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

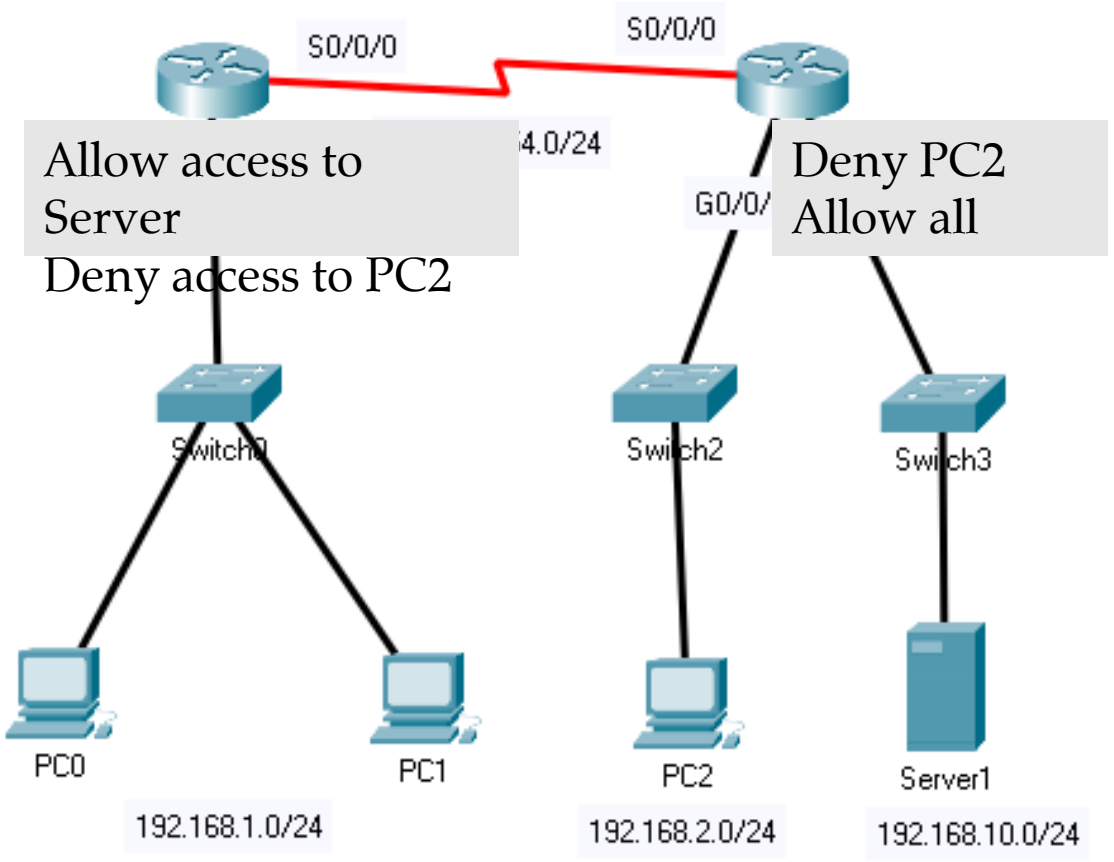
MSc. Trần Thị Dung

# CONTENT

- **ACL overview**
- ACL operations
- Wildcard mask
- ACL configuration

# ACL overview

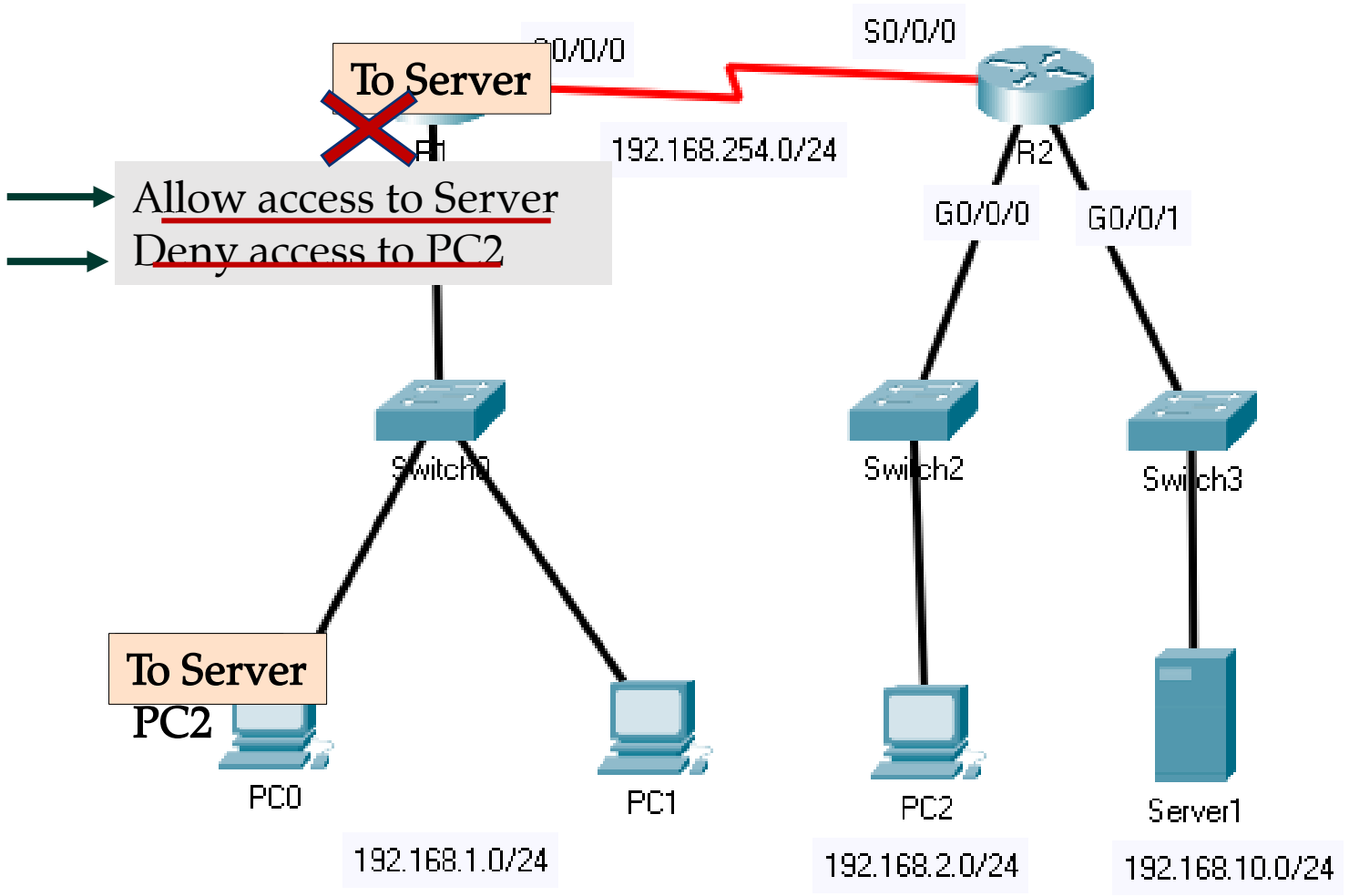
- An ACL is a sequential list of permit or deny statements that control whether a router forwards or drops packets based on information found in the packet header.



# CONTENT

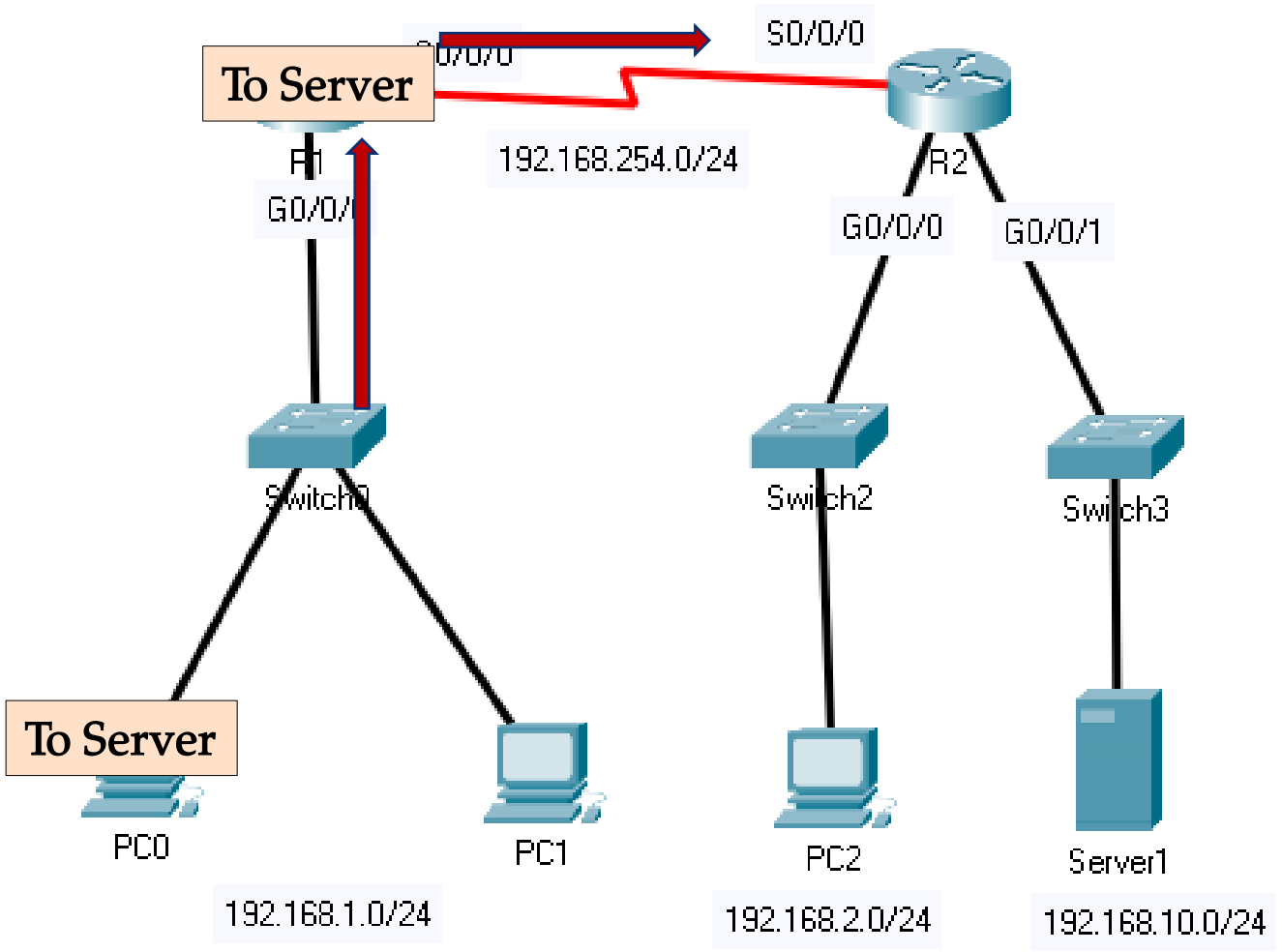
- ACL overview
- **ACL operations**
- Wildcard mask
- ACL configuration

# ACL Operation




- Each statement is an access control entry.
- The router compares the information within the packet against each ACE, in sequential order, to determine if the packet matches one of the ACEs.
- The last statement of an ACL is always an implicit deny

# ACL Operation: Inbound vs Outbound




- Inbound ACL
  - Filter before routing
- Outbound ACL
  - Filter after routing

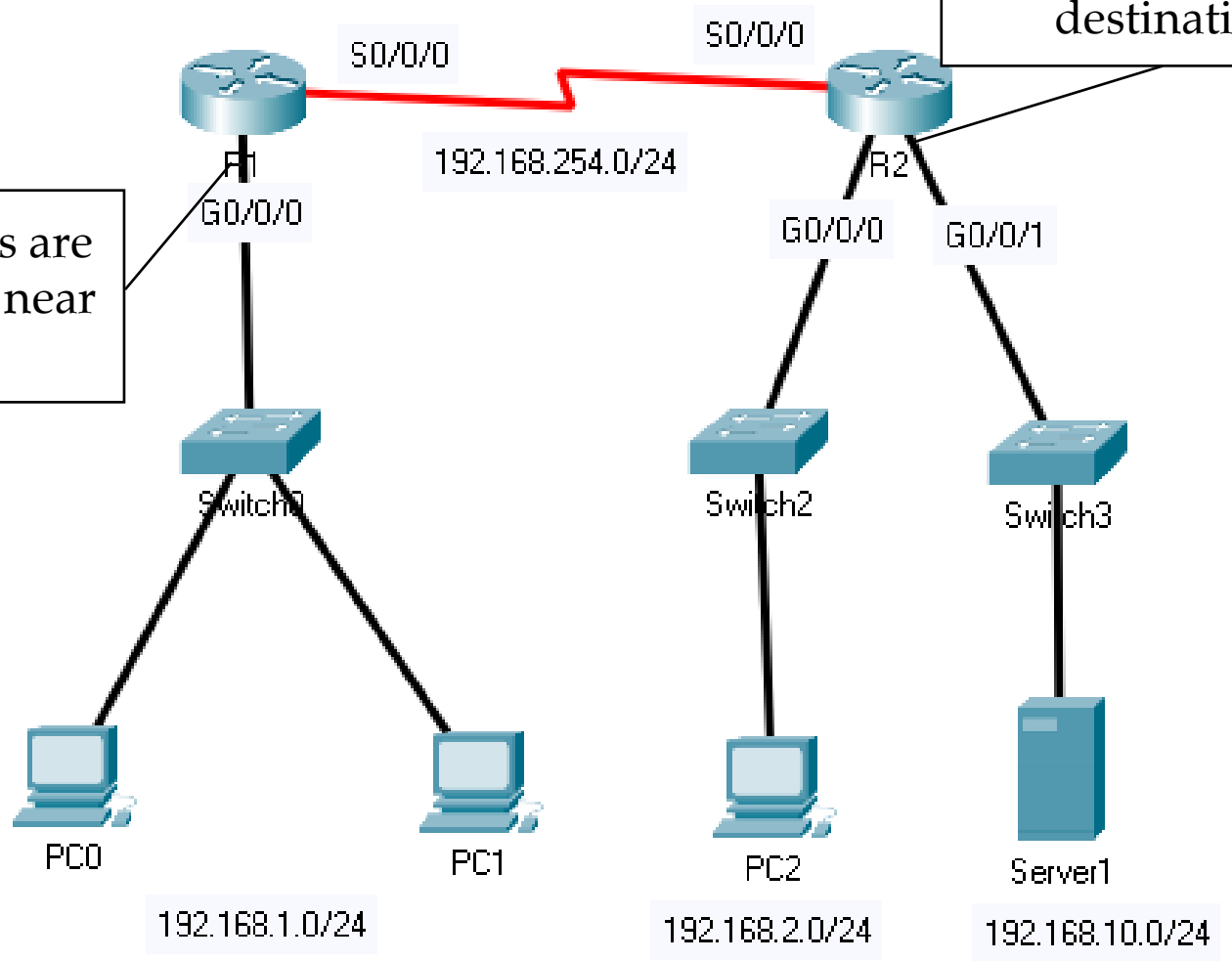
# ACL types and placement

- 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

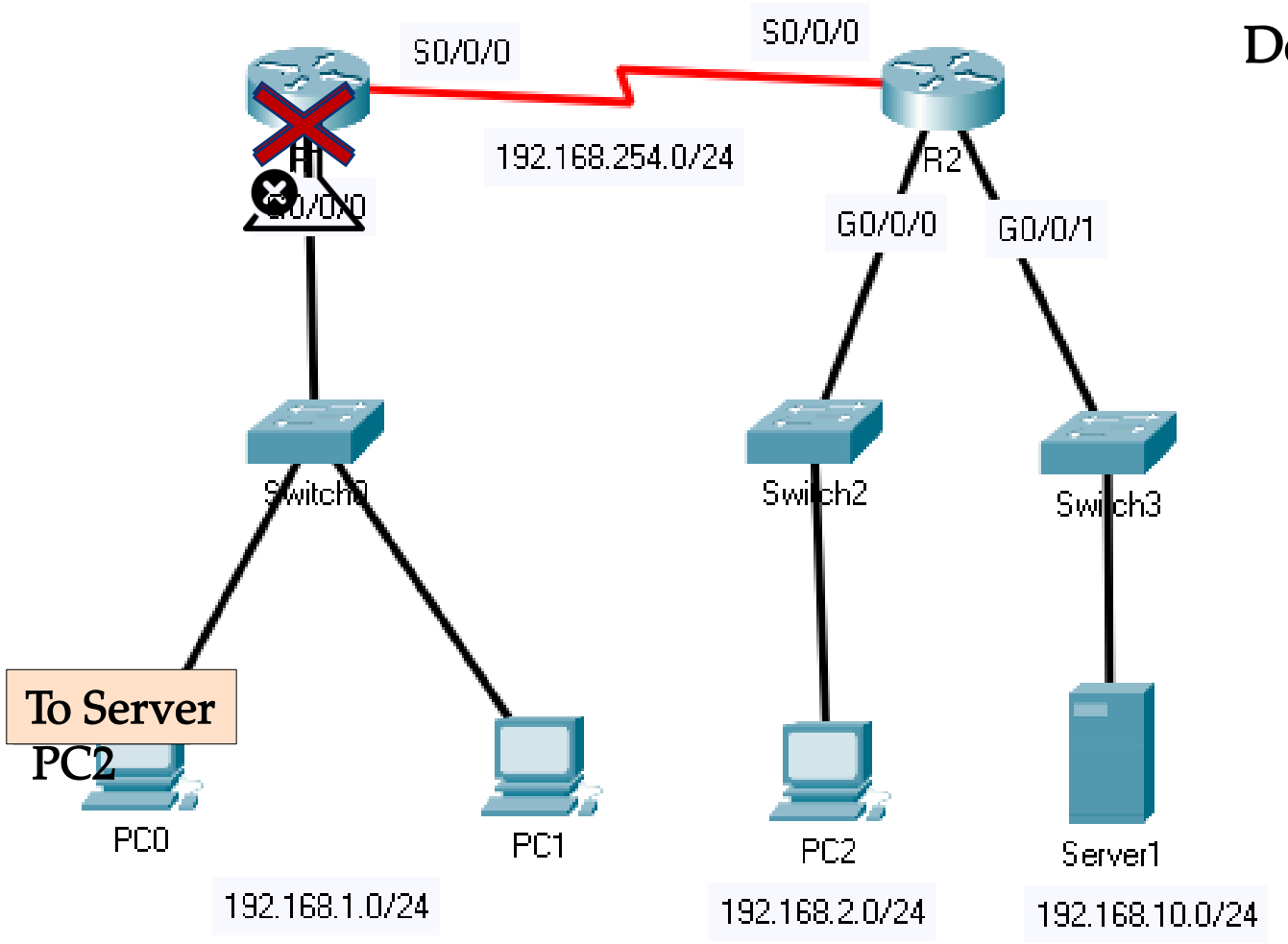
# ACL types and placement

- Standard ACLs
- Extended AC

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

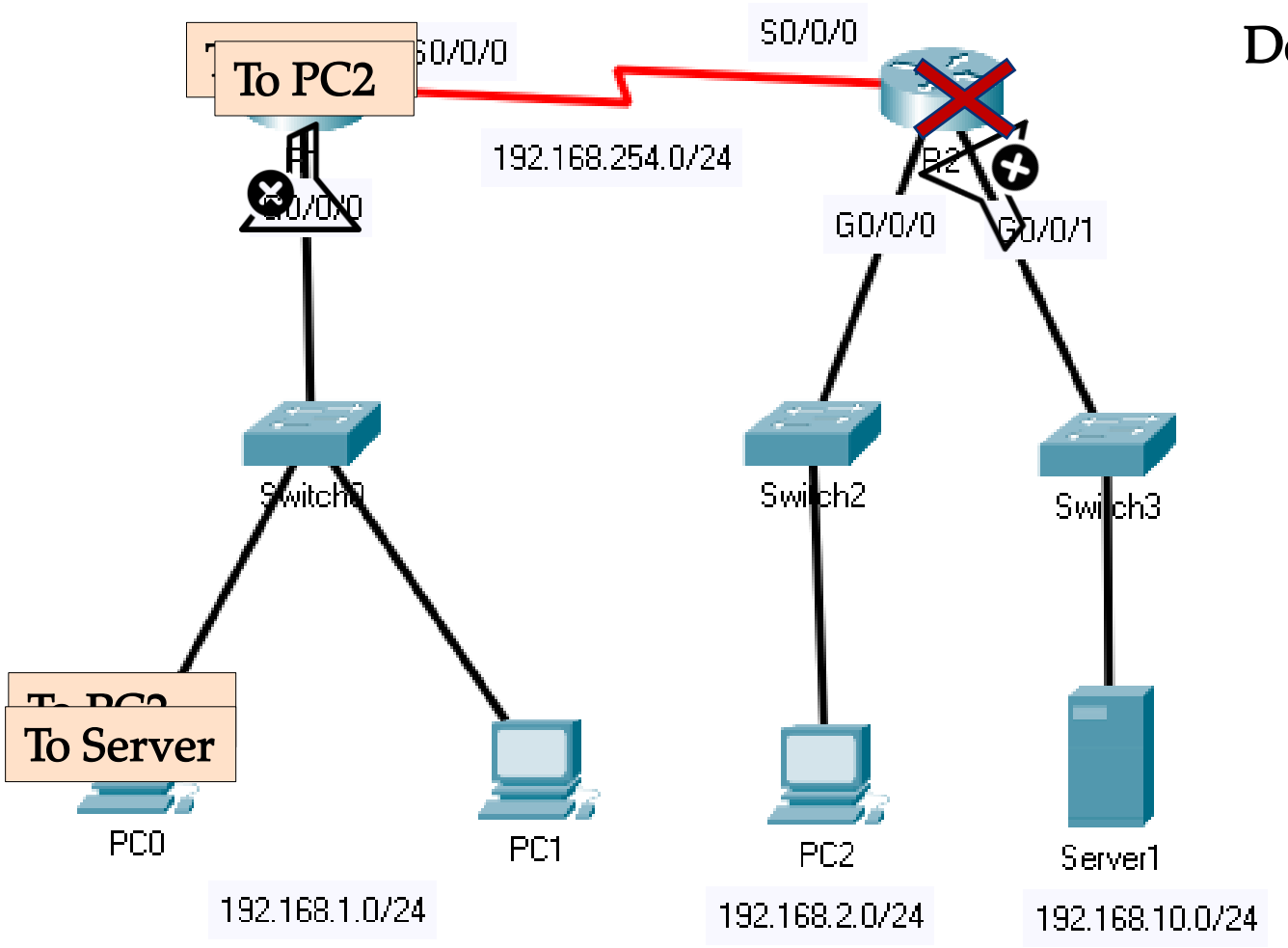


# Standard ACLs



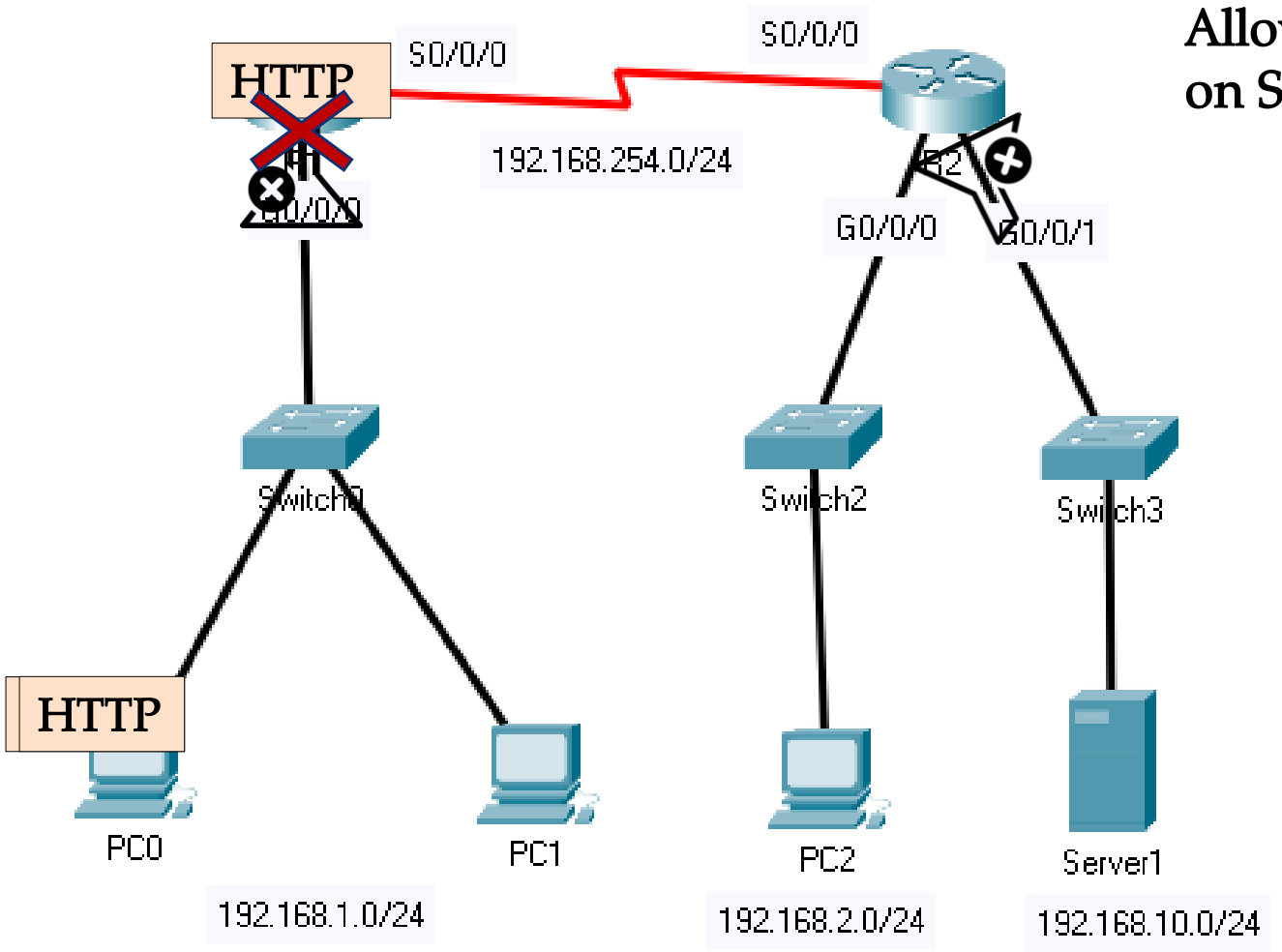

Deny 192.168.1.0/24 network

# Standard ACLs




Deny 192.168.1.0/24 network

# Extended ACLs




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
- **Wildcard mask**
- ACL configuration

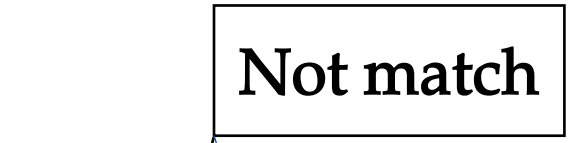
# Wildcard Masks in ACLs

- A wildcard mask is a string of 32 binary digits (1s and 0s) used by the router to determine which bits of the address to examine for a match.
  - 0: match
  - 1: ignore


| | Decimal | Binary |
|---|---|---|
| IP address | 192.168.10.0 | 11000000.10101000.00001010.00000000 |
| Wildcard mask | 0.0.255.255 | 00000000.00000000.11111111.11111111 |
| **Input address** | **192.168.3.1** | **11000000.10101000.00000011.00000001** |

# Wildcard Masks in ACLs

- A wildcard mask is a string of 32 binary digits (1s and 0s) used by the router to determine which bits of the address to examine for a match.
  - 0: match
  - 1: ignore




| | Decimal | Binary |
|---|---|---|
| IP address | 192.168.10.0 | 11000000.10101000.00001010.00000000 |
| Wildcard mask | 0.0.0.255 | 00000000.00000000.00000000.11111111 |
| **Input address** | **192.168.3.1** | 11000000.10101001.00000011.00000001 |

# Wildcard Mask Examples

- Example 1: The wildcard mask matches every bit in the IPv4 192.168.10.1 address.

| IP address | 192.168.10.1 | 11000000.10101000.00001010.00000001 |
|---|---|---|
| Wildcard mask | 0.0.0.0 | 00000000.00000000.00000000.00000000 |

- Example 2: The wildcard mask matches anything.
- Example 3: The wildcard mask matches that any host within the 192.168.1.0/24 network.

# Wildcard Mask Examples

- Example 1: The wildcard mask matches every bit in the IPv4 192.168.1.1 address must match exactly.
- Example 2: The wildcard mask matches that anything will match.

| IP address | 192.168.10.1 | 11000000.10101000.00001010.00000001 |
|---|---|---|
| Wildcard mask | 255.255.255.255 | 11111111.11111111.11111111.11111111 |

- Example 3: The wildcard mask matches that any host within the 192.168.1.0/24 network will match.

# Wildcard Mask Examples

- Example 1: The wildcard mask matches every bit in the IPv4 192.168.1.1 address must match exactly.
- Example 2: The wildcard mask matches that anything will match.
- Example 3: The wildcard mask matches that any host within the 192.168.10.0/24 network will match.

| | | |
|---|---|---|
| IP address | 192.168.10.1 | 11000000.10101000.00001010.00000001 |
| Wildcard mask | 0.0.0.255 | 00000000.00000000.00000000.11111111 |

# Wildcard Mask keyword

- **host** substitutes for the 0.0.0.0 mask
  - 192.168.10.10 0.0.0.0 = host 192.168.10.10

- **any** substitutes for the 255.255.255.255 mask
  - 0.0.0.0 255.255.255.255 = any

# Exercise 1 – Determine wildcard mask

- Deny all hosts from the 10.10.10.0/24 network
- => Wildcard mask: 0.0.0.255

- Deny host 192.168.5.7
- => Wildcard mask: 0.0.0.0

# Exercise 2 - Determine permit or deny

- access-list 50 permit 192.168.122.128 0.0.0.63
- IP address: 192.168.122.195
- => Deny

- access-list 50 permit 192.168.233.64 0.0.0.15
- IP address: 192.168.233.72
- => Permit

# CONTENT

- ACL overview
- ACL operations
- Wildcard mask
- **ACL configuration**

# Standard ACL configuration

- 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

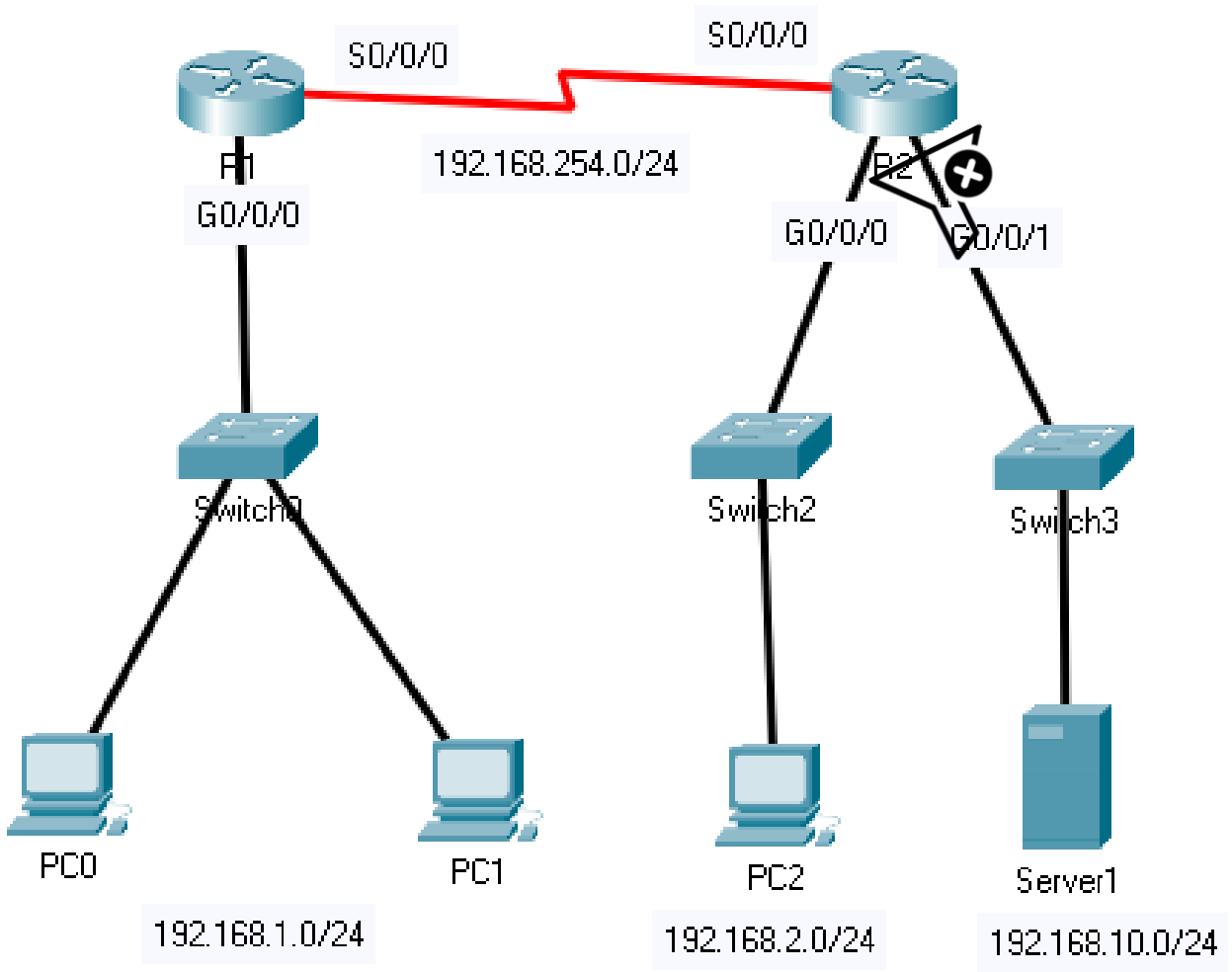
- To remove ACL: `no access-list` *access-list-number*

# 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
```

# Extended ACL configuration

- 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

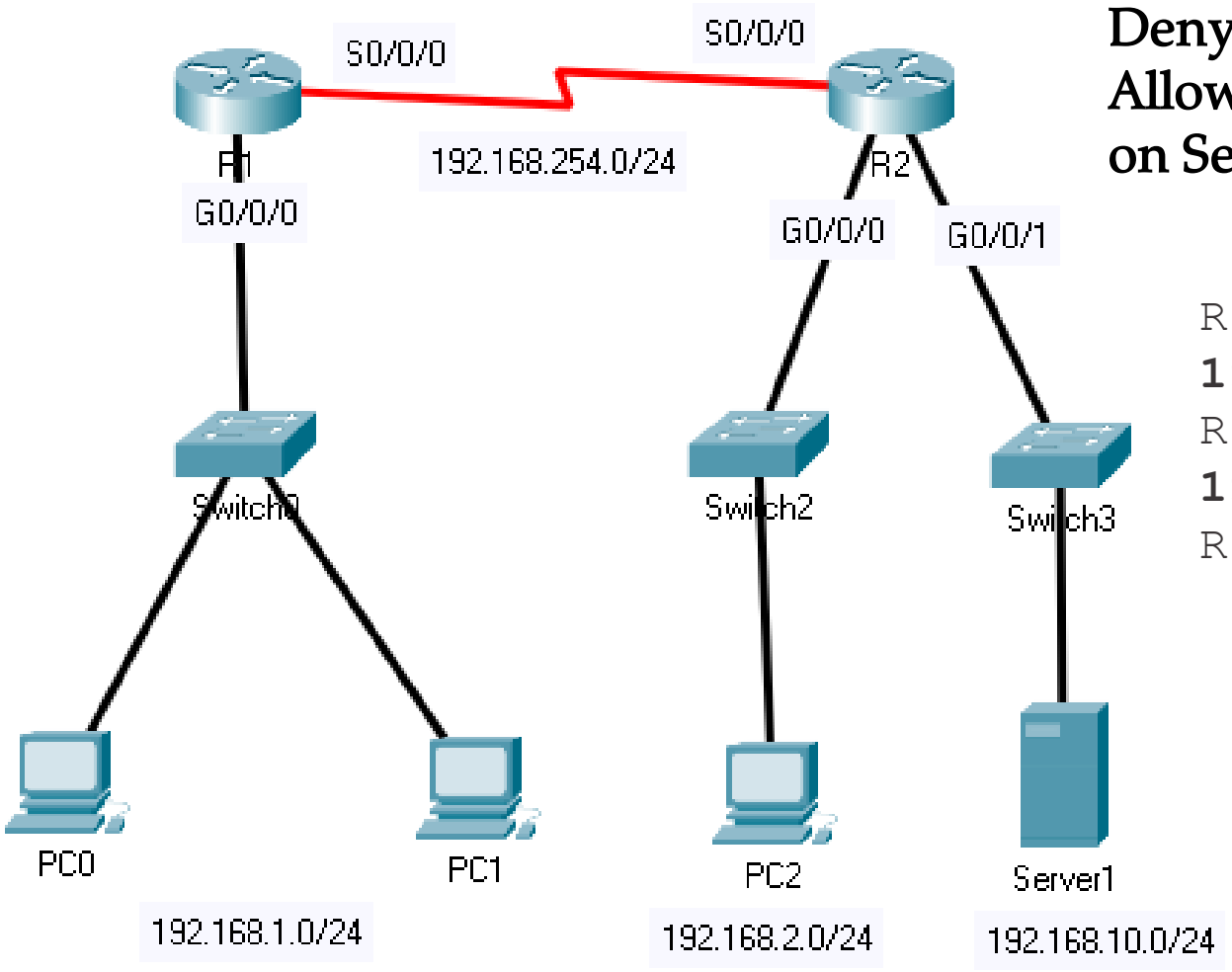
- Syntax to define extended ACL rule
  - *access-list-number:* 100 - 1299
  - *Source:* source IP need to match
  - Operator: lt (less than), gt (greater than), eq (equal)
  - Port number
  - *Destination:* destination IP need to match
  - Operator: lt (less than), gt (greater than), eq (equal)
  - Port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

# Extended ACL configuration

- Apply ACL to Interface

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

# Extended ACLs




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
```