁCH 2: DÙNG SỐ THỨ TỰ TRƯỚC PHÁT BIỂU ACL ĐỂ SỬA CÂU LỆNH



Có thể thay đổi ACL được đánh số bằng cách sử dụng số thứ tự của lệnh

- *Bước 1* – xác định vấn đề: Giả sử câu lệnh deny 192.168.10.99 không chính xác; máy bị từ chối là 192.168.10.10
- *Bước 2* – thực hiện việc thay đổi dựa vào số thứ tự câu lệnh: Câu lệnh bị cấu hình sai phải được xóa bằng lệnh: ***no 10***
- Bước 3 – thay câu lệnh mới: *dùng cú pháp gọi câu lệnh ACL kiểu tên*, câu lệnh mới với địa chỉ máy chính xác đã được thêm vào: ***10 deny host 192.168.10.10***
- Bước 4 – kiểm tra lại câu lệnh thay thế đã được cập nhật?

SOẠN THẢO ACL
CÁCH 2: DÙNG SỐ THỨ TỰ TRƯỚC PHÁT BIỂU ACL ĐỂ SỬA CÂU LỆNH

```
R1# show access-lists
Standard IP access list NO_ACCESS
    10 deny   192.168.11.10
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# 15 deny host 192.168.11.11
R1(config-std-nacl)# end
R1# show access-lists
Standard IP access list NO_ACCESS
    10 deny   192.168.11.10
    15 deny   192.168.11.11
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

- Lệnh **no** *sequence-number* thường được dùng để xóa lệnh riêng lẻ trong ACL

- Dùng lệnh ***show access-list*** để tham chiếu đến *số thứ tự câu lệnh*
- Các câu lệnh riêng lẻ có thể được chèn hoặc xóa dễ dàng.

Vd hình bên trái cho thấy cách chèn một dòng vào ACL kiểu tên. Bằng cách đánh số 15, lệnh mới sẽ được chèn giữa câu lệnh 10 và 20

CANTHO UNIVERSITY

KIỂM TRA VIỆC KHAI BÁO ACL

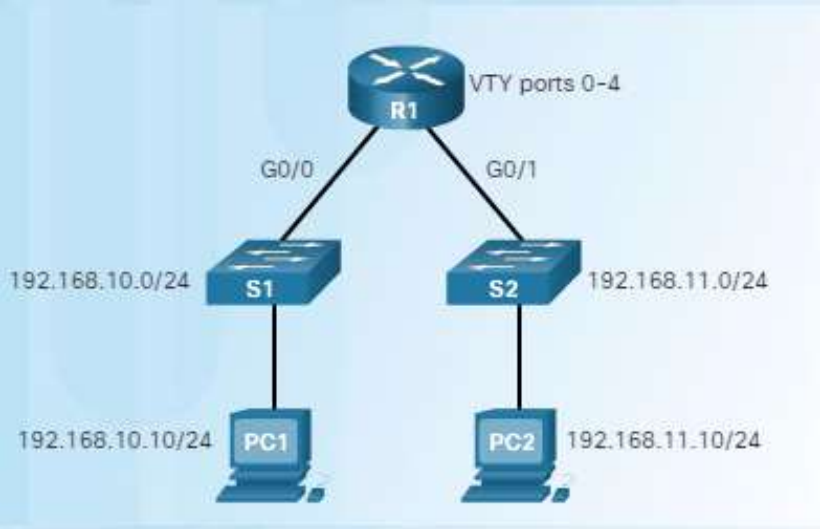
```
R1# show ip interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30
<output omitted>
  Outgoing access list is 1
  Inbound access list is not set
<output omitted>

R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<output omitted>
  Outgoing access list is NO_ACCESS
  Inbound access list is not set
<output omitted>
```

```
R1# show access-lists
Standard IP access list 1
   10 deny 192.168.10.10
   20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
   15 deny 192.168.11.11
   10 deny 192.168.11.10
   20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

- Sử dụng lệnh ***show ip interface*** để kiểm tra xem ACL được áp dụng cho đúng giao diện hay chưa
- Tên của ACL sẽ hiển thị và hướng lưu thông cần kiểm tra (*in/out*) đang được áp dụng trên giao diện
- Lệnh ***show access-lists*** sẽ hiển thị toàn bộ các danh sách truy cập được cấu hình trên router

KIỂM SOÁT TRUY CẬP QUA CÁC CỔNG VIRTUAL TERMINAL (VTY) LỆNH ACCESS-CLASS

CANTHO UNIVERSITY




```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# access-class 21 in
R1(config-line)# exit
R1(config)# access-list 21 permit 192.168.10.0 0.0.0.255
R1(config)# access-list 21 deny any
```

- Quyền truy cập vào các cổng Virtual teletype – VTY – để quản trị nên được hạn chế để giúp cải thiện bảo mật
- Hạn chế truy cập qua các cổng Virtual teletype – VTY – là một kỹ thuật cho phép bạn xác định địa chỉ IP nào được phép truy cập từ xa vào router hay thiết bị mạng
- Lệnh ***access-class*** được định cấu hình trong chế độ cấu hình dòng lệnh sẽ hạn chế các kết nối đến và đi giữa một VTY cụ thể và các địa chỉ trong danh sách truy cập.
- Cú pháp:

Router(config-line) # **access-class** *{access-list-number} {in [vrf-also] | out }*

CANTHO UNIVERSITY

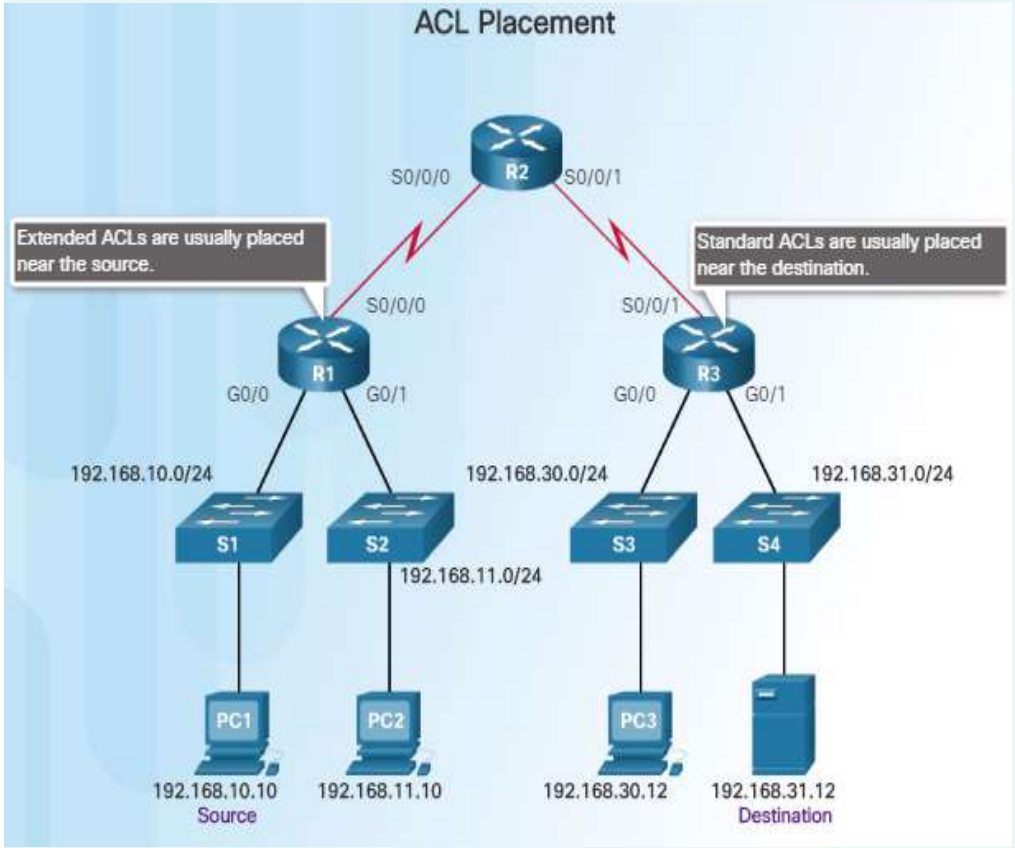
CÁC CHÚ Ý KHI TẠO ACL

Cần thực hiện	Thuận lợi
Tạo ACL dựa trên chính sách an ninh của công ty	Đảm bảo được tính hợp lý và đúng qui định của công ty
Cần có bảng liệt kê chi tiết những chính sách lưu thông cần kiểm soát	Điều này giúp tránh được các nguy cơ tiềm tàng khi triển khai
Dùng một phần mềm soạn thảo văn bản để tạo ACL	Giúp dễ dàng tạo và sử dụng lại khi cần sửa đổi
Kiểm tra cẩn thận trước khi triển khai trên hệ thống thực đang vận hành	Tránh khả năng gây lỗi và khắc phục trên hệ thống thực

- Tạo ACL cần sự chú ý đến các chi tiết. Cấu hình sai lầm có thể gây tổn hại mạng, giảm hiệu suất, tốn nhiều thời gian để kiểm tra, xử lý, khắc phục

CANTHO UNIVERSITY

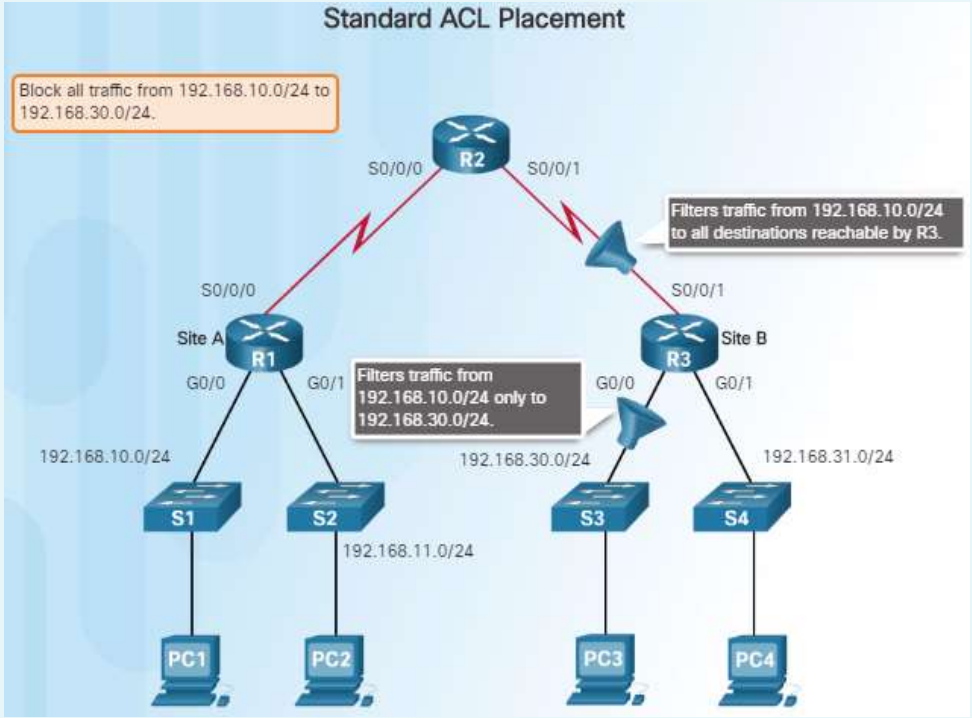
CÁC CHÚ Ý VỊ TRÍ ĐẶT ACL



- Việc đặt ACL đúng cách có thể làm cho mạng hoạt động hiệu quả hơn
- Mỗi ACL nên được đặt ở vị trí mà nó có tác động lớn nhất đến hiệu quả của chính sách an ninh:
  - ***ACL chuẩn*** - Vì ACL chuẩn kiểm tra địa chỉ nguồn của gói tin lưu thông nên ACL *đặt càng gần đích càng tốt*
  - ***ACL mở rộng*** - ACL mở rộng *đặt càng gần nguồn của lưu thông được lọc càng tốt*. Điều này sẽ ngăn chặn từ đầu các lưu thông truy cập không mong muốn, tránh lãng phí hiệu suất mạng

CANTHO UNIVERSITY

VÍ DỤ VỀ VỊ TRÍ ĐẶT ACL



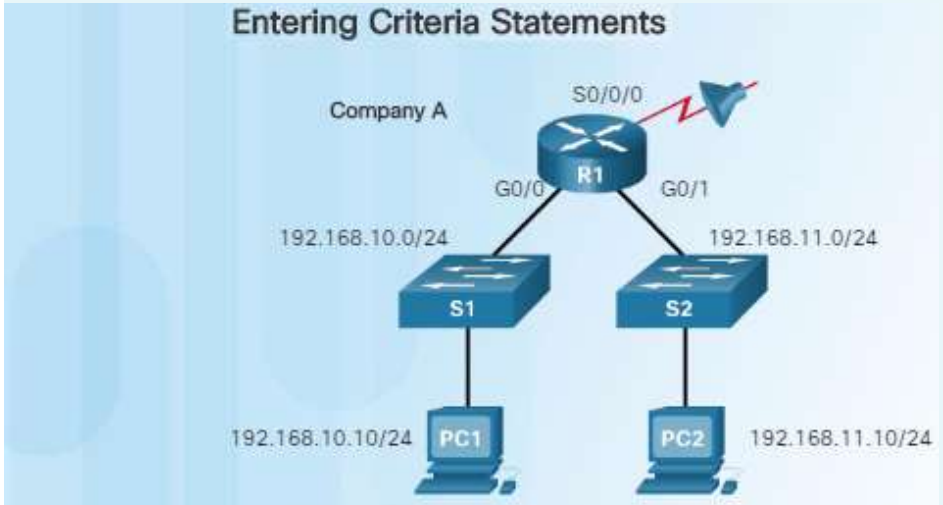
Ví dụ này minh họa vị trí thích hợp của ACL chuẩn được cấu hình để chặn lưu thông truy cập từ mạng 192.168.10.0/24 đến mạng 192.168.30.0/24, có hai nơi có thể để cấu hình ACL trên R3

- Nếu danh sách truy cập được áp dụng cho giao diện S0/0/1, nó sẽ chặn lưu thông truy cập đến mạng 192.168.30.0/24, ngoài ra, nó còn chặn luôn cả lưu thông của mạng 192.168.10.0/24 đối với mạng 192.168.31.0/24
- Nơi tốt nhất để áp dụng ACL là trên giao diện G0/0 của R3. ACL sẽ được áp dụng cho lưu thông đi ra khỏi giao diện G0/0. Các gói từ 192.168.10.0/24 vẫn có thể đến 192.168.31.0/24

MỘT SỐ SAI SÓT THƯỜNG GẶP KHI THIẾT LẬP ACL

CANTHO UNIVERSITY

VẤN ĐỀ deny any ẨN



ACL 1

```
R1(config)# access-list 1 permit ip 192.168.10.0 0.0.0.255
```

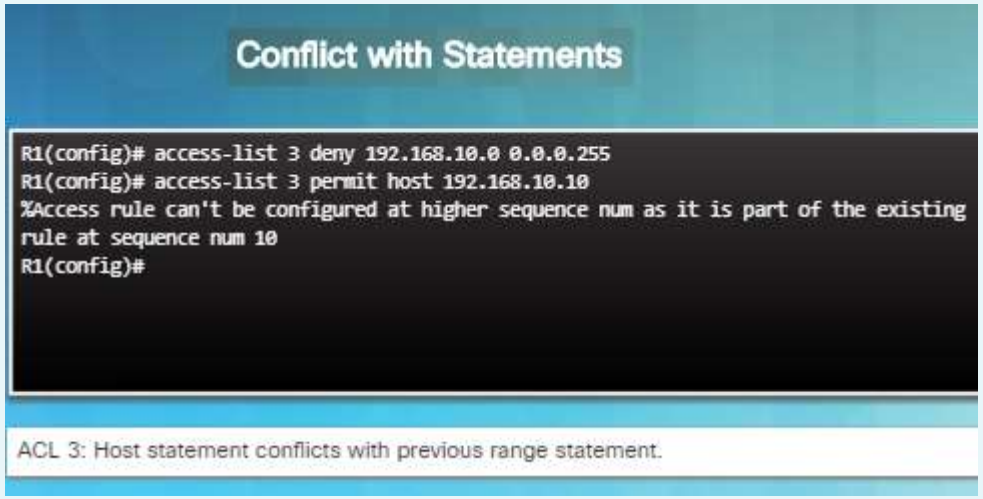
ACL 2

```
R1(config)# access-list 2 permit ip 192.168.10.0 0.0.0.255
R1(config)# access-list 2 deny any
```

- ACL một mục nhập chỉ có *một* khai báo ***deny any*** sẽ từ chối tất cả lưu thông đi qua giao diện
- Trong một ACL phải có *có ít nhất* một mục nhập có từ khóa ***permit***, nếu không thì tất cả các lưu thông sẽ bị chặn
- Quan sát hai ACL 1 & 2 trong hình bên trái:

Kết quả sẽ giống nhau hay khác nhau?

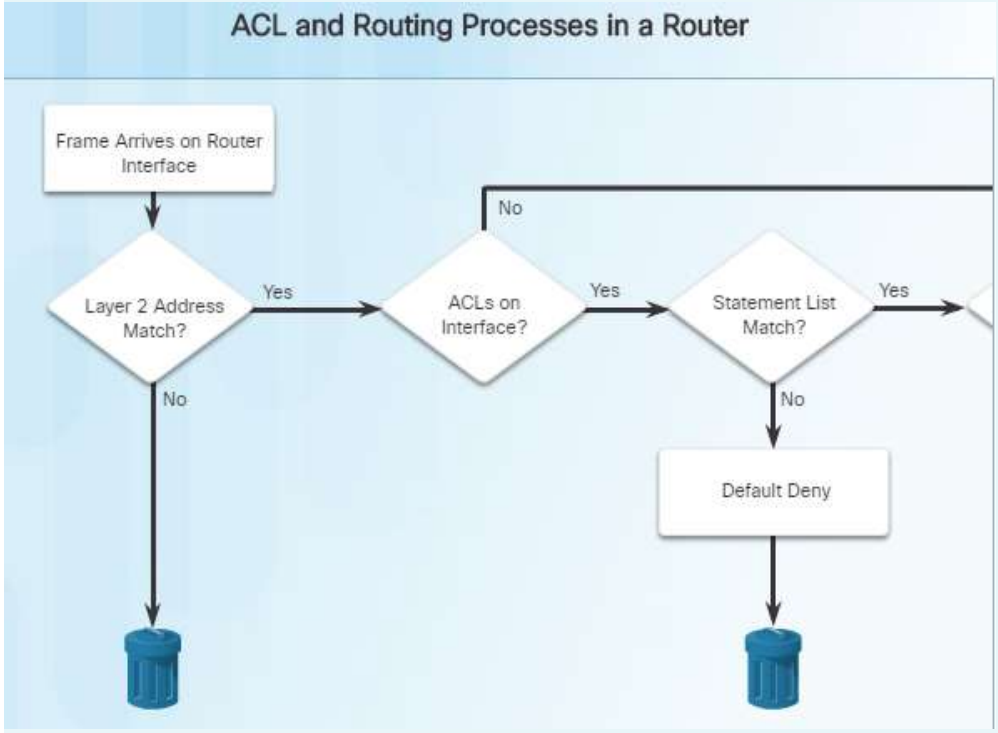
THỨ TỰ CÂU LỆNH TRONG ACL



- Thứ tự câu lệnh trong ACL rất quan trọng vì các câu lệnh được xử lý tuần tự
- Ví dụ: Hình bên trái thể hiện mâu thuẫn giữa hai câu lệnh vì được khai báo không đúng thứ tự, sai logic: Câu lệnh đầu tiên đã chặn tất cả các máy trong mạng 192.168.10.0/24. Tuy nhiên, câu lệnh thứ hai lại cho phép máy 192.168.10.10 lưu thông qua. Câu lệnh này sẽ không có ý nghĩa vì nó là một tập hợp con của câu lệnh trước đó. Đảo ngược thứ tự của hai câu lệnh này sẽ giải quyết được vấn đề.

XỬ LÝ GÓI TIN QUA GIAO DIỆN CÓ ACL
QUÁ TRÌNH ĐỊNH TUYẾN VÀ ACL

CANTHO UNIVERSITY



- Khi một gói tin ***đến*** giao diện của router, quy trình kiểm tra gói tin của router sẽ giống nhau, cho dù ACL có được cấu hình hay không
- Sau khi tháo bỏ header của khung đến, router sẽ đọc thông tin trên header của gói tin và kiểm tra trên ACL đặt ở giao diện gói tin gửi đến:

➢ Nếu một ACL tồn tại, gói tin được kiểm tra dựa trên các phát biểu trong ACL

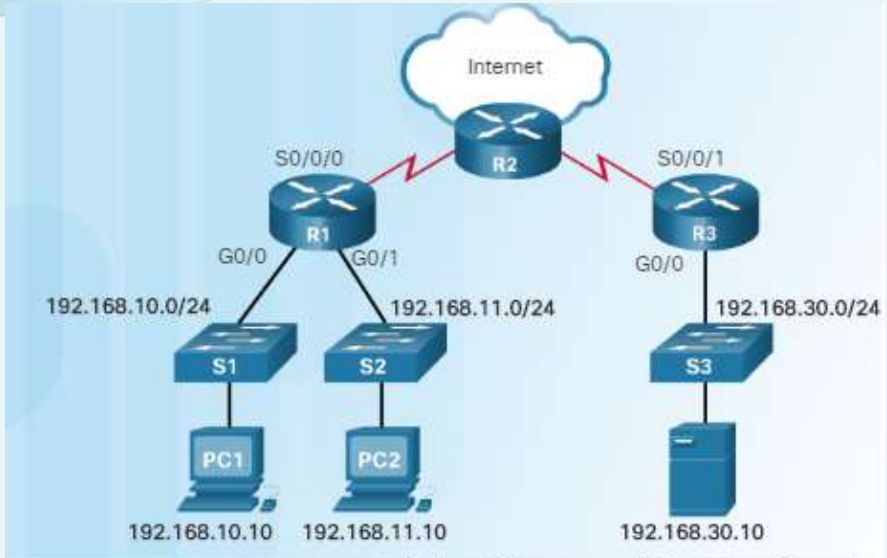
➢ Nếu gói tin khớp với một dòng phát biểu nào đó thì gói tin đó được chuyển tiếp hay vứt bỏ (tùy thuộc vào từ khóa permit/deny)

➢ Ở hướng đi vào, nếu gói tin được phép (permit) và sau khi router xử lý gói, nếu có đường đi, router chuyển mạch qua giao diện ngõ ra

➢ Nếu giao diện ngõ ra có ACL, việc kiểm tra được thực hiện tương tự trước khi quyết định chuyển tiếp

CANTHO UNIVERSITY

MỘT SỐ LỖI KHI CẤU HÌNH ACL
VÍ DỤ 1




```
R3# show access-list
Standard IP access list 10
    10 deny 192.168.11.10
R3#
```

```
R3(config)# access-list 10 permit any
R3(config)# end
R3# show access-list
Standard IP access list 10
    10 deny 192.168.11.10
    20 permit any (4 match(es))
R3#
```

Các lỗi phổ biến nhất liên quan đến ACL:

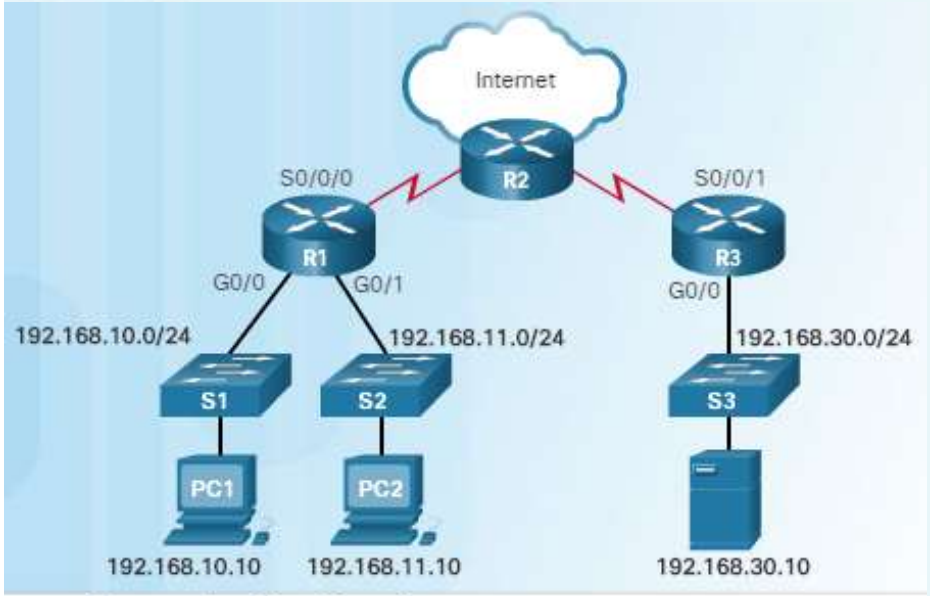
- Nhập các lệnh không đúng thứ tự
- Không chỉ định các quy tắc ACL đầy đủ
- Áp dụng ACL sai hướng, sai giao diện hoặc sai địa chỉ nguồn
- Trong hình bên trái:

  ➢ PC2 sẽ không thể truy cập Server. Tuy nhiên, PC1 cũng không thể truy cập nó vì lệnh show access-list chỉ hiển thị một câu lệnh từ chối trong ACL.

  ➢ Giải quyết: khai báo lại như các lệnh bên phải. Lệnh ***permit any*** cho phép các thiết bị khác truy cập vì deny any ẩn đang chặn lưu thông khác.

MỘT SỐ LỖI KHI CẤU HÌNH ACL
VÍ DỤ 2

CANTHO UNIVERSITY




```
R1# show run | section line vty
line vty 0 4
 access-class PC1-SSH in
 login
 transport input ssh
R1# show access-list
Standard IP access list PC1-SSH
    10 permit 192.168.10.1
    20 deny   any (5 match(es))
R1#
```

- *Yêu cầu:* Chỉ PC1 mới được phép chuyển SSH đến R1
- *Lỗi:* xem cấu hình trong hình bên trái, PC1 không thể SSH thành công đến R1 vì ACL đang cho phép địa chỉ 192.168.10.1 là địa chỉ của giao diện G0/0 chứ không phải địa chỉ của PC1
- *Khắc phục:* xem khai báo lại ở hình bên phải

```
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip access-list standard PC1-SSH
R1(config-std-nacl)# no 10
R1(config-std-nacl)# 10 permit host 192.168.10.10
R1(config-std-nacl)# end
R1# clear access-list counters
R1# show access-list
Standard IP access list PC1-SSH
    10 permit 192.168.10.10 (2 match(es))
    20 deny   any
R1#
```

HẾT CHƯƠNG 9