



TRƯỜNG ĐẠI HỌC THỦY LỢI

KHOA CÔNG NGHỆ THÔNG TIN

Bộ môn: Kỹ thuật máy tính và mạng

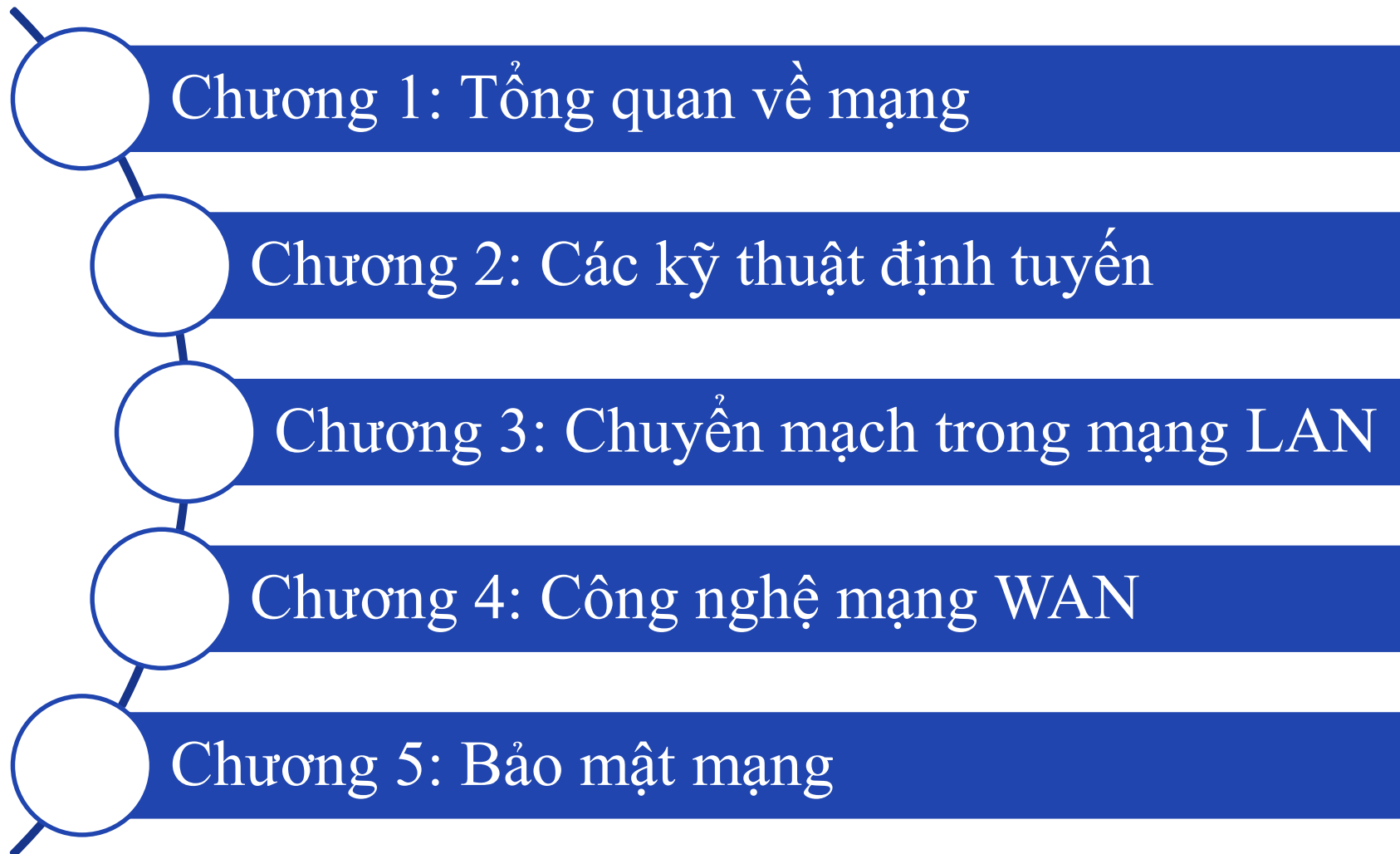
QUẢN TRỊ MẠNG

Giảng viên: Trần Văn Hội

Email: hoitv@tlu.edu.vn

Điện thoại: 0944.736.007

NỘI DUNG MÔN HỌC

- 
- Chương 1: Tổng quan về mạng
 - Chương 2: Các kỹ thuật định tuyến
 - Chương 3: Chuyển mạch trong mạng LAN
 - Chương 4: Công nghệ mạng WAN
 - Chương 5: Bảo mật mạng

CHƯƠNG 5: BẢO MẬT MẠNG



- 1. Giới thiệu chung



- 2. Danh sách điều khiển truy cập ACL



- 3. Bảo mật Switch

BÀI 1: GIỚI THIỆU CHUNG

- ❖ Hệ thống mạng là một tập hợp các máy tính gồm thành phần phần cứng, phần mềm và dữ liệu.
- ❖ Tài nguyên thông tin:
 - ✓ Phần cứng.
 - ✓ Phần mềm.
 - ✓ Dữ liệu.
 - ✓ Môi trường truyền thông giữa các máy tính.
 - ✓ Môi trường làm việc.
 - ✓ Con người.

CÁC MỐI ĐE DOẠ

- ❖ Phá hoại: Phá hỏng thiết bị phần cứng hoặc phần mềm trên hệ thống. Sửa đổi tài nguyên của hệ thống trái phép.
- ❖ Tấn công: kiểu do thám (Bắt gói, dò port, ping quét thông tin).
 - Tấn công kiểu truy xuất
 - Tìm mật khẩu, lỗ hổng...
 - Từ chối dịch vụ DoS.
- ❖ Can thiệp: Bị truy cập bởi những người không có thẩm quyền.
- ❖ Sử dụng Worm, Virus, Trojan horse.

Types of Network Attacks



Reconnaissance



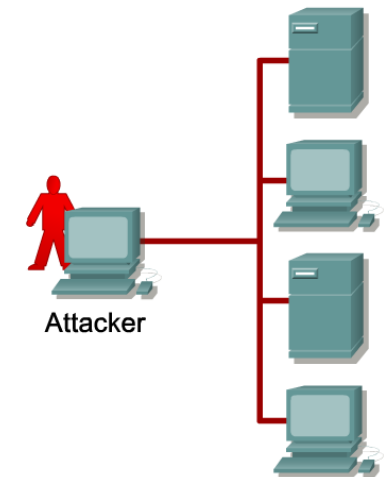
Access



Denial of Services



Worms, Viruses, and Trojan Horses



CÁC MỐI ĐE DỌA

Sau khi tác nhân đe dọa giành được quyền truy cập vào mạng, bốn loại mối đe dọa có thể phát sinh:

- ❖ Đánh cắp thông tin (Information Theft)
- ❖ Mất dữ liệu (Data Loss)
- ❖ Hành vi trộm cắp số nhận dạng (Identity Theft)
- ❖ Làm gián đoạn dịch vụ (Disruption of Service)

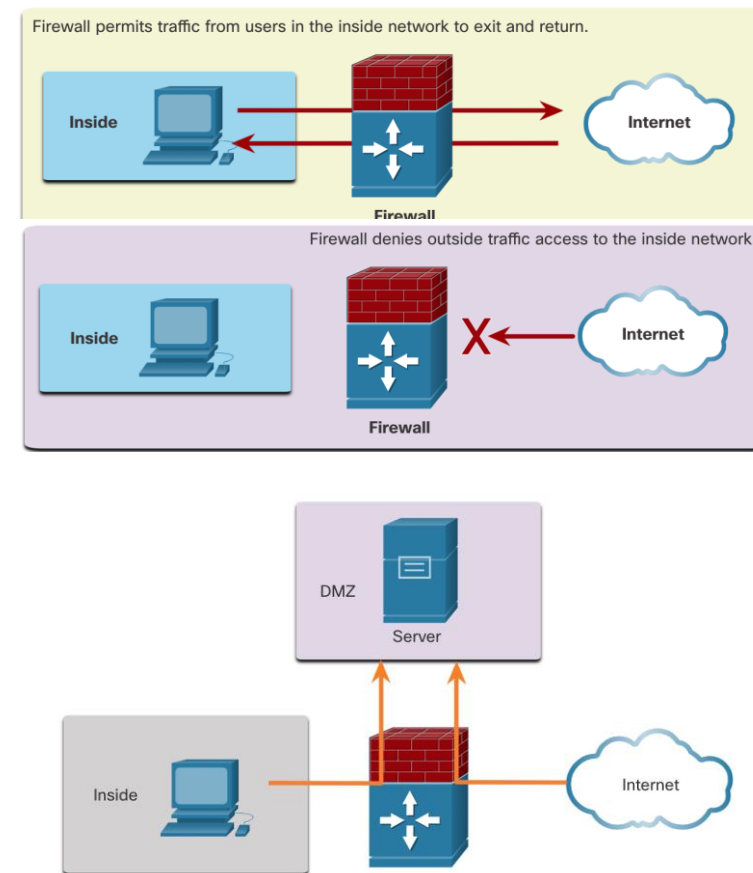
BIỆN PHÁP PHÒNG THỦ

Một số thiết bị và dịch vụ bảo mật được triển khai để bảo vệ người dùng và tài sản của tổ chức trước các mối đe dọa TCP/IP:

- ❖ VPN (Virtual Private Network)
- ❖ Máy chủ AAA (Authentication, Authorization, and Accounting)
- ❖ Tường lửa ASA (Adaptive Security Appliance)
- ❖ IPS/IDS (Intrusion Prevention System / Intrusion Detection System)
- ❖ Danh sách điều khiển ACL
- ❖ Backup dữ liệu
- ❖ Nâng cấp, cập nhật và vá lỗi

TƯỜNG LỬA – FIREWALL

- ❖ Tường lửa mạng nằm giữa hai hoặc nhiều mạng, kiểm soát lưu lượng giữa chúng và giúp ngăn chặn truy cập trái phép.
- ❖ Tường lửa có thể cho phép người dùng bên ngoài truy cập có kiểm soát vào các dịch vụ cụ thể.
- ❖ Ví dụ: các máy chủ mà người dùng bên ngoài có thể truy cập thường được đặt trên một mạng đặc biệt được gọi là khu phi quân sự (DMZ). DMZ cho phép quản trị viên mạng áp dụng các chính sách cụ thể cho các máy chủ được kết nối với mạng đó.

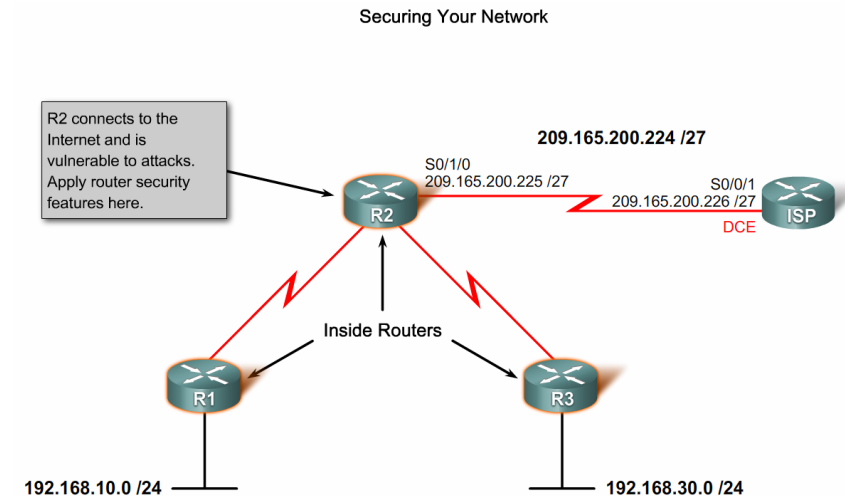


CÁC KIỂU TƯỜNG LỬA

- ❖ Các sản phẩm tường lửa được đóng gói dưới nhiều hình thức khác nhau. Những sản phẩm này sử dụng các kỹ thuật khác nhau để xác định những gì sẽ được phép hoặc bị từ chối truy cập vào mạng.
- ❖ Chúng bao gồm những kiểu sau đây:
 - Lọc gói - Ngăn chặn hoặc cho phép truy cập dựa trên địa chỉ IP hoặc MAC
 - Lọc ứng dụng - Ngăn chặn hoặc cho phép truy cập theo loại ứng dụng cụ thể dựa trên số cổng.
 - Lọc URL - Ngăn chặn hoặc cho phép truy cập vào các trang web dựa trên các URL hoặc từ khóa cụ thể.
 - Kiểm tra trạng thái gói (SPI) - Các gói đến phải là phản hồi hợp pháp đối với các yêu cầu từ máy chủ nội bộ. Các gói không mong muốn bị chặn trừ khi được cho phép cụ thể. SPI cũng có thể bao gồm khả năng nhận dạng và lọc ra các kiểu tấn công cụ thể, chẳng hạn như từ chối dịch vụ (DoS).

BẢO MẬT ROUTER, SWITCH

1. Sử dụng giao diện dòng lệnh CLI
2. Sử dụng phần mềm SDM
(Security Device Manager)



ĐẶT PASSWORD CÔNG CONSOLE

Press RETURN to get started.

Password:

Router> enable

Password:

Router#

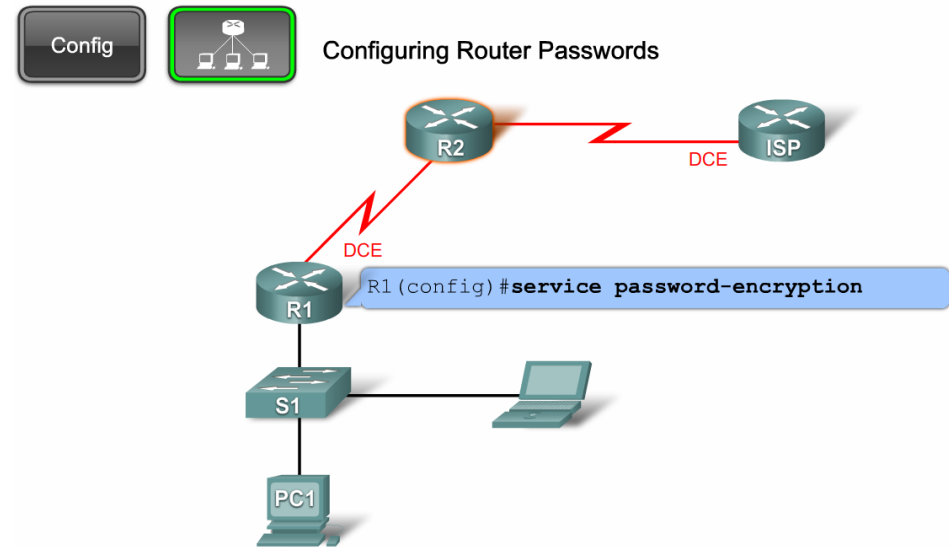
Router(config)# line console 0

Router(config-line)# password cisco

Router(config-line)# login // Bật chế độ kiểm tra mật khẩu

Bỏ mật khẩu

Router(config-line)# no password



Administrator encrypts all passwords in the configuration file.

ĐẶT PASSWORD CHO MỨC PRIVILEGED

Router> enable

Password:

Router# Configure terminal

Router(config)# enable password cisco1

//Hoặc mật khẩu được mã hóa

Router(config)# enable secret cisco2

Router(config)# exit

Xem mật khẩu được mã hóa MD5

Router(config)# Show running-config

ĐẶT PASSWORD TRUY NHẬP TỪ XA

Router# **Configure terminal**

Router(config)# **line vty 0 4**

Router(config-line)# **password cisco**

Router(config-line)# **login**

Thoát ra để thử mật khẩu

Mã hóa tất cả các mật khẩu

Router(config)#**Service password-encryption**

Mã hóa tất cả các mật khẩu

- ❖ Để được thực hiện đảm bảo rằng mật khẩu được giữ bí mật trên bộ định tuyến và chuyển mạch của Cisco, bao gồm các bước sau:
- ❖ Mã hóa tất cả mật khẩu văn bản gốc bằng lệnh mã hóa mật khẩu dịch vụ.
- ❖ Đặt độ dài mật khẩu tối thiểu có thể chấp nhận bằng lệnh độ dài tối thiểu của mật khẩu bảo mật.
- ❖ Ngăn chặn các cuộc tấn công đoán mật khẩu thô bạo bằng khối đăng nhập dành cho # lần thử # trong # lệnh.
- ❖ Vô hiệu hóa quyền truy cập chế độ EXEC đặc quyền không hoạt động sau một khoảng thời gian được chỉ định bằng lệnh exec-timeout.

Router(config)#Service
encryption

password

```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# password cisco
Router(config-line)# exec-timeout 5 30
Router(config-line)# transport input ssh
Router(config-line)# end
Router#
Router# show running-config | section line vty
line vty 0 4
  password 7 03095A0F034F
  exec-timeout 5 30
  login
Router#
```

CHƯƠNG 5: BẢO MẬT MẠNG



- 1. Giới thiệu chung



- 2. Danh sách điều khiển truy cập ACL



- 3. Bảo mật Switch

BÀI 2: DANH SÁCH ĐIỀU KHIỂN TRUY CẬP ACL

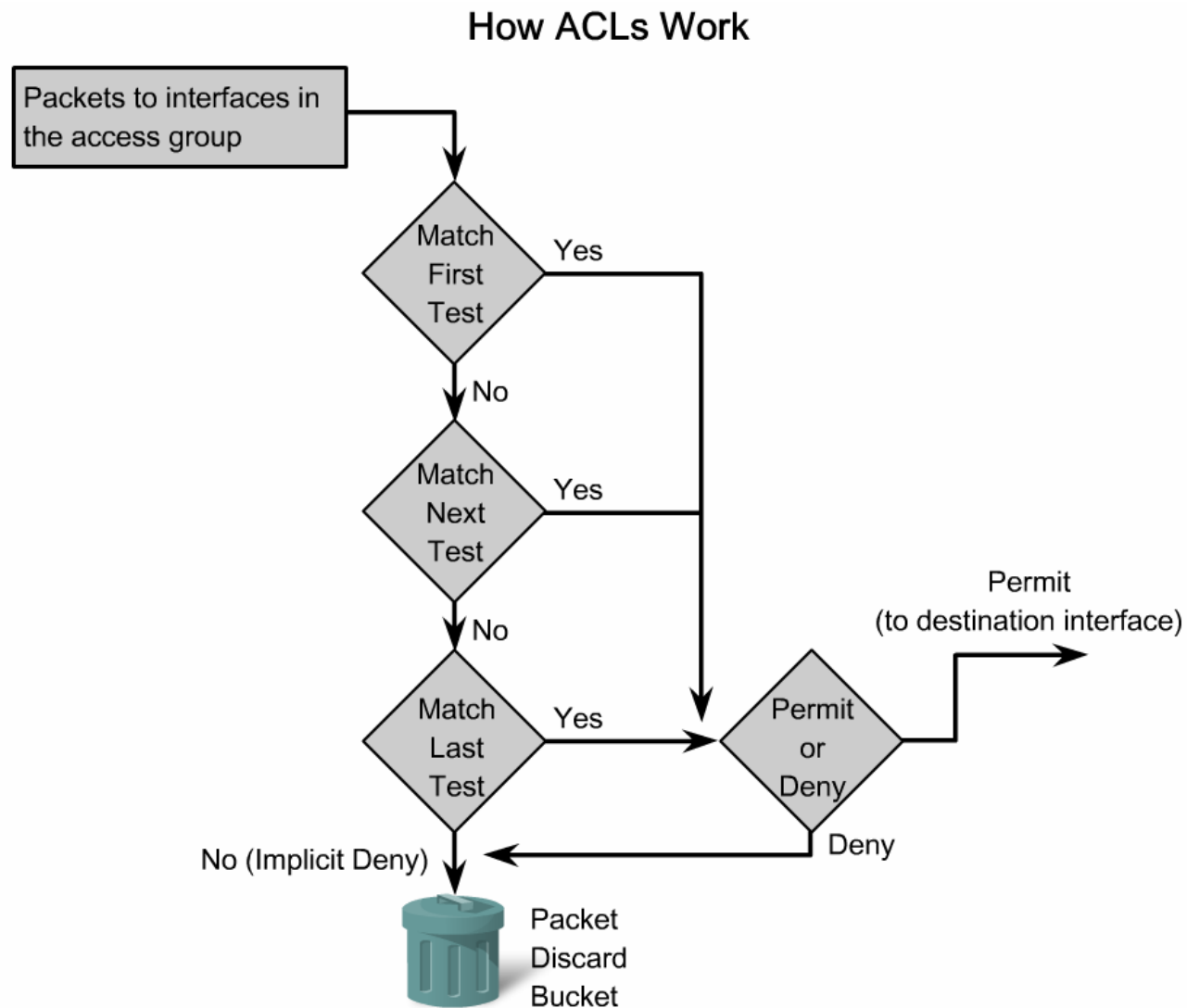
- ❖ ACL là một loạt các lệnh IOS được sử dụng để lọc các gói dựa trên thông tin được tìm thấy trong tiêu đề gói. Theo mặc định, một bộ định tuyến không có bất kỳ ACL nào được cấu hình.
- ❖ Khi ACL được áp dụng cho một giao diện, bộ định tuyến sẽ thực hiện nhiệm vụ bổ sung là đánh giá tất cả các gói mạng khi chúng đi qua giao diện để xác định xem gói có thể được chuyển tiếp hay không.
- ❖ Một ACL sử dụng một danh sách tuần tự các câu lệnh cho phép hoặc từ chối, được gọi là các mục kiểm soát truy cập (ACE).
- ❖ Lưu ý: ACE cũng thường được gọi là câu lệnh ACL. Khi lưu lượng truy cập mạng đi qua một giao diện được định cấu hình bằng ACL, bộ định tuyến sẽ so sánh thông tin trong gói với từng ACE, theo thứ tự tuần tự, để xác định xem gói có khớp với một trong các ACE hay không. Quá trình này được gọi là lọc gói tin.

ACL TRÊN ROUTER CISCO

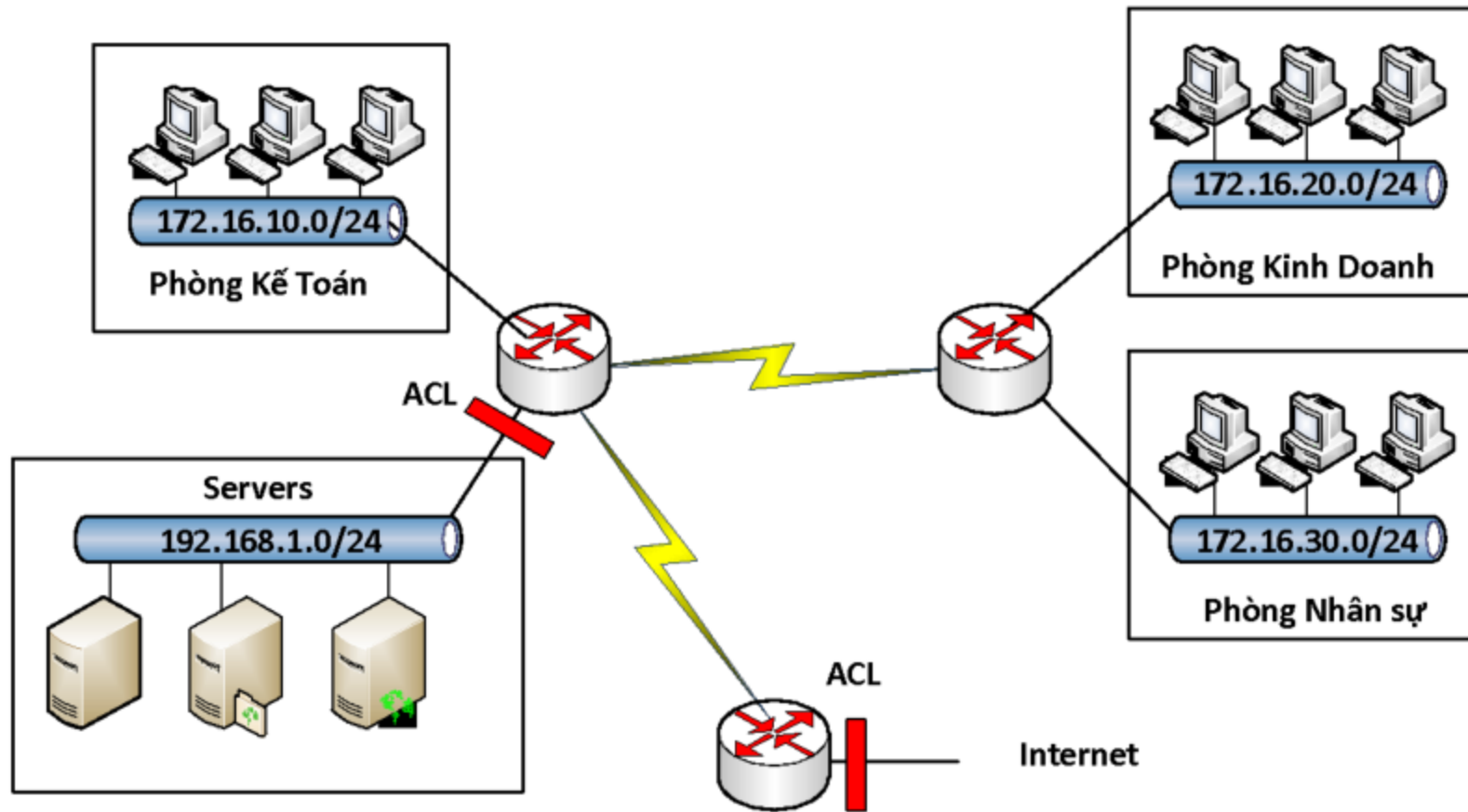
❖ Cấu hình ACL – Access Control List trên router Cisco

- 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 hủy 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.

HOẠT ĐỘNG CỦA ACLs



ACCESS CONTROL LIST



PHÂN LOẠI VÀ HOẠT ĐỘNG 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.

PHÂN LOẠI VÀ HOẠT ĐỘNG ACL

- Trong cấu 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.

CẤU HÌNH ACL

- ❖ Có 2 phương pháp cấu hình ACL:
 - Dựa vào số (numbered ACL)
 - Dựa vào tên (named ACL)
- ❖ 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.

CẤU HÌNH ACL

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:

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

❖ Wildcard “host”

“Wildcard mask” dùng cho một thiết bị hay còn gọi là “wildcard-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

MỘT SỐ THUẬT NGỮ

❖ 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
```

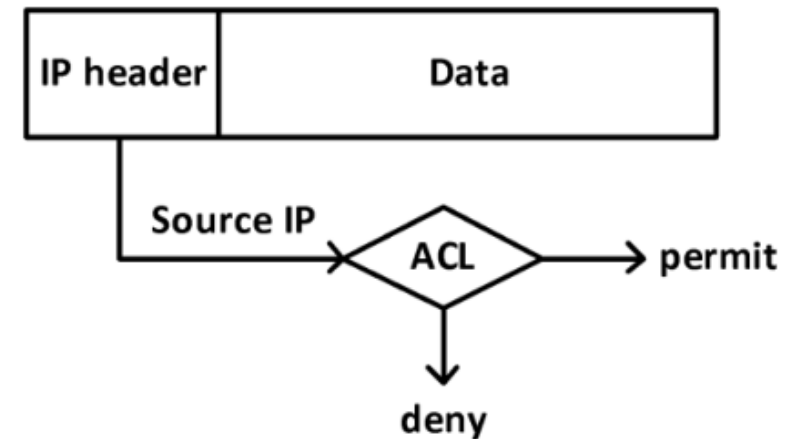
hoặc: R(config)#access-list 1 permit any

❖ 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.

STANDARD ACL

- ❖ Sử dụng “Standard CL” 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 CL” 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

❖ 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

❖ Gán ACL vào một cổng và đặt chế độ kiểm tra cho luồng dữ liệu đi vào hay đi ra khỏi cổng của router.

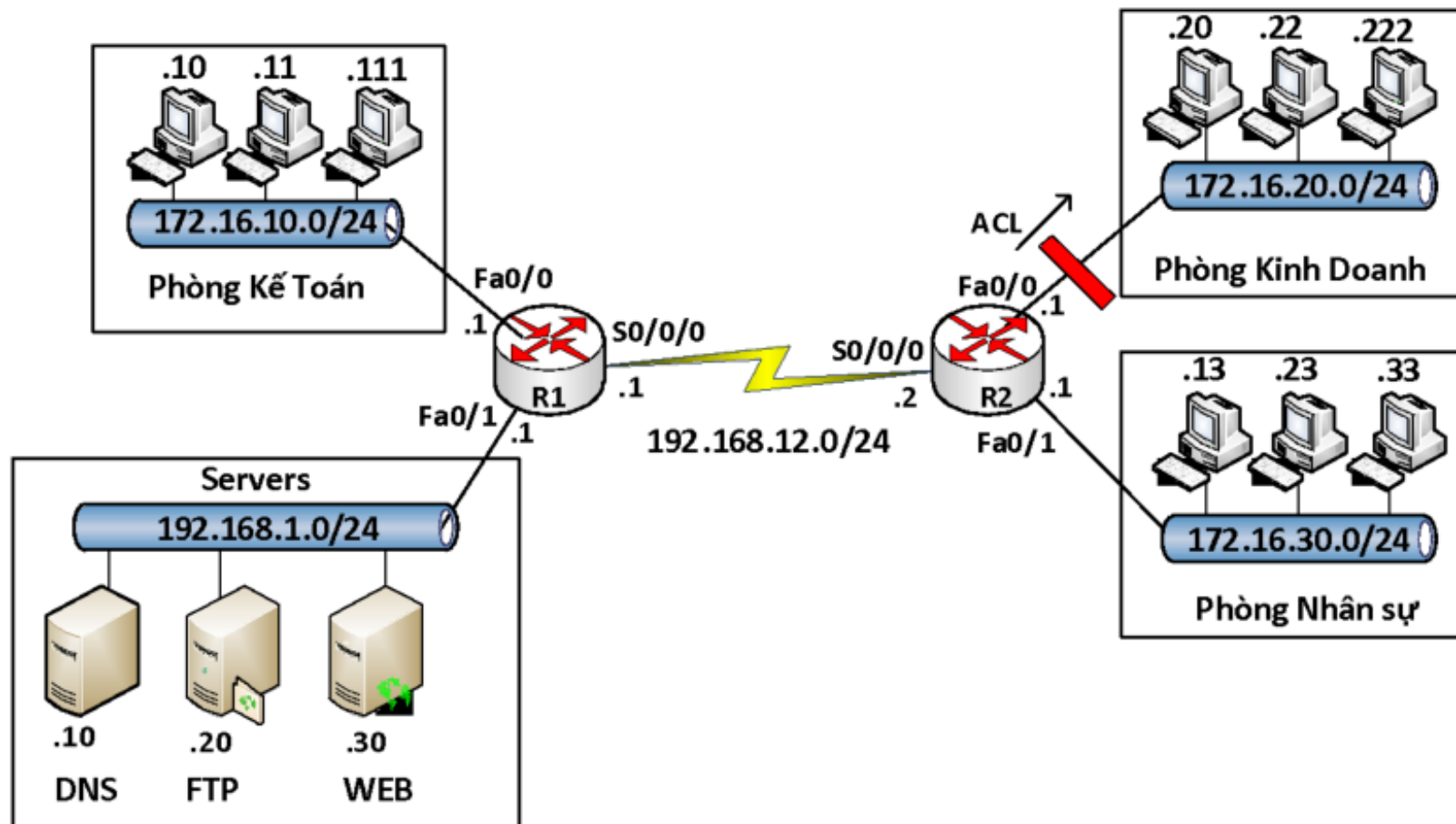
Router(config-if)# **ip access-group** <ACL-number> {**in|out**}

❖ Huỷ bỏ câu lệnh áp đặt ACL vào cổng

Router(config-if)# **no ip access-group** <ACL-number> {**in|out**}

VÍ DỤ

- ❖ Cấm các máy tính thuộc mạng 172.16.10.0/24 truy nhập tới mạng 172.16.20.0/24



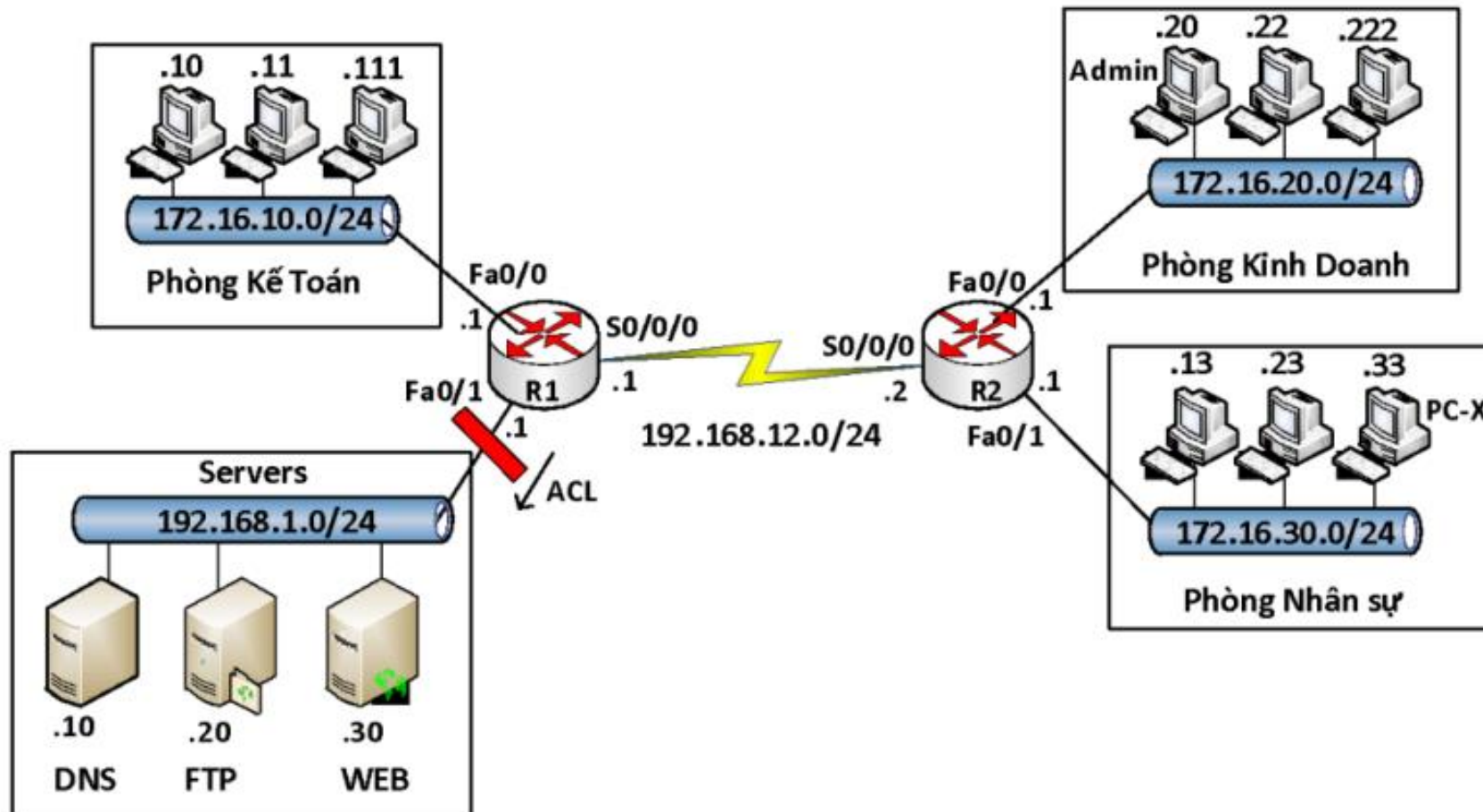
CẤU HÌNH TRÊN ROUTER R2

- ❖ 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

- ❖ R2(config)#ip access-list standard cam10
- ❖ R2(config)# deny 172.16.10.0 0.0.0.255
- ❖ R2(config)#permit any
- ❖ R2(config)#interface fa0/0
- ❖ R2(config-if)#ip access-group cam10 out

BÀI TẬP

❖ 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

DÙNG STANDARD ACL ĐIỀU KHIỂN TELNET

- ❖ Trên router có các “virtual terminal port” được dùng để cấu hình cho mục đích cho phép telnet vào router.
- ❖ 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}**
 - ✓ vty-number: có giá trị 0 đến 4 (Router), 0 đến 15 (Switch)
 - ✓ vty-range: là một dãy liên tiếp các port vty được sử dụng
 - ✓ access-list-number: ACL gán vào các cổng vty để điều khiển truy cập

VÍ DỤ

- ❖ Viết ACL chỉ cho phép Admin có IP 172.16.20.20 telnet vào các router R1, R2 trong mô hình bài tập trên.
- ❖ Trước tiên, cấu hình mở telnet trên R1 và R2.
- ❖ ACL thực hiện yêu cầu đầu bài: trên R1 và R2 sử dụng ACL:

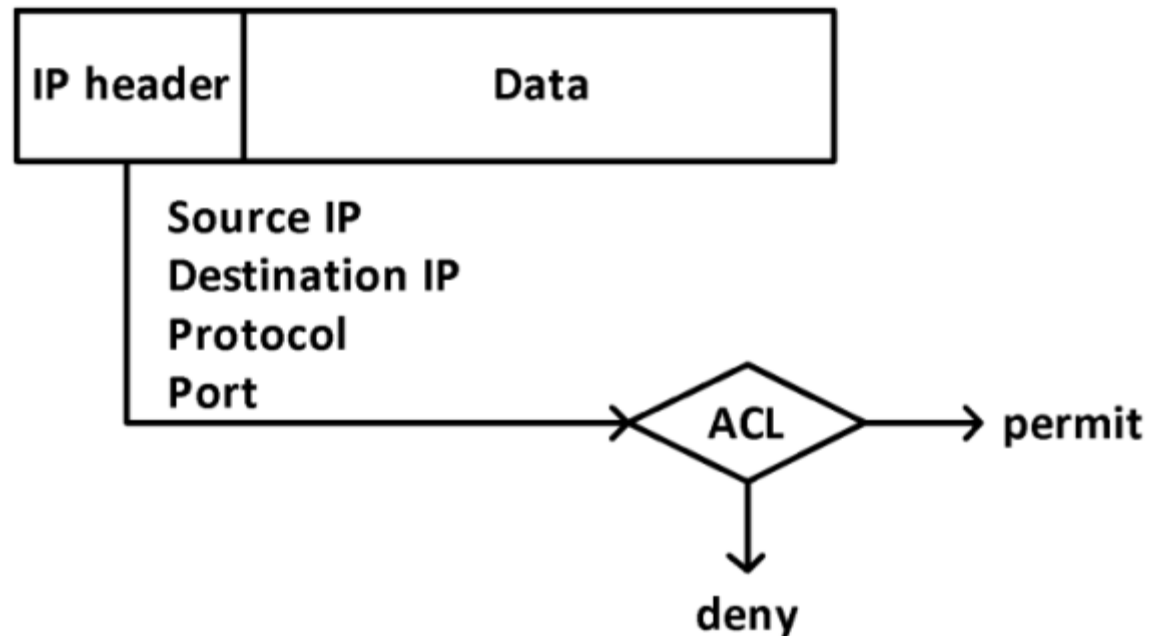
```
R(config)#access-list 20 permit host 172.16.20.20
```

```
R(config)#line vty 0 4
```

```
R(config-line)#access-class 20 in
```

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

❖ Lệnh tạo một điều kiện (ACL entry) trong một ACL access-list-number

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

❖ Trong đó:

➤ access-list-number: có giá trị từ 100 – 199 hoặc 2000 - 2699

➤ protocol: là ip, udp, tcp, icmp,...

➤ operation: 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

CẤU HÌNH EXTENDED ACL

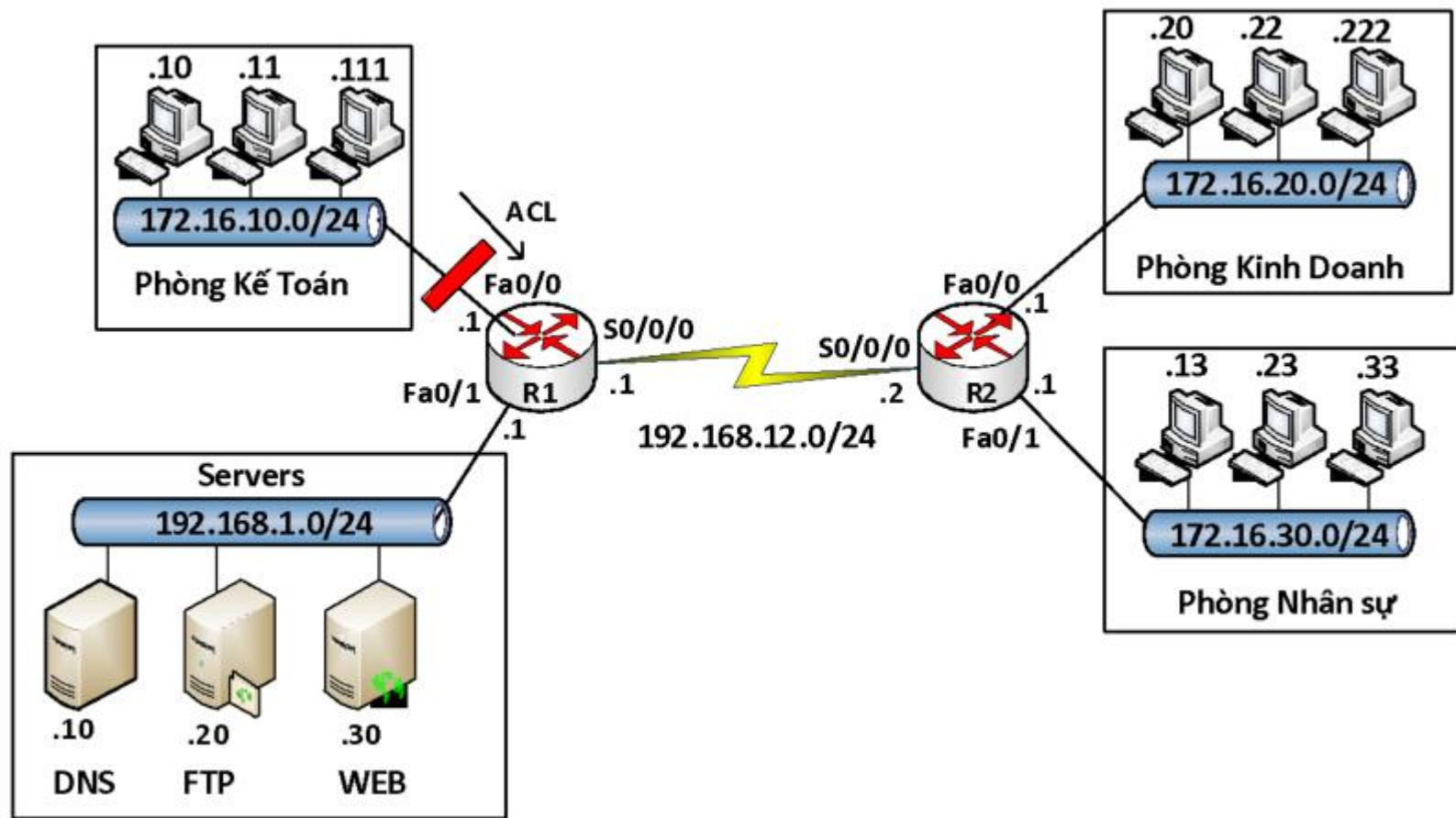
- ❖ Gán danh sách ACL vào interface và chọn hướng (inbound hoặc outbound) các traffic sẽ được kiểm tra.

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.

VÍ DỤ

- ❖ 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.



```
R1(config)#access-list 100 deny icmp 172.16.10.0 0.0.0.255 host 172.16.20.20
```

```
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.

SỬ DỤNG NAME EXTENDED

R1(config)#ip access-list Extended Cam10ftp

R1(config-ext-nac)#deny tcp 172.16.10.0 0.0.0.255 host 192.168.1.20 eq 20

R1(config-ext-nac)#deny tcp 172.16.10.0 0.0.0.255 host 192.168.1.20 eq 21

R1(config-ext-nac)#permit ip any any

R1(config)#interface fa0/0

R1(config-if)#ip access-group 100 in

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}
- ❖ Trong đó: sequence-number là dòng chèn vào danh sách.

MỘT SỐ LỆNH KIỂM TRA CẤU HÌNH ACL

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

Ví dụ: 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

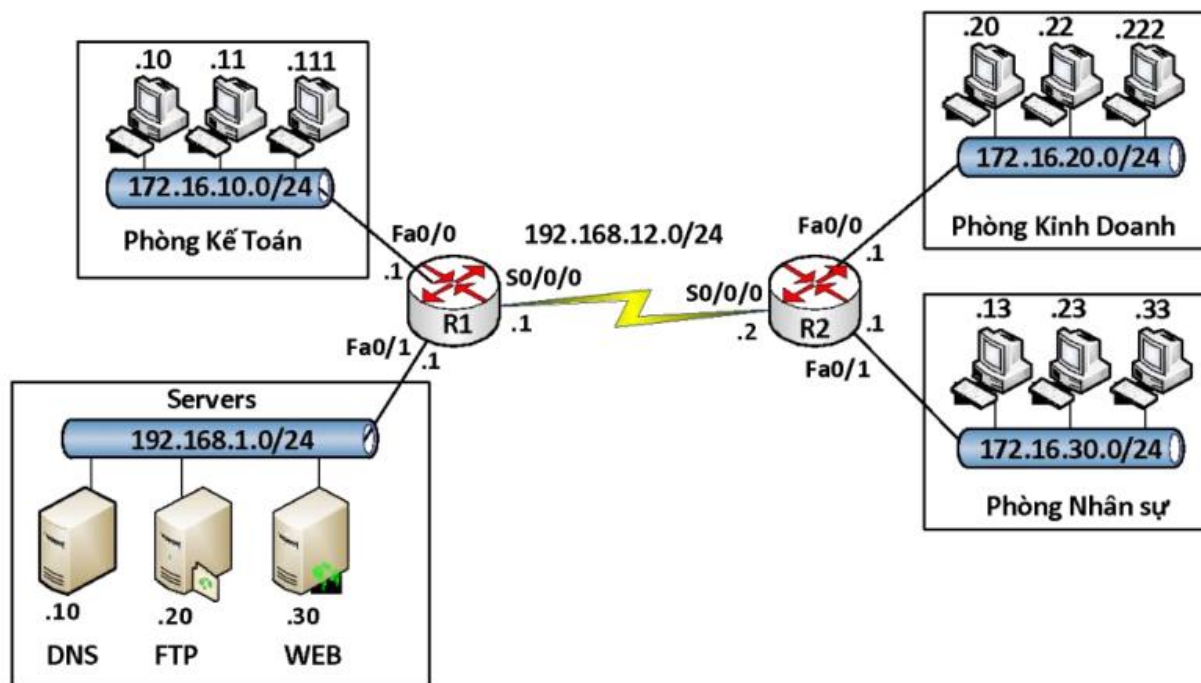
 permit tcp host 10.22.22.1 any eq telnet

 permit tcp host 10.33.33.1 any eq ftp

 permit tcp host 10.44.44.1 any eq ftp-data

VÍ DỤ

1. Cấu hình Extended 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
```

HƯỚNG DẪN CẤU HÌNH

❖ 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 access-group xyz in
```

HƯỚNG DẪN CẤU HÌNH

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

```
R1(config)# ip access-list extended tlu
```

```
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 tlu out
```

HƯỚNG DẪN CẤU HÌNH

(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

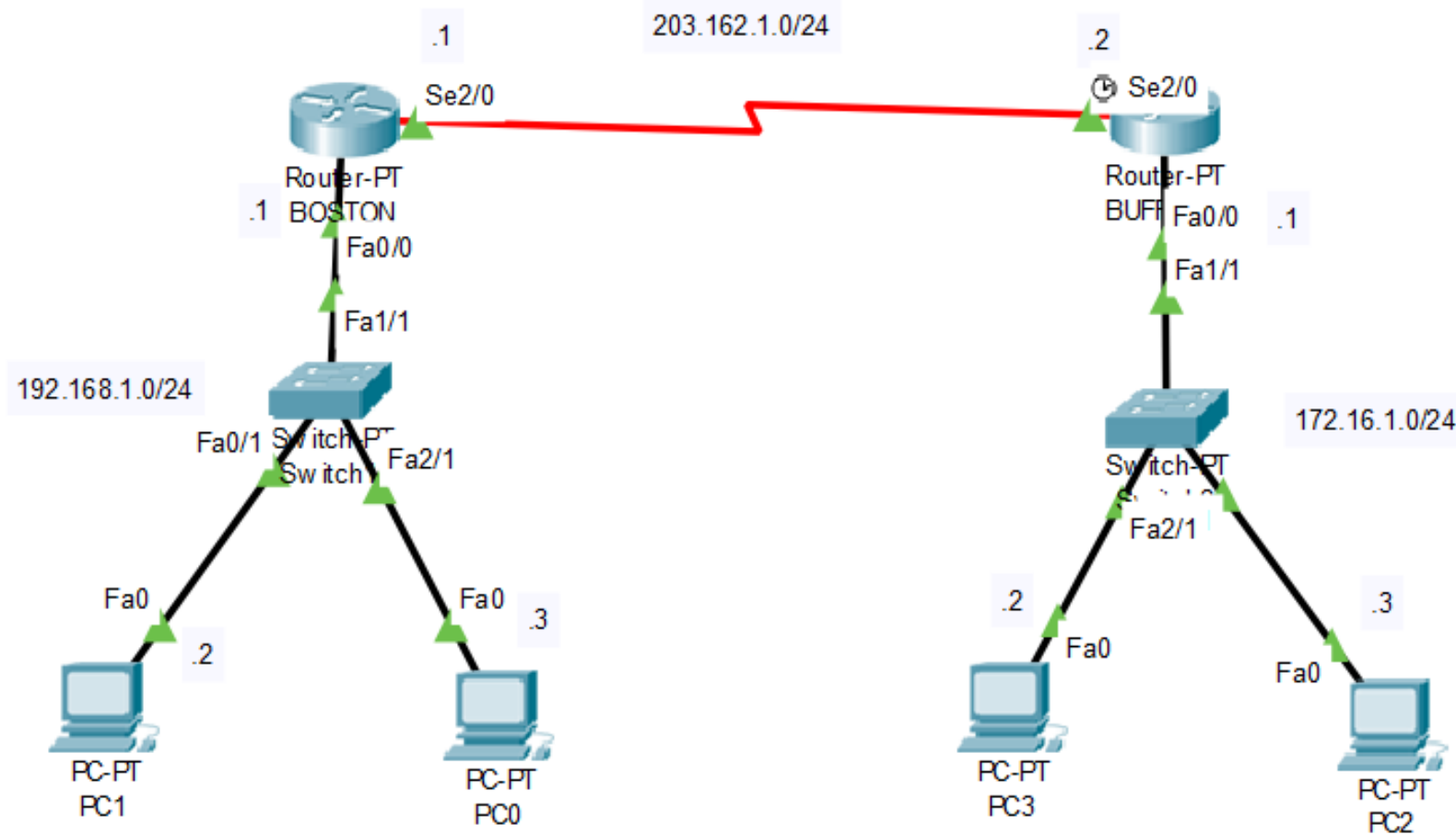
R# show run

R# show ip route

R# show access-lists

BÀI TẬP 1: STANDARD ACL

- ❖ Lọc các packet sử dụng standard ACL, thực hiện cấm tất cả các traffic từ PC1 đến các PC trong mạng 172.16.1.0/24



CẤU HÌNH TRÊN ROUTER BUFFALO

Buffalo(config)#**access-list** 1 **deny** 192.168.1.2 0.0.0.0

(hoặc Buffalo (config)#**access-list** 1 **deny host** 192.168.1.2)

Buffalo(config)#**access-list** 1 **permit ip any**

Buffalo(config)#**interface** f0/0

Buffalo(config-if)#**ip add** 172.16.1.1 255.255.255.0

Buffalo(config-if)#**ip access-group** 1 **out**

Buffalo(config-if)#**no shut**

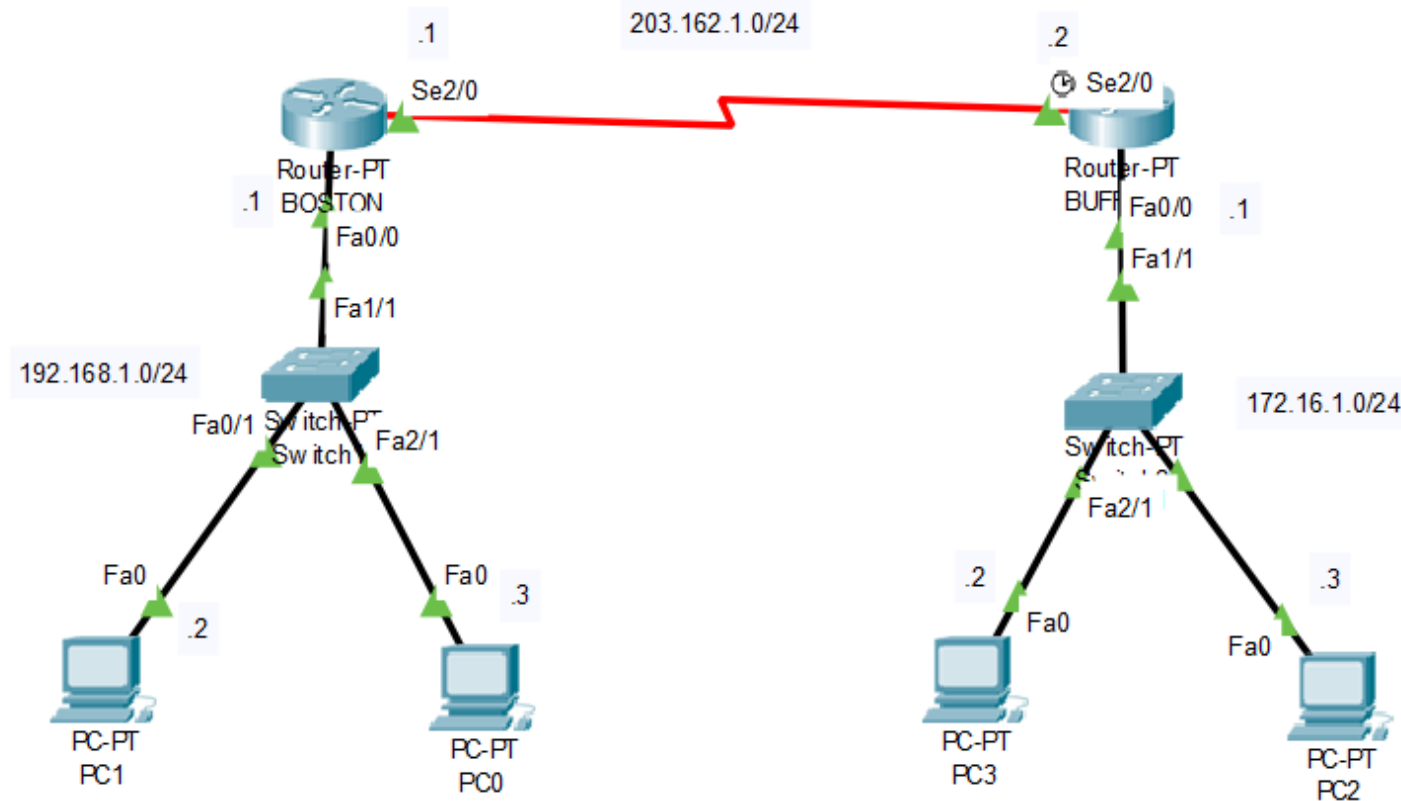
Buffalo(config-if)#**exit**

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

BÀI TẬP 2: EXTENDED ACL

Yêu cầu: Sử dụng Access-list để lọc ngõ vào trên cổng serial của Router Boston cho phép tất cả các lưu lượng từ PC3 tới PC0 và từ chối tất cả các lưu lượng từ PC3 tới PC1.



CẤU HÌNH TRÊN ROUTER BOSTON

❖ Cấu hình ACL

Boston(config)#**access-list** 100 **permit** ip **host** 172.16.1.2 **host** 192.168.1.3

Boston(config)#**access-list** 100 **deny** ip **host** 172.16.1.2 **host** 192.168.1.2

❖ Gán ACL vào cổng serial của RouterA

Boston(config)#**interface** Serial 2/0

Boston(config-if)#**ip** **access-group** 100 **in**

❖ Kiểm tra cấu hình

Từ PC3 ping PC2

Từ PC3 ping PC1

CHƯƠNG 5: BẢO MẬT MẠNG



- 1. Giới thiệu chung



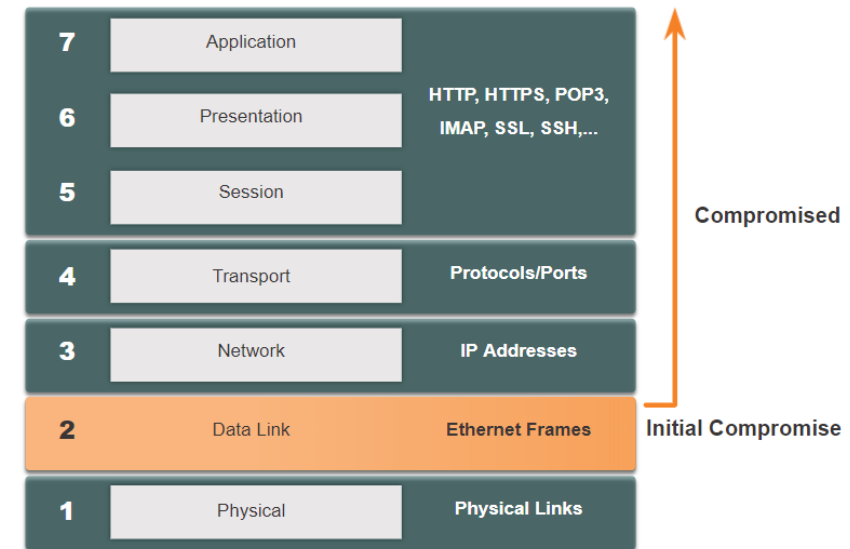
- 2. Danh sách điều khiển truy cập ACL



- 3. Bảo mật Switch

CÁC MỐI ĐE DỌA BẢO MẬT LỚP 2

- ❖ Lỗ hổng lớp 2:
- ❖ Quản trị viên mạng thường xuyên triển khai các giải pháp bảo mật để bảo vệ các thành phần trong Lớp 3 cho đến Lớp 7.
- ❖ Họ sử dụng VPN, tường lửa và thiết bị IPS để bảo vệ các thành phần này. Tuy nhiên, nếu Lớp 2 bị xâm phạm, thì tất cả các lớp bên trên nó cũng bị ảnh hưởng.
- ❖ Ví dụ: nếu một tác nhân đe dọa có quyền truy cập vào mạng nội bộ đã chiếm được các khung Lớp 2, thì tất cả biện pháp bảo mật được triển khai trên các lớp bên trên sẽ trở nên vô dụng. Tác nhân đe dọa có thể gây ra nhiều thiệt hại trên cơ sở hạ tầng mạng LAN lớp 2.



CÁC LOẠI TẤN CÔNG SWITCH

Category	Examples
MAC Table Attacks	Bao gồm các cuộc tấn công tràn ngập địa chỉ MAC.
VLAN Attacks	Bao gồm các cuộc tấn công VLAN hopping và double-tagging. Nó cũng bao gồm các cuộc tấn công giữa các thiết bị trên một VLAN.
DHCP Attacks	Bao gồm các cuộc tấn công DHCP và giả mạo DHCP.
ARP Attacks	Bao gồm các cuộc tấn công giả mạo ARP và đầu độc ARP.
Address Spoofing Attacks	Bao gồm các cuộc tấn công giả mạo địa chỉ MAC và địa chỉ IP.
STP Attacks	Bao gồm các cuộc tấn công điều khiển Giao thức Spanning Tree

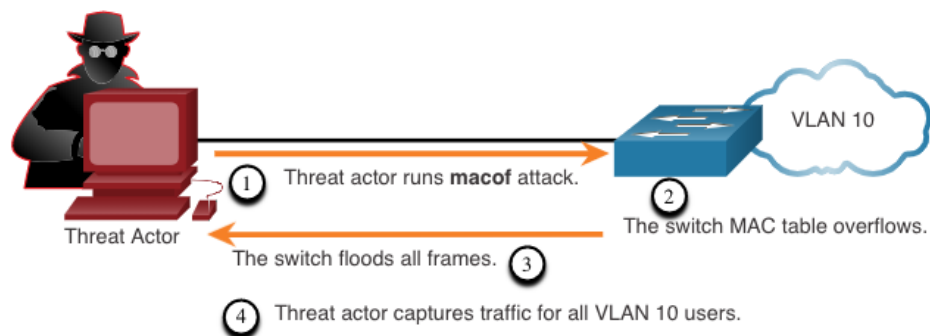
KỸ THUẬT GIẢM THIỂU TẤN CÔNG

Solution	Description
Port Security	Ngăn chặn nhiều kiểu tấn công bao gồm tấn công tràn ngập địa chỉ MAC và tấn công bỏ đói DHCP.
DHCP Snooping	Ngăn chặn các cuộc tấn công giả mạo DHCP
Dynamic ARP Inspection (DAI)	Ngăn chặn các cuộc tấn công giả mạo ARP và đầu độc ARP.
IP Source Guard (IPSG)	Ngăn chặn các cuộc tấn công giả mạo địa chỉ MAC và IP.

- ❖ Các giải pháp Lớp 2 này sẽ không hiệu quả nếu các giao thức quản lý không được bảo mật. Các chiến lược sau đây được khuyến nghị:
- ❖ Luôn sử dụng các giao thức an toàn như: Giao thức quản lý như SSH, Giao thức sao chép an toàn (SCP), FTP an toàn (SFTP) và Bảo mật lớp công bảo mật/lớp vận chuyển (SSL/TLS).
- ❖ Cân nhắc sử dụng mạng quản lý ngoài băng tần để quản lý thiết bị.
- ❖ Sử dụng một VLAN quản lý chuyên dụng, nơi không có gì ngoài lưu lượng quản lý.
- ❖ Sử dụng ACL để lọc truy cập không mong muốn.

MAC ADDRESS TABLE ATTACK

- ❖ Tất cả các bảng MAC đều có kích thước cố định và do đó, một Switch có thể hết tài nguyên để lưu trữ địa chỉ MAC.
- ❖ Các cuộc tấn công tràn ngập địa chỉ MAC lợi dụng hạn chế này bằng cách gửi MAC nguồn giả cho đến khi bảng địa chỉ MAC của switch đầy.
- ❖ Khi điều này xảy ra, Switch coi khung là một unicast không xác định và bắt đầu đồn tất cả lưu lượng truy cập vào ra tất cả các cổng trên cùng một Vlan mà không cần tham khảo bảng MAC.
- ❖ Vậy tác nhân đe dọa nắm bắt tất cả các khung được gửi từ máy chủ này sang máy chủ khác trên mạng LAN cục bộ hoặc VLAN cục bộ.



GIẢM THIỂU TẤN CÔNG BẢNG ĐỊA CHỈ MAC

- ❖ Để giảm thiểu các cuộc tấn công tràn bảng địa chỉ MAC, quản trị viên mạng phải triển khai bảo mật cổng (port security). Port security sẽ chỉ cho phép học một số địa chỉ MAC nguồn cụ thể trên cổng. Bảo mật cổng được thảo luận thêm trong mô-đun khác.
- ❖ Tất cả các cổng (Interface) phải được bảo mật trước khi triển khai sử dụng. Để giúp bảo vệ mạng khỏi sự truy cập trái phép là vô hiệu hóa tất cả các cổng không sử dụng trên một bộ chuyển mạch.
- ❖ Để tắt các cổng ta vào các cổng sau đó dùng lệnh shutdown
Switch(config)# interface range type module/first-number-last-number
Switch(config)# shutdown
- ❖ Nếu một cổng phải được kích hoạt lại sau đó, cổng đó có thể được bật bằng lệnh no shutdown..

GIẢM THIỂU TẤN CÔNG BẢNG ĐỊA CHỈ MAC

- ❖ Phương pháp đơn giản và hiệu quả nhất để ngăn chặn các cuộc tấn công tràn bảng địa chỉ MAC là kích hoạt tính năng bảo mật cổng (**Port security**).
- ❖ Bảo mật cổng giới hạn số lượng địa chỉ MAC hợp lệ được phép trên một cổng. Khi một cổng được cấu hình Port Security nó nhận được một khung, địa chỉ MAC nguồn của khung được so sánh với danh sách các địa chỉ MAC nguồn bảo mật đã được cấu hình thủ công hoặc học động trên cổng.
- ❖ Bằng cách giới hạn số lượng địa chỉ MAC được phép trên một cổng, bảo mật cổng có thể được sử dụng để kiểm soát truy cập trái phép vào mạng.
- ❖ Cấu hình Port Security.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
```

HIỂN THỊ CÀI ĐẶT PORT SECURITY

- ❖ Lệnh hiển thị cài đặt bảo mật cổng (ví dụ FastEthernet 0/1)

Switch(config)#show port-security interface .

- ❖ Lưu ý khi bật bảo mật cổng, thì chế độ violation mode sẽ tắt và cách số lượng địa chỉ MAC tối đa là 1.
- ❖ Nếu một thiết bị được kết nối với cổng, Switch sẽ tự động thêm địa chỉ MAC của thiết bị làm MAC an toàn. Trong ví dụ này, không có thiết bị nào được kết nối với cổng.

```
S1# show port-security interface f0/1
Port Security           : Enabled
Port Status             : Secure-shutdown
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 0
Configured MAC Addresses : 0
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
S1#
```

LIMIT AND LEARN MAC ADDRESSES

- ❖ Sau khi bật bảo mật cổng, bạn có thể định cấu hình các chi tiết cụ thể về bảo mật cổng khác, như minh họa trong ví dụ.

```
S1(config-if)# switchport port-security ?
aging          Port-security aging commands
mac-address    Secure mac address
maximum        Max secure addresses
violation      Security violation mode
<cr>
S1(config-if)# switchport port-security
```

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security maximum ?
<1-8192>       Maximum addresses
S1(config-if)# switchport port-security maximum
```

- ❖ Để đặt số lượng địa chỉ MAC tối đa được phép trên một cổng, ta sử dụng lệnh sau:
Switch (config-if) # switchport port-security maximum *value*
- ❖ Giá trị bảo mật cổng mặc định là 1. Số lượng địa chỉ MAC an toàn tối đa có thể được cấu hình phụ thuộc vào switch và IOS. Trong ví dụ này, giá trị lớn nhất là 8192.

LIMIT AND LEARN MAC ADDRESSES

❖ Switch có thể được cấu hình để học địa chỉ MAC trên một cổng Security theo ba cách:

1. Cấu hình thủ công: Quản trị viên cấu hình thủ công (các) địa chỉ MAC tĩnh bằng cách sử dụng lệnh sau cho từng địa chỉ MAC an toàn trên cổng:

Switch(config-if)# switchport port-security mac-address *mac-address*

2. Đã học động: Khi lệnh `switchport port-security` được nhập, MAC nguồn hiện tại cho thiết bị được kết nối với cổng sẽ tự động được bảo mật nhưng không được thêm vào cấu hình đang chạy. Nếu Switch được khởi động lại, cổng sẽ phải học lại địa chỉ MAC của thiết bị.

3. Học động— Sticky: Quản trị viên có thể cho phép switch tự động học địa chỉ MAC và “dán” chúng vào cấu hình đang chạy bằng cách sử dụng lệnh sau:

Switch(config-if)# switchport port-security mac-address sticky

- ❖ Ví dụ minh họa cấu hình bảo mật cổng hoàn chỉnh cho FastEthernet 0/1.
- ❖ Quản trị viên chỉ định tối đa 4 địa chỉ MAC, định cấu hình thủ công một địa chỉ MAC bảo mật, sau đó định cấu hình cổng để tự động tìm hiểu các địa chỉ MAC bảo mật bổ sung lên đến tối đa 4 địa chỉ MAC bảo mật.
- ❖ Sử dụng hiển thị giao diện cổng bảo mật và lệnh hiển thị địa chỉ cổng bảo mật để xác minh cấu hình.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 4
S1(config-if)# switchport port-security mac-address aaaa.bbbb.1234
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# end
```

```
S1# show port-security interface fa0/1
```

```
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 4
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

```
S1# show port-security address
```

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
----	-----	----	----	-----
1	aaaa.bbbb.1234	SecureConfigured	Fa0/1	-

```
-----
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

```
S1#
```

VERIFY PORT SECURITY

- ❖ Để hiển thị cài đặt bảo mật cổng cho công tắc, hãy sử dụng lệnh `show port-security`.
- ❖ Ví dụ cho biết rằng tất cả 24 giao diện đều được định cấu hình bằng lệnh `switchport port-security` vì mức tối đa cho phép là 1 và chế độ vi phạm bị tắt. Không có thiết bị nào được kết nối, do đó, `CurrentAddr (Count)` bằng 0 cho mỗi giao diện.

```
S1# show port-security
```

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
-------------	--------------------------	------------------------	------------------------------	-----------------

Fa0/1	1	0	0	Shutdown
Fa0/2	1	0	0	Shutdown
Fa0/3	1	0	0	Shutdown

(output omitted)

Fa0/24	1	0	0	Shutdown
--------	---	---	---	----------

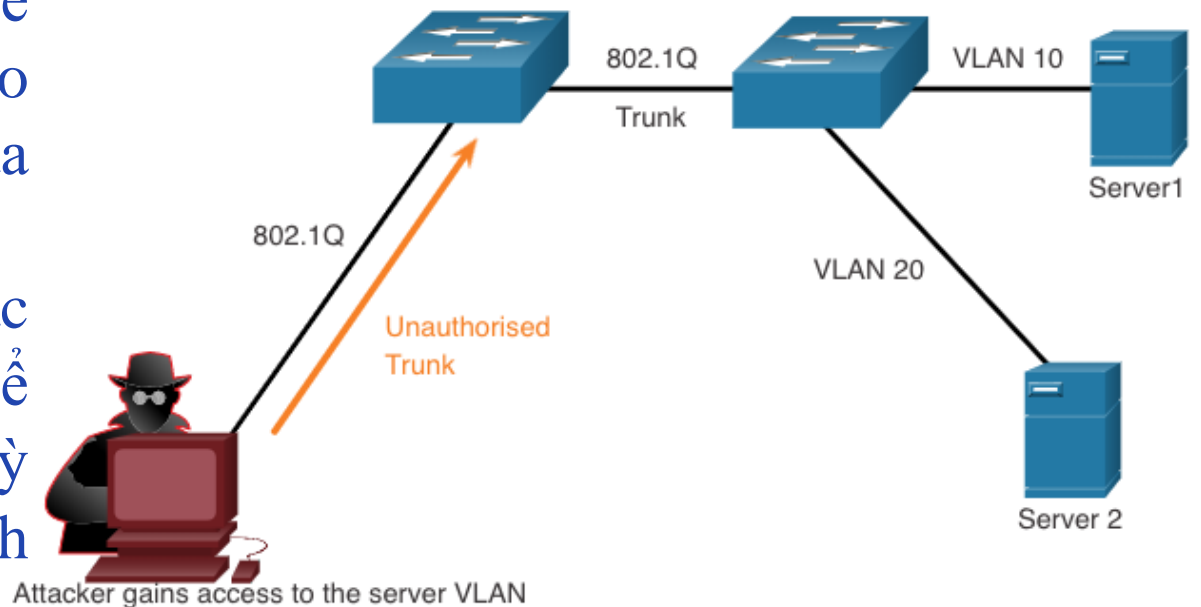
Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 4096

Switch#

VLAN HOPPING ATTACKS

- ❖ Một cuộc tấn công nhảy VLAN cho phép VLAN khác nhìn thấy lưu lượng truy cập từ một VLAN mà không cần sự trợ giúp của bộ định tuyến.
- ❖ Tác nhân đe dọa định cấu hình máy chủ hoạt động giống như một Switch để tận dụng tính năng cổng trung kế tự động được bật theo mặc định trên hầu hết các cổng của bộ chuyển đổi.
- ❖ Tác nhân đe dọa định cấu hình máy chủ để giả mạo tín hiệu 802.1Q và tín hiệu Giao thức Trunking động (DTP) độc quyền của Cisco tới đường trục bằng kết nối Switch.
- ❖ Giờ đây, kẻ đe dọa có thể truy cập tất cả các VLAN trên switch. Tác nhân đe dọa có thể gửi và nhận lưu lượng truy cập trên bất kỳ VLAN nào, nhảy giữa các VLAN một cách hiệu quả.



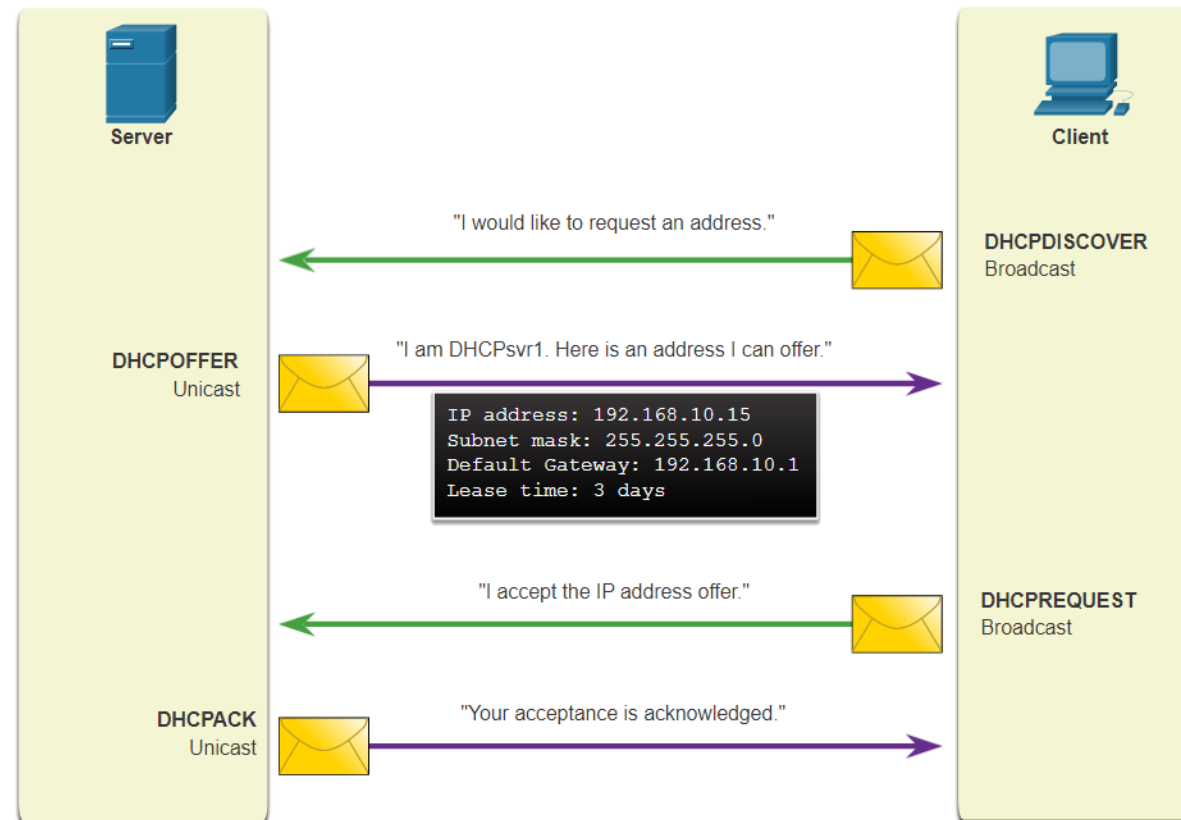
GIẢM THIỂU CÁC CUỘC TẤN CÔNG HOPPING VLAN

Sử dụng các bước sau để giảm thiểu các cuộc tấn công nhảy VLAN:

- ❖ Bước 1: Vô hiệu hóa DTP (**auto trunking**) trên các cổng không phải trung kế bằng cách sử dụng lệnh: **SW(config)#switchport mode access**.
- ❖ Bước 2: Vô hiệu hóa các cổng không sử dụng và đặt chúng vào một VLAN không sử dụng.
- ❖ Bước 3: Bật chế độ Trunk trên cổng trung kế theo cách thủ công bằng cách sử dụng lệnh **SW(config)#switchport mode trunk**.
- ❖ Bước 4: Vô hiệu hóa DTP (**auto trunking**) trên các cổng trung kế bằng cách sử dụng lệnh **SW(config)#switchport nonegotiate**.
- ❖ Bước 5: Đặt Native Vlan thành Vlan khác với Vlan 1 bằng cách sử dụng lệnh
SW(config)#switchport trunk native vlan *vlan_number*

DHCP Messages

- ❖ Máy chủ DHCP cung cấp thông tin cấu hình IP động bao gồm địa chỉ IP, mặt nạ mạng con, cổng mặc định, máy chủ DNS, v.v. cho khách hàng. Xem lại trình tự trao đổi thông báo DHCP giữa máy khách và máy chủ:.



DHCP Attacks

- ❖ Hai kiểu tấn công DHCP là DHCP starvation và DHCP spoofing. Cả hai cuộc tấn công đều được giảm thiểu bằng cách triển khai DHCP snooping.
- ❖ DHCP Starvation Attack – Mục tiêu của cuộc tấn công này là tạo ra một DoS để kết nối các máy khách. Các cuộc tấn công Starvation DHCP yêu cầu một công cụ tấn công như Gobbler.
- ❖ Tấn công giả mạo DHCP – Điều này xảy ra khi một máy chủ DHCP giả mạo được kết nối với mạng và cung cấp các tham số cấu hình IP sai cho các máy khách để tạo ra một cuộc tấn công trung gian. Điều này có thể hoàn toàn không bị phát hiện khi kẻ xâm nhập chặn luồng dữ liệu qua mạng.
- ❖ Máy chủ DNS sai - Máy chủ lừa đảo cung cấp địa chỉ máy chủ DNS không chính xác hướng người dùng đến một trang web bất chính.
- ❖ Địa chỉ IP sai - Máy chủ giả mạo cung cấp địa chỉ IP không hợp lệ, tạo ra một cuộc tấn công DoS trên máy khách DHCP.

MITIGATE DHCP ATTACKS - DHCP SNOOPING

- ❖ DHCP snooping lọc các thông báo DHCP và giới hạn tốc độ lưu lượng DHCP trên các cổng không đáng tin cậy.
- ❖ Các thiết bị dưới sự kiểm soát của quản trị viên (ví dụ: bộ chuyển mạch, bộ định tuyến và máy chủ) là những nguồn đáng tin cậy.
- ❖ Các giao diện đáng tin cậy (ví dụ: liên kết trung kế, cổng máy chủ) phải được cấu hình rõ ràng là đáng tin cậy.
- ❖ Các thiết bị bên ngoài mạng và tất cả các cổng truy cập thường được coi là nguồn không đáng tin cậy.
- ❖ Một bảng DHCP được xây dựng bao gồm địa chỉ MAC nguồn của thiết bị trên một cổng không đáng tin cậy và địa chỉ IP được máy chủ DHCP gán cho thiết bị đó.
- Địa chỉ MAC và địa chỉ IP được liên kết với nhau.
- Do đó, bảng này được gọi là bảng DHCP snooping.

Sử dụng các bước sau để bật DHCP snooping:

❖ Bước 1. Bật DHCP snooping bằng cách sử dụng lệnh:

SW(config)#ip dhcp snooping.

❖ Bước 2. Trên các cổng đáng tin cậy, sử dụng lệnh

SW(config)# ip dhcp snooping trust.

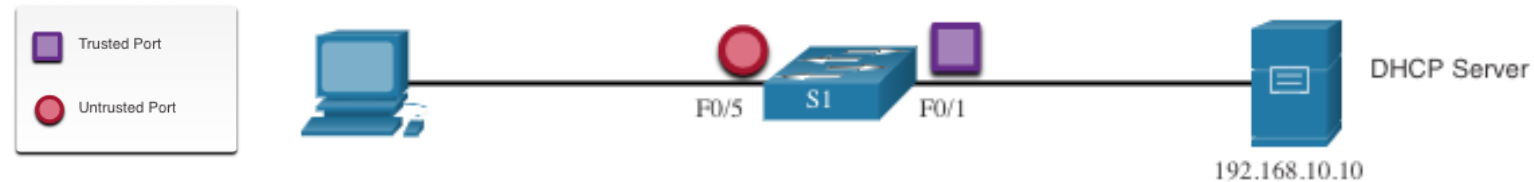
❖ Bước 3: Trên các giao diện không đáng tin cậy, hãy giới hạn số lượng bản tin DHCP discovery có thể nhận được bằng cách sử dụng lệnh:

SW(config)# ip dhcp snooping limit rate *packet-per-second*.

❖ Bước 4. Kích hoạt tính năng DHCP snooping theo VLAN hoặc theo một dải VLAN bằng cách sử dụng **SW(config)# ip dhcp snooping *vlan*.**

DHCP SNOOPING CONFIGURATION EXAMPLE

Tham khảo cấu trúc liên kết mẫu DHCP snooping với các cổng đáng tin cậy và không đáng tin cậy.



- ❖ DHCP snooping đầu tiên được kích hoạt trên S1.
- ❖ Giao diện đường lên tới máy chủ DHCP là tin cậy
- ❖ F0/5 đến F0/24 không đáng tin cậy và do đó, tốc độ giới hạn ở sáu gói mỗi giây.
- ❖ Cuối cùng, DHCP snooping được kích hoạt trên VLANS 5, 10, 50, 51 và 52.

```
S1(config)# ip dhcp snooping
S1(config)# interface f0/1
S1(config-if)# ip dhcp snooping trust
S1(config-if)# exit
S1(config)# interface range f0/5 - 24
S1(config-if-range)# ip dhcp snooping limit rate 6
S1(config-if)# exit
S1(config)# ip dhcp snooping vlan 5,10,50-52
S1(config)# end
S1#
```

DHCP SNOOPING CONFIGURATION EXAMPLE

- ❖ Sử dụng lệnh `show ip dhcp snooping` để xem cài đặt DHCP snooping.
- ❖ Sử dụng lệnh `show ip dhcp snooping binding` để xem các máy khách đã nhận được thông tin DHCP.

```
S1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5,10,50-52
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: 0cd9.96d2.3f80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
Interface                Trusted    Allow option    Rate limit (pps)
-----
FastEthernet0/1          yes       yes             unlimited
  Custom circuit-ids:
FastEthernet0/5          no        no              6
  Custom circuit-ids:
FastEthernet0/6          no        no              6
  Custom circuit-ids:
S1# show ip dhcp snooping binding
MacAddress                IPAddress        Lease(sec)  Type           VLAN  Interface
-----
00:03:47:B5:9F:AD        192.168.10.10   193185     dhcp-snooping  5     FastEthernet0/5
```

ARP ATTACKS

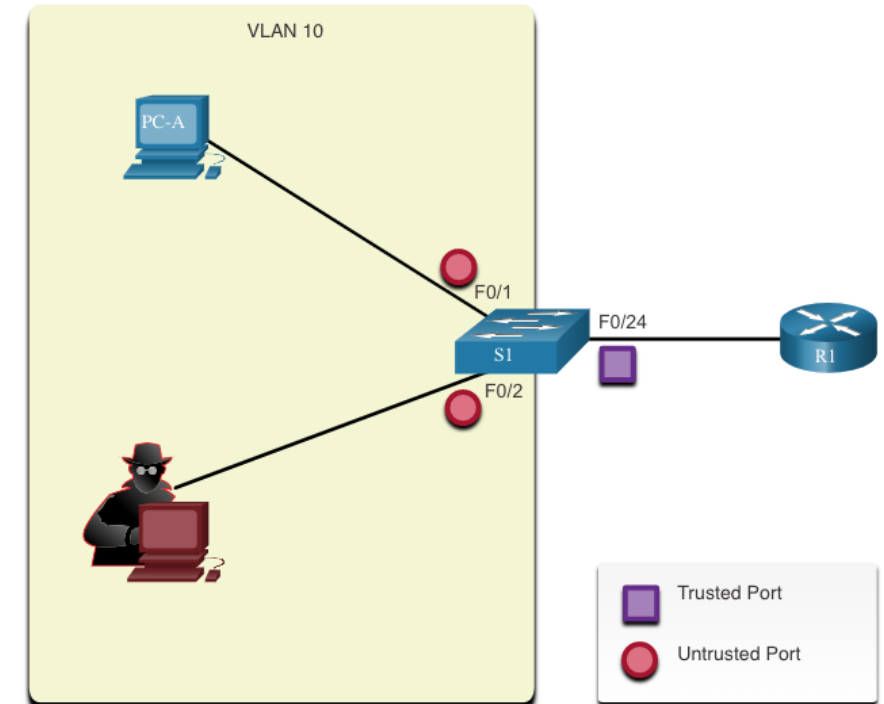
- ❖ Khi một host gửi yêu cầu ARP để xác định địa chỉ MAC của host đích có địa chỉ IP thì tất cả các host trên mạng con nhận và xử lý yêu cầu ARP. Máy host có địa chỉ IP phù hợp trong yêu cầu ARP sẽ gửi trả lời ARP.
- ❖ Một máy client có thể gửi trả lời ARP không được yêu cầu được gọi là “ARP gratuitous”. Các host khác trên mạng con lưu trữ địa chỉ MAC và địa chỉ IP có chứa cả ARP gratuitous trong bảng ARP của chúng.
- ❖ Kẻ tấn công có thể gửi một thông báo ARP gratuitous có chứa địa chỉ MAC giả mạo tới một bộ chuyển mạch và bộ chuyển đổi sẽ cập nhật bảng MAC của nó.
- ❖ Trong một cuộc tấn công điển hình, kẻ đe dọa gửi các phản hồi ARP không mong muốn đến các máy chủ khác trên mạng con với địa chỉ MAC của kẻ đe dọa và địa chỉ IP của cổng mặc định, thiết lập một cuộc tấn công trung gian một cách hiệu quả.

DYNAMIC ARP INSPECTION

- ❖ Trong một cuộc tấn công ARP điển hình, tác nhân đe dọa có thể gửi phản hồi ARP không mong muốn đến các máy chủ khác trên mạng con với Địa chỉ MAC của tác nhân đe dọa và địa chỉ IP gateway.
- ❖ Để ngăn chặn giả mạo ARP và dẫn đến ARP poisoning, một bộ chuyển mạch phải đảm bảo rằng chỉ các Yêu cầu và Trả lời ARP hợp lệ mới được chuyển tiếp.
- ❖ Kiểm tra ARP động (DAI) yêu cầu DHCP snooping và giúp ngăn chặn các cuộc tấn công ARP bằng cách:
- ❖ Không chuyển tiếp ARP không hợp lệ hoặc trả lời ra các cổng khác trong cùng một Vlan.
- ❖ Chặn tất cả các yêu cầu và trả lời ARP trên các cổng không tin cậy.
- ❖ Xác minh từng gói bị chặn để liên kết IP-MAC hợp lệ.
- ❖ Loại bỏ và ghi lại các Phản hồi ARP đến từ IP và MAC không hợp lệ.
- ❖ Lỗi vô hiệu hóa giao diện nếu vượt quá số lượng gói ARP DAI đã định cấu hình.

DAI IMPLEMENTATION GUIDELINES

- ❖ Để giảm thiểu khả năng giả mạo ARP và đầu độc ARP, thực hiện các nguyên tắc triển khai DAI sau:
- ❖ Kích hoạt DHCP snooping.
- ❖ Kích hoạt DHCP snooping trên các Vlan đã chọn.
- ❖ Kích hoạt DAI trên các VLAN đã chọn.
- ❖ Cấu hình giao diện đáng tin cậy để DHCP snooping và ARP inspection.
- ❖ Nói chung nên định cấu hình tất cả các cổng của bộ chuyển mạch truy cập là không đáng tin cậy và cấu hình tất cả các cổng đường lên được kết nối với các bộ chuyển mạch khác là đáng tin cậy.



STP Attack

- ❖ Những kẻ tấn công mạng có thể điều khiển STP(Spanning Tree Protocol) để tiến hành một cuộc tấn công bằng cách giả mạo root bridge và thay đổi cấu trúc liên kết của mạng. Sau đó, những kẻ tấn công có thể bắt tất cả lưu lượng truy cập được chuyển đổi domain ngay lập tức.
- ❖ Để tiến hành một cuộc tấn công điều khiển STP, máy chủ tấn công sẽ phát quản bá các gói tin dữ liệu STP (BPDU - STP bridge protocol data units) chứa các thay đổi về cấu hình và topology điều này sẽ buộc tính toán lại STP. Các BPDU được gửi bởi máy chủ tấn công thông báo mức ưu tiên **bridge priority** thấp hơn để được chọn làm **root bridge**.
- ❖ Cuộc tấn công STP này được giảm thiểu bằng cách triển khai bảo vệ BPDU Guard trên tất cả các cổng truy cập..

CDP Reconnaissance

- ❖ Giao thức CDP (**Cisco Discovery Protocol**) là giao thức khám phá liên kết Lớp 2 độc quyền của Cisco. Nó được bật trên tất cả các thiết bị của Cisco theo mặc định. Quản trị viên mạng cũng sử dụng CDP để giúp định cấu hình và khắc phục sự cố các thiết bị mạng.
- ❖ Thông tin CDP được gửi ra các cổng hỗ trợ CDP theo định kỳ, không được mã hóa, không được xác thực. Thông tin CDP bao gồm địa chỉ IP của thiết bị, phiên bản phần mềm IOS, nền tảng, dung lượng và Native VLAN. Thiết bị nhận tin nhắn CDP sẽ cập nhật cơ sở dữ liệu CDP của nó.
- ❖ Để giảm thiểu việc lợi dụng CDP, hãy hạn chế sử dụng CDP trên các thiết bị hoặc cổng. Ví dụ: tắt CDP trên các cổng cạnh kết nối với các thiết bị không đáng tin cậy.
- ❖ Để tắt CDP chung trên một thiết bị, hãy sử dụng lệnh `R(config)#no cdp run`
- ❖ Để bật CDP, `R(config)#cdp run`.
- ❖ Để tắt CDP trên một cổng, `R(config)# no cdp enable`.
- ❖ Để bật CDP trên một cổng, `R(config)#cdp enable`