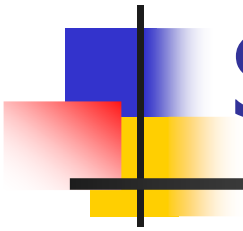
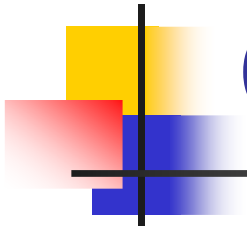


Security

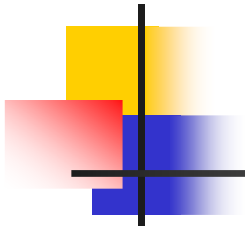
IP Access Control List

Trần Tuấn Toàn



Objectives

- ACL
- Standard & Extended ACL
- Named ACLs



Preamble

- Quản trị mạng cần phải ngăn chặn được các gói tin không hợp lệ từ ngoài vào mà vẫn đảm bảo các kết nối từ trong ra
- Các công cụ bảo mật như Password hay các thiết bị vật lý không linh hoạt

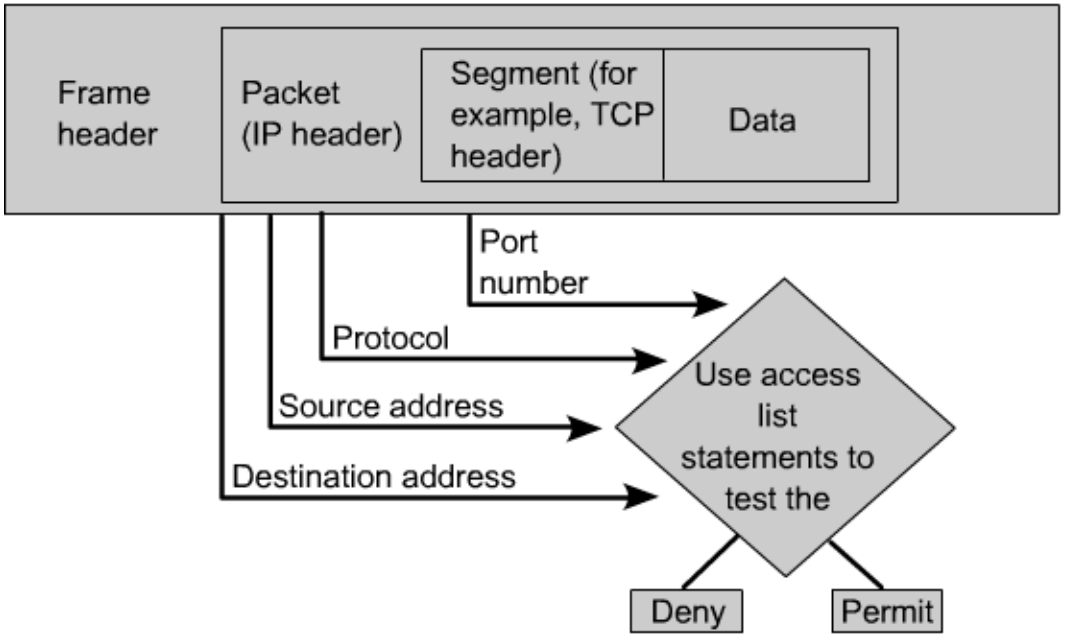
- Ví dụ: Quản trị mạng muốn cho phép (allow) người dùng truy cập internet nhưng lại không cho phép hay từ chối (deny) từ bên ngoài telnet vào mạng LAN

- ⇨Router cung cấp một công cụ có thể giải quyết được vấn đề trên: Access Control List (**ACL**)

What are Access Control Lists

- Một *access list* là một chuỗi các câu lệnh hay bộ lọc
- Danh sách đó cho biết Router sẽ xử lý *packet*:
  - Cho phép (chấp nhận) hay
  - Từ chối
- Dựa trên điều kiện được xác định trong ACL, Router sẽ kiểm tra mỗi *packet* để xác định *forward* hay *drop* nó

- Một số loại ACL sẽ đưa ra quyết định được đối với:
  - IP Source address
  - IP Destination address
  - UDP or TCP protocol
  - Port number



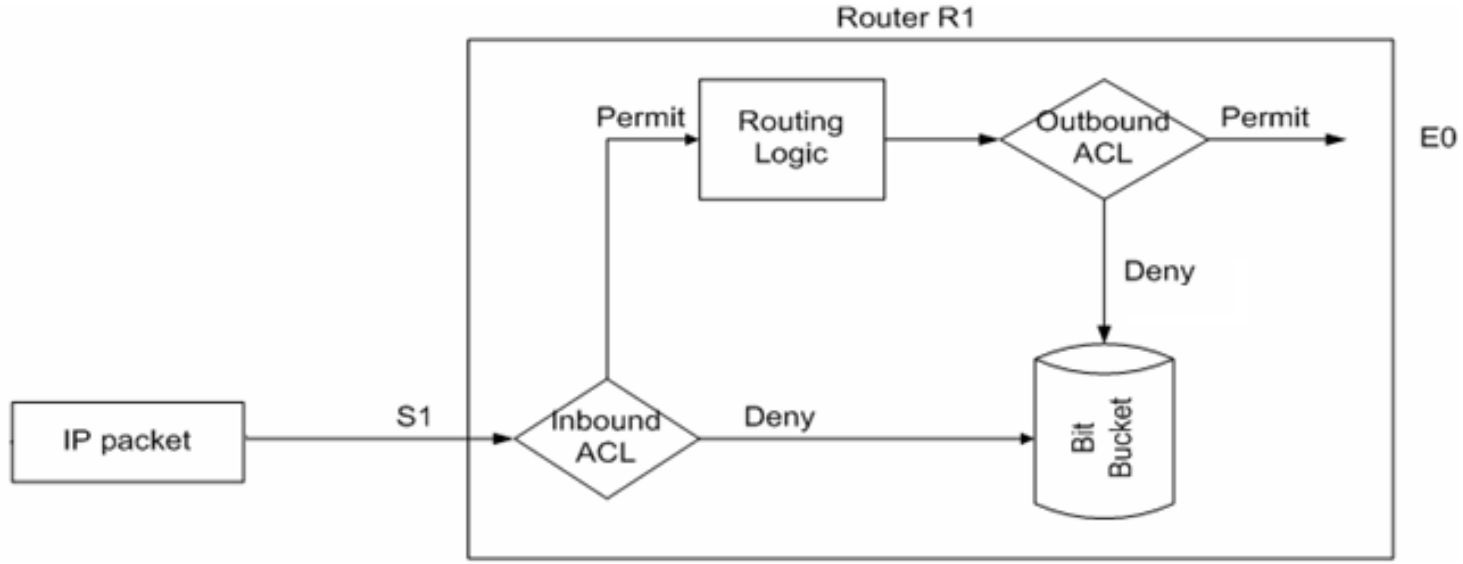
Key features of Cisco access lists

- *Packet* có thể bị lọc khi đi vào *Interface*, trước khi Router quyết định
- *Packet* có thể bị lọc khi đi ra khỏi *Interface*, sau khi Router quyết định
- **Deny, Permit** là từ được Cisco sử dụng trong Cisco IOS:
  - **Deny** : *packet* sẽ bị lọc
  - **Permit** : *packet* sẽ không bị lọc

- Cuối cùng của tất cả các điều kiện lọc trong *access list*, điều kiện "deny all traffic" được mặc định thiết đặt
  - Nếu *packet* không đúng với bất kỳ điều kiện nào ở trên
  - ⇨ *packet* sẽ bị lọc

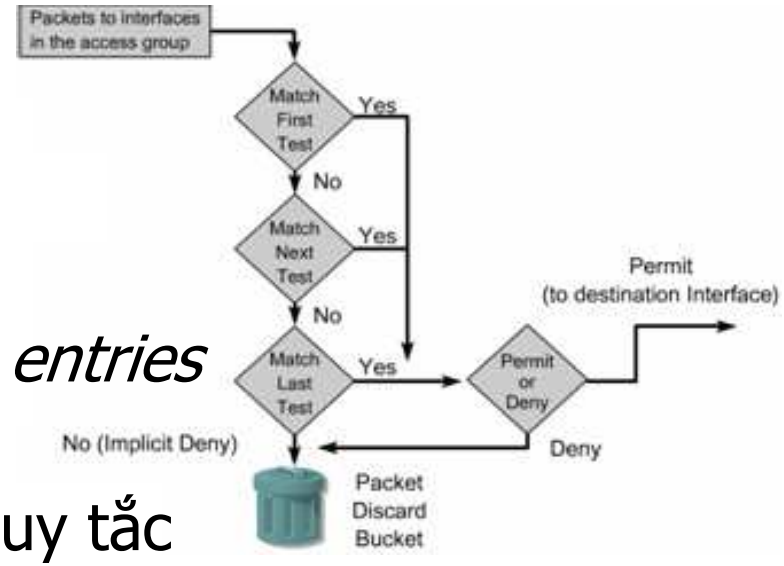
Before using ACL

- Trước khi sử dụng ACL,cần phải cân nhắc:
  - Cần lọc những packet như thế nào
  - Đặt lọc ở đâu trong mạng
  - Interface nào của Router sẽ được thiết đặt lọc
  - Hướng đi của gói tin bị lọc trong ACL

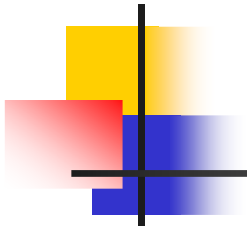


How ACLs work?

- ACL có 2 bước cơ bản:
  - Matching
  - Action
- Một access list có thể có nhiều *entries*



- IOS sẽ lần lượt kiểm tra theo quy tắc tuần tự từ entry đầu tiên đến entry cuối cùng
- ACL sẽ ra lệnh cho Router thực hiện 2 *action:*
  - *Deny / Permit*
- Nếu tất cả các câu lệnh ACL không khớp, một câu lệnh được đưa mặc định vào cuối cùng trong danh sách



How ACLs work?

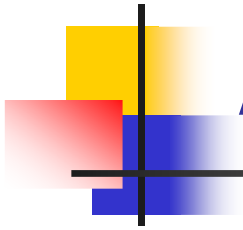
- Chỉ duy nhất **một** *access list* được thiết lập trên một hướng đi của *packet* trên một Interface:
  - Out: *traffic* đã được dẫn đường và đi ra khỏi 01 Interface
  - In: *traffic* đi vào 01 Interface và sẽ được dẫn đường bởi Router
- Chỉ duy nhất **một** *access list* được thiết lập trên một *protocol* trên một Interface
- Có thể thiết lập nhiều *access list* trên một Router

ACLs không chặn các gói tin đi từ chính Router (*ping, telnet,...*)

Something to Remember

- Câu lệnh mới cấu hình sẽ được thêm vào cuối danh sách
- Nếu không có câu lệnh nào khớp, *packet* sẽ bị từ chối
- Câu lệnh "deny any" là mặc định cho danh sách
- Một danh sách chỉ có một câu lệnh đơn là *deny* sẽ được hiểu là *deny* tất cả các *packet*
- ⇨ Phải có ít nhất một câu lệnh *permit* cho các gói tin theo yêu cầu

```
access-list 10 permit 10.1.1.0 0.0.0.255
access-list 10 deny ip any                    (implicit)
```



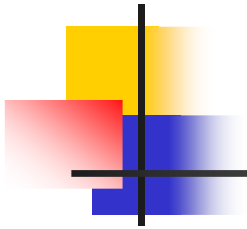
ACL Types

- Standard IP ACLs
  - Chỉ có thể lọc các *packet* từ *Source IP Address*
- Extended IP ACLs
  - Có thể lọc các *packet* theo:
    - Source IP Address
    - Destination IP Address
    - Protocol (TCP, UDP, ICMP)
    - Port number (Telnet:23, HTTP: 80, …)
    - …

Standard IP Access Control List

- Standard IP Access Control List chỉ có thể lọc được các *packet* trong *Source IP Address*

Command	Configure Mode/Description
access-list *access-list-number* {**deny**|**permit**} *source* [*source wildcast mask*] [**log**]	R(**config**)# access-list-number: 1-99 (1300-1999)
access-list *access-list-number* **remark** *text*	Mô tả (Ghi chú) cho access-list hiện tại
ip access-group {*number*|*name*} {**in** | **out**}	Thiết đặt access-list trên Interface nào và hướng đi của *packet*
access-class {*number*|*name*} {**in** | **out**}	Thiết đặt access-list trên Line (trên chính Router) và hướng đi của *packet*



Extended IP Access Control List

- Extended ACL thường được sử dụng nhiều hơn Standard ACL vì có thể mở rộng quy mô điều khiển mạng hơn
- Extended ACL có thể kiểm tra:
  - Source IP Address
  - Destination IP Address
  - Protocols
  - Port number

Extended IP Access Control List

Command	Configure Mode/Desc.
access-list *access-list-number* {**deny**|**permit**} *protocol source* [*source wildcast mask*] *destination* [*destination wildcast mask*][**log**]	R(**config**)# access-list-number: 100-199 (2000-2699)
access-list *access-list-number* {**deny**|**permit**} *tcp source* [*source wildcast mask*] [operator [port]] *destination* [*destination wildcast mask*] [operator [port]] [established] [**log**]	Một phiên bản của Extended ACL cho giao thức TCP cùng với các tham số đi kèm
access-list *access-list-number* **remark** *text*	Mô tả (Ghi chú) cho access-list hiện tại
ip access-group {*number*|*name*} {**in** | **out**}	Thiết đặt access-list trên Interface nào và hướng đi của *packet*
access-class {*number*|*name*} {**in** | **out**}	Thiết đặt access-list trên Line (trên chính Router) và hướng đi của *packet*

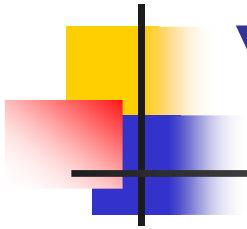
Creating ACLs: 2 steps

- Định nghĩa ra các luật ACLs:

R (config)#**access-list** *access-list-number* {permit | deny} [*test-condition*]

- Các luật ACLs sẽ không có tác dụng cho đến khi thiết đặt trên một Interface cụ thể:

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



"**any**" keyword

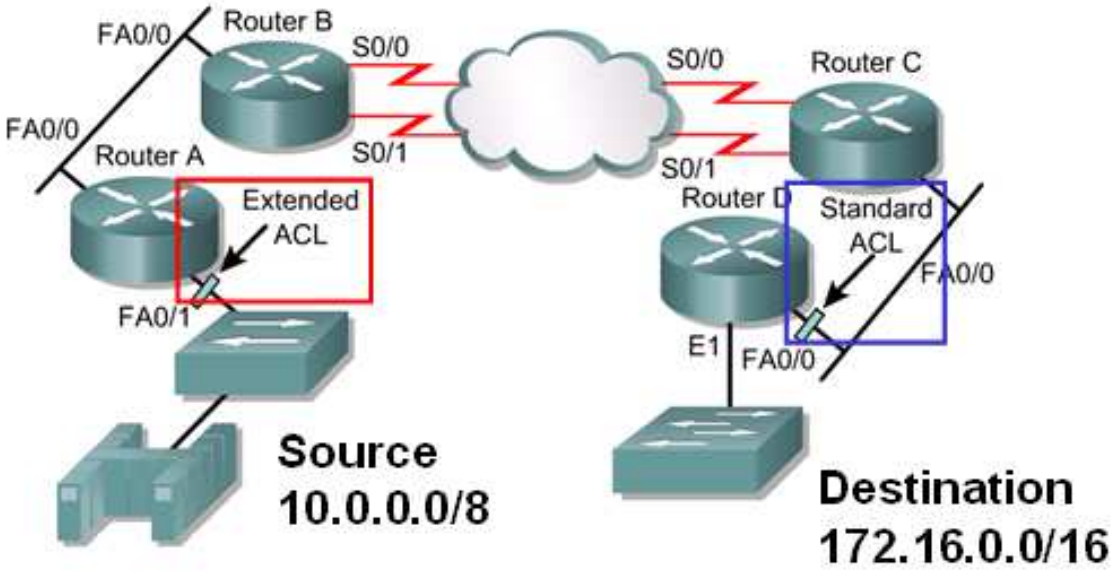
- "any" = 0.0.0.0 **255.255.255.255**
- Lựa chọn "any" sẽ trùng khớp với bất kỳ một IP Address nào cần kiểm tra

```
access-list 10 deny 0.0.0.0 255.255.255.255
or
access-list 10 deny ip any
```

Verifing ACL configuration

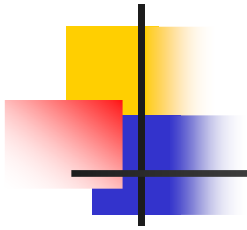
Command
show ip interface [*type number*]
show access-lists [*access-list-number* | *access-list-name*]
show ip access-list [*access-list-number* | *access-list-name*]

Placing ACLs



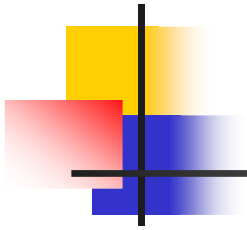
Quy tắc chung:

- Standard ACL thường được đặt tại Interface nào tiếp giáp gần nhất với Destination (*closest Destination*)
- Extended ACL thường được đặt tại Interface nào tiếp giáp gần nhất với Source (*closest Source*)



Miscellanenous ACL Topics

- Named IP Access Lists
- Controlling Telnet Access with ACL
- ACL Implementation Considerations



Named Access Control Lists

- ip access-list {extended | standard} *name*

- Mục đích:
  - Thiết đặt tên cho ACL thay vì dùng số
  - IOS không bị giới hạn về số lượng đặt tên cho ACL
  - Có thể sửa đổi tên mà không cần xóa hay cấu hình lại ACL
- Lưu ý: Named ACL không tương thích với IOS v11.2 trở về trước

Named Access Control Lists

IP Named ACLs

FIGURES

1 2 3 4 5

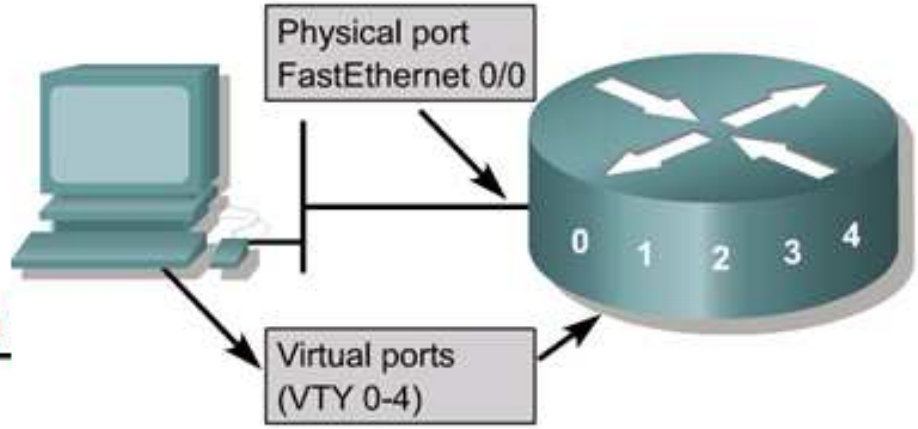
```
Rtl(config)#ip access-list extended server-access
Rtl(config-ext-nacl)#permit tcp any host 131.108.101.99 eq
smtp
Rtl(config-ext-nacl)#permit upd any host 131.108.101.99 eq
domain
Rtl(config-ext-nacl)#remark ACL to allow access to E-mail
and DNS server
Rtl(config-ext-nacl)#deny ip any any log
Rtl(config-ext-nacl)#exit

Rtl(config)#interface fastethernet 0/0
Rtl(config-if)#ip access-group server-access out
Rtl(config-if)#^Z
```

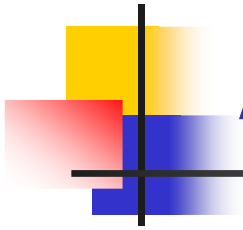
Controlling Telnet Access with ACL

```
Creating the standard access list :
R1(config)# access-list 3 permit 10.1.1.0
0.0.0.255

Applying the access list :
R1(config)# line vty 0 4
R1(config-line)# login
R1(config-line)# password cisco
R1(config-line)# access-class 3 in
```



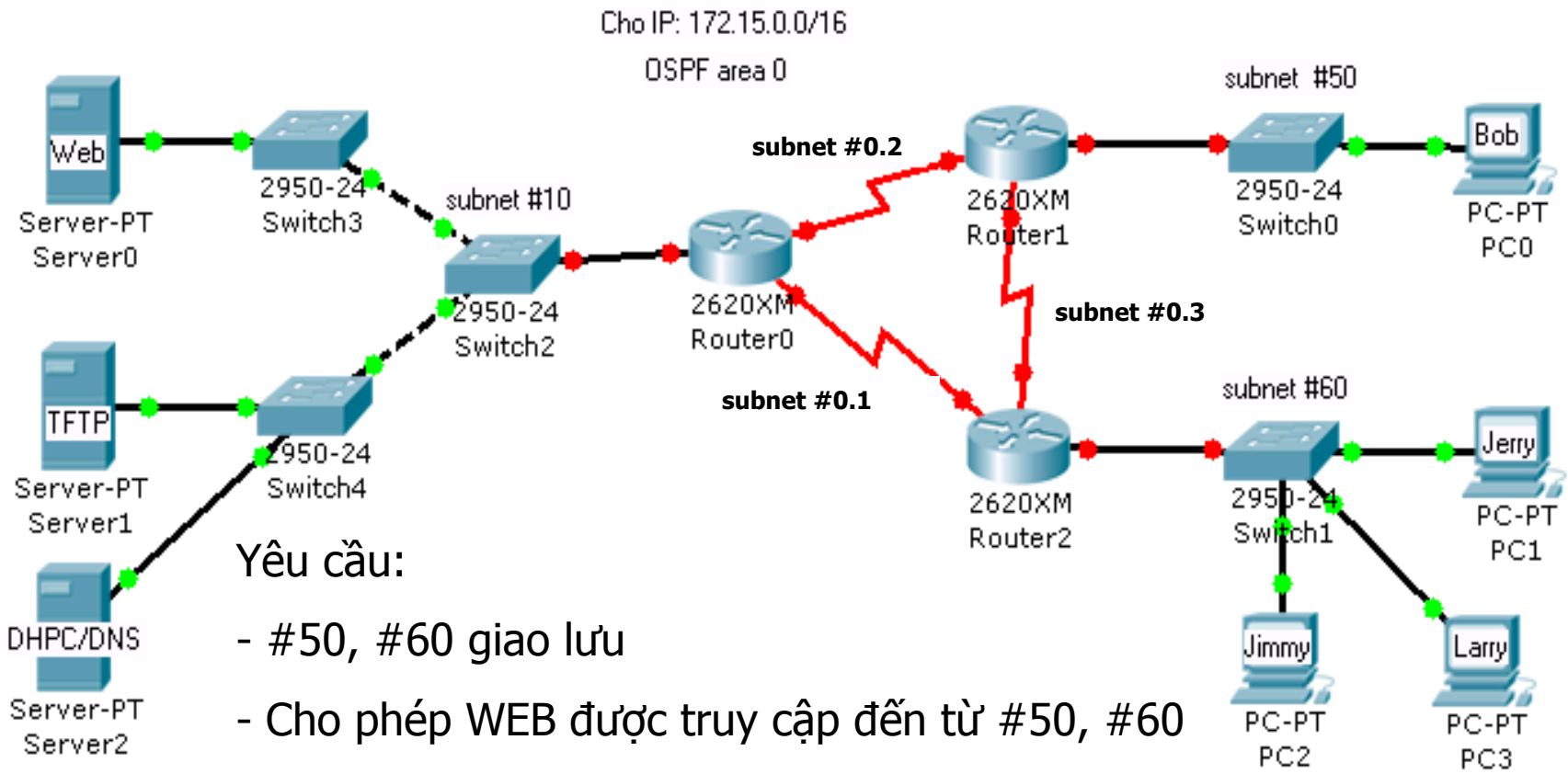
- Việc truy cập vào/ra qua cổng vty của Cisco Route cũng có thể được điều khiển bởi ACL
- Mục đích: tăng mức độ an toàn cho hệ thống mạng



ACL Implementation Considerations

- Tạo các luật ACL trên giấy (notepad) trước, sau đó mới Copy cấu hình đó vào Router.
- Đặt Extended ACL tại nơi làm sao để có thể *discard* gói tin nhanh nhất có thể.
- Đặt Standard ACL tại nơi gần nhất với *destination* (Standard ACL thường discard những packet mà ta không muốn discard tại *source* của packet).
- Cần đặt lệnh mô tả rõ ràng cho mỗi ACL.
- Khi cần tạm thời hủy tác dụng của ACL, nên sử dụng lệnh **no ip access-group** thay vì phải xóa các luật ACL

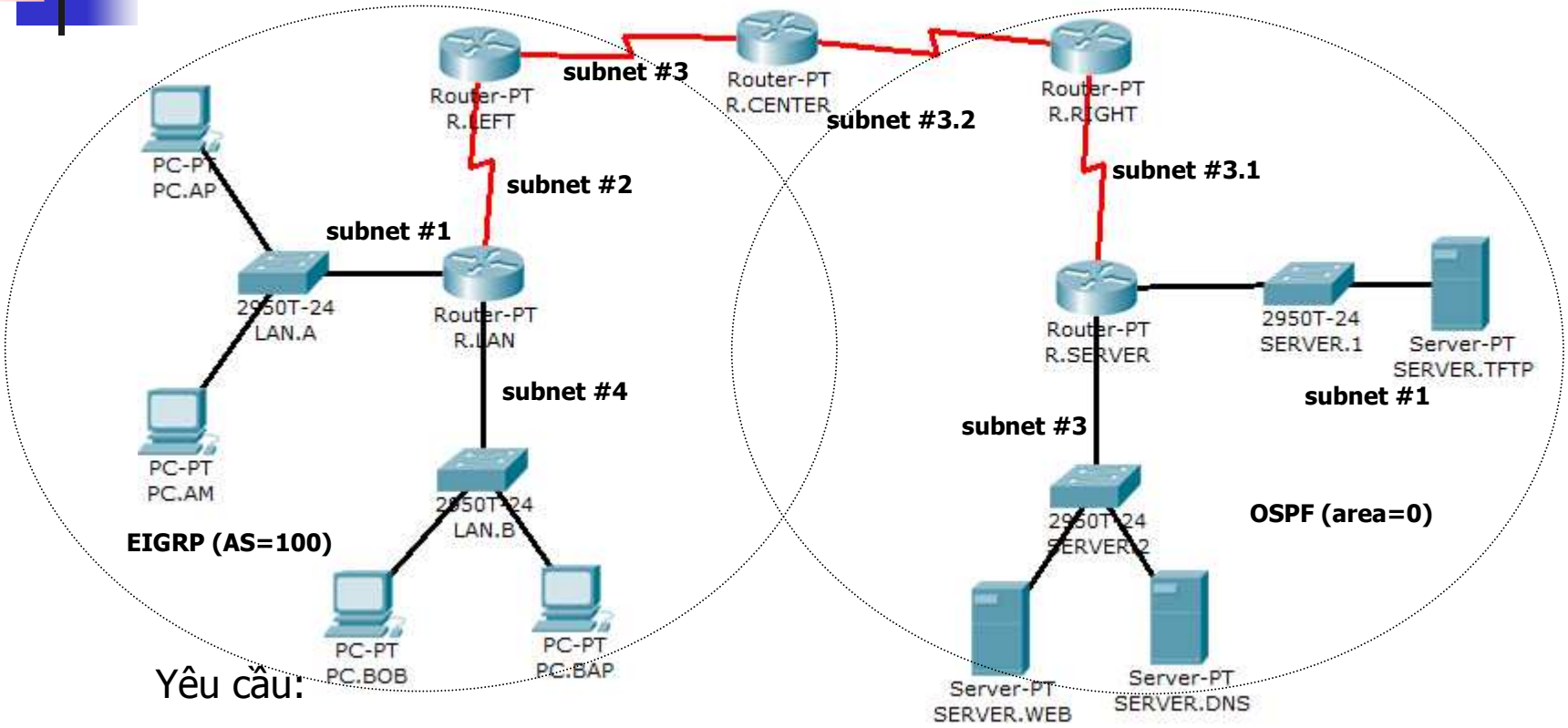
ACL Example 1



Yêu cầu:

- #50, #60 giao lưu
- Cho phép WEB được truy cập đến từ #50, #60
- #50 được phép truy cập tới TFTP
- #50, #60 được phép sử dụng DNS

ACL Example 2



Yêu cầu:

- LAN.A, LAN.B kết nối với nhau
- LAN.A kết nối tới SERVER.WEB
- LAN.B kết nối tới SERVER.DNS
- PC.BOB kết nối tới SERVER.TFTP

Cho:

-EIGRP AS = 100: 192.168.6.0/24

- OSPF Area = 0: 172.16.0.0/16