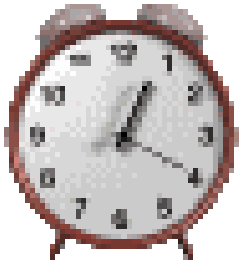
MODULE: XÂY DỰNG HẠ TẦNG MẠNG

MODULE: XÂY DỰNG HẠ TẦNG MẠNG

- Bài 1: GIỚI THIỆU ROUTING VÀ PACKET FORWARDING
- Bài 2: LAYER 2 SWITCHING VÀ VIRTUAL LAN
- Bài 3: DISTANCE VECTOR ROUTING PROTOCOL
- Bài 4: LINK-STATE ROUTING PROTOCOL
- Bài 5: QUẢN LÝ TRAFFIC VỚI ACCESS LIST
- Bài 6: CẤU HÌNH TÍNH NĂNG NÂNG CAO CỦA CISCO IOS
- Bài 7: TRIỂN KHAI HIGH AVAILABILITY CHO HẠ TẦNG MẠNG
- ÔN TẬP
- BÁO CÁO ĐỒ ÁN CUỐI MÔN
- THI CUỐI MÔN

QUY ĐỊNH HỌC TẬP



Đúng giờ

Tắt chuông điện thoại

Lắng nghe

Hỏi lại những gì chưa hiểu

Đóng góp ý kiến và chia sẻ kinh nghiệm

Không hút thuốc trong lớp học

MỤC TIÊU BÀI HỌC
BÀI 5: QUẢN LÝ TRAFFIC VỚI ACCESS LIST

Giới thiệu Access Control List (ACL), Standard Access Lists, Extended Access Lists, Named Access Lists

- Giới thiệu Access Control List (ACL)
- Standard Access Lists
- Extended Access Lists

Named Access Lists

Câu hỏi ôn tập

MỤC TIÊU BÀI HỌC

- Nhận biết được các loại Access List.
- Giải thích được trường hợp áp dụng ACL và vị trí bố trí ACL.
- Trình bày được đặc điểm và các bước tạo và áp dụng ACL.
- Cấu hình được ACL để quản lý traffic mạng.

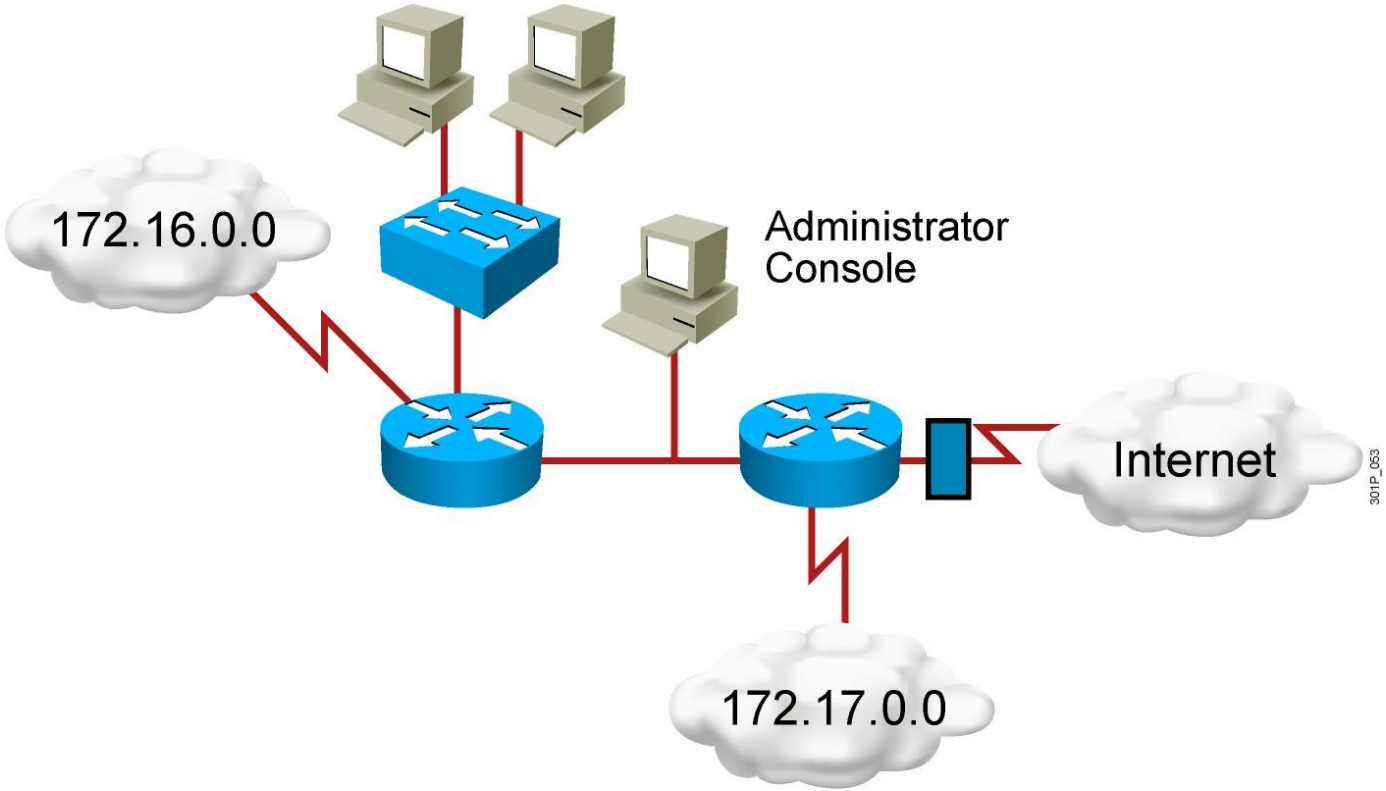
Giới thiệu Access Control List (ACL)

Những khái niệm cơ bản, hoạt động của Access List

- Khái niệm Access Control List
  - ACL là một danh sách các câu lệnh được áp đặt vào các cổng (interface) của router.
  - Danh sách này chỉ ra cho router biết loại packet nào được chấp nhận (permit) và loại packet nào bị hủy bỏ (deny).
  - Sự chấp nhận và huỷ bỏ này có thể dựa vào địa chỉ nguồn, địa chỉ đích hoặc chỉ số port.

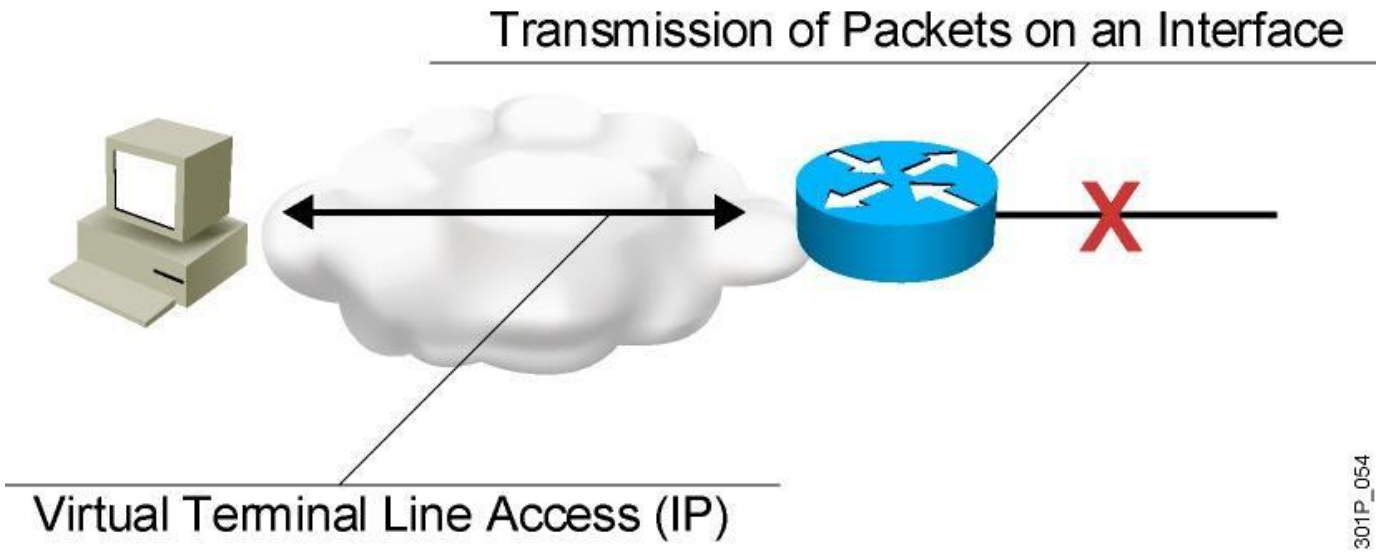
Giới thiệu Access Control List (ACL)

- Mục đích sử dụng ACL
  - Lọc: Quản lý IP traffic truy cập bằng cách lọc các gói tin đi qua router.
  - Phân loại: Xác định loại traffic đặc biệt để xử lý.



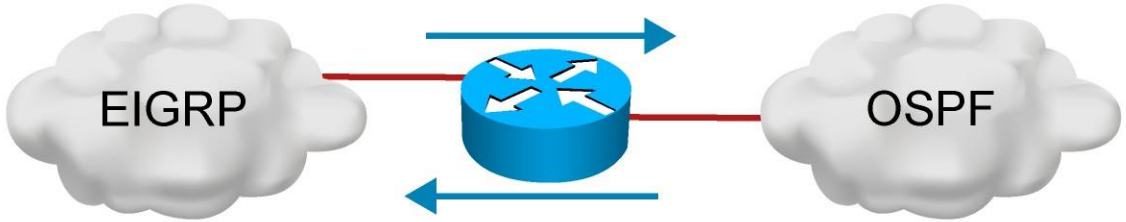
Giới thiệu Access Control List (ACL)

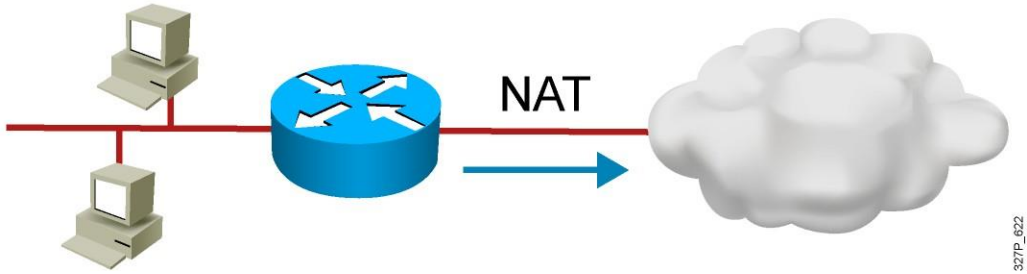
- Mục đích sử dụng ACL
  - Lọc:
    - Cho phép hoặc từ chối các gói tin di chuyển qua Router.
    - Cho phép hoặc từ chối truy cập vty tới router.
    - Nếu không có ACL, các gói dữ liệu có thể truyền đến tất cả các bộ phận của hệ thống mạng.



Giới thiệu Access Control List (ACL)

- Mục đích sử dụng ACL
  - Ứng dụng ACL



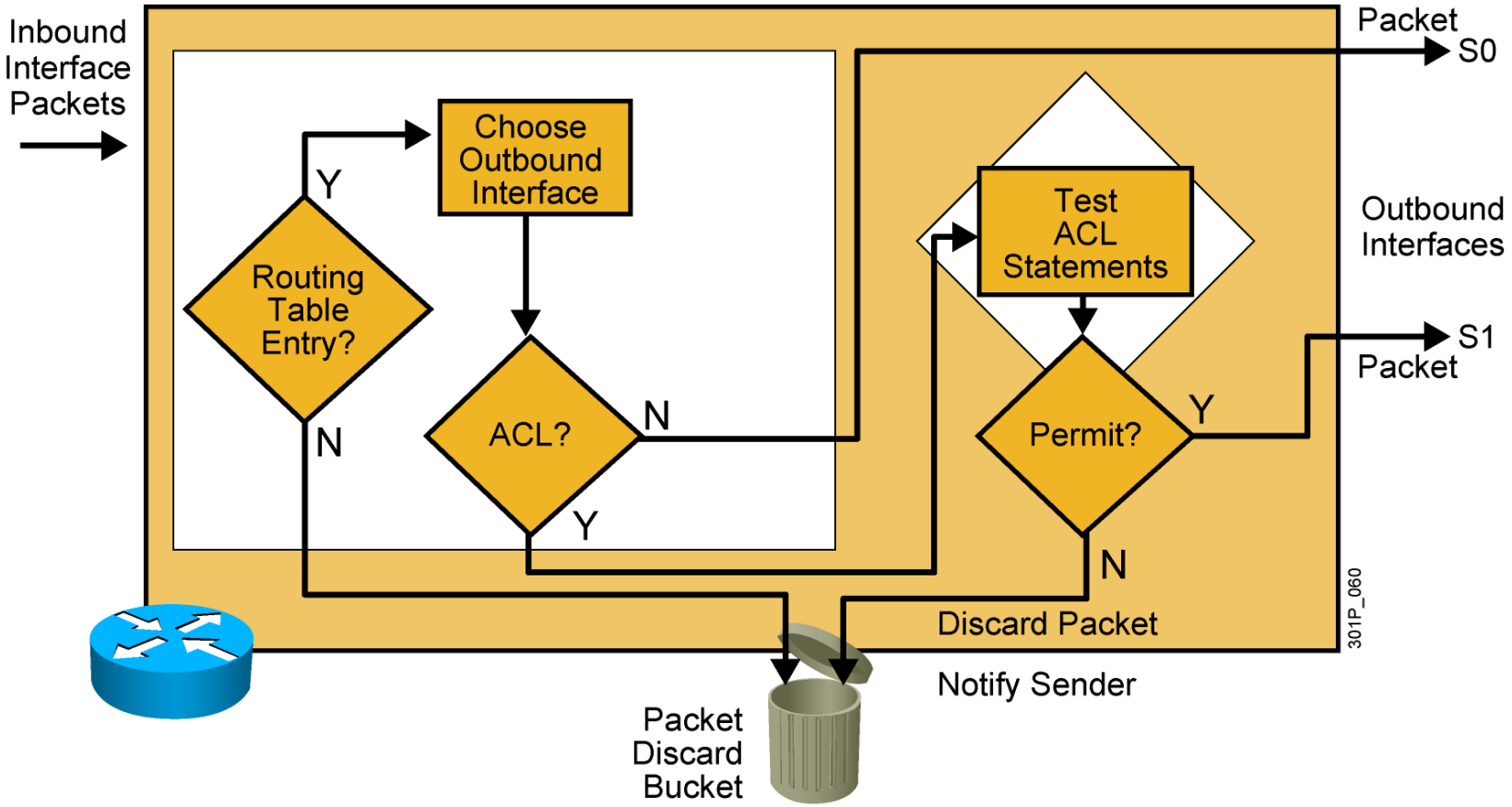


Giới thiệu Access Control List (ACL)

- Áp dụng Access list cho Interface
  - Inbound (in): Lọc các gói dữ liệu đi vào các interface trên Router.
  - Outbound (out): Lọc các gói dữ liệu đi ra từ các interface trên Router.

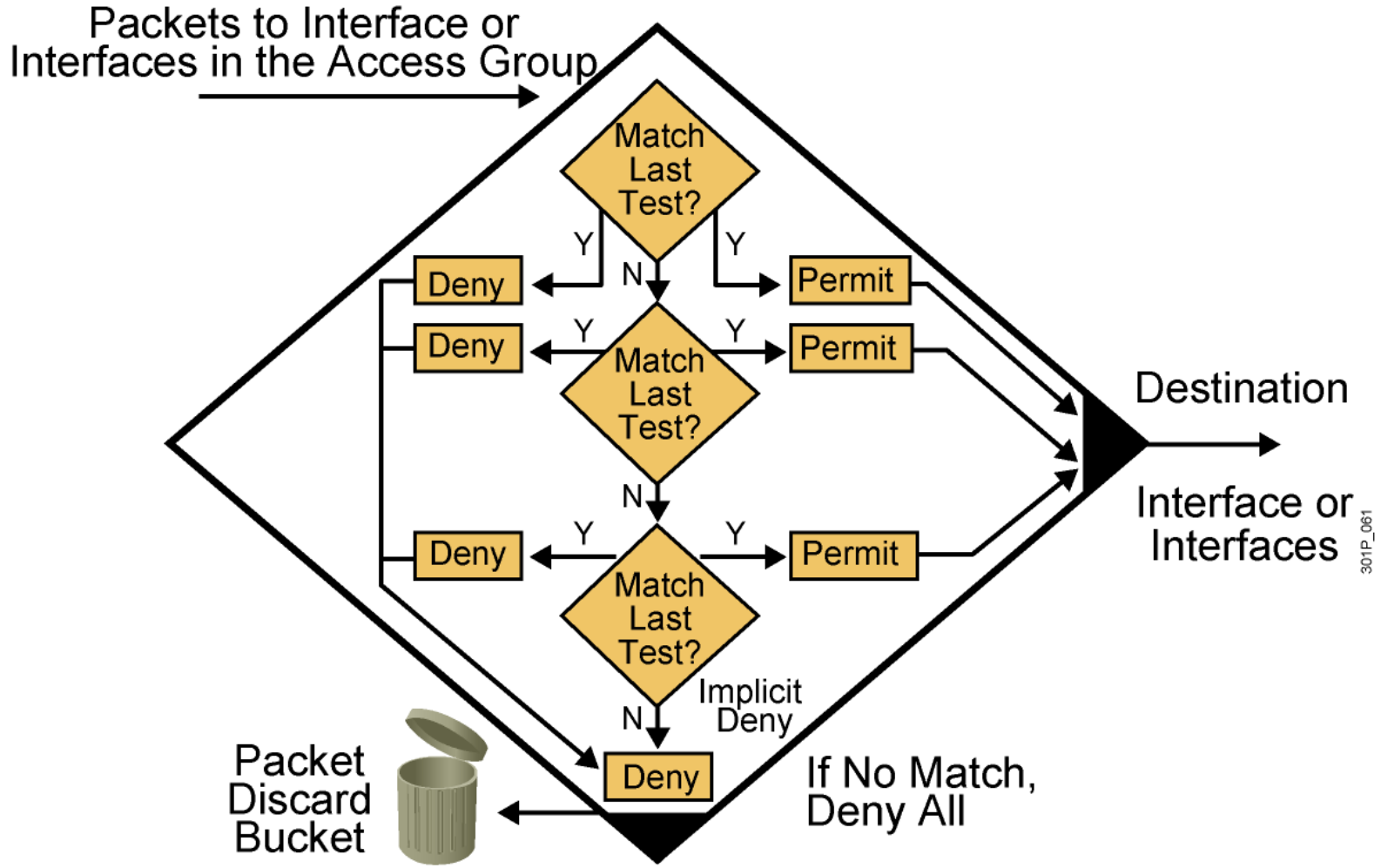
Giới thiệu Access Control List (ACL)

- Hoạt động của ACL



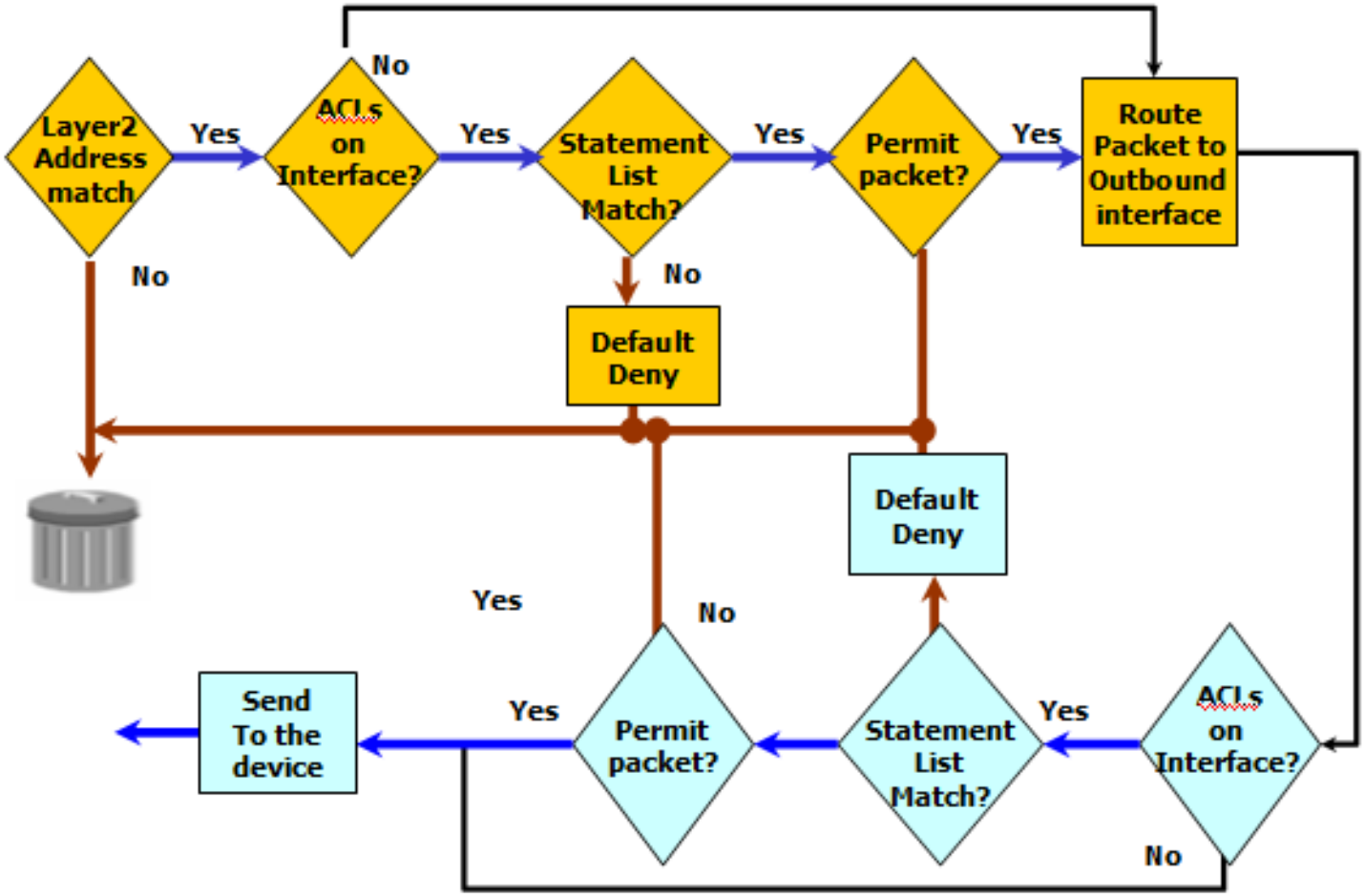
Giới thiệu Access Control List (ACL)

- ACL Entry



Giới thiệu Access Control List (ACL)

- Hoạt động của ACL
  - ACL và Routing Process

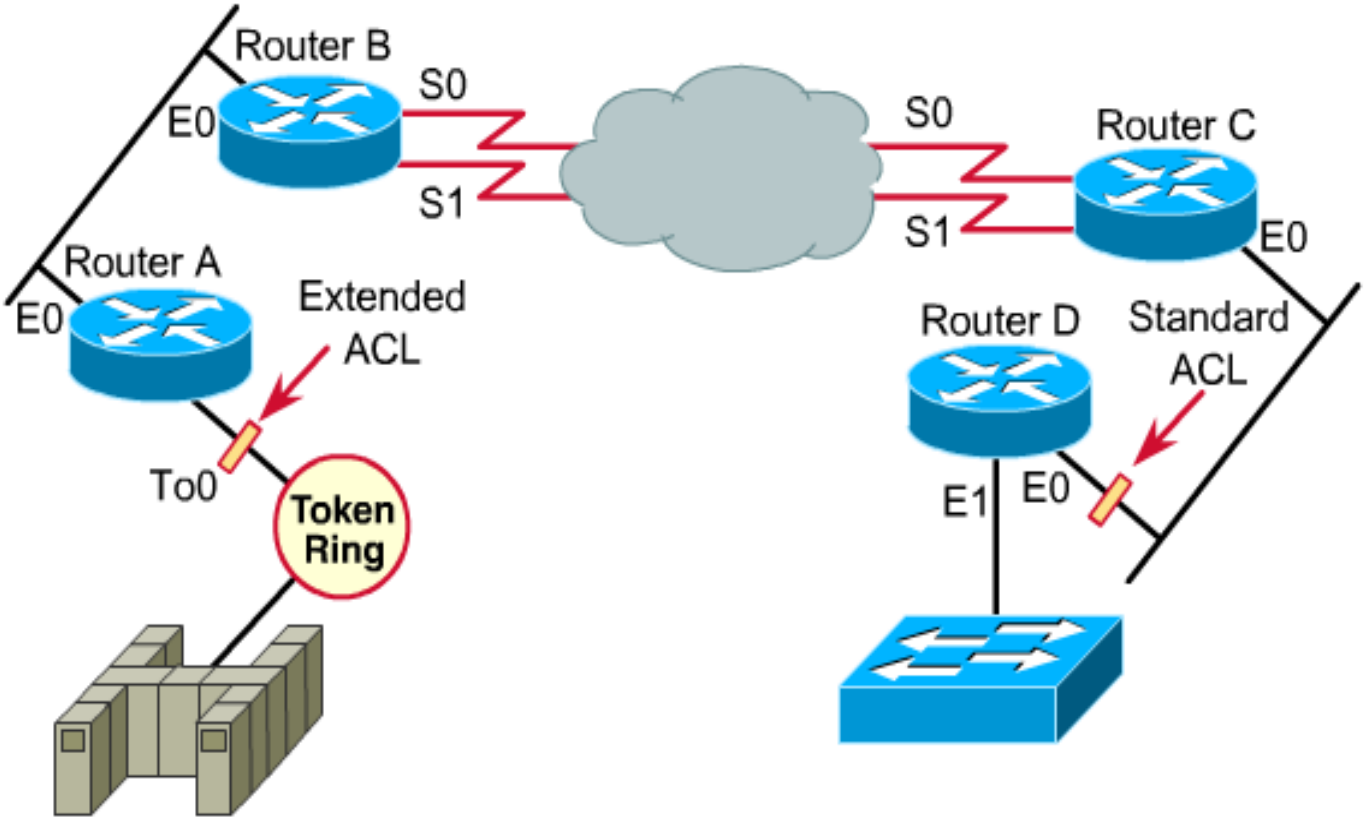


Giới thiệu Access Control List (ACL)

- Các loại Access List
  - Standard ACL
    - Kiểm tra địa chỉ nguồn trong gói tin.
    - Permit hay deny toàn bộ protocol .
  - Extended ACL
    - Kiểm tra cả địa chỉ nguồn, địa chỉ đích, port.
    - Permit hay deny ở một giao thức hay ứng dụng cụ thể.
- Hai phương pháp cấu hình Standard hay Extended ACL
  - Numbered ACL: sử dụng dạng số để xác định
    - Standard ACL: 1-99, 1300 – 1999
    - Extended ACL: 100 – 199, 2000 – 2699
  - Named ACL: sử dụng tên để xác định loại ACL đang được dùng.

Giới thiệu Access Control List (ACL)

- Cách bổ trí ACL
  - Extended ACL đặt nơi cập gần mạng nguồn.
  - Standard ACL đặt gần đến mạng đích.

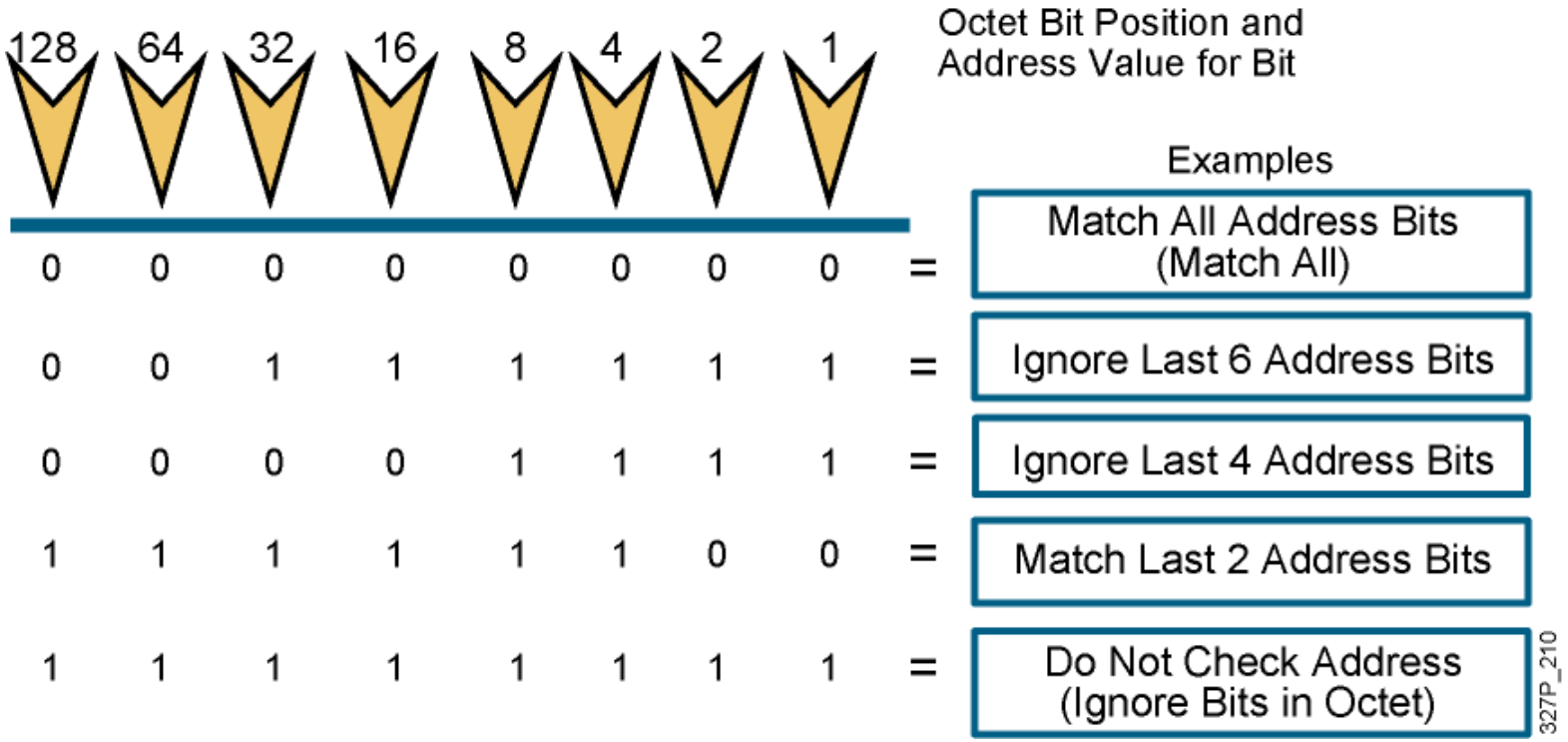


Giới thiệu Access Control List (ACL)

- Wildcard Mask
  - Là chỉ số ngược của Subnetmask dùng để xác định một số lượng host cụ thể dựa trên dải địa chỉ IP của các host.
  - Cung cấp khả năng sử dụng linh động hơn subnet mask.
  - Wildcard mask được xác định bằng các wildcard bits.

Giới thiệu Access Control List (ACL)

- Cách xác định Wildcard bits



- 0 xét các bit địa chỉ tương ứng.
- 1 bỏ qua các bit địa chỉ tương ứng.

Giới thiệu Access Control List (ACL)

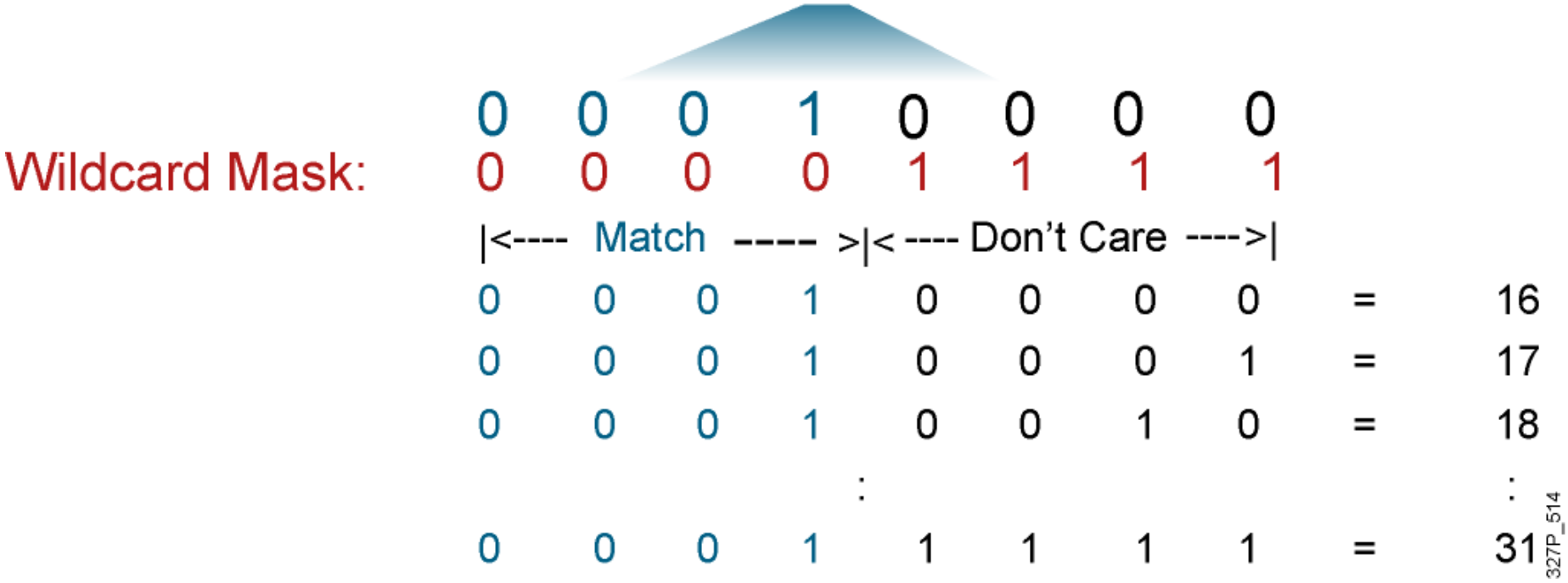
- Cách xác định Wildcard bits

Address và wildcard mask:

172.30.16.0 0.0.15.255

Network.Host

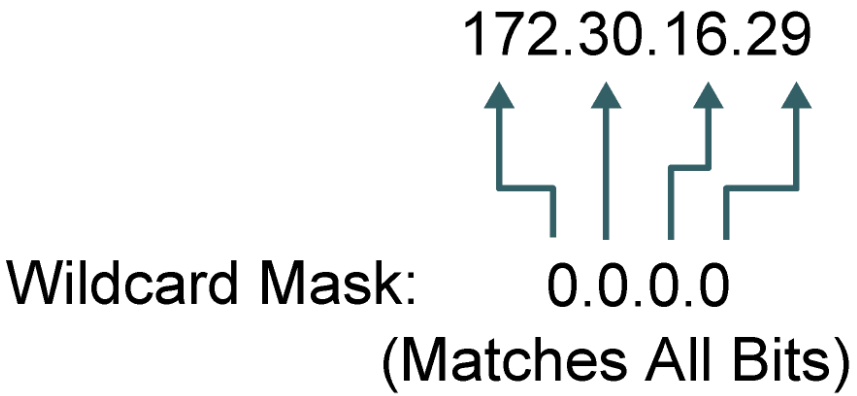
172.30.16.0



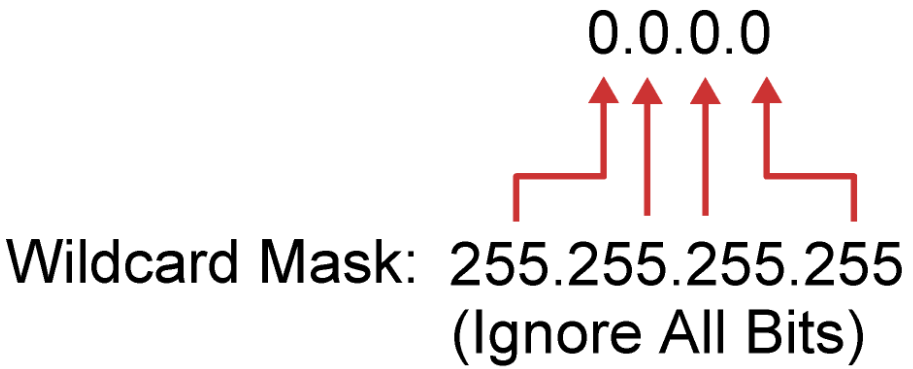
Giới thiệu Access Control List (ACL)

- Cách xác định Wildcard bits

- 172.30.16.29 0.0.0.0 xét tất cả các bit địa chỉ là host
- Có thể viết theo cách khác host 172.30.16.29



- 0.0.0.0 255.255.255.255 bỏ qua tất cả các bit địa chỉ.
- Có thể viết theo cách khác bằng cách dùng từ any.



Giới thiệu Access Control List (ACL)

- Các bước tạo ACL
  - ACL được tạo ra ở Global Configuration Mode. Khi cấu hình ACL trên router, mỗi ACL phải được xác định duy nhất bằng một số chỉ định.

```
Router  (config)#
access-list access-list-number { permit | deny }    {test-conditions}
```

ACL command	Description
access-list	defines an access list
access-list-number	protocol-dependent ACL number
Permit	defines a statement to allow traffic
Deny	defines a statement to disallow traffic
test-conditions	ACL test conditions

Giới thiệu Access Control List (ACL)

- Các bước tạo ACL
  - Chỉ định Access list lên interface

```
Router  (config-if)#
{protocol} access-group access-list-number  in/out
```

  - Áp dụng ACL cho interface

ACL command	Description
protocol	a protocol specified for the interface
access-group	any packets that pass the ACL test conditions can be permitted to use any interface in the access group of interfaces
access-list-number	the ACL identified by this ACL number to be associated to this interface
In/out	Apply inbound or outbound traffic

Giới thiệu Access Control List (ACL)

- Các bước tạo ACL
  - Chỉ định access list trên line VTY 0 4

```
Router  (config-line)#
{protocol}  access-class access-list-number
```

ACL command	Description
protocol	a protocol specified for the interface
access-class	any packets that pass the ACL test conditions can be permitted/deny to use any vty line
access-list-number	the ACL identified by this ACL number to be associated to this interface

Giới thiệu Access Control List (ACL)

- Các luật cơ bản để tạo và áp dụng ACL
  - Một ACL cho mỗi giao thức, mỗi hướng.
  - Standard ACL nên được áp dụng cho interface gần đích đến.
  - Extended ACL nên được áp dụng cho interface gần nguồn.
  - Sử dụng tham chiếu inbound, outbound cho các interface, khi nhìn từ bên trong router.
  - Kiểm tra điều kiện tuần tự từ đầu đến cuối ACL.
  - Có điều kiện deny ở cuối tất cả ACL.

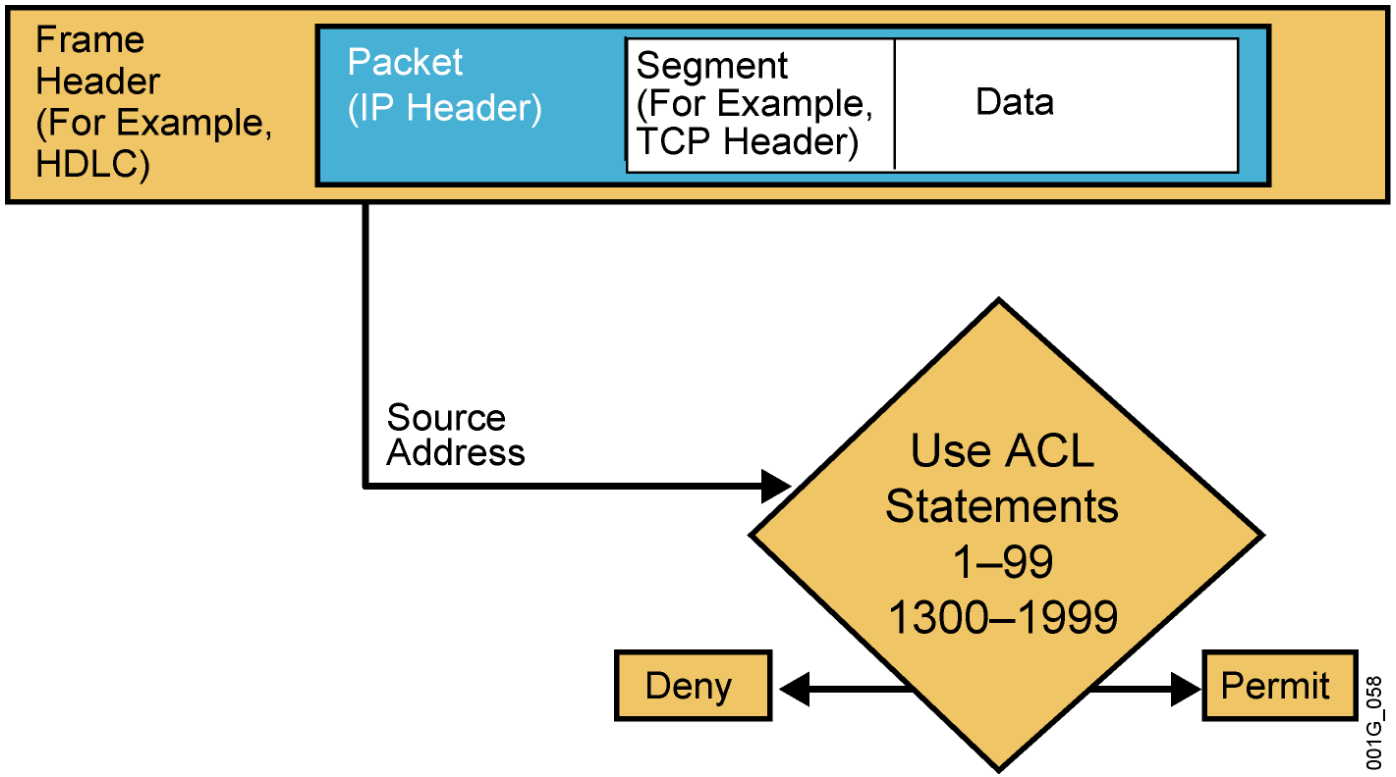
Giới thiệu Access Control List (ACL)

- Các luật cơ bản để tạo và áp dụng ACL
  - Dòng mới luôn được thêm vào cuối ACL.
  - Một ACL IP sẽ gửi một thông điệp ICMP host unreachable tới điểm xuất phát của các gói tin bị từ chối.
  - Nên chú ý khi loại bỏ ACL, tuỳ thuộc vào phiên bản IOS, sẽ có một danh sách mặc định deny chỉ định lên bất kì giao diện nào khi đó các traffic sẽ tạm dừng.
  - Việc lọc Outbound không ảnh hưởng đến traffic inbound.

Standard Access Lists

Standard ACL sử dụng địa chỉ nguồn để lọc gói tin và được áp gần đích

- Tổng quan Standard Access Lists

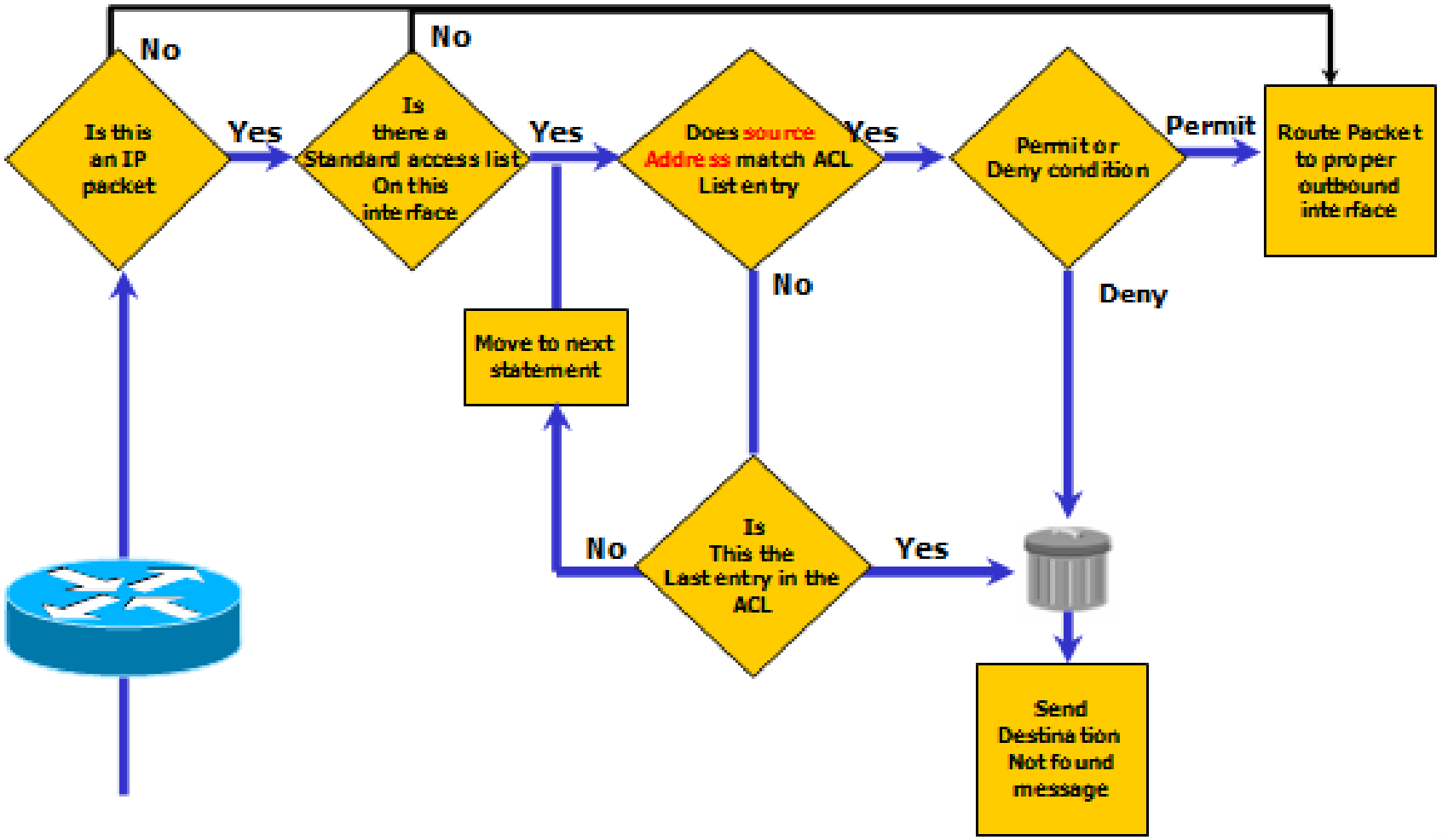


Standard Access Lists

- Tổng quan Standard Access Lists
  - Standard Access Lists là tiến trình kiểm tra gói tin IP .
  - Standard Access Lists kiểm tra địa chỉ nguồn của các gói tin IP có thể được chuyển.
  - Kết quả permit hay deny của bộ giao thức IP dựa trên địa chỉ mạng và địa chỉ HOST.
  - Đặt Standard Access List càng gần mạng đích càng tốt.

Standard Access Lists

- Cách Inbound Standard ACL làm việc.



Standard Access Lists

- Standard ACL command

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

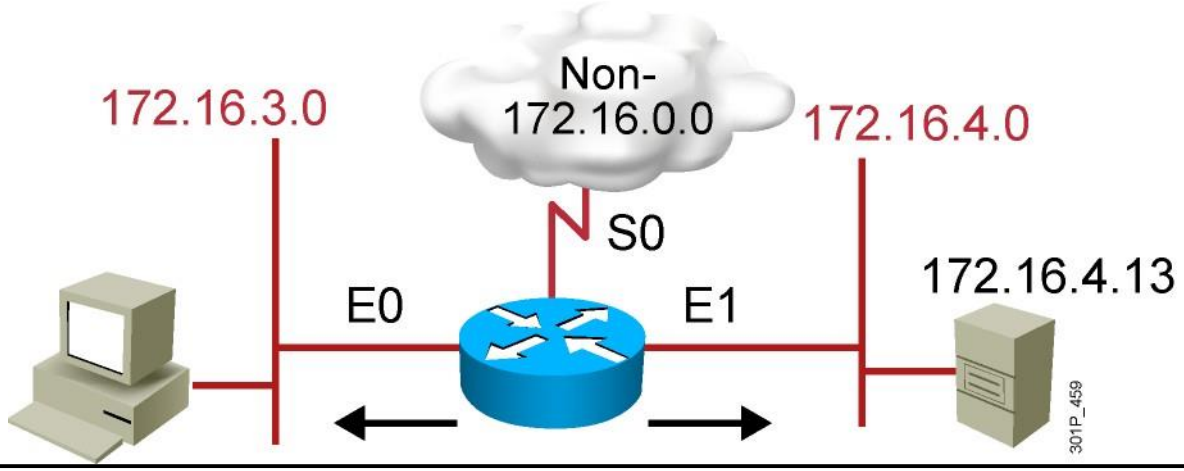
```
Router  (config-if)#
ip access-group access-list-number { in | out   }
```

  - Access list number: 1 → 99
  - Commands:

```
Router#show access-lists
```

Standard Access Lists

- Các ví dụ sử dụng Standard ACL
  - Permit my network only

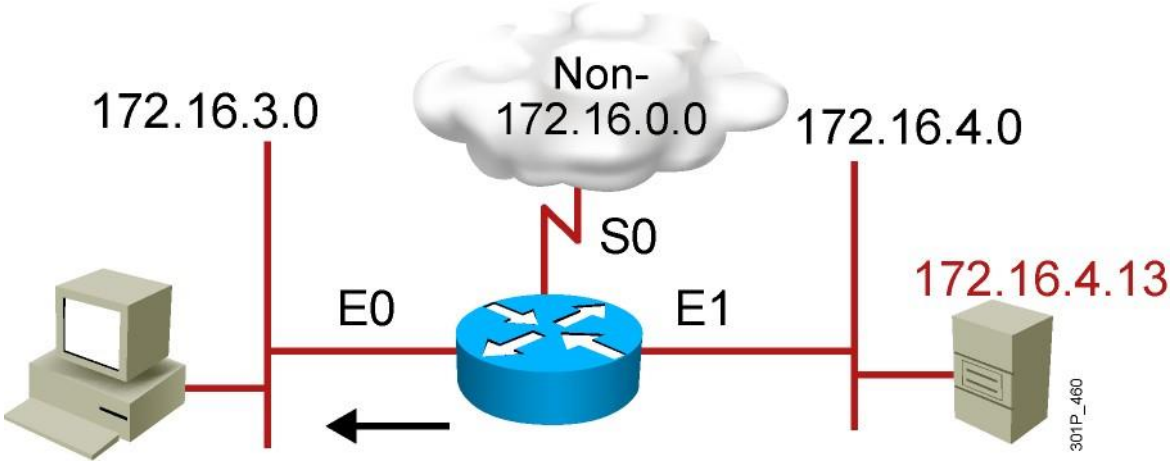



```
RouterX(config)# access-list 1  permit 172.16.0.0   0.0.255.255
(implicit deny all - not visible in the  list)
(access-list 1  deny  0.0.0.0    255.255.255.255)

RouterX(config)# interface ethernet 0
RouterX(config-if)# ip access-group 1 out
RouterX(config)# interface ethernet 1
RouterX(config-if)# ip access-group 1  out
```

Standard Access Lists

- Các ví dụ sử dụng Standard ACL
  - Deny a specific host

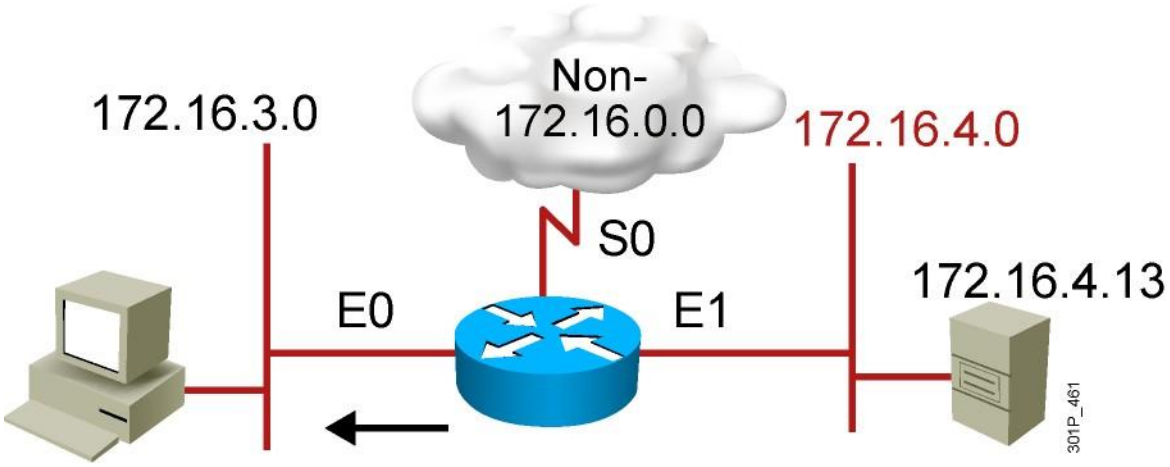



```
RouterX(config)#  access-list 1 deny 172.16.4.13  0.0.0.0
RouterX(config)#  access-list 1 permit 0.0.0.0  255.255.255.255
(implicit deny  all)
(access-list 1 deny  0.0.0.0   255.255.255.255)

RouterX(config)# interface ethernet  0
RouterX(config-if)# ip access-group 1  out
```

Standard Access Lists

- Các ví dụ sử dụng Standard ACL
  - Deny a specific subnet




```
RouterX(config)#  access-list 1 deny  172.16.4.0   0.0.0.255
RouterX(config)#  access-list 1 permit  any
(implicit deny  all)
(access-list 1 deny   0.0.0.0    255.255.255.255)

RouterX(config)# interface ethernet  0
RouterX(config-if)# ip access-group 1  out
```

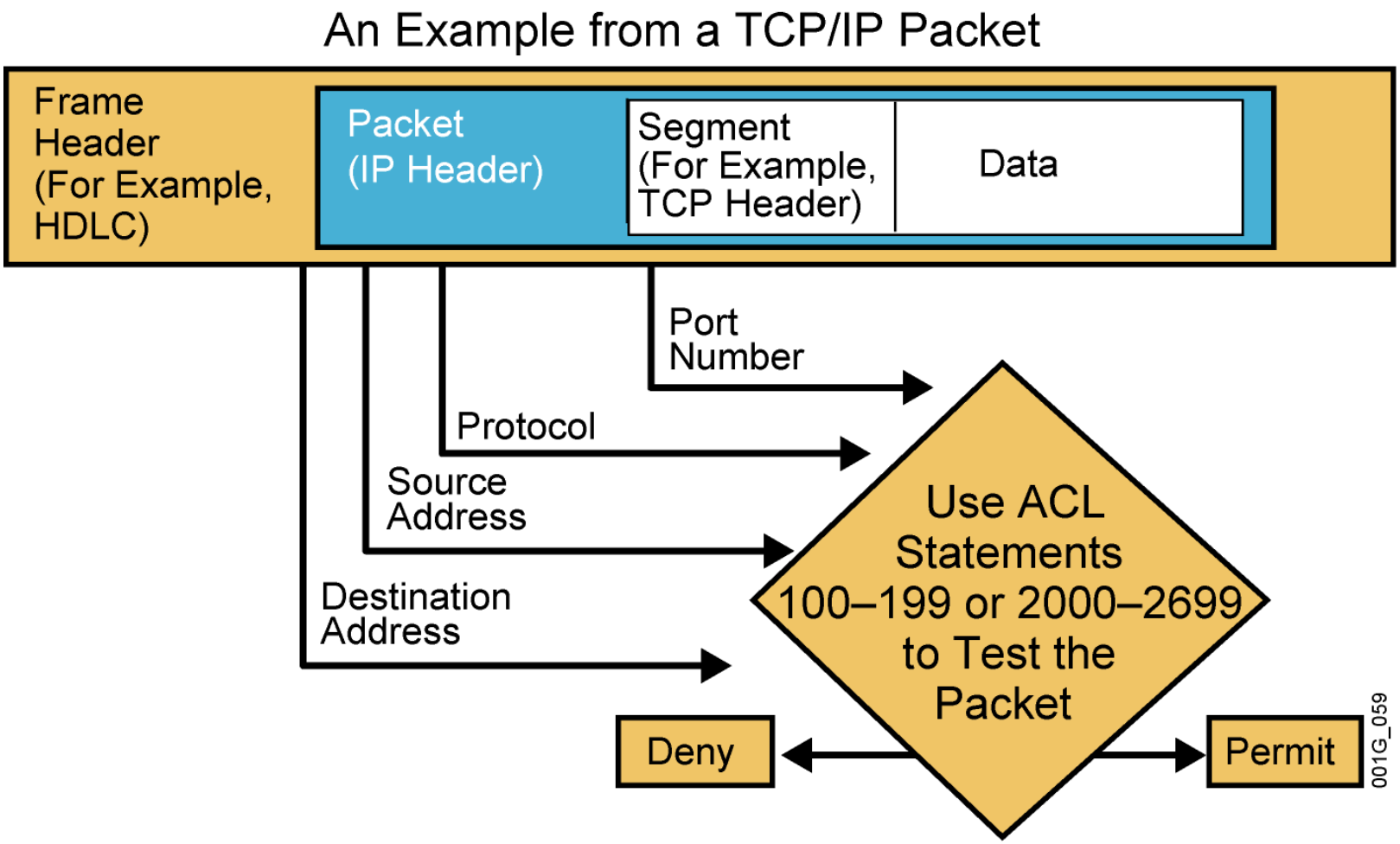
Extended Access Lists

Extended ACL sử dụng địa chỉ nguồn, đại chỉ đích, Port giao thức để lọc gói tin và được áp gần nguồn

- Tổng quan Extended Access Lists
  - Extended Access Lists thường được sử dụng hơn Standard ACLs vì cung cấp phạm vi kiểm soát lớn hơn.
  - Extended Access Lists kiểm tra nguồn các gói tin và địa chỉ đích cũng như các ứng dụng và Port.
  - Tạo ra sự linh hoạt cao hơn để mô tả những gì các ACL sẽ kiểm tra.

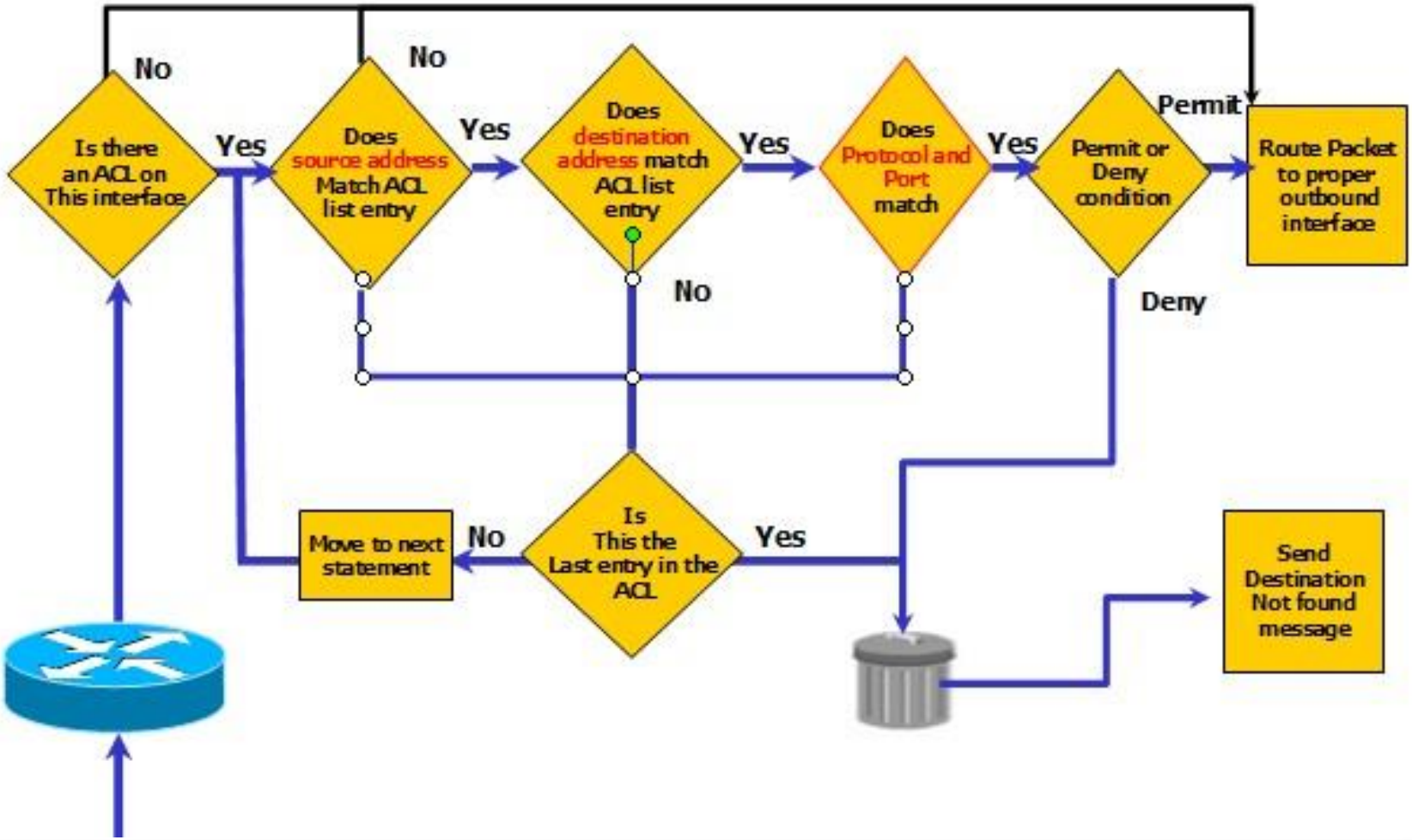
Extended Access Lists

- Tổng quan Extended Access Lists



Extended Access Lists

- Cách Inbound Extended ACL làm việc



Extended Access Lists

- Extended ACL command

```
RouterX(config)#
access-list access-list-number {permit | deny}
protocol source source-wildcard [operator port]
destination destination-wildcard [operator port]
[established]  [log]
```

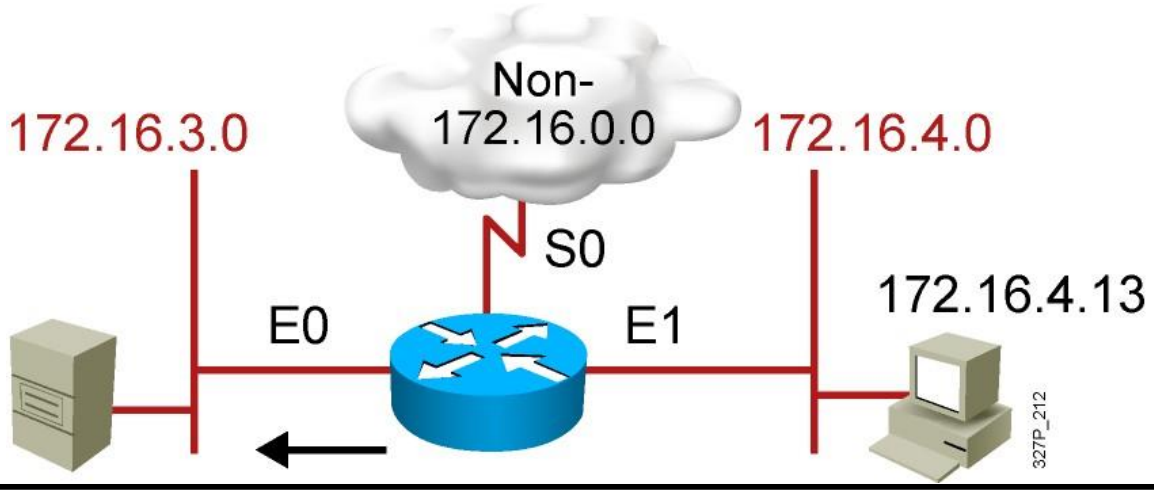
```
RouterX(config-if)#
ip access-group access-list-number  {in | out}
```

- Access list number: 100 → 199
- Commands:

```
Router#show access-lists
```

Extended Access Lists

- Các ví dụ sử dụng Extended ACL
  - Deny FTP from subnet 172.16.4.0 to subnet 172.16.3.0 out of E0.
  - Permit all other traffic.

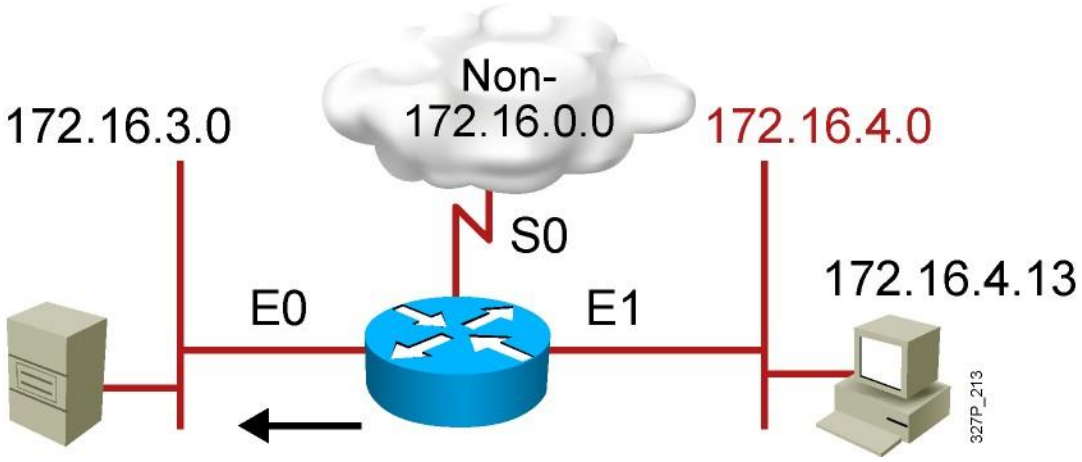



```
RouterX(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
RouterX(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq20
RouterX(config)# access-list 101 permit ip any any
(implicit deny all)
(access-list 101 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255)

RouterX(config)# interface ethernet 0
RouterX(config-if)# ip access-group 101 out
```

Extended Access Lists

- Các ví dụ sử dụng Extended ACL
  - Deny Telnet từ subnet 172.16.4.0 ra khỏi E0.
  - Permit tất cả các traffic khác.




```
RouterX(config)# access-list 101 deny tcp 172.16.4.0  0.0.0.255  any eq 23
RouterX(config)# access-list 101 permit ip any any
(implicit deny all)

RouterX(config)# interface ethernet 0
RouterX(config-if)# ip access-group 101 out
```

Named Access Lists

Named ACL khắc phục hoàn toàn những nhược điểm còn tồn tại của Standard và Extetnded ACL đặt theo số ID

- Tổng quan Named Access Lists
  - Name Access Lists cung cấp khả năng sửa đổi ACL nhưng không xoá đi mà sau đó cấu hình lại chúng.
  - Dòng mới luôn được vào cuối danh sách truy cập.
  - Không được sử dụng cùng một tên cho nhiều ACL.

Named Access Lists

- Named ACL command

```
Router  (config)#
ip access-list {standard | extended}   name

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

Router(config-if)#
ip access-group name {in |  out}

Router#
show  access-lists
```

Named Access Lists

- Named ACL command

```
RouterX# show access-lists {access-list  number|name}
```

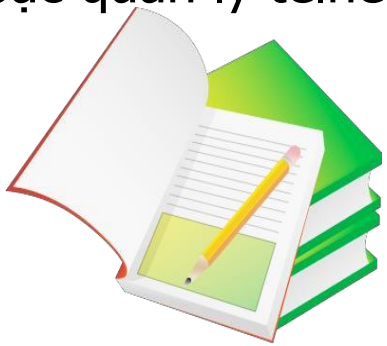
```
RouterX# show  access-lists
Standard IP access list  SALES
    10 deny   10.1.1.0, wildcard bits  0.0.0.255
    20 permit  10.3.3.1
    30 permit  10.4.4.1
    40 permit 10.5.5.1
Extended IP access list  ENG
    10 permit tcp host 10.22.22.1 any eq telnet (25  matches)
    20 permit tcp host 10.33.33.1 any eq ftp
    30 permit tcp host 10.44.44.1 any eq ftp-data
```

Câu hỏi ôn tập

- Cách thức hoạt động của ACL?
- So sánh Standard ACL và Extended ACL?

TÓM LƯỢC BÀI HỌC

- Khái niệm, các hoạt động của ACL.
- Các loại ACL.
- Cấu hình ACL.
- Kết luận
  - Bài học cung cấp những kiến thức về bảo mật mức độ cơ bản cho Router, cho hệ thống dựa trên cấu hình ACL
  - Trên thực tế, đối với các hệ thống nhỏ, ACL rất hữu dụng trong việc lọc traffic mạng. Đối với cá hệ thống vừa và lớn, sử dụng ACL torng mục đích VPN hoặc quản lý telnet, lọc tuyến.



Q & A