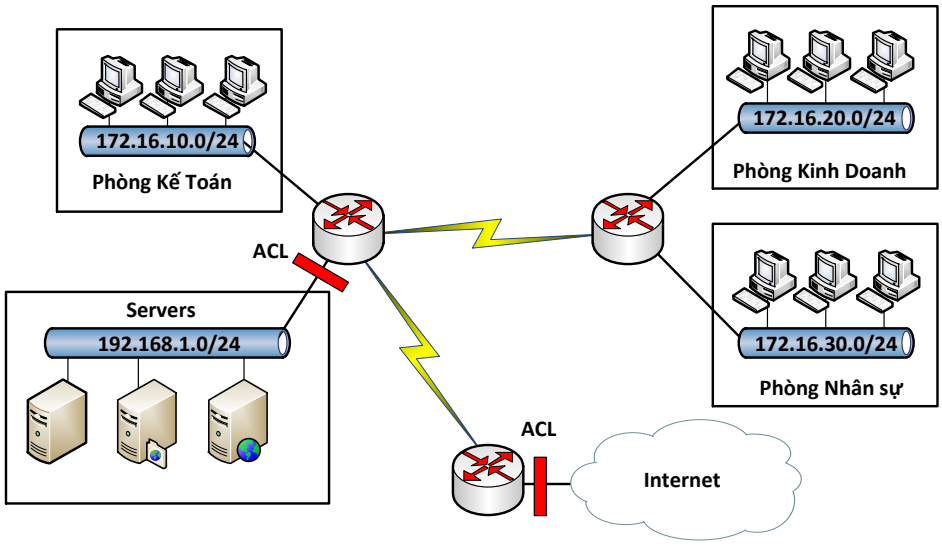
CHƯƠNG ACL

Chương này trình bày chức năng và đặc điểm của việc sử dụng ACL trong hệ thống mạng để điều khiển các truy cập, đặc điểm của các loại ACL và cách thức cấu hình trên thiết bị Cisco. Học xong chương này, người học có khả năng:

- *Xác định được vai trò của ACL trong hệ thống mạng*
- *Phân biệt và cấu hình được "Standard ACL" và "Extended ACL" sử dụng hai phương pháp cấu hình là Numbered ACL và Named ACL*
- *Vận dụng ACL trong các bài toán cụ thể*

1. Giới thiệu

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.

2. Phân loại và hoạt động của 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 so 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. Vì vậy, trong cầu 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.

3. Cấu hình ACL

Có 2 phương pháp cấu hình ACL:

- Dựa vào số (numbered ACL)

- Dựa vào tên (named ACL)

Tổng quát: 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

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**

"Wildcard mask" có 32 bit, chia thành 4 phần, mỗi phần có 8 bit, là tham số được dùng xác định các bit nào sẽ được bỏ qua hay buộc phải so trùng trong việc kiểm tra điều kiện. Bit '1' trong "wildcard mask" có nghĩa là bỏ qua vị trí bit đó khi so sánh, và bit '0' xác định vị trí bit đó phải giống nhau.

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

Mặc dù "Wildcard mask" có cấu trúc 32 bit giống với "Subnet mask" nhưng chúng hoạt động khác nhau. Các bit 0 và 1 trong một "Subnet mask" xác định phần "Network" và phần "Host" trong một địa chỉ IP. Các bit 0 và 1 trong một "wildcard-mask" xác định bit nào sẽ được kiểm tra hay bỏ qua cho mục đích điều khiển truy cập.

- **Wildcard "host"**

- ✓ "Wildcard mask" dùng cho một thiết bị hay còn gọi là "wildcard-host" có dạng: 0.0.0.0 (kiểm tra tất cả các bit)

  Ví dụ: 172.30.16.29 0.0.0.0
- ✓ Ý nghĩa: khi kiểm tra ACL, nó sẽ kiểm tra tất cả các bit trong địa chỉ dùng để so khớp.
- ✓ "Wildcard mask" cho một thiết bị có thể được đại diện bằng từ khóa "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
```

- **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.

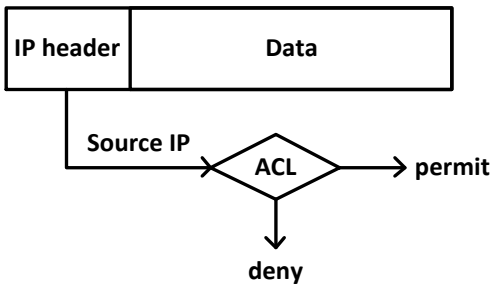
Luồng dữ liệu vào Luồng dữ liệu ra

4. Standard ACL

Sử dụng *"Standard ACL"* 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 ACL" 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

- `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

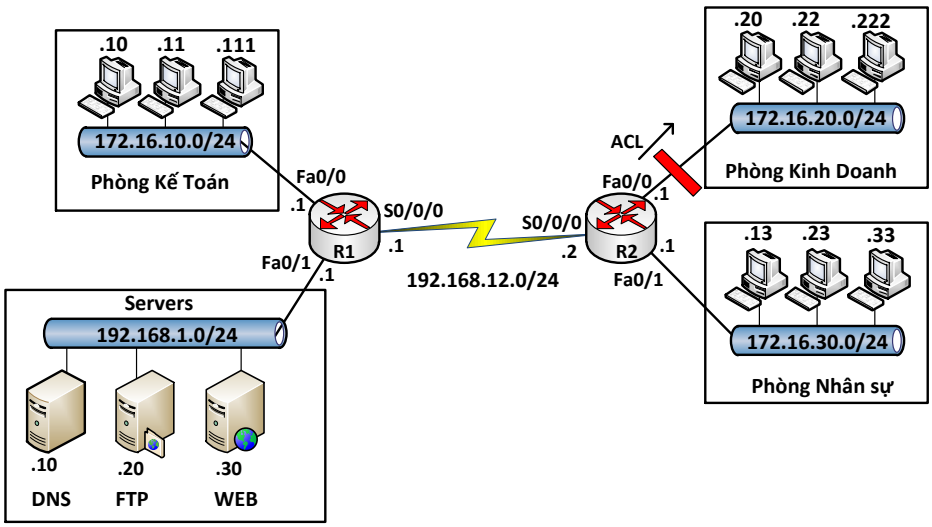
  Wildcast-mask: nếu không được cấu hình sẽ lấy giá trị mặc định là:0.0.0.0

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

Câu lệnh này có tác dụng gán ACL vào một cổng và đặt chế độ kiểm tra cho luồng dữ liệu đi vào hay đi ra khỏi cổng của router.

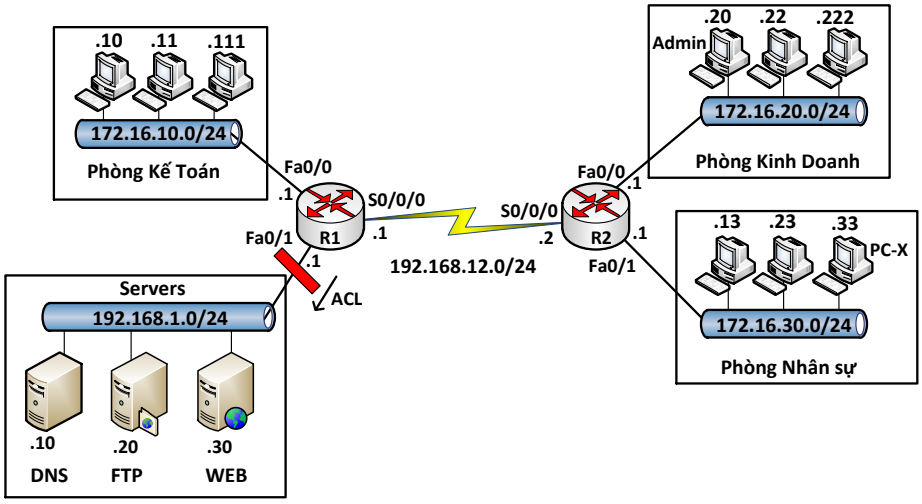
Dùng lệnh **no ip access-group** <*ACL-number*> để không áp đặt ACL vào cổng. Có nghĩa là huỷ bỏ câu lệnh trên.

Ví dụ 1: Cấm các máy tính thuộc mạng 172.16.10.0/24 truy cập tới mạng 172.16.20.0/24.




```
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
```

Ví dụ 2: Cấm 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
```

Ví dụ 3. Sử dụng lại mô hình trong ví dụ 2, viết ACL chỉ cho phép máy Admin có IP 172.16.20.20 telnet vào các router R1, R2.

Hướng dẫn cấu hình: trước tiên, cấu hình mở telnet trên R1 và R2.

ACL thực hiện yêu cầu đầu bài: trên R1 và R2 sử dụng ACL sau

```
R(config)#access-list 20 permit host 172.16.20.20
R(config)#line vty 0 4
R(config-line)#access-class 20 in
```

❖ **Dùng "Standard ACL" để điều khiển telnet**

Trên router có các "virtual terminal port" được dùng để cấu hình cho mục đích cho phép telnet vào router. Telnet cũng là một cách thức cho phép người quản trị cấu hình hay theo dõi thiết bị từ xa. Ta có thể lọc các địa chỉ truy xuất vào các cổng này bằng "Standard ACL".

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}
```

Trong đó:

vty-number: có giá trị 0 đến 4 (mặc định trên Router), có giá trị 0 đến 15 (mặc định trên Switch)

vty-range: là một dãy liên tiếp các port vty được sử dụng. Trong cấu hình ta sẽ cấu hình như sau: line vty start-number end-number

access-list-number: ACL gán vào các cổng **vty** để điều khiển truy cập

Ví dụ:

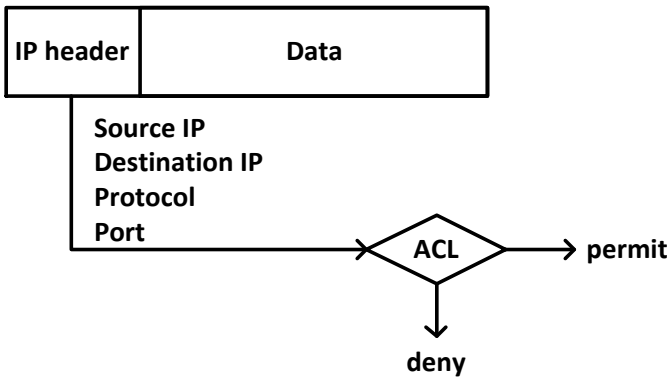
```
access-list 12 permit 192.168.1.0 0.0.0.255
(implicit deny all)
!
line vty 0 4
 access-class 12 in
```

Các câu lệnh cấu hình trên có nghĩa là: chỉ cho phép các thiết bị thuộc mạng 192.168.1.0/24 có thể kết nối vào router thông qua telnet.

5. 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

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

  Trong đó: *access-list-number*: có giá trị từ 100 – 199 hoặc 2000 - 2699

  protocol: là ip, udp, tcp, icmp,…

  operator: thường dùng là **eq**

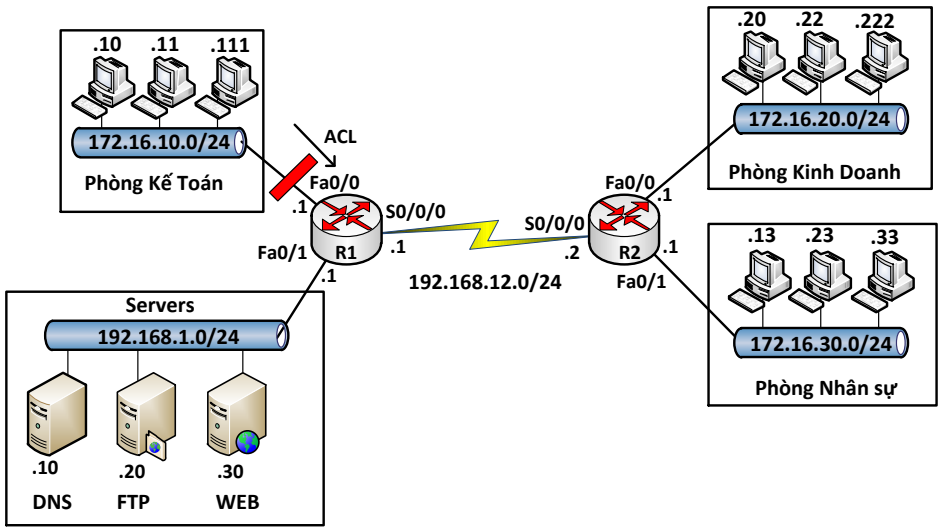
  operand: là chỉ số port của dịch vụ hay tên của dịch vụ. Ví dụ: ta có thể dùng chỉ số port ***23*** hay có thể dùng tên dịch vụ là ***telnet***

  Câu lệnh trên được dùng để tạo một điều kiện (ACL entry) trong một ACL *access-list-number*

- `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. Câu lệnh này có ý nghĩa là gán danh sách ACL vào interface và chọn hướng (*inbound hoặc outbound*) các traffic sẽ được kiểm tra

Ví dụ 1: 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.

6. 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}
```

❖ **Một số lệnh kiểm tra cấu hình ACL**

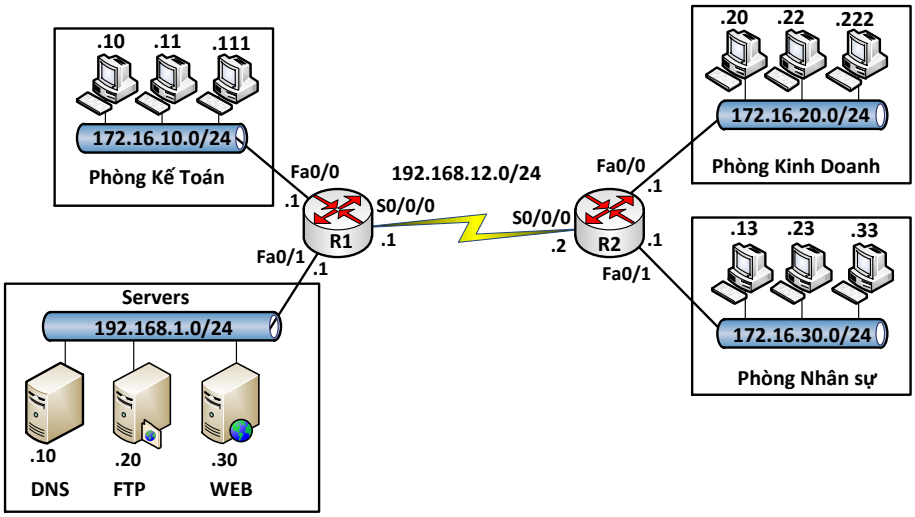
```
Router#show access-list {access-list-number | name}
```

Sau đây một ví dụ về kết quả hiển thị của lệnh *show access-lists*

```
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:



❖ **Yêu cầu:**

(1) Cấu hình standard 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
```

- 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 acccess-group xyz in
```

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

```
R1(config)#ip access-list extended spkt
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 spkt out
```

(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

```
show run
show ip route
show access-lists
```

7. Tổng kết chương

ACL có thể xem như là một tường lửa nhỏ định ra một tập luật để chặn các truy cập bất hợp pháp được cấu hình trên các router.

ACL được chia làm hai loại: *standard ACL* và *Extended ACL*. Trong đó, *standard ACL* thường được đặt ở gần đích, còn *Extended ACL* thường đặt ở gần nguồn cần cấm luồng dữ liệu.

ACL hoạt động theo trình tự cấu hình được thiết lập, khi một điều kiện được so khớp thì các câu lệnh còn lại sẽ không được kiểm tra nữa và cuối danh sách luôn có câu lệnh mặc định là *"deny all"*.

8. Câu hỏi và bài tập

8.1. ACL sau đây được áp đặt vào cổng fa0/0 theo chiều outbound:

```
access-list 123 deny tcp 192.168.1.8 0.0.0.7 eq 20 any
access-list 123 deny tcp 192.168.1.9 0.0.0.7 eq 21 any
```

Cho biết ý nghĩa của ACL trên?

A. Tất cả các gói tin sẽ được cho phép đi qua cổng fa0/0 trừ các gói tin FTP.

B. Cấm các gói tin FTP xuất phát từ 192.168.1.22 đến bất kỳ đâu

C. Cấm các gói tin FTP xuất phát từ 92.168.1.9 đến bất kỳ đâu

D. Tất cả các gói tin đi qua cổng fa0/9 đều bị cấm.

E. Cấm các gói tin FTP từ bất kỳ đâu đến mạng 192.168.1.8/29

8.2. Standard ACL lọc các gói tin dựa vào thành phần nào trong gói tin?

A. Dựa vào địa chỉ IP nguồn và IP đích

B. Dựa vào chỉ số port đích

C. Dựa vào địa chỉ IP nguồn

D. Tất cả các câu trên

8.3. ACL nào sau đây được sử dụng để cấm telnet xuất phát từ mạng 210.93.105.0/24 đến mạng 223.8.151.0/24?.

A.
```
access-list one deny 210.93.105.0 0.0.0.0 any eq 23
access-list one permit any
```

B.
```
access-list 100 deny tcp 210.93.105.0 0.0.0.255 223.8.151.0
0.0.0.255 eq 23
```

C.
```
access-list 100 deny ip 223.8.151.0 0.0.0.255 any 23
access-list 100 permit ip any any
```

D.
```
access-list 100 deny tcp 210.93.105.0 0.0.0.255 223.8.151.0
0.0.0.255 eq telnet
access-list 100 permit ip any any
```

8.4. Câu nào sau đây là "Standard ACL"?.

A. `access-list 10 permit 192.168.1.0 0.0.0.255`

B. `access-list 100 deny host 192.168.1.100`

C. `access-list 101 permit ip any 192.168.1.0 0.0.0.255`

D. `access-list 10 permit tcp 192.168.1.0 0.0.0.255 any`

8.5. Công ty XYZ sử dụng *Subnet mask* /29. *Wildcard mask* được sử dụng để cấu hình ACL để *permit* hay *deny* truy cập cho mạng này?

A. 255.255.255.224

B. 255.255.255.248

C. 0.0.0.224

D. 0.0.0.8

E. 0.0.0.7

F. 0.0.0.3

8.6. Một ACL được cấu hình như sau:

```
access-list 10 permit 172.29.16.0 0.0.0.255
access-list 10 permit 172.29.17.0 0.0.0.255
access-list 10 permit 172.29.18.0 0.0.0.255
```

```
access-list 10 permit 172.29.19.0 0.0.0.255
```

Lệnh nào sau đây có thể thay thế cho tất cả các lệnh trên?

A. `Access-list 10 permit 172.29.16.0  0.0.0.255`

B. `Access-list 10 permit 172.29.16.0  0.0.1.255`

C. `Access-list 10 permit 172.29.16.0  0.0.3.255`

D. `Access-list 10 permit 172.29.16.0  0.0.15.255`

E. `Access-list 10 permit 172.29.0.0  0.0.255.255`

8.7. ACL nào sau đây là ví dụ dùng để cấm các gói tin xuất phát từ một host cụ thể?

A. `router(config)#access list 1 deny 17231.212.74`

B. `router(config)#access list 1 deny 10.6.111.48 host`

C. `router(config)#access list 1 deny 172.16.4.13 0.0.0.0`

D. `router(config)#access list 1 deny 192.168.14.132 255.255.255.0`

E. `router(config)#access list 1 deny 192.168.166.127 255.255.255.255`

8.8. ACL nào sau đây được dùng để cấm tất cả các gói tin telnet đến mạng 10.10.1.0/24?

A. `access-list 15 deny telnet any 10.10.1.0 0.0.0.255 eq 23`

B. `access0list 115 deny udp any 10.10.1.0 eq telnet`

C. `access-list 15 deny tcp 10.10.1.0  255.255.255.0 eq telnet`

D. `access-list 115 deny tcp any 10.10.1.0 0.0.0.255 eq 23`

E. `access-list 15 deny udp any 10.10.1.0 255.255.255.0 eq 23`

8.9. ACL được cấu hình trong router như sau:

```
router#show access-lists
Extended IP access list 110
10 deny tcp 172.16.0.0 0.0.255.255 any eq telnet
20 deny tcp 172.16.0.0 0.0.255.255 any eq smtp
30 deny tcp 172.16.0.0 0.0.255.255 any eq http
40 permit tcp 172.16.0.0 0.0.255.255 any
```

Hãy cho biết router sẽ thực hiện hành động gì khi các gói tin HTTP từ Internet đến 172.16.12.10 nếu các gói HTTP này được ACL kiểm tra.

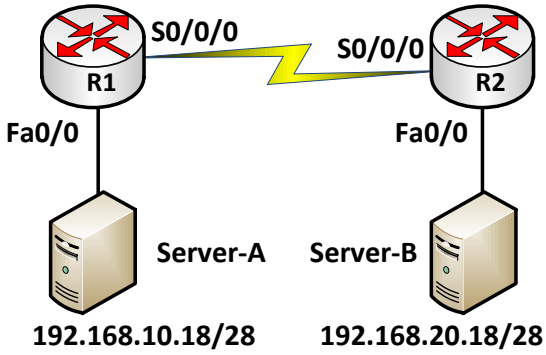
A. Các gói tin này sẽ bị hủy bởi so khớp với điều kiện có số thứ tự 30

B. Các gói tin này sẽ cho phép đi qua bởi so khớp với điều kiện có số thứ tự 40

C. Các gói tin này sẽ bị hủy bởi vì lệnh ngầm định cấm tấc cả ở cuối ACL

D. Các gói tin này sẽ cho phép đi qua bởi vì địa chỉ nguồn không thuộc trong ACL

8.10. Cho mô hình mạng sau



Để điều khiển truy cập trong mạng, người quản trị tạo ACL như sau:

```
access-list 101 permit tcp 192.168.10.16 0.0.0.15 192.168.20.16
0.0.0.15 eq 23
```

Cho biết ý nghĩa của ACL trên và nên đặt ACL này trên router nào, cổng nào và theo hướng nào.

A. Cho phép các gói tin Telnet từ 192.168.1.16/28 đến 192.168.2.16/28.

B. Cho phép các gói tin SMTP từ 192.168.1.16/28 đến 192.168.2.16/28.

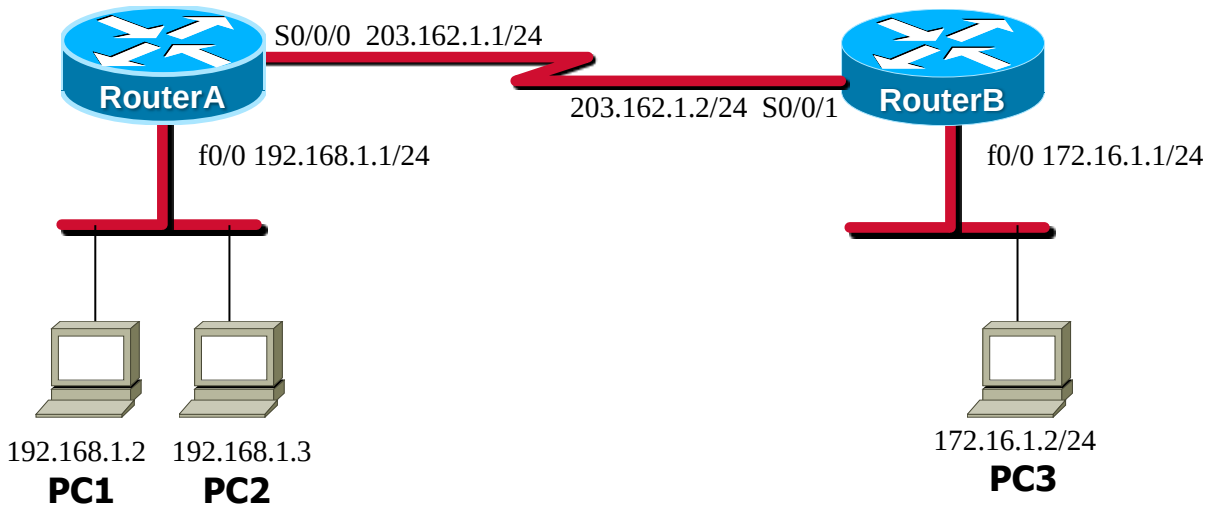
C. ACL cho phép các gói tin từ một host này đến một host khác.

D. ACL nên đặt vào cổng fa0/0 trên Router R1 theo hướng inbound.

E. ACL nên đặt vào cổng fa0/0 trên router R1 theo hướng outbound.

9. Lab. ACL

Lab 5-1. STANDARD ACL



❖ Yêu cầu

Lọc các packet sử dụng standard ACL, thực hiện cấm tất cả các traffic từ PC2 đến các PC trong mạng 172.16.0.0/16

❖ Các bước thực hiện

Bước 1: Cấu hình trên RouterA

```
Router(config)#hostname RouterA
RouterA(config)#int f0/0
RouterA(config-if)#ip add 192.168.1.1  255.255.255.0
RouterA(config-if)#no shutdown
RouterA(config)#int s0/0/0
RouterA(config-if)#ip add 203.162.1.1  255.255.255.0
RouterA(config-if)#clock rate 64000
RouterA(config-if)#no shutdown
```

Bước 2: Cấu hình trên RouterB

```
router(config)#hostname RouterB
RouterB(config)#int s0/0/1
RouterB(config-if)#ip add 203.162.1.2  255.255.255.0
RouterB(config-if)#no shutdown
RouterB(config)#access-list 1 deny 192.168.1.3  0.0.0.0
```

(hoặc `RouterB(config)#access-list 1 deny host 192.168.1.3`)

```
RouterB(config)#access-list 1 permit ip any
RouterB(config)#interface  f0/0
RouterB(config-if)#ip add  172.16.1.1 255.255.255.0
RouterB(config-if)#ip access-group 1 out
RouterB(config-if)#no shut
```

```
RouterB(config-if)#exit
```

❖ **Kiểm tra**

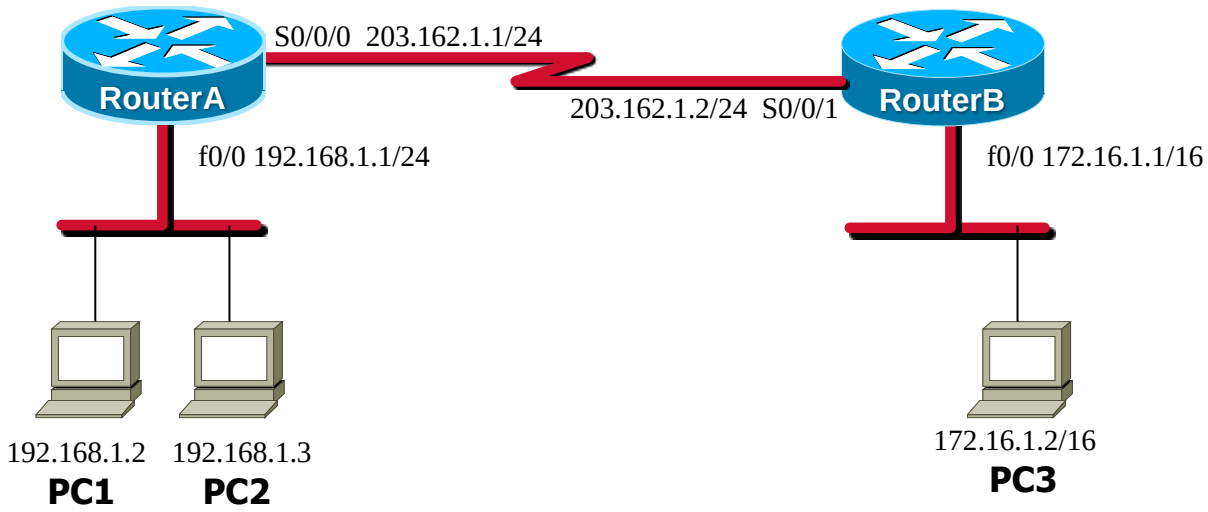
Dùng lệnh ping để theo dõi kết quả hiển thị

- `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`

Lab 5-2. EXTENDED ACL



❖ **Yêu cầu**

- Lọc các gói dữ liệu sử dụng extended access-list. Router RouterA cho phép tất cả các lưu lượng từ PC3 tới PC1 và từ chối tất cả các lưu lượng từ PC3 tới PC2.
- Router **RouterA** và **RouterB** nối bằng đường serial và đặt địa chỉ IP theo như hình trên.
- Access-list được dùng để lọc ngõ vào trên cổng serial của **RouterA**, cho phép các gói từ PC3 tới PC1 và không cho phép các gói từ PC3 tới PC2.

❖ **Các bước cấu hình**

- Cấu hình hostname, các interface

✓ **Cấu hình RouterA**

```
Router>enable
Router#config  terminal
Router(config)#hostname RouterA
RouterA(config)#interface fa0/0
```

```
RouterA(config-if)#ip address 192.168.1.1  255.255.255.0
RouterA(config-if)#no shut
RouterA(config-if)#interface S0/0/0
RouterA(config-if)#ip address 203.162.1.1  255.255.255.0
RouterA(config-if)#clock rate 64000
RouterA(config-if)#no shutdown
RouterA(config-if)#exit
RouterA(config)#
```

✓ **Cấu hình RouterB**

```
Router>enable
Router#config  terminal
Router(config)#hostname RouterB
RouterB(config)#interface fa0/0
RouterB(config-if)#ip address 172.16.1.1  255.255.255.0
RouterB(config-if)#no shutdown
RouterB(config-if)#interface s0/0/1
RouterB(config-if)#ip address 203.162.1.2  255.255.255.0
RouterB(config-if)#no shutdown
RouterB(config-if)#exit
RouterB(config)#
```

- **Cấu hình định tuyến tĩnh**

```
RouterA(config)#ip route 172.16.1.0 255.255.255.0 S0/0/0
RouterB(config)#ip route 192.168.1.0 255.255.255.0 203.162.1.1
```

- **Cấu hình ACL**

```
RouterA(config)#access-list 100 permit ip host 172.16.1.1 host 192.168.1.2
RouterA(config)#access-list 100 deny ip host 172.16.1.1 host 192.168.1.3
```

- **Gán ACL vào cổng serial của RouterA**

```
RouterA(config)#interface Serial 0/0/0
RouterA(config-if)#ip access-group 100 in
```

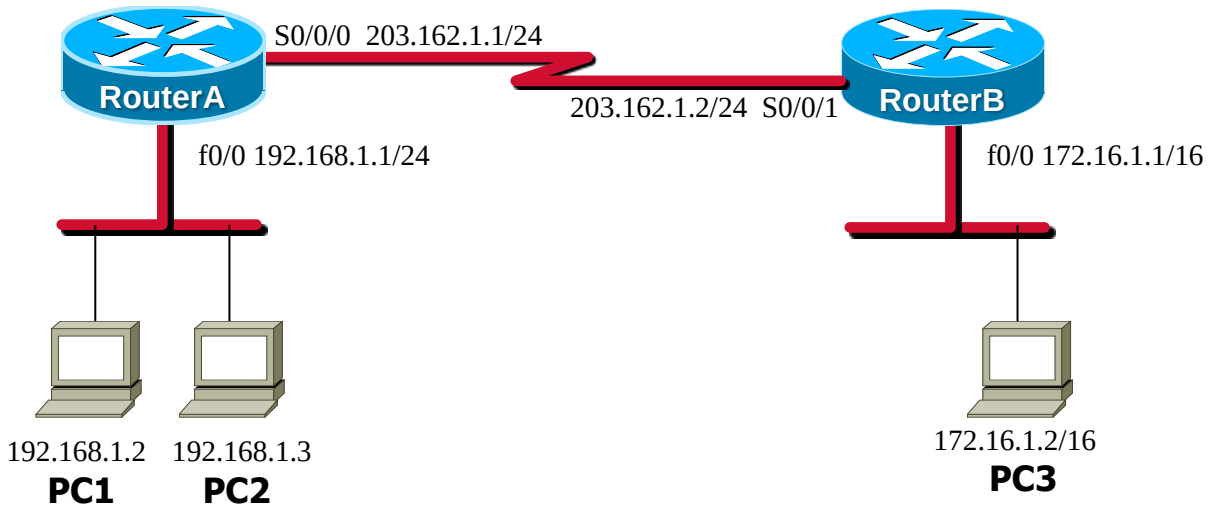
- **Kiểm tra cấu hình**

Từ PC3 `ping` PC2

Từ PC3 `ping` PC1

Trên RouterA dùng lệnh **`show ip access-list`** để xem số lượng các gói thoả mãn điều kiện ACL

Lab 5-3. **ACL (tt)**



Access-list có thể dùng để kiểm soát các kết nối vty tới router. Access-list cho phép xác định trạm nào được telnet vào router dựa trên địa chỉ IP.

❖ **Yêu cầu**

- Chỉ cho PC1 telnet vào RouterB.

❖ **Các bước thực hiện**

- Tạo các access list:

```
RouterB(config)#access-list 1 permit 192.168.1.2  0.0.0.0
```

hoặc:

```
RouterB(config)#access-list 2 permit host 192.168.1.2
```

- Áp access-list 1 vào các line vty để hạn chế truy cập vào RouterB qua telnet

```
RouterB(config)#line vty 0 4
RouterB(config-line)#access-class 1 in
```

❖ **Kiểm tra**

✓ Telnet từ PC3 vào RouterB

✓ Telnet từ PC1 vào RouterB