TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN - ĐHQG-HCM
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

ACCESS CONTROL LIST

QUẢN TRỊ MẠNG VÀ HỆ THỐNG
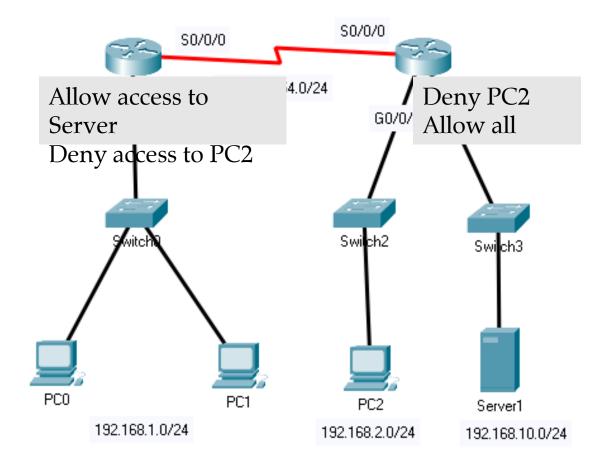*Networks and Systems Administration*

MSc. Trần Thị Dung

CONTENT

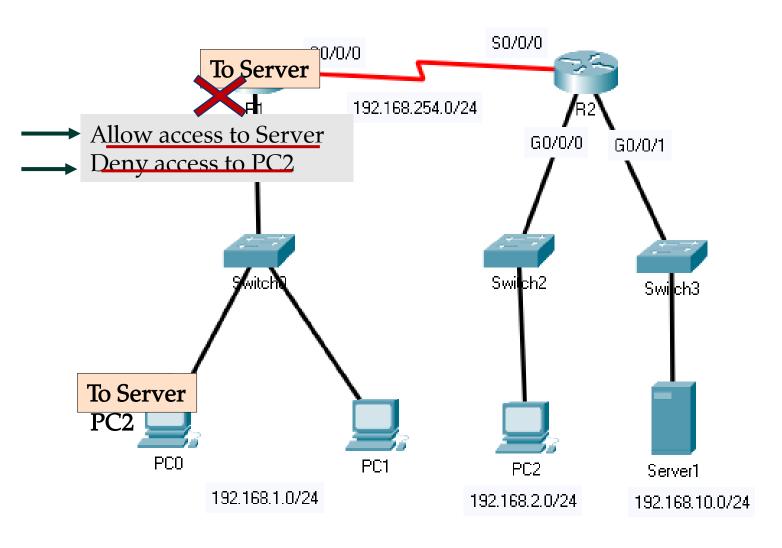- **ACL overview**
- ACL operations
- ACL configuration

o An ACL is a sequential list of permit or deny statements that control whether a router forwards or drops packets based on information found in the packet header.
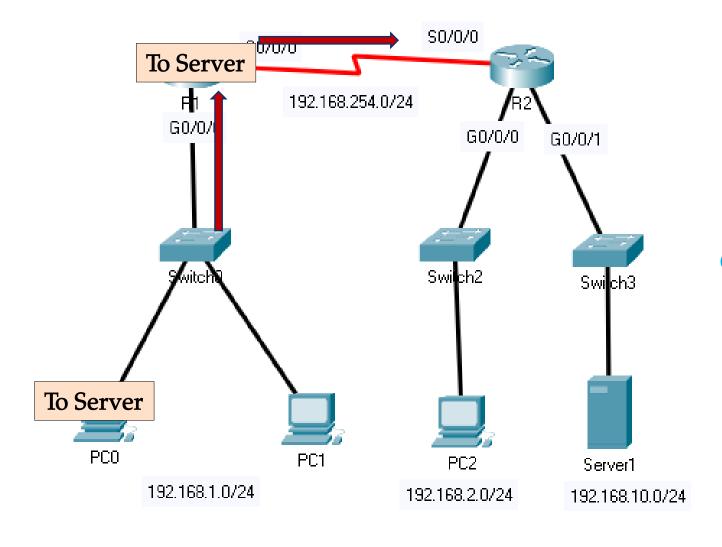

S0/0/0

S0/0/0

Allow access to
Server
Deny access to PC2

4.0/24

G0/0/

Deny PC2
Allow all

Switch0

Switch2

Switch3

PC0

PC1

PC2

Server1

192.168.1.0/24

192.168.2.0/24

192.168.10.0/24

CONTENT

- ACL overview
- **ACL Operations**
- ACL configuration

o Each statement is an access control entry.

o The router compares the information within the packet against each ACE, in sequential order, to determine if the packet matches one of the ACEs.

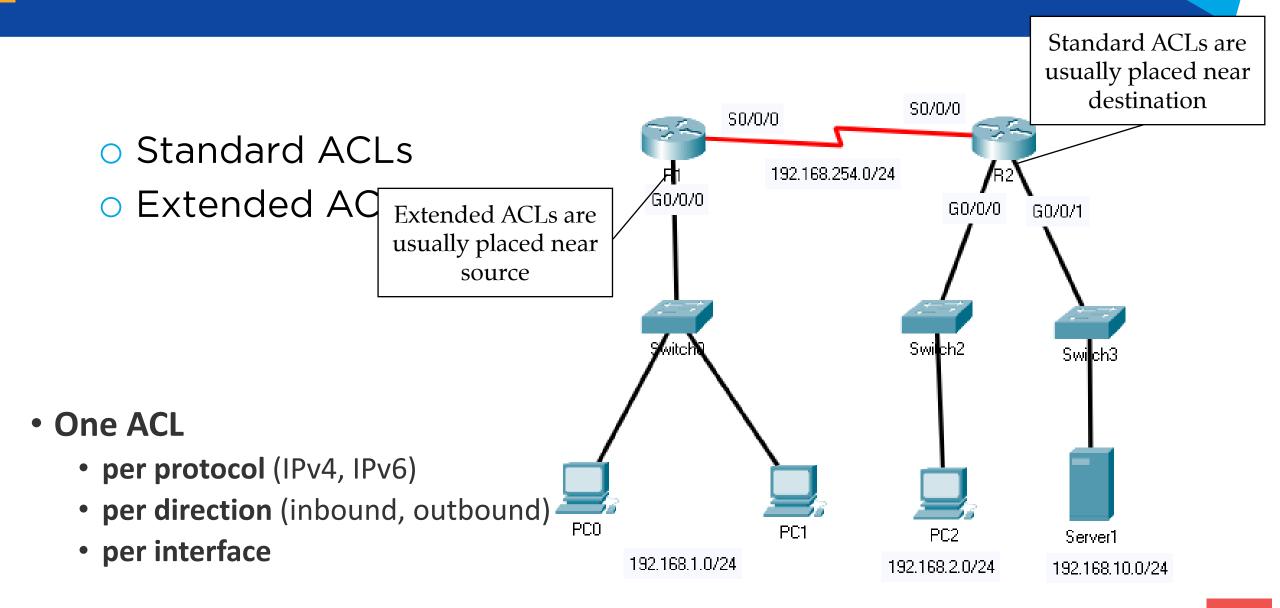o The last statement of an ACL is always an implicit deny

o Inbound ACL
  • Filter before routing

o Outbound ACL
  • Filter after routing
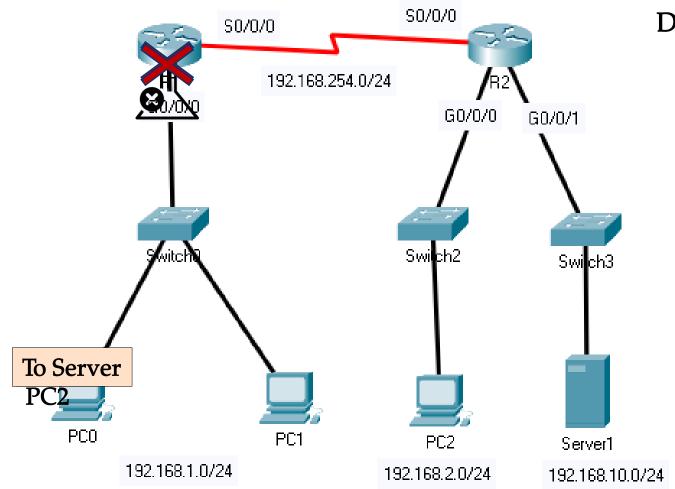
- Standard ACLs: filter IP packets based on source address only
- Extended ACLs: filter IP packets based on
  - Source and destination IP address
  - Protocol type/protocol number
  - Source and destination TCP/UDP port

○ Standard ACLs

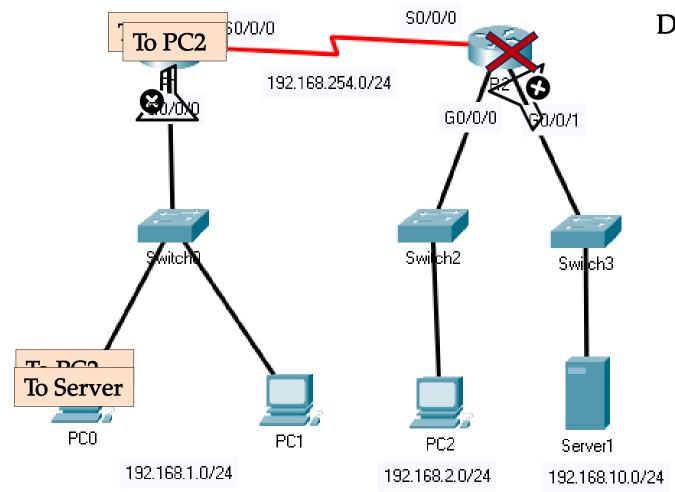○ Extended ACLs

Standard ACLs are usually placed near destination

Extended ACLs are usually placed near source

- **One ACL**
  - **per protocol** (IPv4, IPv6)
  - **per direction** (inbound, outbound)
  - **per interface**

S0/0/0

S0/0/0

R1

192.168.254.0/24

R2

G0/0/0

G0/0/0

G0/0/1

Switch0

Switch2

Switch3

PC0

PC1

PC2

Server1

192.168.1.0/24

192.168.2.0/24

192.168.10.0/24

8

Deny 192.168.1.0/24 network

S0/0/0

S0/0/0

R1

192.168.254.0/24

R2

G0/0/0

G0/0/1

Switch0

Switch2

Switch3

To Server
PC2

PC0

PC1

PC2

Server1

192.168.1.0/24

192.168.2.0/24

192.168.10.0/24

Deny 192.168.1.0/24 network

Deny 192.168.1.0/24 network to access Server1 with SSH
Allow 192.168.1.0/24 network to access HTTP services
on Server 1

Extended ACLs can filter packets based on:
- Source address
- Destination address
- Protocol (ICMP, IP, TCP, UDP…)
- Port number

CONTENT

- ACL overview
- ACL operations
- **ACL configuration**

o Syntax to define standard ACL rule

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

- *access-list-number:*   1-99 or 1300-1999
- *Source:* source IP need to match

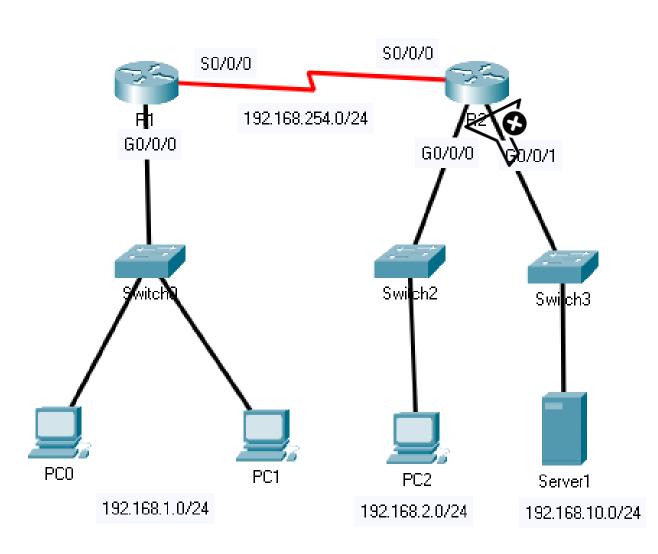o To remove ACL: `no access-list` *access-list-number*

Standard ACL configuration

○ Apply ACL to Interface

```
Router(config)# interface g0/0/0
Router(config-if)# ip access-group access-list-number
{ in | out }
```

Standard ACLs

Deny 192.168.1.0/24 network to access Server 1 and allow the other network

```
Router(config)#  access-list 1 deny
192.168.1.0 0.0.0.255
Router(config)#  access-list 1 permit all
```

```
Router(config)# interface g0/0/0
Router(config-if)# ip access-group 1 out
```

o Syntax to define extended ACL rule

```
Router(config)# access-list access-list-number
{ deny | permit | remark } source [source-wildcard]
[Operator operand] [port port-number or name]
destination [destination-wildcard] [Operator operand]
[port port-number or name] [established]
[ log]
```

Extended ACL configuration

○ Syntax to define extended ACL rule
- *access-list-number:*   100 - 1299
- *Source:* source IP need to match
- Operator: lt (less than), gt (greater than), eq (equal)
- Port number
- *Destination:* destination IP need to match
- Operator: lt (less than), gt (greater than), eq (equal)
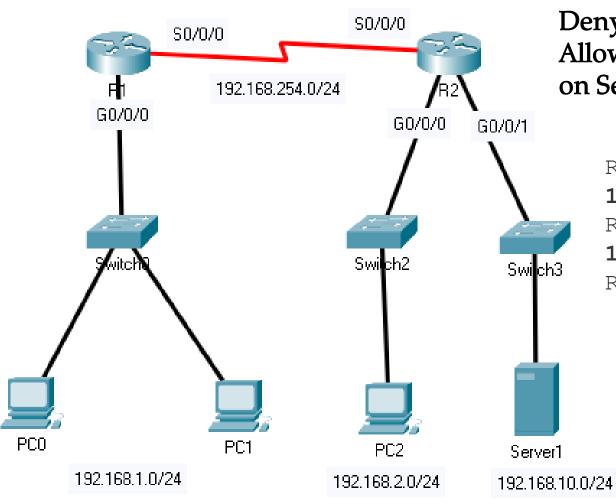- Port number

○ Apply ACL to Interface

```
Router(config)# interface g0/0/0
Router(config-if)# ip access-group access-list-number
{ in | out }
```

Deny 192.168.1.0/24 network to access Server1 with SSH
Allow 192.168.1.0/24 network to access HTTP services
on Server 1

```
R1(config)#  access-list 100 deny tcp
192.168.1.0 0.0.0.255 host 192.168.10.10 eq 22
R1(config)# access-list 100 permit tcp
192.168.1.0 0.0.0.255 host 192.168.10.10 eq 80
R1(config)# access-list 100 permit tcp any any
```

```
R1(config)# interface g0/0/0
R1(config-if)# ip access-group 100 in
```