

**WAREN**  
WE ARE REAL EXPERTS AND NOVATORS



# CCNA 200 - 301

**Implementing and Administering  
Cisco Solutions**

**LAB GUIDE**

Trung Tâm WAREN  
Đào Tạo Chuyên Gia Quản Trị Mạng & Bảo Mật

## MỤC LỤC

<b>MỤC LỤC .....</b>	<b>1</b>
<b>NETWORK BASIC.....</b>	<b>4</b>
<b>Lab 1 – Đăng nhập vào giao diện dòng lệnh của Router .....</b>	<b>5</b>
<b>Lab 2 – Cấu hình cơ bản trên Router .....</b>	<b>8</b>
<b>Lab 3 – CDP, Telnet .....</b>	<b>13</b>
<b>Lab 4 – Static Route .....</b>	<b>17</b>
<b>Lab 5 – Dự phòng đường đi với Static Route.....</b>	<b>22</b>
<b>Lab 6 – Static Route và Proxy – ARP .....</b>	<b>25</b>
<b>SWITCH.....</b>	<b>30</b>
<b>Lab 7 – Tổng quan hoạt động của Switch .....</b>	<b>31</b>
<b>Lab 8 – VLAN, Trunking, VTP.....</b>	<b>35</b>
<b>Lab 9 – Router on a Stick.....</b>	<b>40</b>
<b>Lab 11 – DHCP .....</b>	<b>47</b>
<b>Lab 12 – STP .....</b>	<b>50</b>
<b>Lab 13 – EtherChannel .....</b>	<b>58</b>
<b>Lab 14 – HSRP .....</b>	<b>62</b>
<b>SECURITY.....</b>	<b>67</b>
<b>Lab 15 – Port Security.....</b>	<b>68</b>
<b>Lab 16 – Local Authentication, SSH.....</b>	<b>72</b>
<b>Lab 17 – Xác thực và phân quyền login .....</b>	<b>78</b>
<b>Lab 18 – Xác thực và phân quyền privilege sử dụng TACACS+.....</b>	<b>84</b>
<b>Lab 19 – DHCP Snooping .....</b>	<b>94</b>
<b>Lab 20 – Storm Control .....</b>	<b>98</b>
<b>Lab 21 – Access Control Lists.....</b>	<b>101</b>
<b>Lab 22 – NAT &amp; PAT .....</b>	<b>106</b>
<b>WIRELESS .....</b>	<b>112</b>
<b>Lab 23 – Cấu hình Wireless AP với Single SSID .....</b>	<b>113</b>
<b>Lab 24 – Cấu hình Wireless AP với Multiple SSID.....</b>	<b>119</b>

<b>ROUTING .....</b>	<b>126</b>
<b>Lab 25 – RIP.....</b>	<b>127</b>
<b>Lab 26 – OSPF .....</b>	<b>132</b>
<b>WAN – SERVICE – IPv6.....</b>	<b>137</b>
<b>Lab 27 – PPPoE .....</b>	<b>138</b>
<b>Lab 28 – Syslog, NTP.....</b>	<b>140</b>
<b>Lab 29 – Định tuyến IPv6 .....</b>	<b>143</b>
<b>LAB TỔNG HỢP.....</b>	<b>151</b>
<b>Lab tổng hợp 1 – Switching – ACL – NAT .....</b>	<b>152</b>
<b>Lab tổng hợp 2 – Routing &amp; Switching .....</b>	<b>160</b>

# NETWORK BASIC

## Lab 1 – Đăng nhập vào giao diện dòng lệnh của Router

Sơ đồ:



Hình 1.1 – Sơ đồ bài Lab

Mô tả:

- Bài Lab gồm 1 Router và một PC được kết nối với nhau bằng cáp console.
- Trong bài Lab này, học viên sẽ thực tập truy nhập vào giao diện dòng lệnh của Router Cisco.

Thực hiện:

**Bước 1:** Kết nối thiết bị

Học viên thực hiện kết nối PC đến thiết bị bằng cáp console như hình 1.1.

**Bước 2:** Cài đặt chương trình giao tiếp với Router

Học viên sử dụng phần mềm PuTTY để truy nhập thiết bị. Phần mềm này có thể được tải miễn phí từ trang web <http://www.putty.org/>

PuTTY không cần cài đặt và có thể chạy trực tiếp từ máy tính. Giao diện của chương trình PuTTY (hình 1.2):

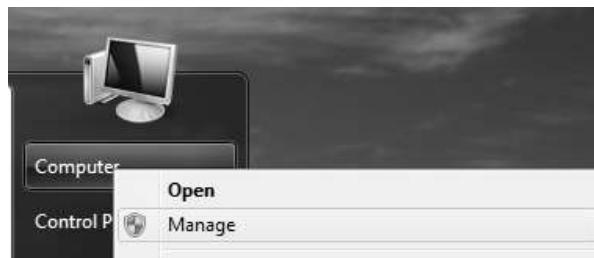


Hình 1.2 – Giao diện chương trình PuTTY

**Bước 3:** Xác định cổng COM được sử dụng trên PC

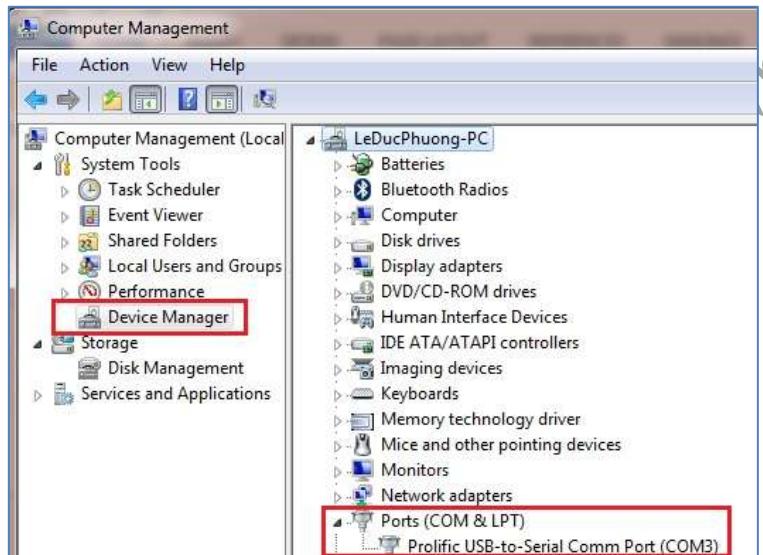
Phần này được hướng dẫn cho Win 7.

Click phải chuột vào phần “Computer” trên menu Start chọn “Manage” (hình 1.3):



Hình 1.3 – Chọn “Manage” của My Computer

Trong cửa sổ “Computer Management”, chọn “Device Manager” ở ô bên trái và click chọn “Ports (COM & LPT)” ở ô bên phải (hình 1.4):



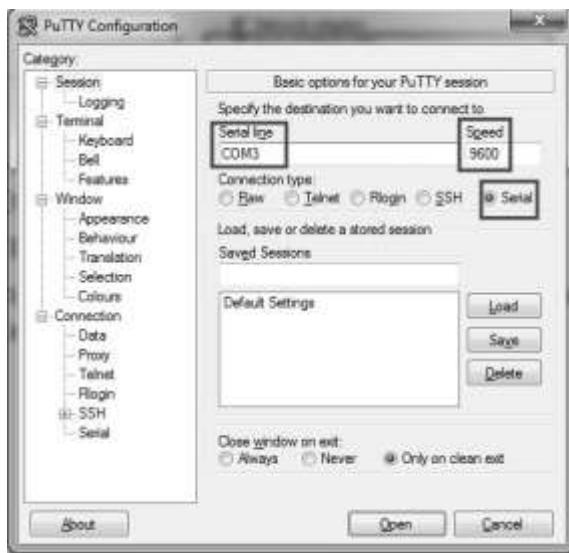
Hình 1.4 – Xác định cổng COM

Tại đây, học viên xác định được cổng COM được sử dụng trên PC của mình. Ví dụ, trong bài Lab này là COM3 (xem hình 1.4).

#### Bước 4: Thiết lập PuTTY

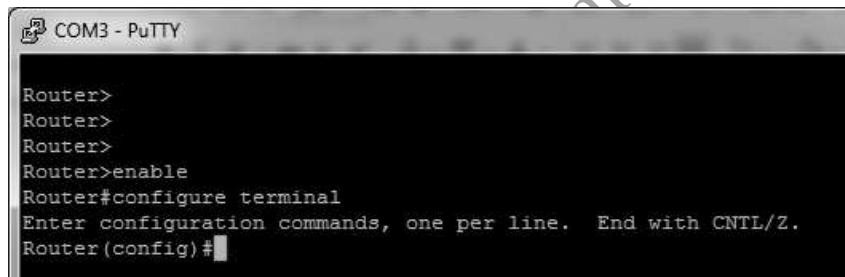
Học viên mở chương trình PuTTY đã chép trên PC và thực hiện chọn mục “Serial” và các thiết lập tương ứng như được chỉ ra trên hình 1.5. Trong đó:

- Mục “Serial line”, ta nhập vào giá trị cổng COM đã xác định ở bước trước, trong bài Lab này là “COM3”.
- Trong mục “Speed”, ta để nguyên giá trị là 9600.



Hình 1.5 – Thiết lập chương trình PuTTY

Sau khi thiết lập xong, thực hiện nhấn “Open”, cửa sổ đăng nhập thiết bị sẽ hiện ra (hình 1.6):

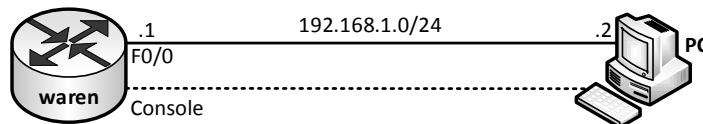


Hình 1.6 – Cửa sổ đăng nhập Router bằng PuTTY

Tại cửa sổ này, học viên có thể bắt đầu thực hiện các thao tác nhập lệnh cấu hình cho Router.

## Lab 2 – Cấu hình cơ bản trên Router

Sơ đồ:



Hình 2.1 – Sơ đồ bài Lab

Mô tả:

- Bài Lab gồm 1 Router và một PC được kết nối bằng cáp mạng Ethernet và console như hình vẽ.
- Trên sơ đồ Lab này, học viên sẽ thực hiện các thao tác cấu hình cơ bản trên Router.

Yêu cầu:

- Kết nối giữa Router và PC như được chỉ ra trên hình 2.1. Thực hiện đăng nhập vào Router.
- Thực hiện di chuyển giữa các mode của giao diện dòng lệnh.
- Xóa cấu hình, khởi động lại Router.
- Đặt hostname cho Router là “waren”.
- Cấu hình enable password cho Router là “waren”.
- Cấu hình console password cho Router là “cisco”.
- Thực hiện mã hóa các password trong file cấu hình.
- Đặt IP trên cổng của Router và cổng của PC như hình 2.1. Ping kiểm tra.
- Lưu cấu hình đã thực hiện.

Thực hiện:

**Bước 1:** Kết nối Router và PC

Học viên thực hiện kết nối giữa PC và Router như được chỉ ra trên hình 2.1.

**Bước 2:** Thực hiện di chuyển giữa các mode của giao diện dòng lệnh

Sau khi khởi động xong thành công, màn hình giao diện sẽ hiển thị dòng thông báo yêu cầu “Enter” để tiếp tục:

```
Router con0 is now available
Press RETURN to get started.
```

Gõ “Enter” để đi vào User mode:

```
Router>
```

Di chuyển từ mode User sang mode Privilege:

```
Router>enable
Router#
```

Di chuyển từ mode Privilege qua mode Config:

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Vào sub – mode cấu hình trên cổng F0/0 của Router:

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#
```

Sử dụng lệnh “exit” và “disable” để đi từ các mode bên trong ra bên ngoài:

```
Router(config-if)#exit
Router(config)#exit
Router#disable
Router>
```

Hoặc có thể đi thẳng từ các sub – mode ra Privilege mode bằng cách nhấn tổ hợp phím “Ctrl - Z” hoặc đánh lệnh “end”:

```
Router(config-if)#end
Router#
```

### Bước 3: Xóa cấu hình, khởi động lại Router

```
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
<- Gõ Enter tại đây.
[OK]
Erase of nvram: complete
Router#
Router#reload

Proceed with reload? [confirm] <- Gõ Enter tại đây.

*Feb 18 02:37:06.563: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

Sau khi quá trình khởi động lại hoàn tất, dòng thông báo dưới đây sẽ hiện ra, ta chọn “no” và gõ Enter:

```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
```

#### Bước 4: Đặt hostname cho Router

```
Router(config)#hostname waren
waren(config) #
```

#### Bước 5: Cấu hình enable password

```
waren(config)#enable password waren
waren(config) #
```

Thực hiện kiểm tra bằng cách quay trở lại mode User rồi đi vào lại mode Privilege:

```
waren(config)#exit
waren#
*Oct 26 03:11:50.343: %SYS-5-CONFIG_I: Configured from console by console
waren#disable
waren>
waren>enable
Password: <-Nhập Password "waren", password sẽ không hiển thị trong quá trình nhập.
waren#
```

#### Bước 6: Cấu hình console password

```
waren#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
waren(config)#line console 0
waren(config-line)#password cisco
waren(config-line)#login
waren(config-line)#exit
waren(config) #
```

Thực hiện kiểm tra bằng cách thoát ra ngoài rồi gõ “Enter” để đi vào User mode:

```
waren#disable
waren>exit

waren con0 is now available
Press RETURN to get started. <-Gõ Enter để di vào User mode.

User Access Verification

Password: <-Nhập Password "cisco", password sẽ không hiển thị trong quá trình nhập.

waren>
```

#### Bước 7: Mã hóa các password trong file cấu hình

Kiểm tra rằng hiện tại các password chưa được mã hóa trong file cấu hình:

```
waren#show running-config
Building configuration...
(...)
enable password waren
...
line con 0
```

```
password cisco
login
line aux 0
line vty 0 4
login
!
scheduler allocate 20000 1000
!
end
```

Thực hiện mã hóa các password:

```
waren(config)#service password-encryption
```

Kiểm tra bằng cách xem lại file cấu hình:

```
waren#show running-config
Building configuration...
(...)
!
enable password 7 104D000A0618
!
(...)
line con 0
password 7 0701355C5D29485744
logging synchronous
login
line aux 0
line vty 0 4
login
!
scheduler allocate 20000 1000
!
end
```

### Bước 8: Đặt IP trên các cổng Router và PC

Trên Router:

```
waren(config)#interface f0/0
waren(config-if)#no shutdown
waren(config-if)#ip address 192.168.1.1 255.255.255.0
waren(config-if)#exit
waren(config) #
```

Trên PC, học viên thực hiện đặt IP trên card mạng LAN có dây của PC là 192.168.1.2/24 kiểm tra trên Router:

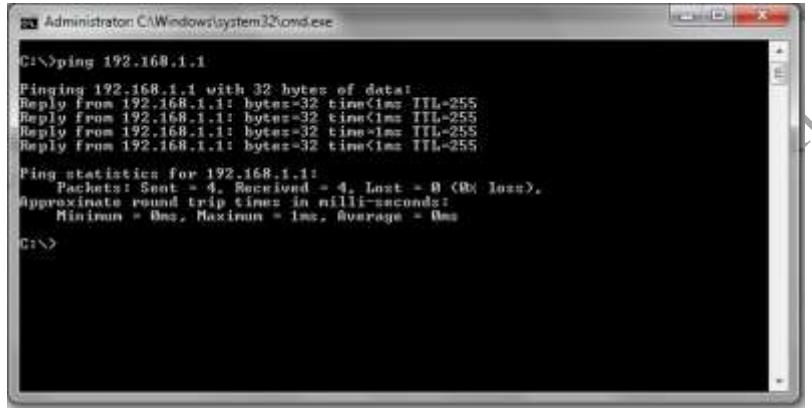
waren#show ip interface brief					
Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.1.1	YES	unset	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down

Ping kiểm tra từ Router xuống PC:

```
waren#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/10ms
waren#
```

Ping kiểm tra từ PC lên Router bằng cách sử dụng chương trình CMD (hình 2.2):



Hình 2.2 – PC ping lên Router

#### Bước 9: Lưu cấu hình

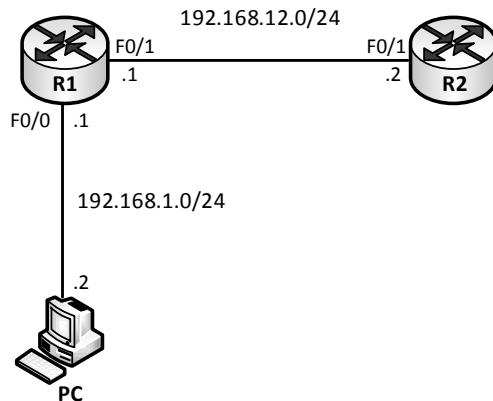
```
waren#copy running-config startup-config
Destination filename [startup-config]? <-Gõ Enter tại đây
Building configuration...
[OK]
waren#
```

Hoặc sử dụng lệnh “write memory” của mode Privilege:

```
waren#write memory
Building configuration...
[OK]
waren#
```

## Lab 3 – CDP, Telnet

Sơ đồ:



Hình 3.1 – Sơ đồ bài Lab

Mô tả:

- Bài Lab gồm 2 Router và 1 PC được đấu nối với nhau như hình 3.1.
- Trên bài Lab này, học viên sẽ thực hiện hiển thị thông tin CDP và thực hiện cấu hình telnet trên các Router.

Yêu cầu:

1. Học viên thực hiện đấu nối dây giữa các Router và PC và thực hiện đặt địa chỉ IP trên các thiết bị như được chỉ ra trên hình 3.1.
2. Thực hiện các lệnh “show cdp...” trên các Router để quan sát thông tin về Router láng giềng.
3. Thực hiện cấu hình telnet trên các Router và kiểm tra kết quả cấu hình bằng cách telnet từ PC đến Router R1 và telnet giữa hai Router đến nhau.

Thực hiện:

**Bước 1:** Đấu nối dây và cấu hình ban đầu

Học viên thực hiện kết nối dây giữa các thiết bị như hình 3.1. Thực hiện cấu hình cơ bản trên các Router và đặt địa chỉ IP như hình vẽ đã chỉ ra.

**Bước 2:** Thao tác với CDP

Từ R1 xem thông tin về thiết bị láng giềng:

```
R1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
```

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
R2	Fas 0/1	164	R S I	2811	Fas 0/1

Các thông tin nhận được:

- Thiết bị láng giềng có hostname là R2 (cột Device ID).
- R1 sử dụng cổng F0/1 để đấu nối đến láng giềng (cột Local Intrfce).
- Láng giềng là một Router 2811 (cột Platform).
- Láng giềng sử dụng cổng F0/1 của nó để đấu nối đến Router đang xét R1 (cổng Port ID).

Có thể xem thông tin chi tiết hơn bằng lệnh “show cdp neighbor detail” hoặc “show cdp entry \*”:

```
R1#show cdp neighbors detail
-----
Device ID: R2
Entry address(es):
IP address: 192.168.12.2
Platform: Cisco 2811, Capabilities: Router Switch IGMP
Interface: FastEthernet0/1, Port ID (outgoing port): FastEthernet0/1
Holdtime: 174 sec

Version:
Cisco IOS Software, 2800 Software (C2800NM-ADVENTERPRISEK9-M), Version 12.4(15)T5, RELEASE
SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Wed 30-Apr-08 14:17 by prod_rel_team

advertisement version: 2
VTP Management Domain: ''
Duplex: full
```

Các lệnh này cho biết thêm các thông tin khác về láng giềng R2 bên cạnh thông tin nhận được từ lệnh “show cdp neighbor” ở trên:

- Địa chỉ IP của láng giềng R2 là: 192.168.12.2.
- Hệ điều hành láng giềng R2 đang sử dụng là “C2800NM-ADVENTERPRISEK9-M, Version 12.4(15)T5”.

Trên R2 có thể thực hiện các lệnh “show cdp...” một cách tương tự.

### Bước 3: Cấu hình Telnet

Cấu hình Telnet trên các Router R1 và R2:

```
R1-2(config)#enable password waren
R1-2(config)#line vty 0 4
R1-2(config-line)#password cisco
R1-2(config-line)#login
R1-2(config-line)#end
```

### PC telnet đến R1:

Thực hiện telnet từ PC vào R1 bằng cách sử dụng lệnh “telnet 192.168.1.1” trên dấu nhắc hệ thống của cửa sổ CMD. Cửa sổ telnet hiện ra, nhập các password để đi vào mode Privilege của Router, tại đây học viên có thể thực hiện các lệnh trên Router giống như với truy nhập qua console (hình 3.2):



Hình 3.2 – PC telnet vào R1

**Chú ý:** Hệ điều hành Window 7 có thể tắt dịch vụ Telnet Client ở mặc định. Nếu không thực hiện Telnet được, hãy bật dịch vụ Telnet client trên Win 7 bằng cách vào Control Panel → Program → Program and Features, chọn “Turn Windows features on or off”. Trong cửa sổ hiện ra, tìm mục “Telnet Client” và check vào ô này.

### Telnet từ Router đến Router:

Từ R2 telnet đến R1:

```
R2#telnet 192.168.12.1
Trying 192.168.12.1 ... Open

User Access Verification

Password:
R1>enable
Password:
R1#
```

Trên R1 thực hiện xem danh sách các host đang telnet đến R1:

```
R1#show users
Line      User      Host(s)          Idle      Location
* 0 con 0    idle        00:00:00
514 vty 0    idle        00:01:59 192.168.12.2
515 vty 1    idle        00:02:31 192.168.1.2

Interface   User      Mode           Idle      Peer Address
```

Hiện có 3 user đang truy nhập vào R1: một user qua cổng console và hai user khác telnet qua các cổng VTY 0 (Router 192.168.12.2) và VTY 1 (PC 192.168.1.2). Có thể ngắt kết nối của các user này bằng lệnh “clear line...”:

```
R1#clear line 514 <- 514 là giá trị định danh cho session telnet từ R2
[confirm] <- Gõ Enter tại đây
[OK]
```

Quan sát trên màn hình console của R2 để thấy rằng R2 đã bị ngắt telnet đến R1:

```
R1>
[Connection to 192.168.12.1 closed by foreign host]
R2#
```

Từ R1 thực hiện telnet đến R2:

```
R1#telnet 192.168.12.2
Trying 192.168.12.2 ... Open

User Access Verification

Password:
R2>enable
Password:
R2#
```

Có thể từ màn hình telnet R2 trở lại màn hình câu lệnh của R1 mà không cần ngắt kết nối telnet bằng cách sử dụng tổ hợp phím “Ctrl + Shift + 6” rồi nhấn phím “X”:

```
R2# <Ctrl + Shift + 6 -> X>
R1#
```

Thực hiện tạo thêm một kết nối telnet nữa từ R1 đến R2:

```
R1#telnet 192.168.12.2
Trying 192.168.12.2 ... Open
User Access Verification
Password:
R2>
```

Trở lại R1 bằng “Ctrl + Shift + 6” → “X” và thực hiện kiểm tra rằng từ R1 hiện có hai kết nối telnet đến R2 bằng lệnh “show session”:

```
R1#show sessions
Conn Host Address Byte Idle Conn Name
  1 192.168.12.2 192.168.12.2 0 2 192.168.12.2
  * 2 192.168.12.2 192.168.12.2 0 2
```

R1 có thể tự ngắt đi một kết nối từ nó đến R2 bằng lệnh “disconnect...”:

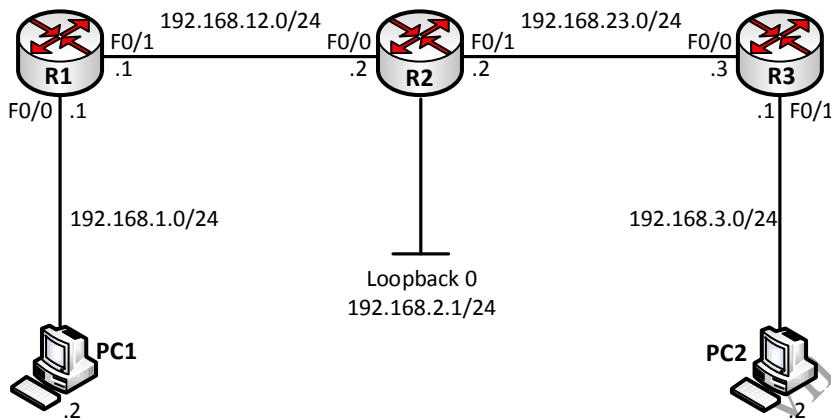
```
R1#disconnect 1
Closing connection to 192.168.12.2 [confirm]
```

Kiểm tra lại rằng R1 chỉ còn một kết nối telnet đến R2:

```
R1#show sessions
Conn Host Address Byte Idle Conn Name
  * 2 192.168.12.2 192.168.12.2 0 1
```

## Lab 4 – Static Route

Sơ đồ:



Hình 4.1 – Sơ đồ bài Lab

Mô tả:

- Sơ đồ Lab gồm 3 Router và 2 PC được đấu nối với nhau như hình 4.1.
- Trên sơ đồ này, học viên sẽ thực tập cấu hình các static route đảm bảo mọi địa chỉ trên sơ đồ thấy được nhau.

Yêu cầu:

1. Học viên thực hiện đấu nối các thiết bị và đặt địa chỉ IP cũng như các hostname của các Router như được chỉ ra trên hình 4.1.
2. Sau khi thiết lập xong sơ đồ, học viên tiến hành cấu hình các static route trên các Router để đảm bảo mọi địa chỉ IP trên sơ đồ có thể đi đến được nhau.
3. Thực hiện các tiện tích ping và traceroute từ PC1 đến PC2 để kiểm tra kết quả cấu hình.

Thực hiện:

**Bước 1:** Kết nối và cấu hình cơ bản

Học viên thực hiện kết nối thiết bị và cấu hình cơ bản trên các thiết bị theo yêu cầu đặt ra.

**Bước 2:** Cấu hình static Route

**Cấu hình**

R1 chưa có route đi đến các subnet 192.168.2.0/24, 192.168.23.0/24 và 192.168.3.0/24. Thực hiện cấu hình các static route đi đến các subnet này trên R1:

```

R1(config)#ip route 192.168.2.0 255.255.255.0 192.168.12.2
R1(config)#ip route 192.168.23.0 255.255.255.0 192.168.12.2

```

```
R1(config)#ip route 192.168.3.0 255.255.255.0 192.168.12.2
```

R2 chưa có route đi đến các subnet 192.168.1.0/24 và 192.168.3.0/24. Thực hiện cấu hình các route đi đến các subnet này trên R2:

```
R2(config)#ip route 192.168.1.0 255.255.255.0 192.168.12.1
R2(config)#ip route 192.168.3.0 255.255.255.0 192.168.23.3
```

R3 chưa có route đi đến các subnet 192.168.1.0/24, 192.168.12.0/24 và 192.168.2.0/24. Thực hiện cấu hình các route đi đến các subnet này trên R2:

```
R3(config)#ip route 192.168.1.0 255.255.255.0 192.168.23.2
R3(config)#ip route 192.168.12.0 255.255.255.0 192.168.23.2
R3(config)#ip route 192.168.2.0 255.255.255.0 192.168.23.2
```

### Kiểm tra:

Bảng định tuyến của các Router:

```
R1#show ip route static
S    192.168.23.0/24 [1/0] via 192.168.12.2
S    192.168.2.0/24 [1/0] via 192.168.12.2
S    192.168.3.0/24 [1/0] via 192.168.12.2

R2#show ip route static
S    192.168.1.0/24 [1/0] via 192.168.12.1
S    192.168.3.0/24 [1/0] via 192.168.23.3

R3#show ip route static
S    192.168.12.0/24 [1/0] via 192.168.23.2
S    192.168.1.0/24 [1/0] via 192.168.23.2
S    192.168.2.0/24 [1/0] via 192.168.23.2
```

Tù mõi Router đã đi đến được tất cả các subnet không kết nối trực tiếp với mình:

```
R1#ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/53/76ms

R1#ping 192.168.23.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/31/48ms

R1#ping 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/55/64ms

R2#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
```

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 8/43/60ms

**R2#ping 192.168.3.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 16/31/60ms

**R3#ping 192.168.1.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 20/56/92ms

**R3#ping 192.168.12.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.12.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/61/88ms

**R3#ping 192.168.2.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/59/80ms

### Bước 3: Ping và Traceroute

Thực hiện ping từ PC1 đến PC2 (hình 4.2):

```
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time=68ms TTL=252
Reply from 192.168.3.2: bytes=32 time=107ms TTL=252
Reply from 192.168.3.2: bytes=32 time=95ms TTL=252
Reply from 192.168.3.2: bytes=32 time=94ms TTL=252

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 68ms, Maximum = 107ms, Average = 91ms

C:\>
```

Hình 4.2 – PC1 ping PC2

Từ PC1 thực hiện Tracert đến PC2:

```
C:\>tracert 192.168.3.2

Tracing route to 192.168.3.2 over a maximum of 30 hops
  1  10 ms   13 ms   13 ms  192.168.1.1
  2  48 ms   30 ms   30 ms  192.168.12.2
  3  48 ms   60 ms   62 ms  192.168.23.3
  4  95 ms   76 ms   92 ms  192.168.3.2

Trace complete.

C:\>
```

Hình 4.3 – PC1 Tracert đến PC2

Từ Router R1 thực hiện Traceroute đến PC2:

```
R1#traceroute 192.168.3.2
```

```
Type escape sequence to abort.  
Tracing the route to 192.168.3.2  
  
 1 192.168.12.2 32 msec 32 msec 32 msec  
 2 192.168.23.3 60 msec 44 msec 64 msec  
 3 192.168.3.2 56 msec 76 msec 88 msec
```

### Cấu hình đầy đủ:

#### R1:

```
!  
interface FastEthernet0/0  
 ip address 192.168.1.1 255.255.255.0  
 duplex auto  
 speed auto  
!  
interface FastEthernet0/1  
 no shutdown  
 ip address 192.168.12.1 255.255.255.0  
 duplex auto  
 speed auto  
!  
ip route 192.168.2.0 255.255.255.0 192.168.12.2  
ip route 192.168.3.0 255.255.255.0 192.168.12.2  
ip route 192.168.23.0 255.255.255.0 192.168.12.2  
!
```

#### R2:

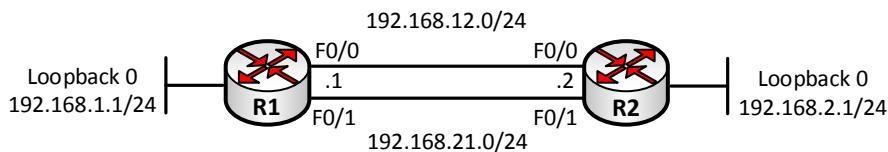
```
!  
interface Loopback0  
 ip address 192.168.2.1 255.255.255.0  
!  
interface FastEthernet0/0  
 ip address 192.168.12.2 255.255.255.0  
 duplex auto  
 speed auto  
!  
interface FastEthernet0/1  
 no shutdown  
 ip address 192.168.23.2 255.255.255.0  
 duplex auto  
 speed auto  
!  
ip route 192.168.1.0 255.255.255.0 192.168.12.1  
ip route 192.168.3.0 255.255.255.0 192.168.23.3  
!
```

**R3:**

```
!
interface FastEthernet0/0
 ip address 192.168.23.3 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no shutdown
 ip address 192.168.3.2 255.255.255.0
 duplex auto
 speed auto
!
ip route 192.168.1.0 255.255.255.0 192.168.23.2
ip route 192.168.2.0 255.255.255.0 192.168.23.2
ip route 192.168.12.0 255.255.255.0 192.168.23.2
!
```

## Lab 5 – Dự phòng đường đi với Static Route

Sơ đồ:



Hình 5.1 – Sơ đồ bài Lab

Mô tả:

- Bài Lab gồm 2 Router được đấu nối với nhau như hình 5.1.
- Trên sơ đồ này, học viên thực hiện cấu hình dự phòng đường đi với kỹ thuật Static Route.

Yêu cầu:

- Học viên thực hiện đấu nối các thiết bị và đặt địa chỉ IP theo sơ đồ được chỉ ra trên hình 5.1.
- Học viên cấu hình dự phòng với static route đảm bảo:
  - R1 đi đến loopback của R2 theo link nối giữa hai cổng F0/0, link nối giữa hai cổng F0/1 chỉ để dự phòng.
  - R2 đi đến loopback của R1 theo link nối giữa hai cổng F0/1, link nối giữa hai cổng F0/0 chỉ để dự phòng.

Thực hiện:

**Bước 1:** Đấu nối thiết bị và đặt IP

Học viên thực hiện đấu nối thiết bị và đặt IP trên các cổng theo như sơ đồ đã chỉ ra.

**Bước 2:** Cấu hình dự phòng đường đi với static route

Cấu hình:

Học viên sử dụng tham số AD trong câu lệnh cấu hình static route trên các Router để thực hiện yêu cầu này.

Trên R1:

```
R1(config)#ip route 192.168.2.0 255.255.255.0 192.168.12.2 5<- Set AD=5
R1(config)#ip route 192.168.2.0 255.255.255.0 192.168.21.2 10<- Set AD=10
```

Trên R2:

```
R2(config)#ip route 192.168.1.0 255.255.255.0 192.168.12.1 10
R2(config)#ip route 192.168.1.0 255.255.255.0 192.168.21.1 5
```

## Kiểm tra:

Bảng định tuyến của R1:

```
R1#show ip route static
S 192.168.2.0/24 [5/0] via 192.168.12.2
```

Hiện tại, R1 đang thực hiện chọn đường đi đến subnet loopback 0 của R2 theo next – hop 192.168.12.2 (đường nối giữa hai cổng F0/0).

Shutdown cổng F0/0 của R1 để giả lập tình huống đứt đường chính:

```
R1(config)#interface f0/0
R1(config-if)#shutdown
R1(config-if)#
*Mar 1 00:06:48.623: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
*Mar 1 00:06:49.623: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
```

Kiểm tra lại bảng định tuyến của R1 để xác nhận rằng lúc này R1 đã tự chuyển sang đi theo đường dự phòng:

```
R1#show ip route static
S 192.168.2.0/24 [10/0] via 192.168.21.2
```

No shutdown cổng F0/0 của R1 để khôi phục lại đường chính:

```
R1(config)#interface f0/0
R1(config-if)#no shutdown
R1(config-if)#
*Mar 1 00:09:50.395: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:09:51.395: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

Kiểm tra bảng định tuyến của R1 để xác nhận rằng R1 đã đi theo đường chính trở lại:

```
R1#show ip route static
S 192.168.2.0/24 [5/0] via 192.168.12.2
```

Thực hiện kiểm tra tương tự cho Router R2 với static route đi đến subnet 192.168.1.0/24 của R1.

## Cấu hình đầy đủ:

### R1:

```
interface Loopback0
ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/0
no shutdown
ip address 192.168.12.1 255.255.255.0
duplex auto
speed auto
!
```

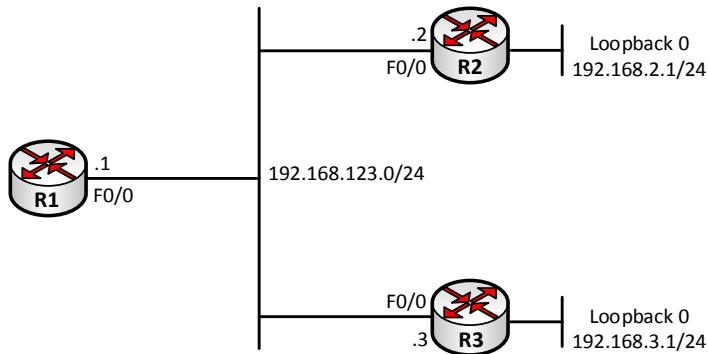
```
interface FastEthernet0/1
no shutdown
ip address 192.168.21.1 255.255.255.0
duplex auto
speed auto
!
ip route 192.168.2.0 255.255.255.0 192.168.12.2 5
ip route 192.168.2.0 255.255.255.0 192.168.21.2 10
```

**R2:**

```
!
interface Loopback0
ip address 192.168.2.1 255.255.255.0
!
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.21.2 255.255.255.0
duplex auto
speed auto
!
ip route 192.168.1.0 255.255.255.0 192.168.21.1 5
ip route 192.168.1.0 255.255.255.0 192.168.12.1 10
!
```

## Lab 6 – Static Route và Proxy – ARP

Sơ đồ:



Hình 6.1 – Sơ đồ bài Lab

Mô tả:

- Bài Lab gồm 3 Router được đấu nối với nhau vào một data link multiaccess như hình 6.1. Học viên có thể sử dụng một layer 2 Switch để xây dựng data link này.
- Trên sơ đồ Lab này, học viên sẽ khảo sát hoạt động tương quan địa chỉ giữa lớp 3 và lớp 2 trong định tuyến tĩnh trên Router.

Yêu Cầu:

- Static route với outgoing interface đảm bảo mọi địa chỉ đi tới nhau.
- Khảo sát hoạt động của Proxy ARP trên R2 và R3.

Thực hiện:

**Bước 1:** Thiết lập ban đầu

Học viên thực hiện kết nối giữa các thiết bị và đặt IP như được chỉ ra trên hình 6.1. Để thiết lập một data link multiaccess đấu nối giữa 3 Router, học viên có thể sử dụng một Switch layer 2.

**Bước 2:** Static route với next – hop IP

Trên R1 thực hiện cấu hình các static route đi đến các subnet trên các loopback 0 của R2 và R3 sử dụng tùy chọn next – hop IP:

```
R1(config)#ip route 192.168.2.0 255.255.255.0 192.168.123.2
R1(config)#ip route 192.168.3.0 255.255.255.0 192.168.123.3
```

Thực hiện ping từ R1 đến các địa chỉ loopback của R2 và R3:

```
R1#ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/35/52ms

R1#ping 192.168.3.1
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/23/32ms
```

Bảng ARP của R1 khi sử dụng tùy chọn next – hop IP trong cấu hình static route:

R1#show ip arp						
Protocol	Address	Age (min)	Hardware Addr	Type	Interface	
Internet	192.168.123.1	-	000c.29e5.bac7	ARPA	FastEthernet0/0	
Internet	192.168.123.2	2	001f.6c6e.90d0	ARPA	FastEthernet0/0	
Internet	192.168.123.3	2	f025.720f.c3c8	ARPA	FastEthernet0/0	

Bảng ARP của R1 chỉ hiển thị kết quả phân giải địa chỉ MAC cho các IP next – hop 192.168.123.2 và 192.168.123.3.

Địa chỉ MAC tương ứng với next – hop 192.168.123.2 được sử dụng để đóng frame đi qua data link multiaccess cho các gói tin IP gửi đến subnet 192.168.2.0/24.

Địa chỉ MAC tương ứng với next – hop 192.168.123.3 được sử dụng để đóng frame đi qua data link multiaccess cho các gói tin IP gửi đến subnet 192.168.3.0/24.

Địa chỉ MAC tương ứng với cột Age bỏ trống chính là địa chỉ MAC interface F0/0 của Router R1.

### Bước 3: Static Route với output interface

Thực hiện cấu hình trên R1 các static route đi đến các subnet loopback của R2 và R3, lần này sử dụng tùy chọn output interface:

```
R1(config)#no ip route 192.168.2.0 255.255.255.0 192.168.123.2
R1(config)#no ip route 192.168.3.0 255.255.255.0 192.168.123.3
R1(config)#ip route 192.168.2.0 255.255.255.0 f0/0
R1(config)#ip route 192.168.3.0 255.255.255.0 f0/0
```

Xóa các entry ARP đã được xây dựng ở bước 2 bằng cách shutdown/no shutdown cổng F0/0:

```
R1(config)#interface f0/0
R1(config-if)#shutdown
R1(config-if)#
*Mar 1 01:07:51.887: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
*Mar 1 01:07:52.887: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
R1(config-if)#no shutdown
R1(config-if)#
*Mar 1 01:07:59.603: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 01:08:00.603: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#exit
```

Thực hiện ping kiểm tra từ R1 đến các loopback của R2 và R3:

```
R1#ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
.!!!!
```

Success rate is 80 percent (4/5), round-trip min/avg/max = 4/26/40ms

R1#ping 192.168.3.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 16/30/40ms

Bảng ARP của R1:

R1#show ip arp

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.2.1	1	001f.6c6e.90d0	ARPA	FastEthernet0/0
Internet	192.168.3.1	1	f025.720f.c3c8	ARPA	FastEthernet0/0
Internet	192.168.123.1	-	000c.29e5.bac7	ARPA	FastEthernet0/0

Kết quả cho thấy, khi không chỉ ra IP next – hop, hoạt động phân giải ARP được tiến hành trực tiếp cho địa chỉ đích của các gói tin IP là 192.168.2.1 và 192.168.3.1. Vì các địa chỉ này không được đặt trên bất kỳ host nào kết nối vào data link multiaccess nên các Router R2 và R3 là những Router có route đi đến các địa chỉ IP đích này phải đứng ra làm đại diện trả lời ARP cho chúng. Hoạt động này được gọi là Proxy – ARP. Kết quả cuối cùng là các địa chỉ IP đích sẽ được phân giải thành các địa chỉ MAC trên các cổng F0/0 của các Router R2 và R3 để từ đó các gói đi đến các IP đích này có thể được đóng frame đi qua data link multiaccess.

Tính năng Proxy ARP được bật lên một cách mặc định trên các cổng Ethernet của Router Cisco.

Thực hiện xóa bảng ARP của R1 bằng cách shutdown/no shutdown cổng F0/0 của R1:

```
R1(config)#interface f0/0
R1(config-if)#shutdown
R1(config-if)#
*Mar  1 01:29:57.791: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
*Mar  1 01:29:58.791: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
R1(config-if)#no shutdown
R1(config-if)#
*Mar  1 01:30:04.503: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 01:30:05.503: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

Lần này, thực hiện tắt proxy – ARP trên các cổng F0/0 của hai Router R2 và R3:

```
R2(config)#interface f0/0
R2(config-if)#no ip proxy-arp
R2(config-if)#exit
R3(config)#interface f0/0
R3(config-if)#no ip proxy-arp
R3(config-if)#exit
```

R1 không còn ping được đến các địa chỉ 192.168.2.1 và 192.168.3.1:

```
R1#ping 192.168.2.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:

....

Success rate is 0 percent (0/5)

```
R1#ping 192.168.3.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:

....

Success rate is 0 percent (0/5)

Bảng ARP của R1:

```
R1#show ip arp
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.123.1	-	000c.29e5.bac7	ARPA	FastEthernet0/0

Kết quả show cho thấy sau khi tắt proxy ARP trên hai Router R2 và R3, không có trả lời ARP cho các địa chỉ IP đích 192.168.2.1 và 192.168.3.1, từ đó hoạt động đóng frame không diễn ra được khiến dữ liệu lớp 3 không thể truyền qua được data link multiaccess dẫn đến ping không thành công.

Thực hiện mở lại proxy – ARP trên R2:

```
R2(config)#interface f0/0
R2(config-if)#ip proxy-arp
R2(config-if)#exit
```

Lúc này R1 có thể ping lại được 192.168.2.1 do phân giải ARP đã diễn ra cho địa chỉ này (nhưng vẫn chưa ping được 192.168.3.1 do phân giải ARP không được thực hiện):

```
R1#ping 192.168.2.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 24/28/32ms

```
R1#ping 192.168.3.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:

....

Success rate is 0 percent (0/5)

Bảng ARP của R1 cho thấy chỉ có địa chỉ 192.168.2.1 được phân giải ARP:

```
R1#show ip arp
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.2.1	3	001f.6c6e.90d0	ARPA	FastEthernet0/0
Internet	192.168.123.1	-	c201.0e3c.0000	ARPA	FastEthernet0/0

Thực hiện bật lại tính năng proxy – ARP trên cổng F0/0 của R3, R1 có thể ping lại được địa chỉ 192.168.3.1 do phân giải ARP đã diễn ra cho địa chỉ này:

```
R3(config)#interface f0/0
R3(config-if)#ip proxy-arp
R3(config-if)#exit

R1#ping 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 20/27/32ms

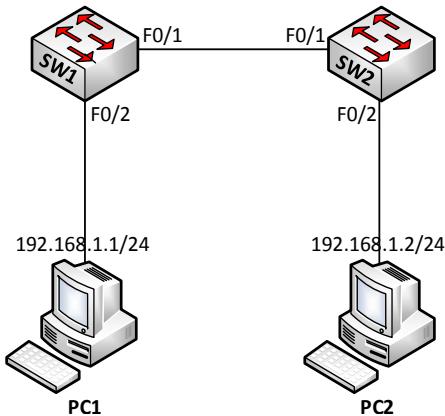
R1#show ip arp
Protocol Address          Age (min)  Hardware Addr      Type    Interface
Internet 192.168.2.1        10        001f.6c6e.90d0  ARPA   FastEthernet0/0
Internet 192.168.3.1         0        f025.720f.c3c8  ARPA   FastEthernet0/0
Internet 192.168.123.1       -        c201.0e3c.0000  ARPA   FastEthernet0/0
```

# SWITCH

www.waren.vn / www.waren.edu.vn

## Lab 7 – Tổng quan hoạt động của Switch

Sơ đồ:



Hình 7.1 – Sơ đồ bài Lab

Mô tả:

- Sơ đồ Lab gồm 2 Switch và 2 PC được đấu nối với nhau như hình 7.1.
- Trên sơ đồ này, học viên sẽ cấu hình và tiến hành khảo sát tìm hiểu quá trình hoạt động của Switch.

Yêu cầu:

1. Học viên thực hiện đấu nối các thiết bị, thực hiện một số cấu hình cơ bản trên Switch như đặt hostname, password console, password enable,... Đặt địa chỉ ip trên 2 PC được chỉ ra trên hình 7.1.
2. Sau khi thiết lập xong sơ đồ, học viên tiến hành ping 2 PC với nhau và kiểm tra quá trình hoạt động của Switch.

Thực hiện:

**Bước 1:** Kết nối và cấu hình cơ bản

Học viên thực hiện kết nối thiết bị và cấu hình cơ bản trên các thiết bị theo yêu cầu đặt ra. Các thao tác cơ bản với Switch trong bước này tương tự như các thao tác đã được thực hành trong bài Lab “Cấu hình cơ bản trên Router”.

**Bước 2:** Khảo sát tổng quan hoạt động của Switch

Quan sát trạng thái của các cổng Switch đang kết nối đến PC và Switch còn lại bằng lệnh “show interfaces status”:

SW1#show interfaces status						
Port	Name	Status	VLAN	Duplex	Speed	Type
Fa0/1		connected	1	a-full	a-100	10/100BaseTX
Fa0/2		connected	1	a-full	a-1000	10/100BaseTX
(...)						

```
SW2#show interfaces status
```

Port	Name	Status	VLAN	Duplex	Speed	Type
Fa0/1		connected	1	a-full	a-100	10/100BaseTX
Fa0/2		connected	1	a-full	a-100	10/100BaseTX
(...)						

Cột “Status” chỉ báo “connected” cho thấy các thiết bị đã đấu nối thành công và chính xác theo sơ đồ 7.1.

Tiếp theo, ta bắt đầu khảo sát tổng quan quá trình hoạt động của Switch bằng cách thực hiện ping PC1 tới PC2. Trước khi ping ta kiểm tra một số thông tin.

Kiểm tra bảng ARP trên PC:

```
C:\Users\PC1>arp -a
No ARP Entries Found.
```

Kiểm tra bảng MAC trên SW1:

```
SW1#show mac address-table
      Mac Address Table
-----
Vlan      Mac Address          Type      Ports
----      -----
(...)

 1        f4ac.c1ec.9a03    DYNAMIC   Fa0/1
Total Mac Addresses for this criterion: 21
```

Trên port F0/1 của Switch học được 1 địa chỉ MAC, đó chính là địa chỉ cổng F0/1 của SW2 thông qua các bản tin trao đổi định kỳ của 2 switch, ví dụ như CDP (Cisco Discovery Protocol),...

Thực hiện kiểm tra địa chỉ MAC trên cổng F0/1 của SW2 để thấy rằng đây đúng là địa chỉ MAC đã được học vào trong bảng MAC của SW1:

```
SW2#show interface f0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is f4ac.c1ec.9a03 (bia f4ac.c1ec.9a03)
(...)
```

Thực hiện ping từ PC1 tới PC2:

```
C:\Users\PC1>ping 192.168.1.2
```

```
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
(...)
```

Kiểm tra bảng ARP trên PC1 để thấy rằng PC1 đã thực hiện phân giải ARP để tìm kiếm được thành công địa chỉ MAC tương ứng với IP 192.168.1.2 (chính là MAC trên card mạng của PC2):

```
C:\Users\PC1>arp -a
Interface: 192.168.1.1 --- 0xd
    Internet Address          Physical Address          Type
192.168.1.200-1c-c0-86-00-eb      dynamic
```

Kiểm tra bảng MAC trên SW1 để thấy rằng MAC của PC1 đã được học vào bảng MAC tương ứng với cổng F0/2 và MAC của PC2 đã được học vào bảng MAC tương ứng với cổng F0/1:

```
SW1#show mac address-table
Mac Address Table
-----
Vlan     Mac Address           Type      Ports
----     -----
 (...) 
 1       001c.c086.00eb        DYNAMIC   Fa0/1<- Địa chỉ MAC của PC1
 1       10bf.4836.c14e        DYNAMIC   Fa0/2<- Địa chỉ MAC của PC2
 1       f4ac.c1ec.9a03        DYNAMIC   Fa0/1
Total Mac Addresses for this criterion: 23
```

Kiểm chứng rằng địa chỉ MAC học được trên cổng F0/2 chính là MAC của PC1:

```
C:\Users\PC1>ipconfig/all

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . . . . . : 
  Description . . . . . : Realtek PCIe GBE Family Controller
  Physical Address. . . . . : 10-BF-48-36-C1-4E
  DHCP Enabled. . . . . : No
  IPv4 Address. . . . . : 192.168.1.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :
```

Kiểm tra bảng MAC trên SW2:

```
SW2#show mac address-table
Mac Address Table
-----
Vlan     Mac Address           Type      Ports
----     -----
 (...) 
 1       001c.c086.00eb        DYNAMIC   Fa0/2<- MAC của PC2
 1       0026.99b7.0603        DYNAMIC   Fa0/1<- MAC của cổng F0/1 của SW1
 1       10bf.4836.c14e        DYNAMIC   Fa0/1<- MAC của PC1
```

Kiểm chứng rằng địa chỉ MAC học được trên cổng F0/2 chính là MAC của PC2:

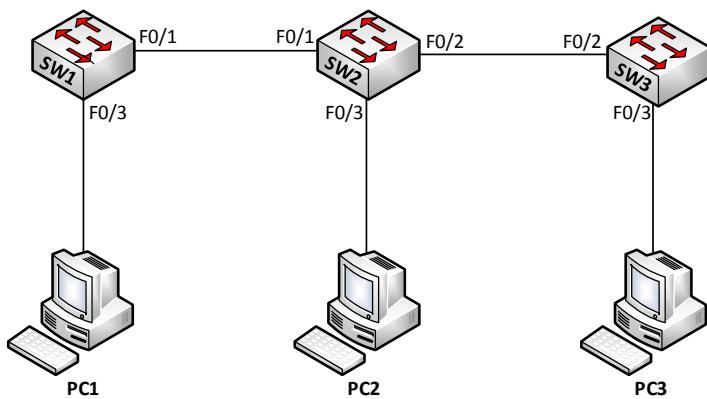
```
C:\Users\PC2>ipconfig/all
Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . :
  Description . . . . . : Intel<R> PRO/100 VE Network Connection
  Physical Address. . . . . : 00-1C-C0-86-00-EB
  DHCP Enabled. . . . . : No
  IPv4 Address. . . . . : 192.168.1.2 (Preferred)
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :
```

www.waren.vn / www.waren.edu.vn

## Lab 8 – VLAN, Trunking, VTP

Sơ đồ:



Hình 8.1 – Sơ đồ bài Lab

Mô tả:

- Sơ đồ Lab gồm 3 Switch và 3 PC được đấu nối với nhau như hình 8.1
- Học viên sẽ cấu hình VLAN, thiết lập các đường Trunk và sử dụng VTP để đồng bộ thông tin VLAN giữa các Switch.
- Quy hoạch IP như sau:
  - VLAN 10: 192.168.10.0/24
  - VLAN 20: 192.168.20.0/24
  - VLAN 30: 192.168.30.0/24

Yêu cầu:

1. Học viên thực hiện đấu nối các thiết bị, thực hiện một số cấu hình cơ bản trên Switch như đặt hostname, password console, password enable,... Đặt địa chỉ IP trên 3 PC được chỉ ra trên hình 8.1.
2. Cấu hình các đường Trunk: thiết lập các đường Trunk đấu nối giữa các Switch.
3. Cấu hình VTP:
  - SW1: server, SW2: transparent, SW3: client.
  - VTP domain: waren.
4. Cấu hình VLAN:
  - Trên SW1 tạo các VLAN 10, VLAN 20, VLAN 30 đặt tên cho các VLAN, kiểm tra thông tin về các VLAN vừa cấu hình.
  - Kiểm tra rằng cấu hình VLAN được tạo trên SW1 đã lan truyền đến SW3.
  - Trên SW2, cấu hình các VLAN 10 và 20.

## 5. Gán port cho các VLAN trên các Switch:

- VLAN 10: F0/3-6
- VLAN 20: F0/7-10
- VLAN 30: F0/11-15

Sau đó, thực hiện ping kiểm tra giữa các PC1, 2, 3 theo 3 trường hợp:

- TH1: PC1, PC2, PC3 cùng thuộc VLAN 10.
- TH2: PC1, PC3 thuộc VLAN 30, PC2 thuộc VLAN 10.
- TH3: Tạo VLAN 30 trên SW2 và thực hiện ping kiểm tra giữa PC1 với PC3.

### Thực hiện:

#### Bước 1: Kết nối và cấu hình cơ bản

Học viên thực hiện kết nối thiết bị và cấu hình cơ bản trên các thiết bị theo yêu cầu đặt ra.

#### Bước 2: Cấu hình trunk

Thiết lập các đường trunk đầu nối giữa các switch:

```
SW1(config)#int f0/1
SW1(config-if)#switchport trunk encapsulation dot1q <- Đối với các Switch hỗ trợ 2
chuẩn dot1q và isl ta phải chỉ rõ sử dụng chuẩn nào
SW1(config-if)#switchport mode trunk
```

Kiểm tra thông tin đường trunk:

```
SW1#show interfaces trunk

Port      Mode          Encapsulation  Status      Native vlan
Fa0/1    on           802.1q        trunking       1

Port      Vlans allowed on trunk
Fa0/1    1-4094

Port      Vlans allowed and active in management domain
Fa0/1    1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    1
```

Thực hiện cấu hình tương tự với các cổng F0/1, F0/2 của SW2 và F0/2 của SW3.

#### Bước 4: Cấu hình VTP

Cấu hình VTP server trên SW1:

```
SW1(config)#vtp mode server
SW1(config)#vtp domain waren
Changing VTP domain name from NULL to waren
```

Kiểm tra kết quả:

```
SW1#show vtp status
VTP Version capable : 1 to 3
VTP version running : 1
VTP Domain Name : waren
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : c062.6b35.2c80
Configuration last modified by 0.0.0.0 at 3-1-93 01:21:47

Feature VLAN:
-----
VTP Operating Mode : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 8
Configuration Revision : 4
```

Cấu hình VTP transparent trên SW2:

```
SW2(config)#vtp mode transparent
SW2(config)#vtp domain waren
```

Kiểm tra kết quả:

```
SW2#sh vtp status
VTP Version capable : 1 to 3
VTP version running : 1
VTP Domain Name : waren
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 0026.99b7.0600
Configuration last modified by 0.0.0.0 at 3-1-93 01:21:47

Feature VLAN:
-----
VTP Operating Mode : Transparent
Maximum VLANs supported locally : 1005
Number of existing VLANs : 8
Configuration Revision : 0
```

Cấu hình VTP client trên SW3:

```
SW3(config)#vtp mode client
SW3(config)#vtp domain waren
```

Kiểm tra kết quả:

```
SW3#sh vtp status
VTP Version : running VTP1 (VTP2 capable)
Configuration Revision : 4
Maximum VLANs supported locally : 1005
Number of existing VLANs : 8
```

VTP Operating Mode	:	Client
VTP Domain Name	:	waren
VTP Pruning Mode	:	Disabled

Kiểm tra thông tin VLAN đồng bộ từ VTP server. Thông số revision hiện tại là 4, lưu ý khi cấu hình không để số revision trên client cao hơn server nếu không sẽ xảy ra tình huống client đồng bộ ngược thông tin VLAN cho server và từ đó lan ra toàn hệ thống.

Kiểm tra thông tin VLAN đồng bộ từ VTP server:

SW3#show vlan

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2
10 Ke Toan	active	
20 IT	active	
30 Marketing	active	

### Bước 5: Cấu hình VLAN cho sơ đồ

Trên SW1, tạo các VLAN 10, 20, 30:

```
SW1(config)#vlan 10
SW1(config-vlan)#name "Ke Toan"
SW1(config)#vlan 20
SW1(config-vlan)#name "IT"
SW1(config)#vlan 30
SW1(config-vlan)#name "Marketing"
```

Kiểm tra cấu hình VLAN vừa tạo trên SW1:

SW1#show VLAN

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
10 Ke Toan	active	
20 IT	active	
30 Marketing	active	
(...)		

Xác nhận rằng cấu hình VLAN này đã được đồng bộ trên SW3:

SW3#show vlan

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2
10 Ke Toan	active	
20 IT	active	
30 Marketing	active	
(...)		

Trên SW2 chỉ tạo các VLAN 10 và 20:

```
SW1(config)#vlan 10
SW1(config-vlan)#exit
SW1(config)#vlan 20
SW1(config-vlan)#exit
```

#### Bước 6: Gán port cho các VLAN

Thực hiện gán port theo yêu cầu:

```
SW1(config)#int range f0/3-6
SW1(config-if-range)#switchport access VLAN 10
SW1(config-if-range)#int range f0/7-10
SW1(config-if-range)#switchport access VLAN 20
SW1(config-if-range)#int range f0/11-15
SW1(config-if-range)#switchport access VLAN 30
```

Kiểm tra kết quả:

SW1#show VLAN brief

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gi0/1, Gi0/2
10 Ke Toan	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6
20 IT	active	Fa0/7, Fa0/8, Fa0/9, Fa0/10
30 Marketing	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15

**Kết quả Ping kiểm tra như sau:**

Trường hợp 1: Các PC ping thành công với nhau.

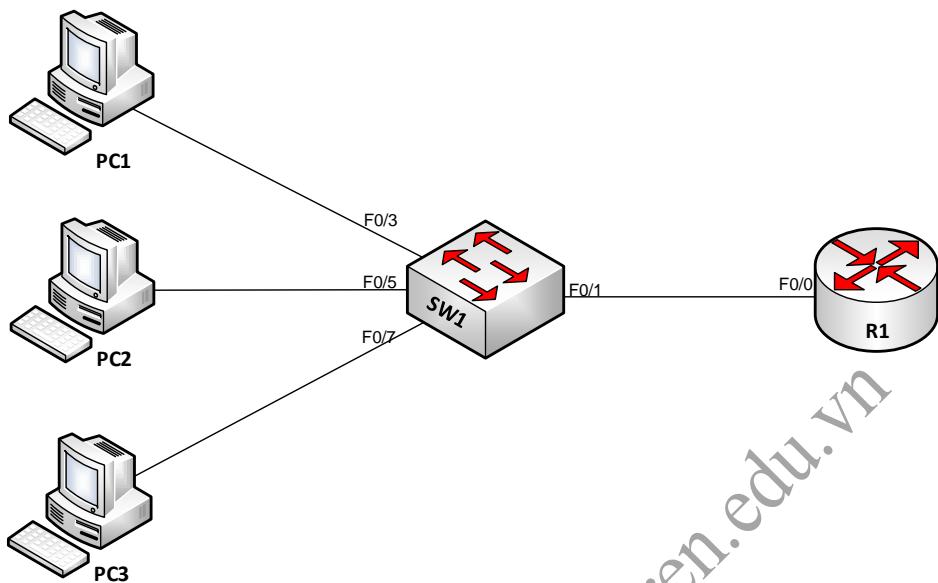
Trường hợp 2: - PC1, PC3 ping không thành công PC2 do khác VLAN.

- PC1 ping không thành công PC3 do thiếu VLAN 30 trên SW2.

Trường hợp 3: - PC1 ping thành công PC3 do VLAN 30 đã được bổ sung trên SW2.

## Lab 9 – Router on a Stick

Sơ đồ:



Hình 9.1 – Sơ đồ bài Lab

Mô tả:

- Sơ đồ Lab gồm 1 Router, 1 Switch và 3 PC được đấu nối với nhau như hình 9.1.
- Qua sơ đồ trên, học viên tiến hành cấu hình định tuyến giữa các VLAN khác nhau.
- Quy hoạch IP trên các cổng mạng của các thiết bị được chỉ ra theo bảng 11.1 dưới đây:

Bảng 1 – Quy hoạch IP cho sơ đồ Lab

STT	Thiết bị	Cổng	IP	Chú thích
1	<b>R1</b>	Fa0/0	192.168.1.1/24	Gateway cho các PC thuộc VLAN 1
		Fa0/0.2	192.168.2.1/24	Gateway cho các PC thuộc VLAN 2
		Fa0/0.3	192.168.3.1/24	Gateway cho các PC thuộc VLAN 3
2	<b>SW1</b>	VLAN 1	192.168.1.251/24	Địa chỉ quản lý cho SW1
3	<b>PC1</b>	NIC	192.168.1.2/24	
4	<b>PC2</b>	NIC	192.168.2.2/24	
5	<b>PC3</b>	NIC	192.168.3.2/24	

Yêu cầu:

1. Học viên thực hiện đấu nối các thiết bị, thực hiện một số cấu hình cơ bản trên Switch và Router như đặt hostname, password console, password enable, telnet...
2. Cấu hình định tuyến cho phép các PC khác VLAN giao tiếp được với nhau.

## Thực hiện:

### Bước 1: Kết nối và cấu hình cơ bản

Học viên thực hiện kết nối thiết bị và cấu hình cơ bản trên các thiết bị theo yêu cầu đặt ra.

### Bước 2: Định tuyến giữa các VLAN

Tạo các sub – interface ứng với các VLAN:

```
Router(config)#int f0/0
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no sh

Router(config)#int f0/0.2
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip add 192.168.2.1 255.255.255.0

Router(config)#int f0/0.3
Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ip add 192.168.3.1 255.255.255.0
```

Đối với VLAN 1, vì là native VLAN, ta sử dụng cổng vật lý F0/0 để giao tiếp giữa Router và các host thuộc VLAN 1.

### Kiểm tra:

Router#show ip interface brief					
Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.1.1	YES	manual	up	up
FastEthernet0/0.2	192.168.2.1	YES	manual	up	up
FastEthernet0/0.3	192.168.3.1	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down

Thiết lập trunking cho cổng F0/1 trên Switch:

```
Switch(config)#int f0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
```

### Kiểm tra:

Switch#show interface trunk					
Port	Mode	Encapsulation	Status	Native vlan	
Fa0/1	on	802.1q	trunking	1	
Port	Vlans allowed on trunk				
Fa0/1	1-4094				
Port	Vlans allowed and active in management domain				
Fa0/1	1-3				
Port	Vlans in spanning tree forwarding state and not pruned				
Fa0/1	none				

### Tạo và gán port cho các VLAN:

```
Switch(config)#vlan 2,3
Switch(config)#int range f0/4-6
Switch(config-if-range)#switchport access VLAN 2
Switch(config)#int range f0/7-9
Switch(config-if-range)#switchport access VLAN 3
```

### Kiểm tra:

```
Switch#show VLAN brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24 Gi0/1, Gi0/2
2 VLAN0002	active	Fa0/4, Fa0/5, Fa0/6
3 VLAN0003	active	Fa0/7, Fa0/8, Fa0/9
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

### Kiểm tra thông tin định tuyến trên Router:

```
Router#show ip route
(...)
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0.2
C    192.168.3.0/24 is directly connected, FastEthernet0/0.3
```

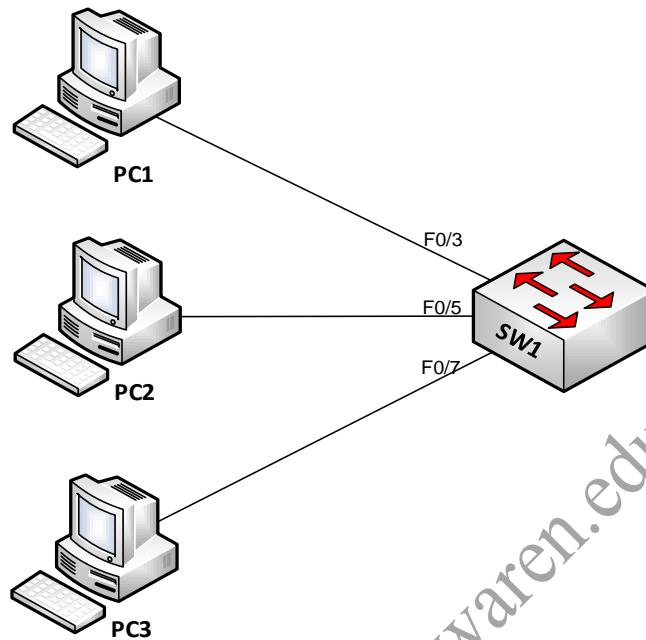
### Tiến hành ping kiểm tra giữa các PC:

```
C:\Users\PC1>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time=1ms TTL=127

C:\Users\PC1>ping 192.168.3.2
Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time<1ms TTL=127
Reply from 192.168.3.2: bytes=32 time<1ms TTL=127
Reply from 192.168.3.2: bytes=32 time<1ms TTL=127
Reply from 192.168.3.2: bytes=32 time=1ms TTL=127
```

## Lab 10 – Sử dụng SVI

Sơ đồ:



Hình 10.1 – Sơ đồ bài Lab

Mô tả:

- Sơ đồ Lab gồm 1 Switch và 3 PC được đấu nối với nhau như hình 10.1.
- Qua sơ đồ trên, học viên tiến hành cấu hình định tuyến giữa các VLAN khác nhau.
- Quy hoạch IP trên các cổng mạng của các thiết bị được chỉ ra theo bảng 10.1 dưới đây:

Bảng 1 – Quy hoạch IP cho sơ đồ Lab

STT	Thiết bị	Cổng	IP	Chú thích
1	<b>SW1</b>	VLAN 1	192.168.1.1/24	Gateway cho các PC thuộc VLAN 1
		VLAN 2	192.168.2.1/24	Gateway cho các PC thuộc VLAN 2
		VLAN 3	192.168.3.1/24	Gateway cho các PC thuộc VLAN 3
2	<b>PC1</b>	NIC	192.168.1.2/24	
3	<b>PC2</b>	NIC	192.168.2.2/24	
4	<b>PC3</b>	NIC	192.168.3.2/24	

**Yêu cầu:**

Cấu hình định tuyến cho phép các PC khác VLAN giao tiếp với nhau sử dụng Switch layer 3.

www.waren.vn / www.waren.edu.vn

## Thực hiện:

Tạo và gán port cho các VLAN:

```
Switch(config)#vlan 2,3
Switch(config)#int range f0/4-6
Switch(config-if-range)#switchport access VLAN 2
Switch(config)#int range f0/7-9
Switch(config-if-range)#switchport access VLAN 3
```

## Kiểm tra:

**Switch#show VLAN brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24 Gi0/1, Gi0/2
2	VLAN0002	active	Fa0/4, Fa0/5, Fa0/6
3	VLAN0003	active	Fa0/7, Fa0/8, Fa0/9
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Bật chức năng định tuyến trên Switch:

```
Switch(config)#ip routing
```

## Cấu hình các SVI:

```
Switch(config)#int VLAN 1
Switch(config-if)#ip add 192.168.1.1 255.255.255.0
Switch(config-if)#no sh
Switch(config)#int VLAN 2
Switch(config-if)#ip add 192.168.2.1 255.255.255.0
Switch(config-if)#no sh
Switch(config)#int VLAN 3
Switch(config-if)#ip add 192.168.3.1 255.255.255.0
Switch(config-if)#no sh
```

## Kiểm tra:

**Switch#show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.1	YES	manual	up	
Vlan2	192.168.2.1	YES	manual	up	
Vlan3	192.168.3.1	YES	manual	up	

## Kiểm tra thông tin định tuyến trên Switch:

```
Switch#show ip route
(...)
  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, Vlan1
L    192.168.1.1/32 is directly connected, Vlan1
  192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.2.0/24 is directly connected, Vlan2
L    192.168.2.1/32 is directly connected, Vlan2
  192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.3.0/24 is directly connected, Vlan3
L    192.168.3.1/32 is directly connected, Vlan3
```

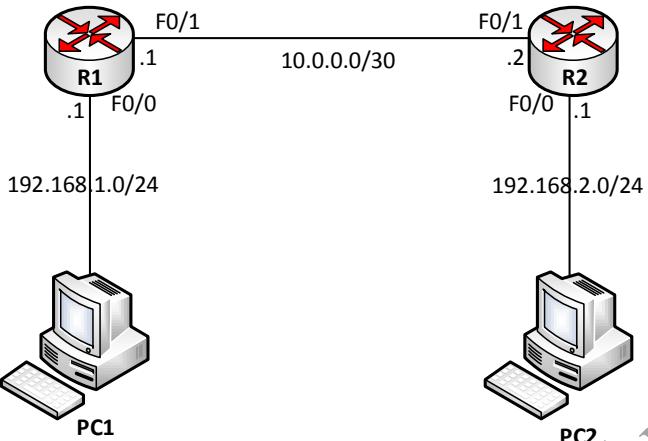
## Tiến hành ping kiểm tra các PC với nhau:

```
C:\Users\PC1>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time=1ms TTL=127

C:\Users\PC1>ping 192.168.3.2
Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time<1ms TTL=127
Reply from 192.168.3.2: bytes=32 time=1ms TTL=127
Reply from 192.168.3.2: bytes=32 time<1ms TTL=127
Reply from 192.168.3.2: bytes=32 time<1ms TTL=127
```

## Lab 11 – DHCP

Sơ đồ:



Hình 11.1 – Sơ đồ bài Lab

Mô tả:

- Sơ đồ Lab gồm 2 Router và 2 PC được đấu nối với nhau như hình 11.1.
- Học viên sẽ cấu hình kiểm tra quá trình hoạt động của giao thức DHCP.

Yêu cầu:

1. Học viên thực hiện đấu nối các thiết bị, thực hiện một số cấu hình cơ bản trên Router như đặt hostname, password console, password enable, telnet...
2. Cấu hình DHCP:
  - Trường hợp 1: R1 và R2 làm DHCP server cấp IP cho PC1, PC2.
  - Trường hợp 2: R1 làm DHCP server cấp IP cho cả hai PC, R2 làm DHCP relay agent.

Thực hiện:

**Bước 1: Kết nối và cấu hình cơ bản**

Học viên thực hiện kết nối thiết bị và cấu hình cơ bản trên các thiết bị theo yêu cầu đặt ra. Các thao tác cơ bản với Router trong bước này tương tự như các thao tác đã được thực hành trong bài Lab “Cấu hình cơ bản trên Router”.

**Bước 2: Cấu hình DHCP**

**Trường hợp 1: R1 và R2 làm DHCP server**

Trên R1:

Tạo ra một DHCP pool cho mạng 192.168.1.0/24, tên của pool là LAN1:

```
R1(config)#ip dhcp pool LAN1
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
R1(dhcp-config)#default-Router 192.168.1.1
```

```
R1 (dhcp-config) #dns-server 8.8.8.8
```

Bạn có thể dùng lệnh “ip dhcp excluded-address” để loại trừ dãy không cấp phát:

```
R1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

Tại PC1 thực hiện “ipconfig /release” và “ipconfig /renew”:

```
C:\Users\PC1>ipconfig /release
Windows IP Configuration
Ethernet adapter LOCAL Area Connection 2:
  Connection-specific DNS Suffix . :
  Default Gateway . . . . . :

C:\Users\PC1>ipconfig /renew
Windows IP Configuration
Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . :
  IPv4 Address. . . . . : 192.168.1.11
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1
```

Sau khi PC1 đã nhận được IP, ta thực hiện lệnh kiểm tra danh sách địa chỉ IP đã cấp phát trên R1 bằng câu lệnh ”show ip dhcp binding”:

```
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address Client-ID/ Lease expiration Type
Hardware address/
User name
192.168.1.11 0050.7966.6800.ff Mar 02 1993 01:07 AM Automatic
```

Thực hiện cấu hình DHCP một cách tương tự trên R2:

```
R2(config)#ip dhcp pool LAN2
R2(dhcp-config)#network 192.168.2.0 255.255.255.0
R2(dhcp-config)#default-Router 192.168.2.1
R2(dhcp-config)#dns-server 8.8.8.8
```

### Trường hợp 2: R1 làm DHCP server, R2 làm DHCP relay agent

Xóa pool LAN2 đã tạo trên R2 ở trường hợp 1:

```
R2(dhcp-config)#no ip dhcp pool LAN2
```

Trên R1 tạo thêm một DHCP pool có tên là LAN2 cho mạng 192.168.2.0/24:

```
R1(config)#ip dhcp pool LAN2
R1(dhcp-config)#network 192.168.2.0 255.255.255.0
R1(dhcp-config)#default-Router 192.168.2.1
R1(dhcp-config)#dns-server 8.8.8.8
R1(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.10
```

Cấu hình R2 thành DHCP Relay Agent, phục vụ cho việc chuyển tiếp các gói tin DHCP từ các client trên cổng F0/0 đến DHCP server R1:

```
R2(config)#int f0/0
R2(config-if)#ip helper-address 10.0.0.1
```

Cấu hình static route để R1 có thể gửi trả các thông tin DHCP về mạng 192.168.2.0/24:

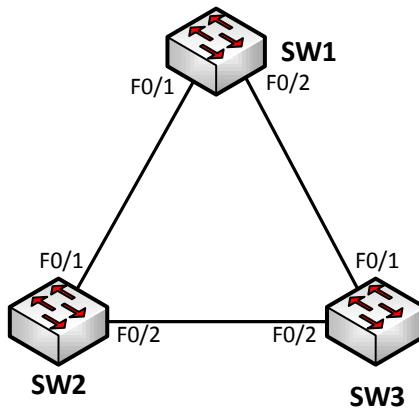
```
R1(config)#ip route 192.168.2.0 255.255.255.0 10.0.0.2
```

Sau khi PC2 đã nhận được IP, thực hiện kiểm tra danh sách những địa chỉ IP mà DHCP server R1 đã cấp phát bằng câu lệnh “show ip dhcp binding”:

```
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/           Lease expiration      Type
                  Hardware address/
                  User name
192.168.1.11        0050.7966.6800.ff    Mar 02 1993 01:07 AM  Automatic
192.168.2.11        0050.7966.6801.ff    Mar 02 1993 01:15 AM  Automatic
```

## Lab 12 – STP

Sơ đồ:



Hình 12.1 – Sơ đồ bài Lab

Mô tả:

- Bài Lab gồm 3 Switch được đấu nối với nhau như hình 12.1.
- Trên sơ đồ Lab này, học viên sẽ ôn tập lại cách thức cấu hình trunking và VTP đã thực hiện ở bài Lab trước và thực tập cấu hình hiệu chỉnh hoạt động của giao thức Spanning – Tree Protocol (STP) trên các switch.

Yêu cầu:

1. Học viên thực hiện đấu nối dây và cấu hình cơ bản trên các Switch như được chỉ ra trên hình 12.1.
2. Thực hiện cấu hình để tất cả các đường link đấu nối giữa các Switch là các đường trunk dot1Q.
3. Cấu hình VLAN và VTP trên các Switch theo yêu cầu sau:
  - Các Switch tham gia VTP domain là “cisco” với VTP password là “waren”.
  - SW1 làm server, các Switch SW2 và SW3 làm client.
  - Trên SW1 cấu hình các VLAN 2 và 3; thực hiện kiểm tra rằng cấu hình VLAN này đã được lan truyền đến các Switch SW2 và SW3.
4. Cấu hình hiệu chỉnh STP đảm bảo SW1 làm root Switch cho VLAN 1, SW2 làm root Switch cho VLAN 2 và SW3 làm root Switch cho VLAN 3.
5. Cấu hình để SW2 làm secondary root Switch cho VLAN 1 và trên VLAN 1, SW3 bị khóa cổng F0/1.

Thực hiện:

Bước 1: Đấu nối dây và cấu hình cơ bản

Học viên thực hiện đấu nối dây và cấu hình cơ bản trên các Switch như được chỉ ra trên sơ đồ Lab tại hình 12.1.

## Bước 2: Cấu hình trunk giữa các Switch

### Cấu hình:

Trên các switch:

```
SW1-2-3(config)#interface f0/1
SW1-2-3(config-if)#switchport trunk encapsulation dot1q
SW1-2-3(config-if)#switchport mode trunk

SW1-2-3(config)#interface f0/2
SW1-2-3(config-if)#switchport trunk encapsulation dot1q
SW1-2-3(config-if)#switchport mode trunk
```

### Kiểm tra:

**SW1#show interfaces trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1
Fa0/2	on	802.1q	trunking	1
(...)				

**SW2#show interfaces trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1
Fa0/2	on	802.1q	trunking	1
(...)				

**SW3#show interfaces trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1
Fa0/2	on	802.1q	trunking	1
(...)				

## Bước 3: Cấu hình VLAN và VTP

### Cấu hình:

SW1:

```
SW1(config)#vtp mode server
SW1(config)#vtp domain cisco
SW1(config)#vtp password waren

SW1(config)#vlan 2
SW1(config-vlan)#exit

SW1(config)#vlan 3
SW1(config-vlan)#exit
```

SW2 và SW3:

```
SW2-3(config)#vtp mode client
SW2-3(config)#vtp domain cisco
SW2-3(config)#vtp password waren
```

**Kiểm tra:**

Kiểm tra trạng thái hoạt động VTP trên các switch:

```
SW1#show vtp status
VTP Version capable : 1 to 3
VTP version running : 1
VTP Domain Name : cisco
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 0023.5ecd.0f00
Configuration last modified by 0.0.0.0 at 3-1-93 00:18:42
Local updater ID is 0.0.0.0 (no valid interface found)
Feature VLAN:
-----
VTP Operating Mode : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 8
Configuration Revision : 3
MD5 digest : 0xF4 0xCA 0xFA 0x4D 0x01 0x69 0x90 0x19
               0x14 0x39 0xD4 0x85 0x15 0x2F 0x4A 0xE1

SW2#show vtp status
VTP Version capable : 1 to 3
VTP version running : 1
VTP Domain Name : cisco
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 0023.5ecc.9d00
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Feature VLAN:
-----
VTP Operating Mode : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs : 5
Configuration Revision : 0
MD5 digest : 0x70 0xEC 0x13 0x07 0xBE 0x07 0x82 0x33
               0xDA 0xA1 0xD9 0x0B 0x29 0xDA 0xF4 0x50

SW3#show vtp status
VTP Version capable : 1 to 3
VTP version running : 1
VTP Domain Name : cisco
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 0023.abfa.0580
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Feature VLAN:

```
VTP Operating Mode : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs : 5
Configuration Revision : 0
MD5 digest : 0x70 0xEC 0x13 0x07 0xBE 0x07 0x82 0x33
               0xDA 0xA1 0xD9 0x0B 0x29 0xDA 0xF4 0x50
```

Kiểm tra rằng cấu hình VLAN trên SW1 đã được lan truyền sang SW2 và SW3:

**SW1#show VLAN brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gi0/1, Gi0/2
2	VLAN0002	active	
3	VLAN0003	active	
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Cấu hình VLAN trên các SW2 và 3:

**SW2-3#show VLAN brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gi0/1, Gi0/2
2	VLAN0002	active	
3	VLAN0003	active	
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

**Bước 3: Cấu hình root switch**

**Cấu hình:**

```
SW1(config)#spanning-tree VLAN 1 root primary
SW2(config)#spanning-tree VLAN 2 root primary
```

```
SW3(config)#spanning-tree VLAN 3 root primary
```

### Kiểm tra:

```
SW1#show spanning-tree VLAN 1
```

VLAN0001

```
Spanning tree enabled protocol ieee
Root ID Priority 24577
Address 0023.5ecd.0f00
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 24577 (priority 24576 sys-id-ext 1)
Address 0023.5ecd.0f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.1	P2p
Fa0/2	Desg	FWD	19	128.2	P2p

```
SW2#show spanning-tree VLAN 2
```

VLAN0002

```
Spanning tree enabled protocol ieee
Root ID Priority 24578
Address 0023.5ecc.9d00
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 24578 (priority 24576 sys-id-ext 2)
Address 0023.5ecc.9d00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.1	P2p
Fa0/2	Desg	FWD	19	128.2	P2p

```
SW3#show spanning-tree VLAN 3
```

VLAN0003

```
Spanning tree enabled protocol ieee
Root ID Priority 24579
Address 0023.abfa.0580
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 24579 (priority 24576 sys-id-ext 3)
```

```
Address      0023.abfa.0580
Hello Time   2 sec   Max Age 20 sec   Forward Delay 15 sec
Aging Time   300 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.1	P2p
Fa0/2	Desg	FWD	19	128.2	P2p

#### Bước 4: Khóa cổng thích hợp

##### Cấu hình:

```
SW2(config)#spanning-tree VLAN 1 root secondary
SW3(config)#interface f0/1
SW3(config-if)#spanning-tree VLAN 1 cost 39
```

##### Kiểm tra:

Trước khi hiệu chỉnh cost, cổng F0/2 bị khóa:

```
SW3#show spanning-tree VLAN 1

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
              Address     0023.5ecd.0f00
              Cost         19
              Port        1 (FastEthernet0/1)
              Hello Time  2 sec   Max Age 20 sec   Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0023.abfa.0580
              Hello Time  2 sec   Max Age 20 sec   Forward Delay 15 sec
              Aging Time  300 sec

  Interface   Role Sts Cost      Prio.Nbr Type
  ----- -----
  Fa0/1       Root FWD 19        128.1    P2p
  Fa0/2       Altn BLK 19        128.2    P2p
```

Sau khi hiệu chỉnh cost, cổng F0/1 bị khóa:

```
SW3#show spanning-tree VLAN 1

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
              Address     0023.5ecd.0f00
              Cost         38
              Port        2 (FastEthernet0/2)
              Hello Time  2 sec   Max Age 20 sec   Forward Delay 15 sec
```

```
Bridge ID Priority    32769 (priority 32768 sys-id-ext 1)
Address          0023.abfa.0580
Hello Time       2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time      300 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Altn	BLK	39	128.1	P2p
Fa0/2	Root	FWD	19	128.2	P2p

### Cấu hình đầy đủ:

#### SW1:

```
!
interface f0/1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface f0/2
switchport trunk encapsulation dot1q
switchport mode trunk
!
vtp domain cisco
vtp password waren
!
vlan 2
exit
!
vlan 3
exit
!
spanning-tree VLAN 1 root primary
```

#### SW2:

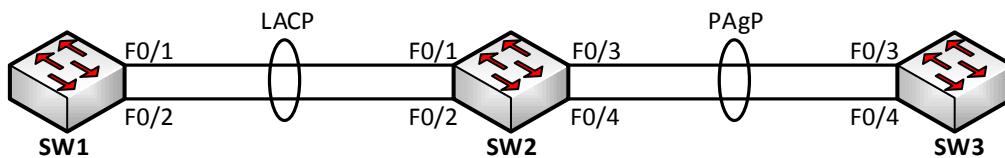
```
!
interface f0/1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface f0/2
switchport trunk encapsulation dot1q
switchport mode trunk
!
vtp domain cisco
vtp password waren
vtp mode client
!
spanning-tree VLAN 1 root secondary
spanning-tree VLAN 2 root primary
```

**SW3:**

```
!
interface f0/1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface f0/2
switchport trunk encapsulation dot1q
switchport mode trunk
!
vtp domain cisco
vtp password waren
vtp mode client
!
spanning-tree VLAN 3 root primary
!
interface f0/1
spanning-tree VLAN 1 cost 39
```

## Lab 13 – EtherChannel

Sơ đồ:



Hình 13.1 – Sơ đồ bài Lab

Mô tả:

- Sơ đồ Lab gồm 3 Switch đấu nối với nhau như hình 13.1.
- Trên sơ đồ này, học viên sẽ thực tập cấu hình các đường EtherChannel kết nối giữa 3 Switch.

Yêu cầu:

1. Học viên thực hiện đấu nối các thiết bị và đặt hostname của các Switch như được chỉ ra trên hình 13.1.
2. Sau khi thiết lập xong sơ đồ, học viên tiến hành cấu hình thiết lập EtherChannel giữa SW1 & SW2 sử dụng giao thức LACP và thiết lập EtherChannel giữa SW2 & SW3 sử dụng giao thức PAgP.

Thực hiện:

**Bước 1:** Kết nối và cấu hình cơ bản

Học viên thực hiện kết nối thiết bị và cấu hình cơ bản trên các thiết bị theo yêu cầu đặt ra.

**Bước 2:** Cấu hình EtherChannel giữa SW1 và SW2

**Cấu hình:**

```
SW1(config)#int range f0/1 - 2
SW1(config-if-range)# channel-protocol lacp
SW1(config-if-range)# channel-group 1 mode active

SW2(config)#int range f0/1 - 2
SW2(config-if-range)# channel-protocol lacp
SW2(config-if-range)# channel-group 1 mode passive
```

LACP có 2 mode: Active và Passive. Port ở trạng thái Active được cấu hình ở mode active sẽ gửi gói tin thiết lập EtherChannel tới đầu xa, Port ở trạng thái Passive sẽ bị động lắng nghe các gói tin thiết lập EtherChannel được gửi đến từ phía đầu Active.

**Kiểm tra:**

Để kiểm tra kết nối EtherChannel, ta thực hiện câu lệnh “show etherchannel summary”:

```
SW1#show etherchannel summary
```

```
Flags: D - down          P - in port-channel
      I - stand-alone  S - suspended
      H - Hot-standby (LACP only)
      R - Layer3         S - Layer2
      U - in use          f - failed to allocate aggregator
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port
```

Number of channel-groups in use: 1

Number of aggregators: 1

Group	Port-channel	Protocol	Ports
-------	--------------	----------	-------

1	Po1 (SU)	LACP	Fa0/1 (P) Fa0/2 (P)
---	----------	------	---------------------

#### SW2#show etherchannel summary

```
Flags: D - down          P - in port-channel
      I - stand-alone  S - suspended
      H - Hot-standby (LACP only)
      R - Layer3         S - Layer2
      U - in use          f - failed to allocate aggregator
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port
```

Number of channel-groups in use: 1

Number of aggregators: 1

Group	Port-channel	Protocol	Ports
-------	--------------	----------	-------

1	Po1 (SU)	LACP	Fa0/1 (P) Fa0/2 (P)
---	----------	------	---------------------

### Bước 3: Cấu hình Etherchannel giữa SW2 và SW3

#### Cấu hình:

```
SW2(config)#int range f0/3 - 4
SW2(config-if-range)# channel-protocol pagp
SW2(config-if-range)# channel-group 2 mode desirable

SW3(config)#int range f0/3 - 4
SW3(config-if-range)# channel-protocol pagp
SW3(config-if-range)# channel-group 2 mode auto
```

PAgP có 2 mode: Desirable và Auto. Port ở trạng thái Desirable được cấu hình ở mode Desirable sẽ gửi gói tin thiết lập EtherChannel tới đầu xa, Port ở trạng thái Auto sẽ bị động lắng nghe các gói tin thiết lập EtherChannel được gửi đến từ phía đầu Desirable.

#### Kiểm tra:

Sử dụng câu lệnh “show etherchannel summary” để thực hiện kiểm tra:

```
SW2#show etherchannel summary
```

```
Flags: D - down          P - in port-channel
      I - stand-alone  S - suspended
      H - Hot-standby (LACP only)
      R - Layer3         S - Layer2
      U - in use          f - failed to allocate aggregator
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port
```

Number of channel-groups in use: 1

Number of aggregators: 1

Group	Port-channel	Protocol	Ports
-------	--------------	----------	-------

2	Po2 (SU)	PAgP	Fa0/3 (P) Fa0/4 (P)
---	----------	------	---------------------

#### SW3#show etherchannel summary

```
Flags: D - down          P - in port-channel
      I - stand-alone  S - suspended
      H - Hot-standby (LACP only)
      R - Layer3         S - Layer2
      U - in use          f - failed to allocate aggregator
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port
```

Number of channel-groups in use: 1

Number of aggregators: 1

Group	Port-channel	Protocol	Ports
-------	--------------	----------	-------

2	Po2 (SU)	PAgP	Fa0/3 (P) Fa0/4 (P)
---	----------	------	---------------------

### Cấu hình đầy đủ:

#### SW1:

```
!
interface FastEthernet0/1
  channel-protocol lacp
  channel-group 1 mode active
exit
!
interface FastEthernet0/2
  channel-protocol lacp
  channel-group 1 mode active
exit
```

#### SW2:

```
interface FastEthernet0/1
  channel-protocol lacp
  channel-group 1 mode passive
exit
!
interface FastEthernet0/2
```

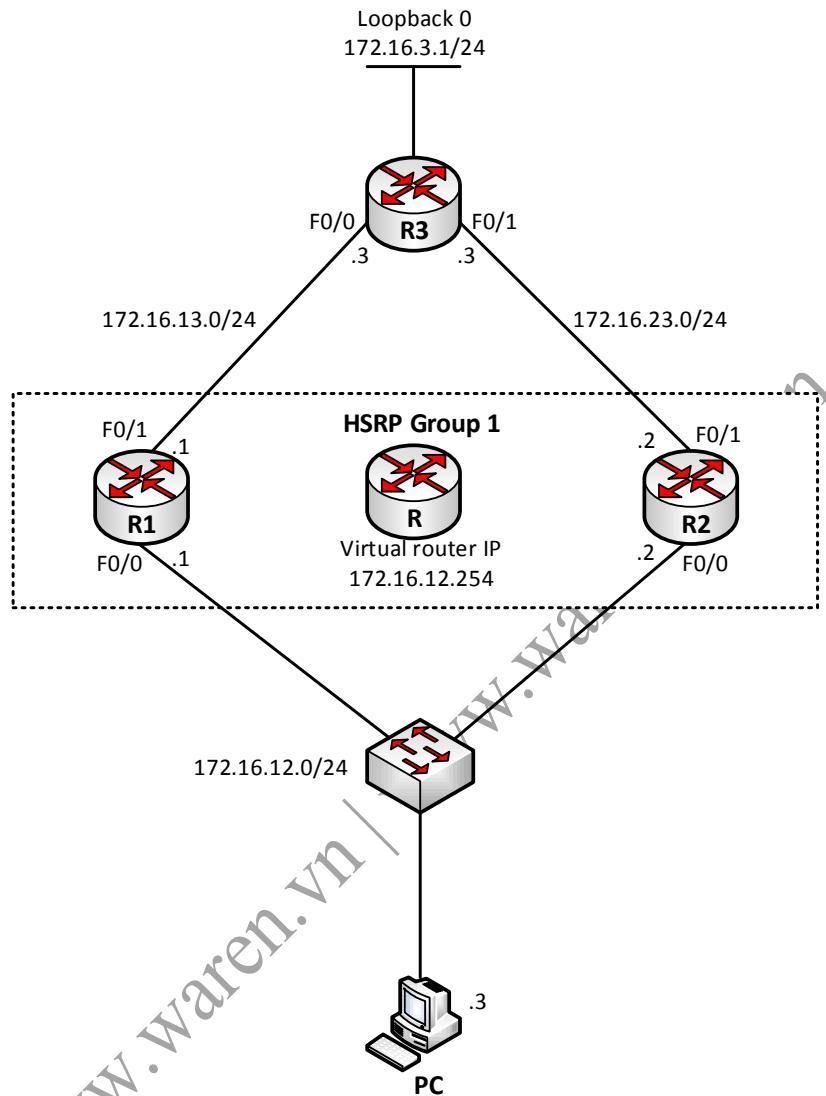
```
channel-protocol lacp
channel-group 1 mode passive
exit
!
interface FastEthernet0/3
channel-protocol pagp
channel-group 2 mode desirable
exit
!
interface FastEthernet0/4
channel-protocol pagp
channel-group 2 mode desirable
exit
!
```

**SW3:**

```
!
interface FastEthernet0/3
channel-protocol pagp
channel-group 2 mode auto
exit
!
interface FastEthernet0/4
channel-protocol pagp
channel-group 2 mode auto
exit
!
```

## Lab 14 – HSRP

Sơ đồ:



Hình 14.1 – Sơ đồ bài Lab

Mô tả:

- Bài Lab gồm các Router, Switch và PC được đấu nối với nhau như hình 14.1.
- Trên sơ đồ này, các Router R1 và R2 đóng vai trò là các gateway cho mạng LAN 172.16.12.0/24. Hai Router này cùng tham gia một nhóm HSRP để cung cấp cơ chế dự phòng gateway cho các host thuộc LAN này.
- Học viên sẽ thực hiện cấu hình HSRP trên các Router R1 và R2 để đáp ứng yêu cầu được nêu ra ở trên.

## Yêu cầu:

1. Học viên thực hiện đấu nối dây và đặt IP trên các thiết bị như hình vẽ.
2. Thực hiện cấu hình định tuyến tĩnh trên các Router đảm bảo mọi subnet trên sơ đồ thấy nhau. Bên cạnh đó, thực hiện cấu hình để R3 đi về subnet 172.16.12.0/24 theo đường chính là hướng R1 và đường theo hướng R2 chỉ dùng để dự phòng.
3. Cấu hình HSRP trên hai Router R1 và R2 để hai Router này cùng tham gia HSRP nhóm 1 thực hiện dự phòng gateway cho các host thuộc LAN 172.16.12.0/24. R1 đảm nhận vai trò Active và R2 đảm nhận vai trò Standby.

## Thực hiện:

### Bước 1: Đấu nối thiết bị và cấu hình cơ bản

Học viên thực hiện đấu nối dây các thiết bị và thực hiện cấu hình cơ bản trên các thiết bị theo yêu cầu được chỉ ra trên hình 14.1.

### Bước 2: Cấu hình định tuyến tĩnh

#### Cấu hình:

Cấu hình để từ R1 và R2 đi đến được subnet 172.16.3.0/24 của R3:

```
R1(config)#ip route 172.16.3.0 255.255.255.0 172.16.13.3
R2(config)#ip route 172.16.3.0 255.255.255.0 172.16.23.3
```

Cấu hình để R3 đi về mạng 172.16.12.0/24 theo đường chính qua hướng R1 và đường qua hướng R2 chỉ để dự phòng:

```
R3(config)#ip route 172.16.12.0 255.255.255.0 172.16.13.1 5
R3(config)#ip route 172.16.12.0 255.255.255.0 172.16.23.2 10
```

#### Kiểm tra:

Bảng định tuyến của R1 và R2 đã có route đi đến subnet 172.16.3.0/24 của R3:

```
R1#show ip route static
    172.16.0.0/24 is subnetted, 3 subnets
S        172.16.3.0 [1/0] via 172.16.13.3

R2#show ip route static
    172.16.0.0/24 is subnetted, 3 subnets
S        172.16.3.0 [1/0] via 172.16.23.3
```

R3 sử dụng đường đi qua R1 để đi đến subnet 172.16.12.0/24:

```
R3#show ip route static
    172.16.0.0/24 is subnetted, 4 subnets
S        172.16.12.0 [5/0] via 172.16.13.1
```

R1 và R2 đã đi đến được subnet 172.16.3.0/24:

```
R1#ping 172.16.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/14/24ms
R2#ping 172.16.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/15/24ms
```

### Bước 3: Cấu hình HSRP

#### Cấu hình:

R1:

```
R1(config)#interface f0/0
R1(config-if)#standby 1 ip 172.16.12.254
R1(config-if)#standby 1 priority 150
R1(config-if)#standby 1 preempt
```

R2:

```
R2(config)#interface f0/0
R2(config-if)#standby 1 ip 172.16.12.254
R2(config-if)#standby 1 preempt
```

#### Kiểm tra:

Trạng thái HSRP của hai Router R1 và R2:

```
R1#show standby brief
          P indicates configured to preempt.
          |
Interface  Grp  Pri  P State   Active      Standby           Virtual IP
Fa0/0       1    150  P Active  local      172.16.12.2    172.16.12.254

R2#show standby brief
          P indicates configured to preempt.
          |
Interface  Grp  Pri  P State   Active      Standby           Virtual IP
Fa0/0       1    100  P Standby  172.16.12.1  local      172.16.12.254
```

Kết quả show cho thấy R1 với priority cao hơn đã được bầu chọn làm Active và R2 đóng vai trò Standby. Hai Router thống nhất tạo ra Router ảo làm default – gateway cho mạng LAN với IP là 172.16.12.254.

PC thực hiện trỏ default – gateway về IP của Router ảo (hình 14.2):

IPv4 Address	172.16.12.3
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	172.16.12.254

Hình 14.2 – Cấu hình IP và default - gateway trên PC

Với gateway này, PC có thể đi ra được một địa chỉ ở bên ngoài mạng LAN:

```
c:\>ping 172.16.3.1

Pinging 172.16.3.1 with 32 bytes of data:
Reply from 172.16.3.1: bytes=32 time=35ms TTL=254
Reply from 172.16.3.1: bytes=32 time=31ms TTL=254
Reply from 172.16.3.1: bytes=32 time=31ms TTL=254
Reply from 172.16.3.1: bytes=32 time=21ms TTL=254

Ping statistics for 172.16.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 35ms, Average = 29ms
```

Kết quả phân giải ARP trên PC xuất hiện cặp IP – MAC của Router ảo

```
c:\>arp -a

Interface: 172.16.12.3 --- 0x19
      Internet Address          Physical Address      Type
172.16.12.254          00-00-0c-07-ac-01  dynamic
  172.16.12.255          ff-ff-ff-ff-ff-ff  static
  224.0.0.2              01-00-5e-00-00-02  static
  224.0.0.22             01-00-5e-00-00-16  static
  224.0.0.252            01-00-5e-00-00-fc  static
  239.255.255.250         01-00-5e-7f-ff-fa  static
  255.255.255.255         ff-ff-ff-ff-ff-ff  static
```

Thực hiện shutdown hai cổng F0/0 và F0/1 của R1 để giả lập tình huống R1 down:

```
R1(config)#interface f0/0
R1(config-if)#shutdown
R1(config)#interface f0/1
R1(config-if)#shutdown
```

Lúc này, R2 chuyển sang trạng thái Active và trở thành Router chuyển dữ liệu ra ngoài cho LAN 172.16.12.0/24:

```
R2#show standby brief
      P indicates configured to preempt.
      |
Interface  Grp  Pri  P State      Active           Standby           Virtual IP
Fa0/0       1     100  P Active   local           unknown          172.16.12.254
```

R3 cũng đã chuyển route đi đến mạng 172.16.12.0/24 theo hướng R2 khi R1 down:

```
R3#show ip route static
  172.16.0.0/24 is subnetted, 3 subnets
S      172.16.12.0 [10/0] via 172.16.23.2
```

PC vẫn có thể đi ra bên ngoài để đi đến subnet 172.16.3.0/24:

```
C:\>ping 172.16.3.1
Pinging 172.16.3.1 with 32 bytes of data:
Reply from 172.16.3.1: bytes=32 time=57ms TTL=254
Reply from 172.16.3.1: bytes=32 time=32ms TTL=254
Reply from 172.16.3.1: bytes=32 time=48ms TTL=254
Reply from 172.16.3.1: bytes=32 time=45ms TTL=254
Ping statistics for 172.16.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 32ms, Maximum = 57ms, Average = 45ms
```

### Cấu hình đầy đủ:

#### R1:

```
ip route 172.16.3.0 255.255.255.0 172.16.13.3
!
interface f0/0
  standby 1 ip 172.16.12.254
  standby 1 priority 150
  standby 1 preempt
```

#### R2:

```
ip route 172.16.3.0 255.255.255.0 172.16.23.3
!
interface f0/0
  standby 1 ip 172.16.12.254
  standby 1 preempt
```

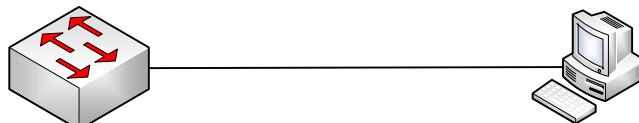
#### R3:

```
ip route 172.16.12.0 255.255.255.0 172.16.13.1 5
ip route 172.16.12.0 255.255.255.0 172.16.23.2 10
```

# SECURITY

## Lab 15 – Port Security

Sơ đồ:



Hình 15.1. Sơ đồ bài Lab

Mô tả:

- Sơ đồ Lab gồm 1 Switch và 1 PC được đấu nối với nhau như hình 15.1.
- Trên sơ đồ này, học viên sẽ thực hiện khảo sát tính năng port – security.

Yêu cầu:

- a. Học viên thực hiện đấu nối các thiết bị, thực hiện một số cấu hình cơ bản trên Switch.
- b. Cấu hình tính năng Port – security trên Switch theo yêu cầu sau:
  - Trên cổng F0/1: cấu hình tĩnh cho phép chỉ một địa chỉ MAC được truy nhập, phương thức xử lý vi phạm là shutdown.
  - Trên cổng F0/2: cấu hình cho phép chỉ một địa chỉ MAC được truy nhập và địa chỉ này được Switch học tự động sticky, phương thức xử lý vi phạm là restrict.

Thực hiện:

Bước 1: Kết nối và cấu hình cơ bản

Học viên thực hiện kết nối thiết bị và cấu hình cơ bản trên các thiết bị theo yêu cầu đặt ra.

Bước 2: Cấu hình Port Security

Cấu hình trên cổng F0/1:

Đưa F0/1 về port access và tiến hành bật tính năng port-security:

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address 10BF.4836.C14E
Switch(config-if)#switchport port-security violation shutdown
```

Kiểm tra tính năng port-security trên cổng f0/1:

```
Switch#show port-security interface f0/1
Port Security          : Enabled
Port Status             : Secure-down
Violation Mode         : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses      : 1
```

```
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

```
Switch#show port-security address
      Secure Mac Address Table
```

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	10bf.4836.c14e	SecureConfigured	Fa0/1	-
Total Addresses in System (excluding one mac per port) : 0				
Max Addresses limit in System (excluding one mac per port) : 6144				

Thực hiện kiểm tra hoạt động của port – security bằng cách kết nối một PC với MAC khác với MAC được cho phép trên cổng, hoạt động xử phạt diễn ra:

```
01:17:02.575: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/1, putting
Fa0/1 in err-disable state
01:17:02.575: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused
by MAC address 001c.c086.00eb on port FastEthernet0/1.
01:17:03.582: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to down
01:17:04.580: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
```

Kiểm tra lại các thông số:

```
Switch#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 : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : 001c.c086.00eb:1
Security Violation Count : 1
```

Lúc này số lần vi phạm (Violation Count) đã tăng lên 1.

Kiểm tra trạng thái của cổng F0/1:

```
Switch#show interfaces f0/1
FastEthernet0/1 is down, line protocol is down (err-disabled)
```

Cổng bị đưa vào trạng thái down/down không còn sử dụng được.

Kết nối lại PC với MAC hợp lệ vào cổng F0/1 và thực hiện reset cổng để cổng hoạt động bình thường trở lại:

```
Switch(config)#int f0/1
Switch(config-if)#shutdown
Switch(config-if)#no shutdown
```

Cấu hình trên cổng F0/2:

```
Switch(config)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation restrict
```

Kiểm tra thông tin port-security trên cổng F0/2:

```
Switch#show port-security interface f0/2
Port Security : Enabled
Port Status : Secure-down
Violation Mode : Restrict
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
```

Địa chỉ MAC được tự động đưa vào danh sách địa chỉ được phép truy nhập trên cổng khi thực hiện kết nối PC lên cổng:

```
Switch#show port-security address
Secure Mac Address Table
-----
Vlan      Mac Address          Type          Ports      Remaining Age
                                         (mins)
-----  -----
1        10bf.4836.c14e    SecureConfigured   Fa0/1      -
1        001c.c086.00eb    SecureSticky     Fa0/2      -
-----
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 6144
```

Thực hiện kết nối một PC với MAC không hợp lệ lên cổng F0/2. Khi sự vi phạm xảy ra Port vẫn ở trạng thái up/up, nhưng frame vi phạm sẽ bị loại bỏ và một thông điệp cảnh báo được phát ra:

```
02:09:44.804: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
```

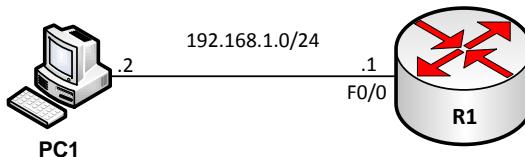
```
Switch#show port-security interface f0/2
```

```
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode        : Restrict
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses   : 1
Configured MAC Addresses : 0
Sticky MAC Addresses  : 1
Last Source Address:Vlan : 10bf.4836.c14e:1
Security Violation Count : 155
```

Nếu thay phương thức “restrict” bằng phương thức “protect”, cách thức xử phạt frame vi phạm sẽ diễn ra giống như trên nhưng không có thông điệp cảnh báo nào được phát ra.

## Lab 16 – Local Authentication, SSH

Sơ đồ:



Hình 16.1 – Sơ đồ bài Lab

Mô tả:

- Sơ đồ Lab gồm 1 Router và 1 PC được đấu nối với nhau như hình 16.1.
- Trong bài Lab này, học viên thực hiện khảo sát hoạt động của SSH với Cisco IOS.

Yêu cầu:

1. Học viên thực hiện đấu nối các thiết bị, thực hiện một số cấu hình cơ bản trên Router như đặt hostname, password enable, password console,...
2. Cấu hình Telnet trên Router. Khảo sát local authentication.
3. Cấu hình SSH trên Router. Sử dụng chương trình bắt gói Wireshark trong từng trường hợp để xác nhận rằng SSH thực hiện mã hóa dữ liệu trao đổi giữa client và server còn Telnet thì không.

Thực hiện:

Bước 1: Kết nối và cấu hình cơ bản

Học viên thực hiện kết nối thiết bị và cấu hình cơ bản trên các thiết bị theo yêu cầu đặt ra:

```
Router(config)#hostname R1
R1(config)#enable password waren
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
```

Bước 2: Khảo sát Local Authentication

Tạo tài khoản user mới bằng câu lệnh sau:

```
R1(config)#username user01 password user01pass
```

Sử dụng local authentication trên cổng console:

```
R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#end
R1#exit
```

Thoát ra ngoài kiểm tra xác thực trên cổng console:

```
R1 con0 is now available, Press RETURN to get started.
```

Sử dụng tài khoản user01 và password được cấu hình trước đó để đăng nhập.

Cấu hình telnet trên Router:

```
R1(config)#line vty 0 4
R1(config-line)#password ciscovtypass
R1(config-line)#login
```

Thực hiện telnet từ PCA đến R1:

```
PC-A>telnet 192.168.1.1
```

Lúc này vẫn phải sử dụng password được cấu hình ở `line vty` để thực hiện telnet. Thay đổi thành local authentication và thực hiện telnet lại để kiểm tra:

```
R1(config)#line vty 0 4
R1(config-line)#login local
```

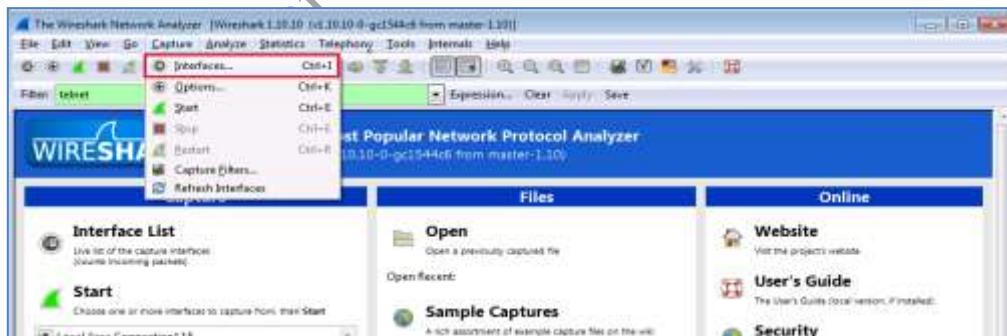
Telnet từ PCA đến R1:

```
PC-A>telnet 192.168.1.1
```

Sử dụng tài khoản user01 và password được cấu hình trước đó để đăng nhập.

**Bước 3:** Cấu hình telnet và SSH, dùng wireshark kiểm tra

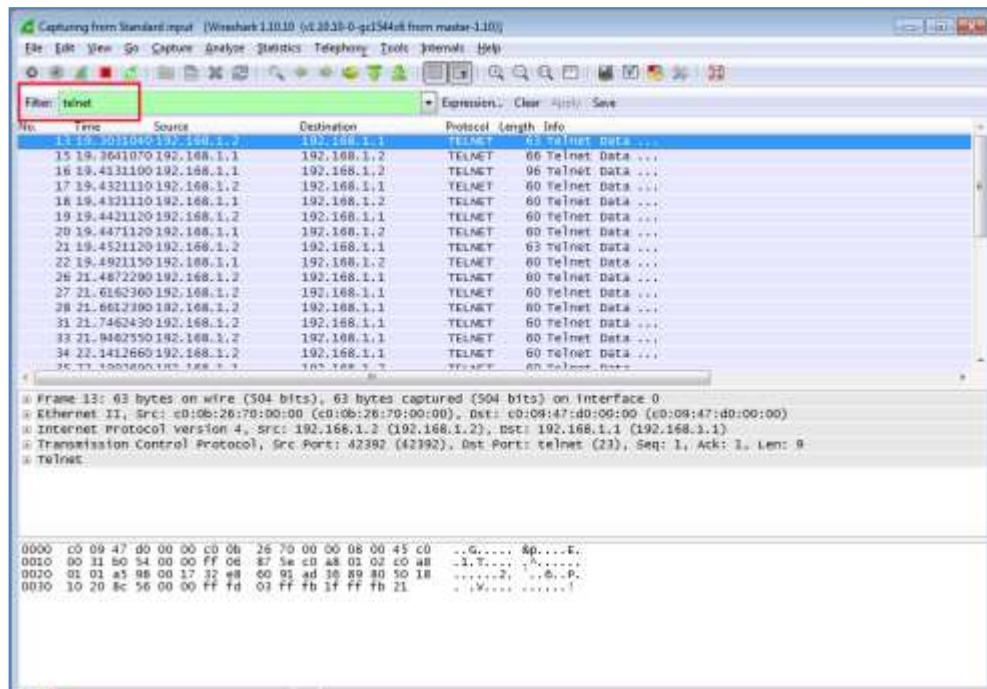
Trên PC, chạy chương trình bắt gói Wireshark, chọn interafces là NIC gắn với switch, bấm Start (hình 16.2):



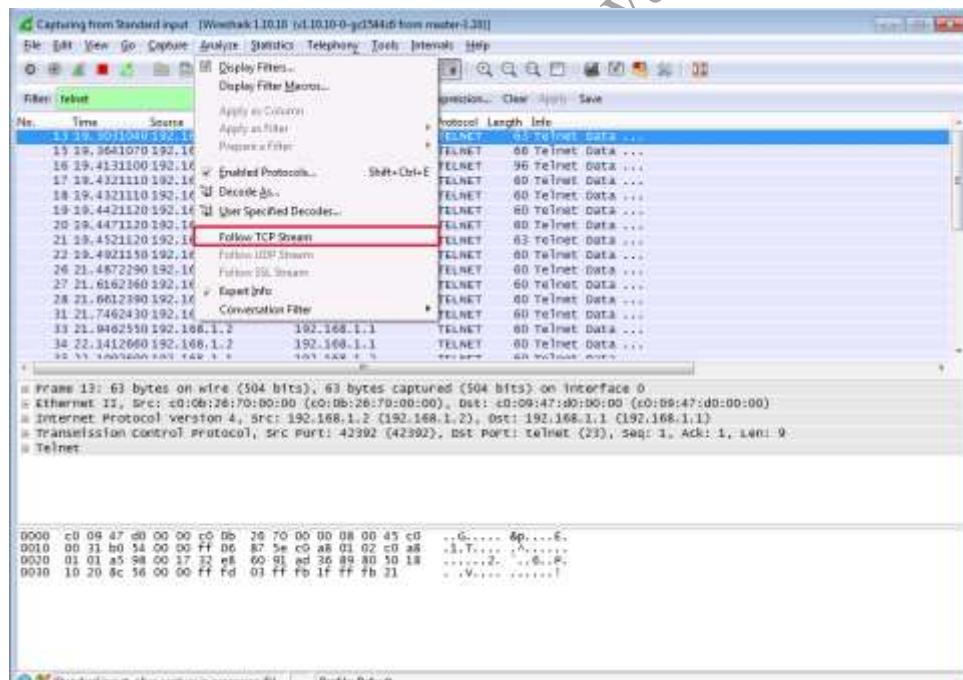
Hình 16.2 – Chọn Interface là card mạng đầu nối đến switch

Tiến hành telnet từ PC đến Router và kiểm tra kết quả các gói bắt được bằng wireshark.

Trong ô “Filter”, chọn “telnet” để theo dõi các gói Telnet (hình 16.3):

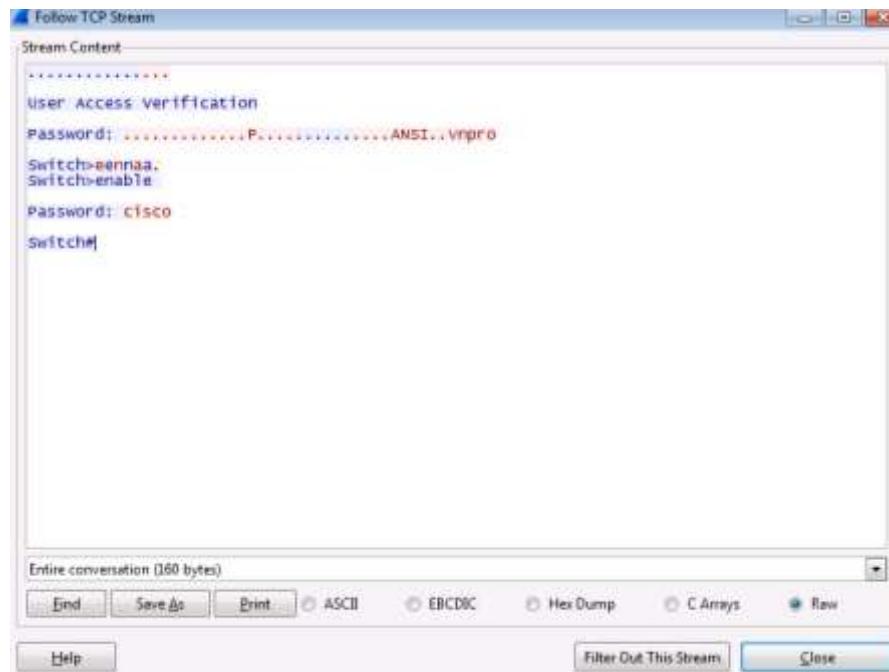


Hình 16.3 – Filter các gói Telnet



Hình 16.4 – Trong “Analyze”, chọn “Follow TCP Stream”

Kết quả bắt gói cho thấy nội dung của session Telnet đã thực hiện, bao gồm cả các password đã cấu hình (hình 16.5):



Hình 16.5 – Kết quả bắt gói với Telnet

### Cấu hình SSH:

Cấu hình domain-name cho mục đích định danh các key mã hóa:

```
Router(config)#ip domain-name waren.vn
```

Thực hiện phát sinh key mã hóa:

```
Router(config)#crypto key generate rsa
The name for the keys will be: Switch.waren.vn
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

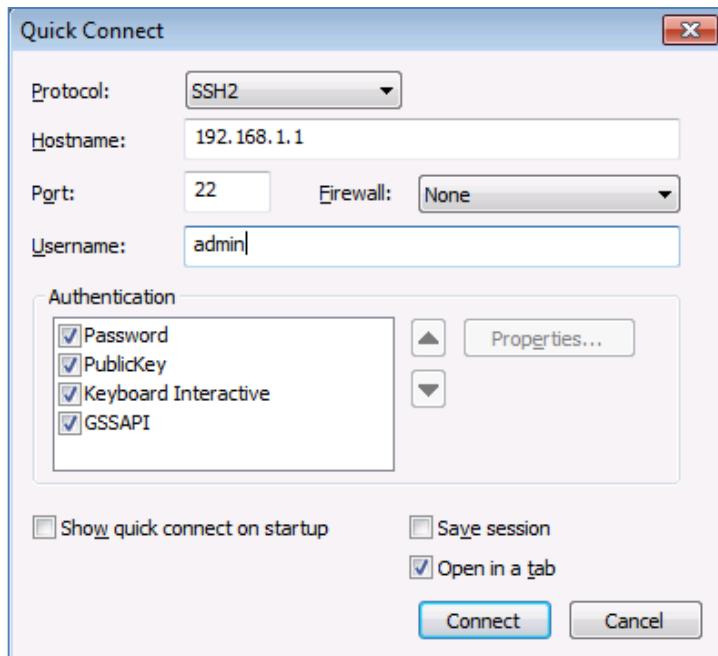
Sử dụng SSH version 2, tạo username và password xác thực đăng nhập:

```
Router(config)#ip ssh ver 2
Router(config)#username admin password waren
```

Cấu hình chuyển đổi phương thức truy nhập từ xa trên các cổng VTY thành SSH:

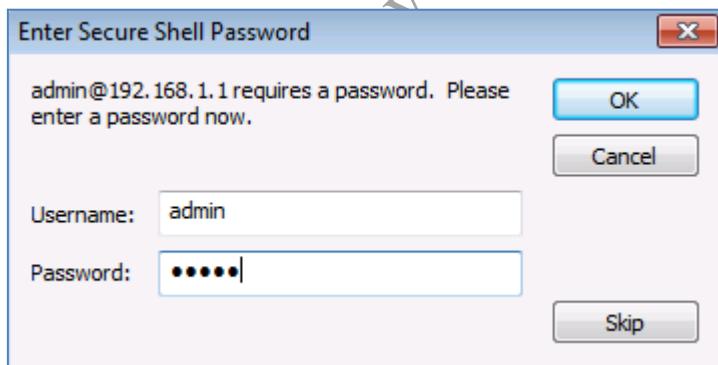
```
Router(config)#line vty 0 15
Router(config-line)#transport input ssh    <- Chỉ cho phép thực hiện SSH
Router(config-line)#login local           <- Xác thực dùng database local
```

Sử dụng SecureCRT trên PC để SSH tới thiết bị (hình 16.6):



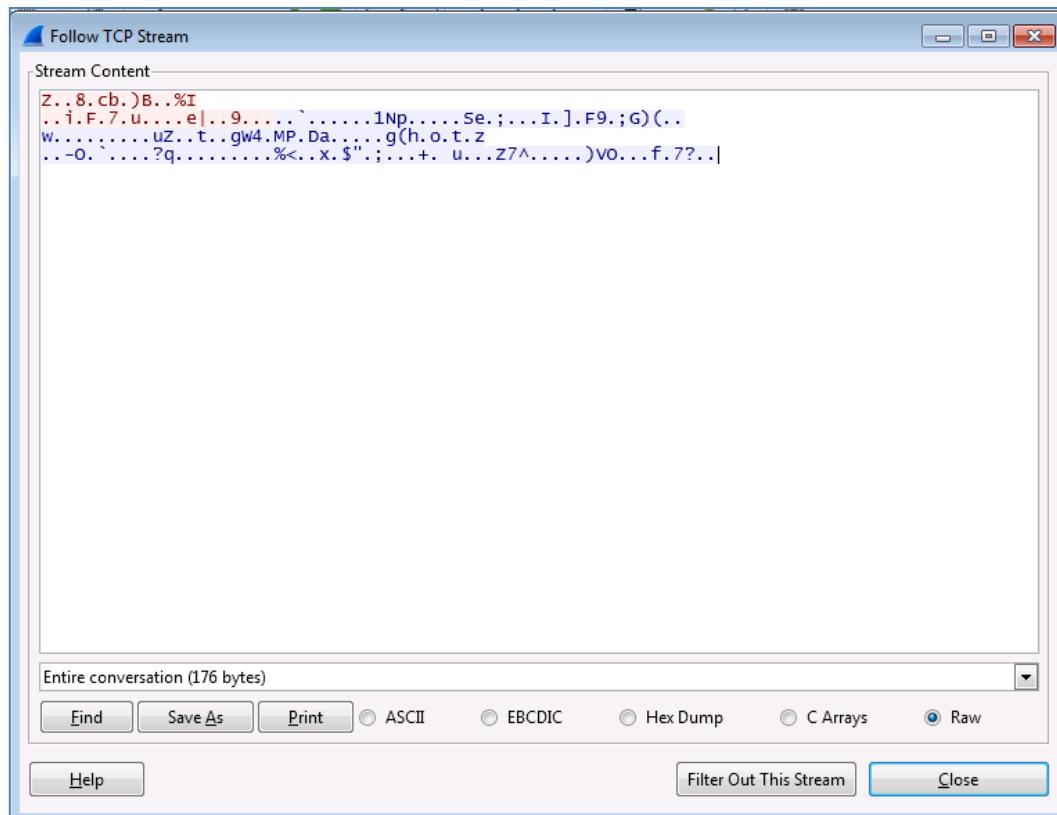
Hình 16.6 – Truy nhập SSH với Secure CRT

Nhập các thông tin xác thực (hình 16.7):



Hình 16.7 – Xác thực truy nhập SSH

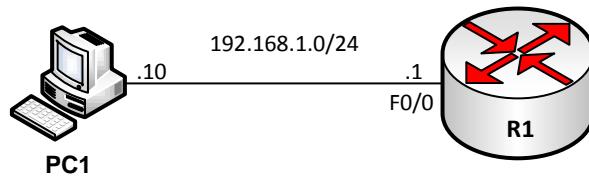
Kiểm tra kết quả bắt gói trên Wireshark cho thấy lần này dữ liệu đã được mã hóa (hình 16.8):



Hình 16.8 – Kết quả bắt gói với SSH

## Lab 17 – Xác thực và phân quyền login

Sơ đồ:



Hình 17.1 – Sơ đồ bài lab.

Mô tả:

- Trong bài lab này, học viên sẽ thực hiện khảo sát hoạt động xác thực và phân quyền cho user khi user đăng nhập vào router.

Yêu cầu:

### Xác thực và phân quyền local:

- Trên R1 thực hiện phân quyền dòng lệnh cho các privilege level như sau:
  - Level 0** – Bên cạnh các lệnh mặc định, các user thuộc level 0 chỉ được thực hiện thêm các lệnh sau đây:
    - ping
    - telnet
    - traceroute
    - show ip route
    - show ip protocols
    - show ip interface brief
    - show ip eigrp neighbors
  - Level 1** – Bên cạnh các lệnh của level 0, các user thuộc level 1 còn được phép cấu hình định tuyến cho thiết bị. Ngoài ra, level này không được phép cấu hình thêm bất cứ thông số nào khác.
  - Level 2** – Các user thuộc level 2 bên cạnh cấu hình định tuyến như với level 1, còn được phép thay đổi cấu hình IP trên các interface và shutdown/no shutdown các interface của thiết bị.
- Thực hiện tạo các tài khoản truy nhập như sau:
  - Username: *guest*, password: *123456*, privilege level *0*.
  - Username: *admin1*, password: *waren1*, privilege level *1*.
  - Username: *admin2*, password: *waren2*, privilege level *2*.
  - Username: *admin*, password: *waren*, privilege level *15*.
- Cấu hình xác thực và phân quyền cho hoạt động telnet đến router R1 theo database nội bộ đã xây dựng ở trên.

## Cấu hình:

Cisco IOS cung cấp 16 cấp độ truy nhập lên thiết bị gọi là các *privilege level*. Số lượng câu lệnh user có thể thi hành tùy thuộc vào cấp độ mà user ấy truy nhập vào thiết bị. Privilege của user càng cao, số lượng câu lệnh được phép thi hành càng nhiều. Privilege cao hơn sẽ bao hàm các lệnh được thi hành ở privilege thấp hơn.

Mặc định có 3 privilege level được định nghĩa sẵn trên thiết bị:

- **Privilege level 0:** User level này chỉ có thể thực thi các lệnh disable, enable, exit, help và logout. Dấu nhắc hệ thống của user tại level này là “Router”.
- **Privilege level 1:** Sử dụng dấu nhắc hệ thống là “Router” giống như level 0. Mặc định khi đăng nhập vào thiết bị qua cổng console hoặc VTY, user sẽ được đặt vào level này. Level này còn được gọi bằng một tên khác là “User – EXEC mode”. Bên cạnh các lệnh của level 0, user tại level 1 còn có thể thực hiện thêm một số lệnh khác như ping, telnet,... và “show” được một số thông số cơ bản trên thiết bị. Mặc định, user thuộc level 1 không được phép tiến vào chế độ config để thực hiện các thao tác cấu hình.
- **Privilege level 15:** Sử dụng dấu nhắc hệ thống “Router#”. Tại level này, user được quyền hiển thị mọi thông tin về thiết bị với các lệnh “show” và được quyền đi vào mode config thay đổi mọi cấu hình của thiết bị. Level này còn được gọi tên là “Privilege – EXEC mode”.

Các privilege level từ 2 đến 14 nếu không được khai báo gì thêm sẽ chỉ được quyền sử dụng tập lệnh giống như của level 1 nhưng sử dụng dấu nhắc hệ thống giống như của level 15: “Router#”. Nhắc lại rằng privilege cao hơn sẽ bao hàm các lệnh được thi hành ở privilege thấp hơn.

Nhu đã nêu ở trên, tập lệnh được phép sử dụng của level 0 rất hạn chế, cần phải thực hiện bổ sung thêm lệnh để user level 0 có thể thực hiện được các lệnh theo yêu cầu đặt ra:

```
R1(config)#privilege exec level 0 ping
R1(config)#privilege exec level 0 telnet
R1(config)#privilege exec level 0 show ip route
R1(config)#privilege exec level 0 show ip protocols
R1(config)#privilege exec level 0 show ip interface brief
R1(config)#privilege exec level 0 show ip eigrp neighbors
```

Mặc định, level 1 không được phép cấu hình thay đổi hoạt động thiết bị. Thực hiện bổ sung thêm các lệnh được phép thực hiện trên level 1 như yêu cầu đã nêu ra:

```
R1(config)#privilege exec level 1 configure terminal
R1(config)#privilege configure all level 1 router
```

Với phân quyền vừa thực hiện ở trên, level 1 đã được phép sử dụng lệnh “configure terminal” để đi vào mode config. Trong mode config, level 1 được phép thực hiện lệnh “router” với mọi tùy chọn đi kèm (thông số “all” cho phép thực hiện mọi tùy chọn của câu lệnh được khai báo).

Như vậy, một user level 1 đã có thể thực hiện cấu hình định tuyến cho router. Tuy nhiên, vì không bổ sung thêm các lệnh khác ngoài cấu hình định tuyến, các user thuộc level 1 sẽ không được phép tiến hành thêm bất kỳ hoạt động cấu hình nào khác.

Tiếp theo, thực hiện cấu hình bổ sung các lệnh được thực hiện trên level 2 theo yêu cầu đặt ra:

```
R1(config)#privilege configure level 2 interface
R1(config)#privilege interface all level 2 ip
R1(config)#privilege interface level 2 shutdown
R1(config)#privilege interface level 2 no shutdown
```

Level 2 sẽ bao hàm các lệnh của level 1 nên không cần phải khai báo lại lệnh “configure terminal” cho level 2 cũng như các lệnh liên quan đến cấu hình định tuyến vì các lệnh này đã được khai báo ở level 1. Level 2 được bổ sung thêm các lệnh liên quan đến cấu hình trên interface về khai báo các thông số IP cũng như quyền shutdown/no shutdown cổng.

Kế tiếp, thực hiện khai báo các user thuộc các level theo yêu cầu đặt ra:

```
R1(config)#username guest privilege 0 password 123456
R1(config)#username admin1 privilege 1 password waren1
R1(config)#username admin2 privilege 2 password waren2
R1(config)#username admin privilege 15 password waren
```

Cuối cùng, thực hiện xác thực và phân quyền hoạt động telnet đến R1 theo cơ sở dữ liệu nội bộ vừa khai báo ở trên:

```
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#exit
```

### **Kiểm tra:**

Thực hiện telnet từ PC đến R1 để kiểm tra cấu hình đã thực hiện.

Telnet với username “guest”:

Sử dụng kí tự “?” để kiểm tra các lệnh có thể được thực hiện với user này:

```
R1>?
Exec commands:
<1-99> Session number to resume
disable Turn off privileged commands
enable Turn on privileged commands
exit Exit from the EXEC
help Description of the interactive help system
logout Exit from the EXEC
ping Send echo messages
show Show running system information
telnet Open a telnet connection
```

Có thể thấy, bên cạnh các lệnh mặc định, các lệnh “ping”, “telnet” và “show” đã được bổ sung cho user với privilege level 0.

Thực hiện kiểm tra thực thi các lệnh:

```
R1>show interface f0/0
^
% Invalid input detected at '^' marker.

R1>show running-config
^
% Invalid input detected at '^' marker.
```

Có thể thấy, ở level 0, bên cạnh những lệnh đã khai báo, user guest không thực thi được các lệnh nào khác.

Tiếp theo, từ PC, thực hiện telnet đến R1 bằng tài khoản “admin1” để tiếp tục hoạt động kiểm tra với privilege level 1:

Sử dụng lệnh “show privilege” để xác nhận rằng level của user admin1 là level 1:

```
R1>show privilege
Current privilege level is 1
```

Với level 1, thông số “privilege” trong lệnh “show” là thông số ẩn, cần phải gõ tường minh để thi hành lệnh, không thể sử dụng phím “Tab” hay “?” để hiển thị thông số này.

Kiểm tra rằng user admin1 có thể thực hiện được các thao tác định tuyến:

```
R1>configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)>router ?
bgp      Border Gateway Protocol (BGP)
eigrp    Enhanced Interior Gateway Routing Protocol (EIGRP)
isis     ISO IS-IS
iso-igrp IGRP for OSI networks
mobile   Mobile routes
odr      On Demand stub Routes
ospf     Open Shortest Path First (OSPF)
rip      Routing Information Protocol (RIP)

R1(config)>router eigrp 100
R1(config-router)>?
Router configuration commands:
address-family      Enter Address Family command mode
auto-summary        Enable automatic network number summarization
default             Set a command to its defaults
default-information Control distribution of default information
default-metric      Set metric of redistributed routes
distribute-list     Filter networks in routing updates
eigrp               EIGRP specific commands
(...)

R1(config-router)>network ?
A.B.C.D Network number
R1(config-router)>no auto-summary ?
<cr>
```

User admin1 không thể thực hiện được các thao tác cấu hình khác, ví dụ như đổi hostname hay can thiệp vào cấu hình trên interface:

```
R1(config)>hostname R11
^
% Invalid input detected at '^' marker.

R1(config)>interface f0/0
^
% Invalid input detected at '^' marker.
```

Tiếp theo, thực hiện telnet vào R1 từ PC với tài khoản “admin2” để kiểm tra hoạt động phân quyền cho user này:

Có thể thấy, khác với level 0 và level 1, dấu nhắc hệ thống từ level 2 đã chuyển thành “Router#”. Tương tự như với user admin1, có thể sử dụng lệnh “show privilege” để xác nhận rằng level của user admin2 là level 2:

```
R1#show privilege
Current privilege level is 2
```

Thực hiện kiểm tra các lệnh có thể được thực hiện tại level 2:

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ?
bgp      Border Gateway Protocol (BGP)
eigrp    Enhanced Interior Gateway Routing Protocol (EIGRP)
isis     ISO IS-IS
iso-igrp IGRP for OSI networks
mobile   Mobile routes
odr      On Demand stub Routes
ospf    Open Shortest Path First (OSPF)
rip     Routing Information Protocol (RIP)

R1(config)#router eigrp 100
R1(config-router) #?
Router configuration commands:
address-family      Enter Address Family command mode
auto-summary        Enable automatic network number summarization
bfd                 BFD configuration commands
default             Set a command to its defaults
default-information Control distribution of default information
default-metric      Set metric of redistributed routes
distance            Define an administrative distance
distribute-list     Filter networks in routing updates
(...)

R1(config)#interface f0/0
R1(config-if) #?
Interface configuration commands:
default             Set a command to its defaults
exit                Exit from interface configuration mode
help                Description of the interactive help system
```

```
ip           Interface Internet Protocol config commands
no          Negate a command or set its defaults
shutdown   Shutdown the selected interface
(...)

R1(config-if)#ip ?
Interface IP configuration subcommands:
access-group      Specify access control for packets
accounting        Enable IP accounting on this interface
address          Set the IP address of an interface
admission         Apply Network Admission Control
auth-proxy        Apply authentication proxy
authentication    authentication subcommands
bandwidth-percent Set EIGRP bandwidth limit
(...)

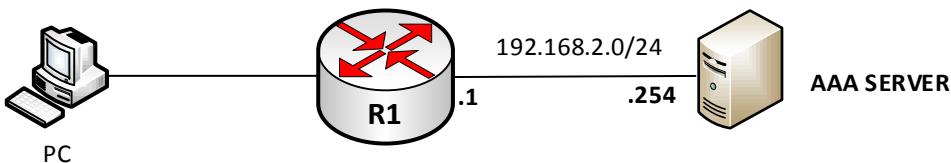
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#shutdown
R1(config-if)#no shutdown
```

Cuối cùng, kiểm tra rằng user admin sẽ được cấp quyền level 15 khi telnet vào R1:

```
R1#show privilege
Current privilege level is 15
```

## Lab 18 – Xác thực và phân quyền privilege sử dụng TACACS+

Sơ đồ:



Hình 18.1 – Sơ đồ bài lab

**Yêu cầu:**

- Tiến hành xác thực và phân quyền privilege cho các user truy nhập telnet đến R1 theo yêu cầu sau:
  - Username: *guest*, password: *123456*, privilege level *0*.
  - Username: *admin1*, password: *waren1*, privilege level *1*.
  - Username: *admin2*, password: *waren2*, privilege level *2*.
  - Username: *admin*, password: *waren*, privilege level *15*.
- Hoạt động xác thực/phân quyền phải được thực hiện theo TACACS+ server, nếu hoạt động này không thành công, chuyển qua phương thức xác thực/phân quyền local đã được cấu hình ở yêu cầu 2.
- TACACS+ server có địa chỉ là 192.168.2.254, pre – shared key là CISCO.

**Cấu hình:**

Trên R1, cấu hình xác thực login và phân quyền privilege theo yêu cầu đặt ra:

```

R1(config)#aaa new-model
R1(config)#aaa authentication login VTY group tacacs+ local
R1(config)#aaa authorization exec VTY group tacacs+ local

R1(config)#line vty 0 4
R1(config-line)#login authentication VTY
R1(config-line)#authorization exec VTY
R1(config-line)#exit

R1(config)#tacacs-server host 192.168.2.254 key CISCO
  
```

Method – list được sử dụng cho hoạt động xác thực và phân quyền privilege trên các cổng VTY được đặt tên là “VTY”. Với method – list này, server TACACS + sẽ được sử dụng trước trong hoạt động xác thực và phân quyền; nếu server TACACS + không hoạt động hoặc không đi đến được, sẽ được sử dụng để thay thế. Điều này cung cấp một cơ chế dự phòng cho hoạt động xác thực/phân quyền.

Một method – list mặc định có tên là “default” luôn tồn tại trên các line cho hoạt động xác thực/phân quyền. Trong câu lab này, method – list VTY được định nghĩa và áp vào các line vty từ 0 đến 4 trên router:

```
R1(config)#line vty 0 4
R1(config-line)#login authentication VTY
R1(config-line)#authorization exec VTY
R1(config-line)#exit
```

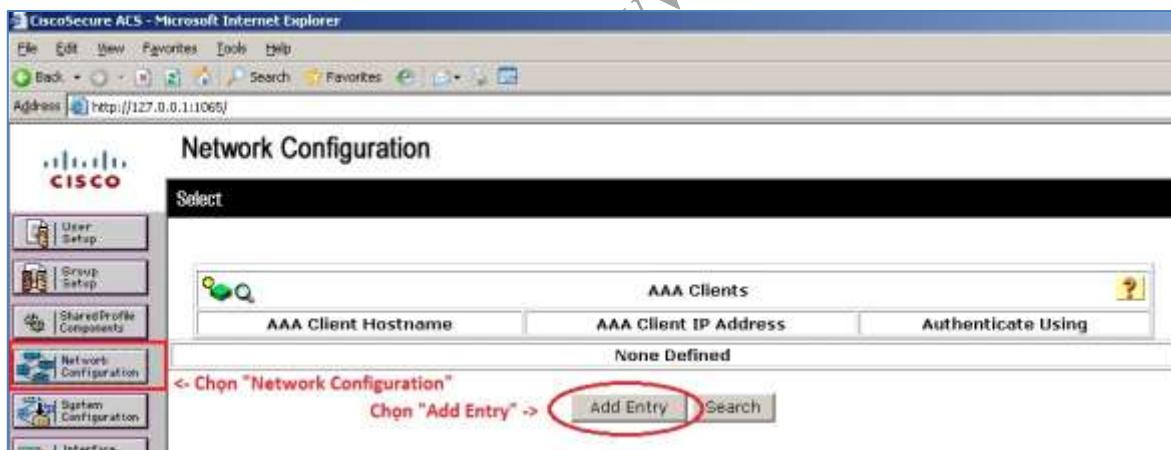
Khi một method – list khai báo tường minh được sử dụng, IOS trên router sẽ ưu tiên method – list này hơn method – list default. Như vậy, trên các cổng VTY từ 0 đến 4, method – list VTY sẽ được thực thi, method – list default sẽ không được sử dụng trong trường hợp này.

Nhu yêu cầu đặt ra, TACACS + server cho hoạt động xác thực/phân quyền trên router R1 có địa chỉ 192.168.2.254 và pre – shared key được sử dụng là CISCO:

```
R1(config)#tacacs-server host 192.168.2.254 key CISCO
```

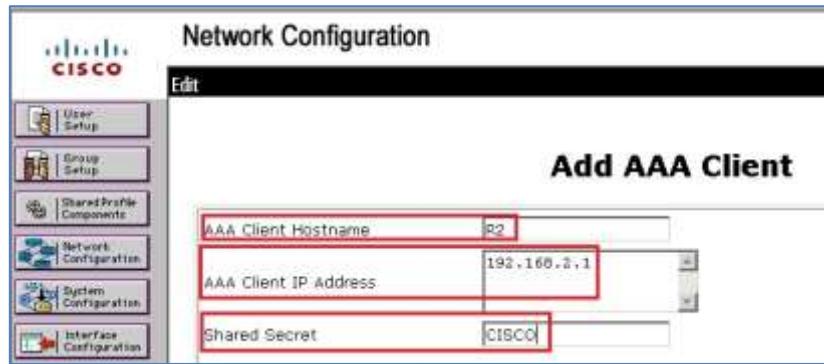
Sau khi đã hoàn tất cấu hình trên router R1, kế tiếp sẽ là phần thiết lập trên TACACS + server. TACACS + server trong bài lab này được triển khai trên chương trình ACS Server version 4.2 của Cisco, chạy trên nền Window server 2003.

Đầu tiên, trên TACACS + server cần phải khai báo TACACS + client, client này chính là router R1. Thực hiện chọn tab “Network Configuration” trên giao diện chương trình ACS; trong cửa sổ hiện ra, chọn “Add Entry” (hình 2):



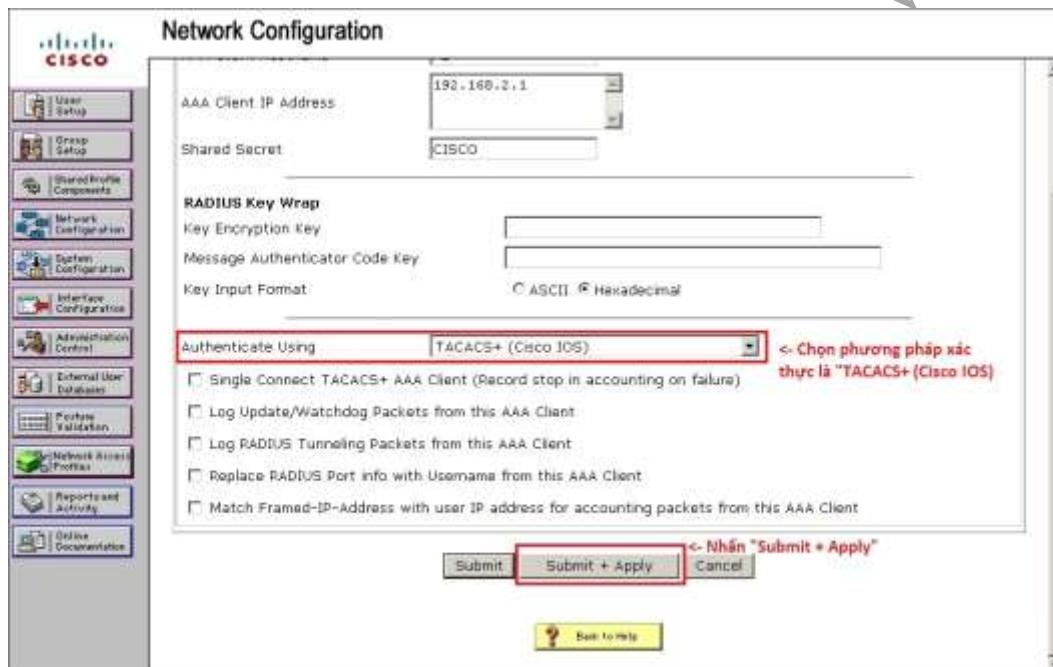
Hình 18.2 – Cửa sổ “Network Configuration”.

Sau khi nhấn “Add Entry”, một cửa sổ hiện ra cho phép khai báo AAA Client. Trong cửa sổ này thực hiện khai báo AAA Client là router R1 (hình 18.3):



Hình 18.3 – Khai báo AAA Client là router R1.

Sau khi khai báo xong, kéo thanh cuộn xuống và nhấn “Submit + Apply” để cập nhật client này vào cơ sở dữ liệu của ACS server (hình 18.4):



Hình 18.4 – Nhấn “Submit + Apply” để cập nhật AAA Client.

Sau khi cập nhật, màn hình giao diện quay trở lại cửa sổ “Network Configuration”, có thể thấy rằng R1 đã được hiển thị trong danh sách các AAA Client trên cửa sổ này (hình 18.5):

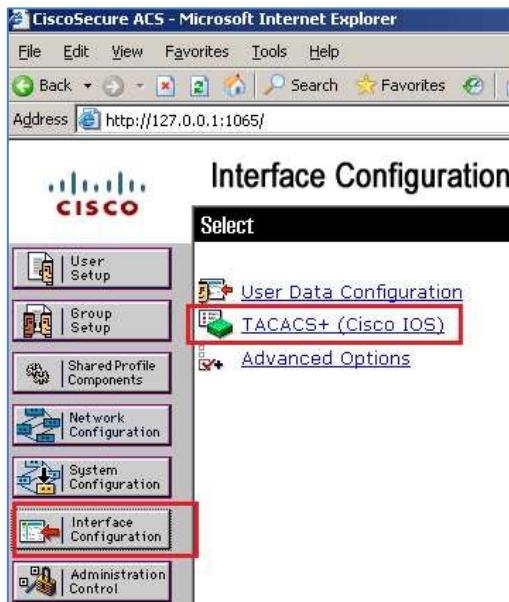
AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
R2	192.168.2.1	TACACS+ (Cisco IOS)

Hình 18.5 – Danh sách AAA Client.

Đến đây, AAA Client R1 đã được khai báo thành công trên TACACS + server.

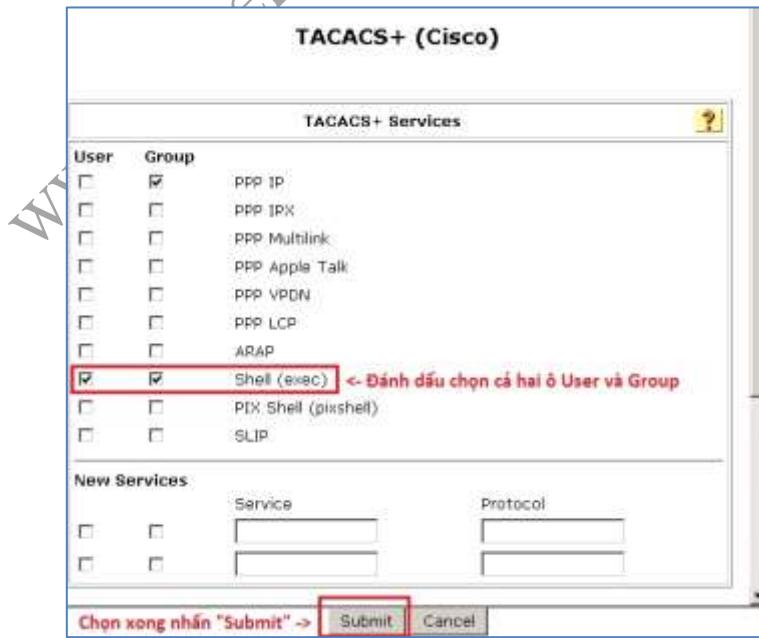
Tiếp theo, trên TACACS + server, thực hiện khai báo các user với các privilege level theo yêu cầu đặt ra.

Trên giao diện chương trình ACS, chọn thẻ “Interface Configuration”; khi cửa sổ của phần này hiện ra, click chọn “TACACS+ Cisco IOS” (hình 18.6):



Hình 18.6 – Giao diện “Interface Configuration”.

Trong cửa sổ hiện ra, đánh dấu chọn dịch vụ “Shell (exec)” cho cả hai ô User và Group; sau khi chọn xong, nhấn “Submit” để cập nhật (hình 18.7):



Hình 18.7 – Chọn dịch vụ “Shell (exec)” cho user.

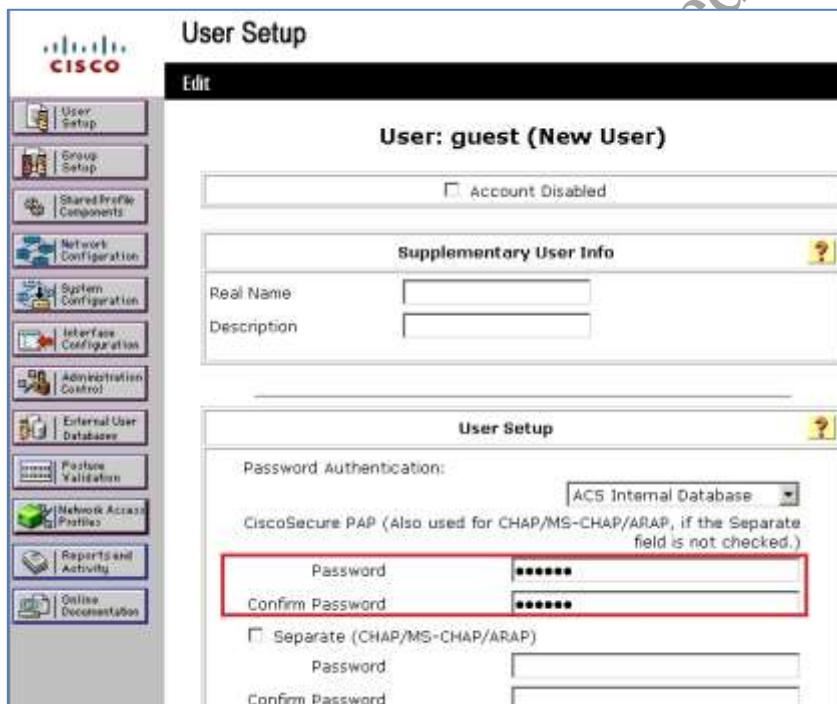
Trong các thao tác tiếp theo, chúng ta thực hiện khai báo các user.

Chọn thẻ “User Setup”, trong cửa sổ hiện ra, nhập username của user thứ nhất: “guest” và nhấn “Add/Edit” (hình 18.8):



Hình 18.8 – Khai báo user “guest” và nhấn “Add/Edit”.

Trong cửa sổ khai báo thông tin cho user hiện ra sau đó, thực hiện khai báo password cho user. Theo yêu cầu đặt ra, password cho user “guest” sẽ là “123456” (hình 18.9):



Hình 18.9 – Khai báo password cho user “guest”.

Tiếp tục kéo xuống phần “TACACS+ Settings”, đánh dấu chọn vào ô “Shell” và ô “Privilege level”. Trong ô giá trị của “Privilege level” khai báo giá trị 0 – chính là level sẽ phân quyền cho user guest khi user này đăng nhập. Sau khi hoàn tất, nhấn “Submit” để cập nhật thông tin cho user “guest” vừa khai báo. Các thao tác vừa nêu được chỉ ra trên hình 18.10:



Hình 18.10 – Các thiết lập TACACS + của user “guest”.

Sau khi nhấn “Submit”, giao diện được đưa trở lại cửa sổ “User Setup”. Có thẻ kiểm tra kết quả vừa thiết lập bằng cách nhấn “List all users” và danh sách các user đã khai báo sẽ hiện ra ở cửa sổ bên phải của giao diện. Có thể thấy rằng user “guest” đã được cập nhật (hình 18.11):

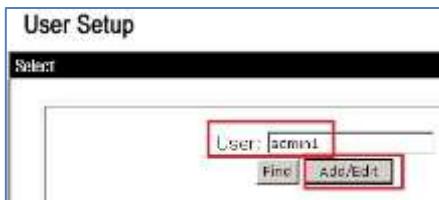
User	Status	Group	Network Access Profile
guest	Enabled	Default Group (1 users)	(Default)

Hình 18.11 – User “guest” trong danh sách các user.

Đến đây, user “guest” đã được khai báo thành công trên TACACS + server.

Quá trình khai báo được thực hiện tương tự cho các user còn lại.

Trong cửa sổ “User Setup”, khai báo user “admin1” và nhấn “Add/Edit” (hình 18.12):



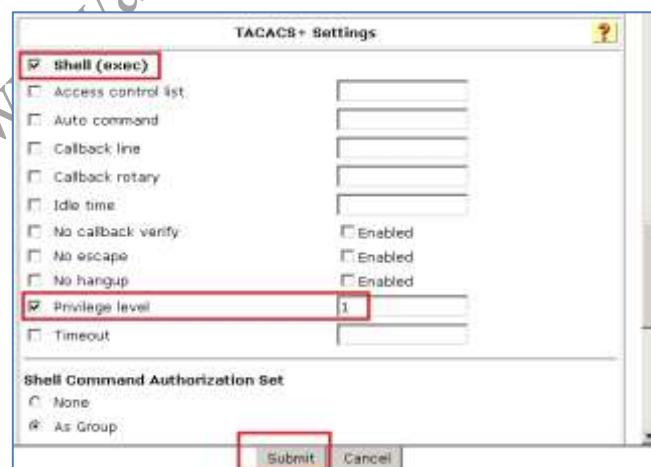
Hình 18.12 – Khai báo user “admin1”.

Nhập password tương ứng cho user admin1 (hình 18.13):



Hình 18.13 – Khai báo password cho user admin1.

Kéo thanh trượt xuống và nhập privilege level cho user này là 1 rồi nhấn “Submit” để cập nhật user admin1 vào cơ sở dữ liệu của ACS (hình 18.14):



Hình 18.14 – Khai báo Privilege level cho user admin1.

Kiểm tra rằng user admin1 đã xuất hiện trong danh sách các user (hình 18.15):

User	Status	Group	Network Access Profile
admin	Enabled	Default Group (2 users)	(Default)
guest	Enabled	Default Group (2 users)	(Default)

Danh sách các user đã khai báo

Hình 18.15 – Danh sách các user đã khai báo.

Quá trình khai báo user này được thực hiện hoàn toàn tương tự cho các user còn lại. Sau khi khai báo hoàn tất, danh sách các user trên ACS server sẽ có đầy đủ các user như trên hình 18.16:

User	Status	Group	Network Access Profile
admin	Enabled	Default Group (4 users)	(Default)
admin1	Enabled	Default Group (4 users)	(Default)
admin2	Enabled	Default Group (4 users)	(Default)
guest	Enabled	Default Group (4 users)	(Default)

Hình 18.16 – Danh sách các user sau khi hoàn tất khai báo.

Đến đây, phần cấu hình đã được hoàn thành.

### Kiểm tra:

Trên AAA client R1, thực hiện bật debug để quan sát quá trình xác thực/phân quyền với AAA:

```
R1#debug aaa authentication
AAA Authentication debugging is on

R1#debug aaa authorization
AAA Authorization debugging is on

R1#debug tacacs authentication
TACACS+ authentication debugging is on

R1#debug tacacs authorization
TACACS+ authorization debugging is on
```

Có thể thực hiện kiểm tra việc xác thực/phân quyền privilege với một trong các user đã khai báo, ví dụ, user admin2.

Thực hiện telnet đến R1 từ PC:

Trên R1, hoạt động xác thực diễn ra:

- Method – list được chọn là “VTY”.
- Server TACACS+ 192.168.2.254 được tham vấn để xác thực.
- Router R1 nhận được yêu cầu về khai báo username từ server xác thực:

```
R1#  
*Mar 1 01:41:34.675: AAA/BIND(0000000D): Bind i/f  
*Mar 1 01:41:34.675: AAA/AUTHEN/LOGIN (0000000D): Pick method list 'VTY'  
*Mar 1 01:41:34.675: TPLUS: Queuing AAA Authentication request 13 for processing  
*Mar 1 01:41:34.675: TPLUS: processing authentication start request id 13  
*Mar 1 01:41:34.675: TPLUS: Authentication start packet created for 13()  
*Mar 1 01:41:34.675: TPLUS: Using server 192.168.2.254  
(...)  
*Mar 1 01:41:34.723: TPLUS(0000000D)/0/READ: read entire 28 bytes response  
*Mar 1 01:41:34.723: TPLUS(0000000D)/0/666156F0: Processing the reply packet  
*Mar 1 01:41:34.723: TPLUS: Received authen response status GET_USER (7)
```

Trên PC, tiến hành nhập username “admin2” để R1 chuyển lên TACACS + :

```
Username: admin2  
Password:
```

Server sau khi nhận được username chuyển đến từ R1, tiếp tục thực hiện truy vấn password:

```
Mar 1 01:41:52.939: TPLUS: Queuing AAA Authentication request 13 for processing  
*Mar 1 01:41:52.939: TPLUS: processing authentication continue request id 13  
*Mar 1 01:41:52.943: TPLUS: Authentication continue packet generated for 13  
(...)  
*Mar 1 01:41:52.963: TPLUS(0000000D)/0/READ: read entire 28 bytes response  
*Mar 1 01:41:52.963: TPLUS(0000000D)/0/666156F0: Processing the reply packet  
*Mar 1 01:41:52.963: TPLUS: Received authen response status GET_PASSWORD (8)
```

Nhập password:

```
Username: admin2  
Password: <- Nhập password là "waren2"
```

Sau khi nhập password, R1 chuyển password này lên server, server trả kết quả về là xác thực đã diễn ra thành công (“PASS”):

```
*Mar 1 01:42:08.135: TPLUS: Queuing AAA Authentication request 13 for processing  
*Mar 1 01:42:08.139: TPLUS: processing authentication continue request id 13  
*Mar 1 01:42:08.139: TPLUS: Authentication continue packet generated for 13  
(...)  
*Mar 1 01:42:08.191: TPLUS(0000000D)/0/666156F0: Processing the reply packet  
*Mar 1 01:42:08.191: TPLUS: Received authen response status PASS (2)<- Xác thực thành công
```

Sau khi xác thực thành công, hoạt động phân quyền diễn ra, server 192.168.2.254 được tham vấn cho hoạt động này:

```
*Mar 1 01:42:08.199: AAA/AUTHOR (0xD): Pick method list 'VTY'  
*Mar 1 01:42:08.203: TPLUS: Queuing AAA Authorization request 13 for processing  
*Mar 1 01:42:08.203: TPLUS: processing authorization request id 13  
(...)  
*Mar 1 01:42:08.211: TPLUS: Authorization request created for 13(admin2)  
*Mar 1 01:42:08.211: TPLUS: using previously set server 192.168.2.254 from group tacacs+
```

Server trả về kết quả phân quyền cho user admin2 là privilege level 2 như đã thực hiện cấu hình trước đó:

```
*Mar 1 01:42:08.267: TPLUS: Processed AV priv-lvl=2
*Mar 1 01:42:08.271: TPLUS: received authorization response for 13: PASS
*Mar 1 01:42:08.271: AAA/AUTHOR/EXEC(0000000D): processing AV cmd=
*Mar 1 01:42:08.271: AAA/AUTHOR/EXEC(0000000D): processing AV priv-lvl=2
*Mar 1 01:42:08.275: AAA/AUTHOR/EXEC(0000000D): Authorization successful
```

Có thể kiểm tra điều này trên R1. sau khi đã telnet thành công đến R1:

```
Username: admin2
```

```
Password:
```

```
R1#
```

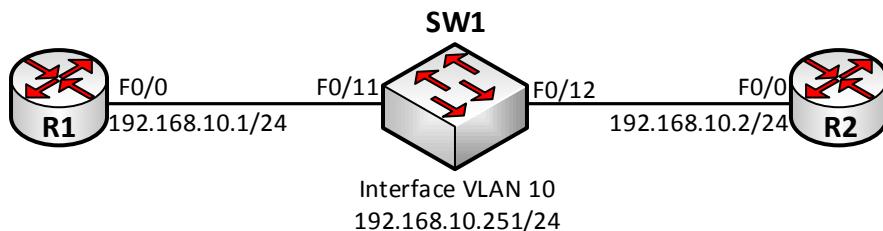
```
R1#show privilege
```

```
Current privilege level is 2
```

Như vậy, hoạt động xác thực và phân quyền với TACACS + server đã diễn ra thành công.

## Lab 19 – DHCP Snooping

Sơ đồ:



Hình 19.1 – Sơ đồ bài lab

Mô tả:

- Cấu hình để R1 đóng vai trò DHCP server cấp phát IP cho tất cả các host thuộc VLAN 10 (VLAN 10 được quy hoạch subnet IP 192.168.10.0/24).
- Cấu hình tính năng DHCP snooping trên VLAN 10 của SW1 đảm bảo ngăn chặn tất cả các hoạt động tấn công giả mạo DHCP server diễn ra trên VLAN này.

Cấu hình:

Thực hiện cấu hình R1 thành DHCP server cấp phát IP cho VLAN 10:

```

R1(config)#ip dhcp excluded-address 192.168.10.1
R1(config)#ip dhcp excluded-address 192.168.10.251
R1(config)#ip dhcp pool VLAN10
R1(dhcp-config)#network 192.168.10.0 /24
R1(dhcp-config)#default-router 192.168.10.1
R1(dhcp-config)#exit
    
```

Cấu hình tính năng DHCP snooping cho VLAN 10 trên SW1:

```

SW1(config)#ip dhcp snooping
SW1(config)#ip dhcp snooping vlan 10
SW1(config)#interface f0/11
SW1(config-if)#ip dhcp snooping trust
SW1(config-if)#exit
SW1(config)#no ip dhcp snooping information option
    
```

Ghi chú:

Cấu hình DHCP snooping đã thực hiện ở trên có thể được giải thích ngắn gọn thông qua một vài ý như sau:

- Tính năng DHCP Snooping được sử dụng để ngăn chặn phương thức tấn công giả mạo DHCP (DHCP Spoofing) trên một VLAN. Với phương thức tấn công này, kẻ tấn công dựng lên một DHCP server giả để rót thông tin IP sai lệch xuống cho người dùng cùng VLAN từ

đó gây ảnh hưởng đến việc truy nhập mạng hoặc đánh cắp thông tin từ người dùng. Tính năng này được bật trên một VLAN của một switch bằng các lệnh:

```
SW1(config)#ip dhcp snooping <- Bật DHCP snooping trên SW1
SW1(config)#ip dhcp snooping vlan 10 <- Áp dụng cho VLAN 10
```

- Khi tính năng DHCP snooping được bật trên VLAN, các cổng thuộc VLAN được chia thành hai loại: *trusted port* và *untrusted port*.
  - Trên *trusted port*, thiết bị kết nối được quyền gửi vào port tất cả các loại gói tin DHCP. Các trusted port là các port kết nối đến DHCP server hoặc các port uplink.
  - Trên *untrusted port*, thiết bị chỉ được phép gửi vào port các loại gói tin mà DHCP server gửi xuống cho client. Các untrusted port được dùng để kết nối đến các end – user trong VLAN. Khi được kết nối vào untrusted port, end – user không thể dụng DHCP server giả vì mọi gói tin cấp phát IP đến từ DHCP server giả mạo của end – user sẽ bị chặn khi đi đến untrusted port.
  - Mặc định, các cổng thuộc VLAN được áp DHCP snooping sẽ hoạt động ở chế độ untrusted. Người quản trị phải chỉ định tường minh các cổng trusted bằng lệnh “`ip dhcp snooping trust`” trên các cổng kết nối đến DHCP server hoặc uplink. Trong câu lab này, cổng F0/11 kết nối đến DHCP server R1 được chỉ định là trusted port:

```
SW1(config)#interface f0/11
SW1(config-if)#ip dhcp snooping trust
SW1(config-if)#exit
```

- Khi tính năng DHCP snooping được bật trên switch, switch tự động thực hiện chèn thêm option – 82 cho các gói tin DHCP đi đến DHCP server.

Option 82 là một loại option được sử dụng để cung cấp thêm thông tin về Agent đến cho DHCP server. Các gói tin DHCP mà có chèn thêm option 82 thường có trường “giaddr” nhận giá trị khác 0 vì trường này được sử dụng để mang theo địa chỉ của DHCP relay agent. Tuy nhiên, trong tình huống sử dụng DHCP snooping, switch thực hiện chèn vào option 82 nhưng nó lại không phải là DHCP relay agent nên trường “giaddr” phải nhận giá trị là 0. Điều này dẫn đến DHCP server sẽ coi gói DHCP nhận được là bị lỗi (xuất hiện option 82 nhưng lại có giaddr = 0) và loại bỏ gói này khiến cho các client sẽ không nhận được cấu hình IP.

Để khắc phục vấn đề vừa nêu, khi cấu hình DHCP snooping trên switch, cần phải thực hiện tắt thao tác chèn option 82 hoặc cấu hình DHCP server chấp nhận các gói tin có option 82 nhưng trường giaddr lại bằng 0.

Để tắt option 82 với DHCP snooping trên switch, sử dụng lệnh:

```
SW(config)#no ip dhcp snooping information option
```

Để DHCP server chấp nhận các gói tin DHCP với option 82 nhưng lại có giaddr = 0, sử dụng lệnh:

```
R(config)#ip dhcp relay information trust-all
```

Hoặc câu lệnh ở mode interface:

```
R(config-if)#ip dhcp relay information trusted
```

Trong câu lab này, cách tắt option 82 trên switch được lựa chọn để thực hiện:

```
SW1(config)#no ip dhcp snooping information option
```

### Kiểm tra:

Thực hiện kiểm tra các thông số của DHCP snooping trên switch:

```
SW1#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
DHCP snooping is operational on following VLANs:
10
Smartlog is configured on following VLANs:
none
Smartlog is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is disabled
  circuit-id default format: vlan-mod-port
    remote-id: a40c.c304.9d00 (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)
-----
FastEthernet0/11    yes         yes             unlimited
Custom circuit-ids:
```

Thực hiện chuyển R2 thành một client xin cấp phát IP từ DHCP server R1:

```
R2(config)#interface f0/0
R2(config-if)#no ip address
R2(config-if)#ip address dhcp
R2(config-if)#end
R2#
*May 13 07:27:30.763: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned DHCP
address 192.168.10.2, mask 255.255.255.0, hostname R2
```

Có thể thấy rằng R2 đã được cấp phát động địa chỉ IP 192.168.10.2/24.

Tính năng DHCP snooping bên cạnh chống giả mạo DHCP còn tiến hành theo dõi mọi gói tin DHCP đi ngang qua switch để xây dựng bảng DHCP snooping dùng cho các tính năng DAI và IP sourceguard. Thực hiện kiểm tra bảng DHCP snooping binding trên switch:

SW1#show ip dhcp snooping binding					
MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
-----	-----	-----	-----	-----	-----

```
00:00:11:11:22:22 192.168.10.2      86382      dhcp-snooping    10      FastEthernet0/12
Total number of bindings: 1
```

Từ kết quả show có thể thấy, switch đã giám sát được hoạt động cấp phát IP bằng DHCP cho các client. Với mỗi client, switch biết được rằng client có địa chỉ MAC là gì, được DHCP server cấp phát cho địa chỉ IP nào và đang được kết nối vào interface nào của VLAN 10. Ví dụ: hiện nay client với MAC 0000.1111.2222 kết nối vào cổng F0/12 thuộc VLAN 10 đã được cấp địa chỉ IP là 192.168.10.2.

Tiếp theo, thực hiện kiểm tra hoạt động chống tấn công giả mạo DHCP server của DHCP snooping bằng cách chuyển cổng F0/11 nối đến R1 thành untrusted port. Lúc này R1 sẽ bị coi là DHCP giả mạo và không thể cấp phát IP cho các end – user thuộc VLAN 10 được nữa.

Chuyển cổng F0/11 thành untrusted port:

```
SW1(config)#interface f0/11
SW1(config-if)#no ip dhcp snooping trust
```

R2 thực hiện xin cấp phát lại IP nhưng không còn xin được IP từ R1:

```
R2(config)#interface f0/0
R2(config-if)#no ip address
R2(config-if)#ip address dhcp
R2(config-if)#end

R2#show ip interface brief f0/0
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0     unassigned     YES  DHCP   up           up
```

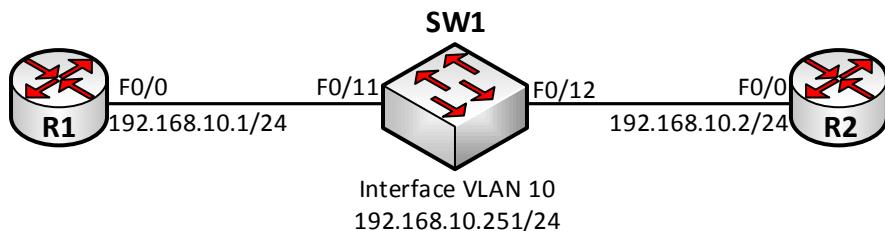
Chuyển lại F0/11 thành trusted port, R2 lại nhận được IP cấp phát tự động từ R1:

```
SW1(config)#interface f0/11
SW1(config-if)#ip dhcp snooping trust

R2#
*May 13 07:56:29.207: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned DHCP
address 192.168.10.2, mask 255.255.255.0, hostname R2
```

## Lab 20 – Storm Control

Sơ đồ:



Hình 20.1 – Sơ đồ bài lab.

Yêu cầu:

### 1. Cấu hình ban đầu:

- Trên SW1 tạo VLAN 10 và thực hiện gán tất cả các cổng Fast Ethernet của switch vào VLAN 10 vừa tạo.
- Thực hiện cấu hình các địa chỉ IP trên các interface của các thiết bị như được chỉ ra trên hình 20.1.

### 2. Storm – control:

- Cấu hình tính năng storm – control trên cổng F0/11 đảm bảo tốc độ gửi gói unicast vào cổng này không được vượt quá 100 gói/s.
- Cấu hình tính năng storm – control trên cổng F0/12 đảm bảo tốc độ gửi gói broadcast vào cổng này không được vượt quá 10 gói/s.
- Khi số lượng gói tin gửi vào trên cổng vượt quá số lượng cho phép, cổng sẽ bị shutdown.

### Cấu hình

Trên SW1:

```
SW1 (config) #interface f0/11
SW1 (config-if) #storm-control action shutdown
SW1 (config-if) #storm-control unicast level pps 100
SW1 (config-if) #exit

SW1 (config) #interface f0/12
SW1 (config-if) #storm-control action shutdown
SW1 (config-if) #storm-control broadcast level pps 10
SW1 (config-if) #exit
```

Tính năng Storm – control được sử dụng để giới hạn số lượng traffic unicast, multicast hoặc broadcast nhận được trên một cổng.

Tùy thuộc vào hệ điều hành được sử dụng, câu lệnh “storm-control” có thể sử dụng đơn vị là phần trăm băng thông trên cổng, pps (packets per second), bps (bits per second),... Khi cấu hình, có thể sử dụng dấu “?” trong câu lệnh để xác định xem những loại đơn vị nào có thể được sử dụng.

Bên cạnh đó, người quản trị có thể cấu hình hiệu chỉnh ứng xử trên cổng khi hạn mức dữ liệu trên cổng vượt quá mức độ được chỉ ra:

```
SW1(config-if)#storm-control action ?
  shutdown  Shutdown this interface if a storm occurs
  trap      Send SNMP trap if a storm occurs
```

Trong đó:

- shutdown: với tùy chọn này, cổng sẽ bị shutdown khi số lượng dữ liệu gửi vào cổng vượt quá định mức quy định.
  - trap: switch sẽ chỉ phát đi một trap SNMP cảnh báo đến thiết bị giám sát.

## Kiểm tra:

Kiểm tra kết quả cấu hình đã thực hiện:

```
SW1#show storm-control unicast
Interface Filter State    Upper          Lower          Current
----- -----
Fa0/11   Forwarding      100 pps       100 pps       0 pps

SW1#show storm-control broadcast
Interface Filter State    Upper          Lower          Current
----- -----
Fa0/12   Forwarding      10 pps        10 pps       0 pps
```

Thực hiện ping unicast tốc độ cao từ R1 để số lượng gói tin đi vào cổng F0/11 vượt quá 100 gói/s:

```
R1#ping 192.168.10.2 repeat 100000
Type escape sequence to abort.
Sending 100000, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!!! !!!!!!! !!!!!!! !!!!!!! !!!!!!! !!!!!!! !!!!!!! !!!!!!! !!!!!!! !!!!!!!
!!!!!! !!!!!!! !!!!!!! !!!!!!! !!!!!!! !!!!!!! !!!!!!! !!!!!!! !!!!!!! !!!!!!!
!!!!!! !!!!!!! !!!!!!! !!!!!!! !!!!!!! !!!!!!! !!!!!!! !!!!!!! !!!!!!! !!!!!!!
(...)
```

Khi số lượng gói tin đi vào cổng F0/11 vượt quá 100 gói/s, cổng sẽ bị đưa vào trạng thái err – disable và chuyển sang trạng thái down:

```
SW1#
*Mar 1 00:44:23.290: %PM-4-ERR_DISABLE: storm-control error detected on Fa0/11,
putting Fa0/11 in err-disable state
*Mar 1 00:44:23.290: %STORM_CONTROL-3-SHUTDOWN: A packet storm was detected on
Fa0/11. The interface has been disabled.
SW1#
*Mar 1 00:44:23.299: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/11, changed state to down
SW1#
*Mar 1 00:44:25.295: %LINK-3-UPDOWN: Interface FastEthernet0/11, changed state to
down
```

SW1#show storm-control unicast

Interface	Filter	State	Upper	Lower	Current
Fa0/11		Link Down	100 pps	100 pps	0 pps

Thực hiện ping broadcast số lượng lớn từ phía R2 để lưu lượng broadcast gửi vào cổng F0/12 của SW1 vượt quá 10 gói/s, có thể phải thực hiện điều này trong một khoảng thời gian khá dài:

R2#ping 255.255.255.255 repeat 1000 timeout 0

```
Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 255.255.255.255, timeout is 0 seconds:
..
Reply to request 2 from 192.168.10.1, 1 ms.
Reply to request 4 from 192.168.10.1, 1 ms...
Reply to request 8 from 192.168.10.1, 1 ms
Reply to request 8 from 192.168.10.251, 1 ms.
(...)
Reply to request 359 from 192.168.10.1, 1 ms...
Reply to request 363 from 192.168.10.1, 1 ms....
Reply to request 368 from 192.168.10.1, 4 ms...
Reply to request 372 from 192.168.10.1, 1 ms.....
```

Cổng F0/12 của SW1 bị đưa vào trạng thái err – disable và chuyển sang trạng thái down:

```
SW1#
*Mar 1 01:10:29.812: %PM-4-ERR_DISABLE: storm-control error detected on Fa0/12,
putting Fa0/12 in err-disable state
*Mar 1 01:10:29.812: %STORM_CONTROL-3-SHUTDOWN: A packet storm was detected on
Fa0/12. The interface has been disabled.
SW1#
*Mar 1 01:10:29.821: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/12, changed state to down
SW1#
*Mar 1 01:10:31.817: %LINK-3-UPDOWN: Interface FastEthernet0/12, changed state to
down

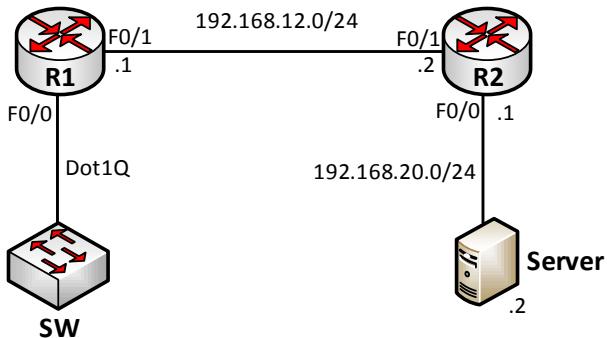
SW1#show storm-control broadcast
Interface Filter State Upper Lower Current
----- -----
Fa0/12 Link Down 10 pps 10 pps 0 pps
```

Sau khi kiểm tra xong, thực hiện reset các cổng F0/11 và F0/12 để trả các cổng này về lại trạng thái active:

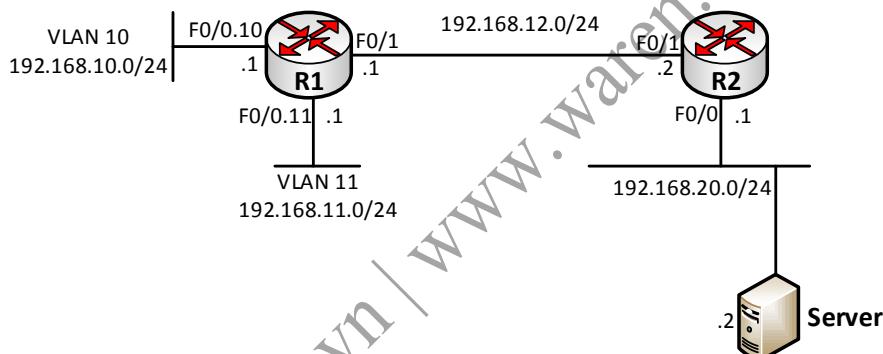
```
SW1(config)#interface range f0/11,f0/12
SW1(config-if-range)#shutdown
SW1(config-if-range)#no shutdown
```

## Lab 21 – Access Control Lists

Sơ đồ:



Hình 21.1 – Sơ đồ bài Lab



Hình 21.2 – Sơ đồ layer 3

Mô tả:

- Bài Lab gồm hai Router và một Switch được đấu nối với nhau như hình 21.1.
- Học viên sử dụng một PC đấu nối vào cổng F0/0 của R2 để giả lập một server.
- Trên sơ đồ này, học viên sẽ thực tập cấu hình các loại access – list đã được học trong chương trình.

Yêu cầu:

### 1. Cấu hình ban đầu:

- Thực hiện đặt IP trên các cổng Router và trên server như được chỉ ra trên các hình vẽ.
- Cấu hình các VLAN thích hợp và định tuyến VLAN trên R1 để có được sơ đồ lớp 3 như hình 21.2.
- Cấu hình định tuyến tĩnh đảm bảo mọi địa chỉ trên sơ đồ thấy nhau.
- Cấu hình telnet trên R2 với password telnet là “cisco”.

## 2. Cấu hình Standard ACL (1):

Viết một standard ACL trên R2 đáp ứng yêu cầu sau:

- Cấm các IP từ 192.168.10.32 đến 192.168.10.47 của mạng 192.168.10.0/24 đi đến server 192.168.20.2.
- Cấm các IP từ 192.168.11.224 đến 192.168.11.255 của mạng 192.168.11.0/24 đi đến server 192.168.20.2.
- Cho phép các IP khác được đi đến server 192.168.20.2/24.

## 3. Cấu hình Standard ACL (2):

- Viết một standard ACL khác trên R2 cấm các IP chẵn của mạng 192.168.10.0/24 và các IP lẻ của mạng 192.168.11.0/24 telnet vào R2.
- Cho phép các IP khác được telnet đến R2.

## 4. Cấu hình Extended ACL:

- Trên R1 viết một ACL chỉ cho phép lưu lượng HTTP được đi đến mạng 192.168.10.0/24.
- ACL này phải được đặt trên cổng F0/1 của R1 theo chiều in và không được ảnh hưởng tới lưu lượng đi tới mạng 192.168.11.0/24.

### Thực hiện:

#### Bước 1: Cấu hình ban đầu cho bài Lab

Học viên thực hiện cấu hình ban đầu theo yêu cầu đã được đặt ra:

- Đầu nối dây và đặt IP trên các cổng của các Router.
- Tạo VLAN 10, 11 trên SW, cấu hình đường trunk nối giữa SW và Router R1.
- Cấu hình R1 định tuyến giữa hai VLAN 10 và 11.
- Cấu hình định tuyến tĩnh trên R1 và R2.

#### Bước 2: Standard ACL (1)

### Cấu hình:

```
R2(config)#access-list 20 deny 192.168.10.32 0.0.0.15
R2(config)#access-list 20 deny 192.168.11.224 0.0.0.31
R2(config)#access-list 20 permit any

R2(config)#interface f0/0
R2(config-if)#ip access-group 20 out
```

### Kiểm tra:

Thực hiện đổi lại địa chỉ IP trên cổng F0/0.10 và F0/0.11 của Router R1 để thực hiện kiểm tra:

```
R1(config)#interface f0/0.10
R1(config-if)#ip address 192.168.10.33 255.255.255.0
R1(config)#interface f0/0.11
R1(config-if)#ip address 192.168.11.225 255.255.255.0
```

Khi sử dụng source là các địa chỉ này, R1 không đi đến được 192.168.20.2:

```
R1#ping 192.168.20.2 source 192.168.10.33
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.33
U.U.U
Success rate is 0 percent (0/5)

R1#ping 192.168.20.2 source 192.168.110.225
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.110.225
U.U.U
Success rate is 0 percent (0/5)
```

Thực hiện ping lại từ R1 nhưng sử dụng source IP trên cổng F0/1:

```
R1#ping 192.168.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/25/30ms
```

Ping diễn ra thành công.

### Bước 3: Standard ACL (2)

#### Cấu hình:

```
R2(config)#access-list 2 deny 192.168.10.0 0.0.0.254
R2(config)#access-list 2 deny 192.168.11.1 0.0.0.254
R2(config)#access-list 2 permit any
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#access-class 2 in
R2(config-line)#exit
```

#### Kiểm tra:

IP trên cổng F0/0.10 của R2 đang là 192.168.10.33, R1 có thể telnet được đến R2 với địa chỉ này:

```
R1#telnet 192.168.12.2 /source-interface f0/0.10
Trying 192.168.12.2 ... Open
```

User Access Verification

Password: **<- Nhập password là "cisco"**

R2>exit

[Connection to 192.168.12.2 closed by foreign host]

R1#

Đổi lại địa chỉ trên cổng F0/0.10 của R1 thành 192.168.10.2 – là một địa chỉ chẵn:

```
R1(config)#interface f0/0
R1(config-if)#ip address 192.168.10.2 255.255.255.0
```

R1 không thể telnet được vào R2 với source này nữa:

```
R1#telnet 192.168.12.2 /source-interface f0/0.10
Trying 192.168.12.2 ...
% Connection refused by remote host
```

Thực hiện kiểm tra tương tự với source IP lấy từ cổng F0/0.11

Với các địa chỉ khác, việc telnet đến R2 diễn ra bình thường:

```
R1#telnet 192.168.12.2
Trying 192.168.12.2 ... Open

User Access Verification

Password:
R2>exit

[Connection to 192.168.12.2 closed by foreign host]
R1#
```

Sau khi thực hiện các thao tác kiểm tra, trả lại IP của các cổng F0/0.10 và F0/0.11 của R1 đúng như sơ đồ:

```
R1(config)#interface f0/0.10
R1(config-if)#ip address 192.168.10.1 255.255.255.0

R1(config)#interface f0/0.11
R1(config-if)#ip address 192.168.11.1 255.255.255.0
```

#### Bước 4: Extended ACL

##### Cấu hình:

```
R1(config)#access-list 100 permit tcp any 192.168.10.0 0.0.0.255 eq 80
R1(config)#access-list 100 deny ip any 192.168.10.0 0.0.0.255
R1(config)#access-list 100 permit ip any any

R1(config)#interface f0/1
R1(config-if)#ip access-group 100 in
```

##### Kiểm tra:

Thực hiện cấu hình R1 thành HTTP server để kiểm tra:

```
R1(config)#ip http server
```

Thực hiện truy nhập bằng HTTP từ R2 đến một địa chỉ của mạng 192.168.10.0/24:

```
R2#telnet 192.168.10.1 80
Trying 192.168.10.1, 80 ... Open

exit
HTTP/1.1 400 Bad Request
Date: Fri, 01 Mar 2002 01:04:22 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request

[Connection to 192.168.10.1 closed by foreign host]
```

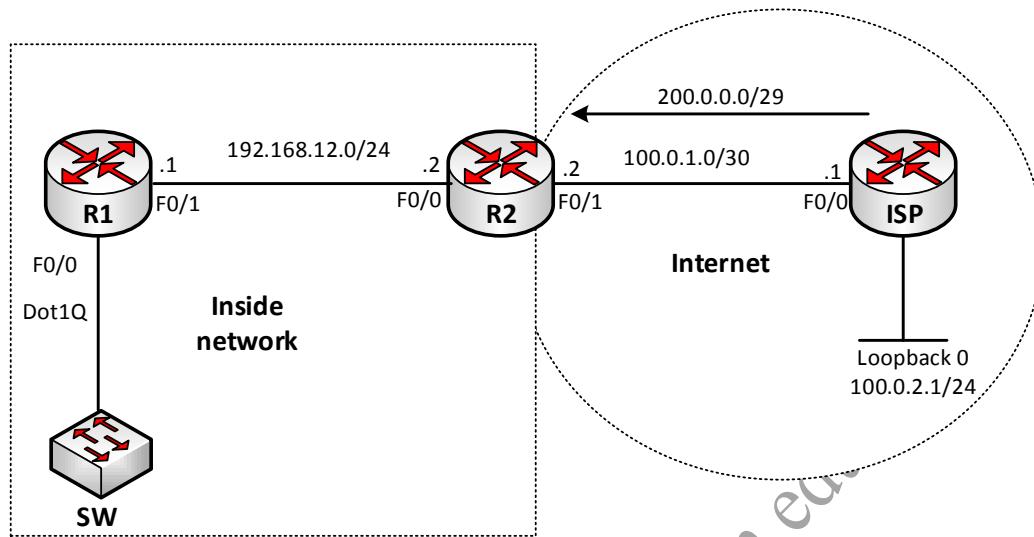
Việc truy nhập bằng HTTP đến mạng 192.168.10.0/24 đã diễn ra thành công.

Từ bên ngoài vẫn đi đến được mạng LAN 192.168.11.0/24:

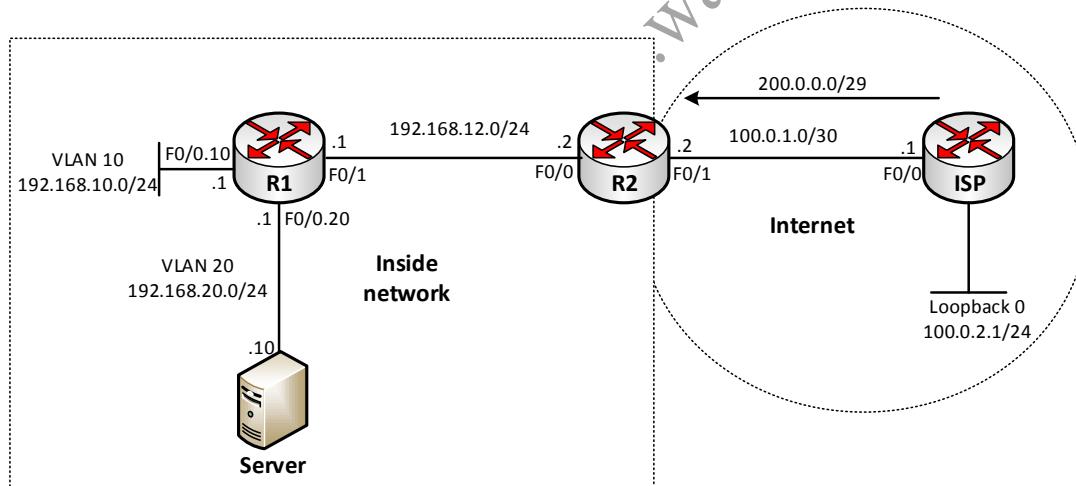
```
R2#ping 192.168.11.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/19/32ms
```

## Lab 22 – NAT & PAT

Sơ đồ:



Hình 22.1 – Sơ đồ bài Lab



Hình 22.2 – Sơ đồ layer 3

Mô tả:

- Bài Lab gồm 3 router: Router R1 và R2 giả lập các Router của một mạng doanh nghiệp và Router ISP giả lập môi trường Internet.
- Học viên thực hiện cấu hình NAT trên Router biên R2 để đảm bảo các địa chỉ IP Private của mạng doanh nghiệp có thể đi đến được các địa chỉ Public trên Internet.
- Học viên có thể sử dụng một PC cá nhân để giả lập server 192.168.20.10 trên hình 22.2.

**Yêu cầu:****1. Cấu hình ban đầu:**

- Học viên thực hiện đấu nối dây và đặt IP trên các thiết bị như hình 22.1.
- Trên Switch thực hiện cấu hình các VLAN thích hợp và cấu hình trunking giữa Switch và Router R1.
- Cấu hình R1 và R2 chạy một hình thức định tuyến bất kỳ đảm bảo mọi địa chỉ thấy nhau. ISP không chạy định tuyến với các Router R1 và R2.
- Cấu hình để ISP cấp về cho R2 dải IP 200.0.0.0/29.

**2. Cấu hình Static NAT:**

Thực hiện cấu hình Static NAT trên Router biên R2 đảm bảo các địa chỉ trên Internet có thể đi đến được server 192.168.20.10 của mạng bên trong thông qua IP Public 200.0.0.1.

**3. Cấu hình Dynamic NAT:**

- Cấu hình Dynamic NAT để các địa chỉ IP từ 192.168.10.1 đến 192.168.10.5 có thể đi được Internet.
- Các địa chỉ vừa nêu sử dụng các IP Public 200.0.0.2 đến 200.0.0.6 để đi ra bên ngoài.

**4. Cấu hình NAT overload:**

- Cấu hình để toàn bộ mạng 192.168.20.0/24 (ngoại trừ địa chỉ 192.168.20.10) sử dụng địa chỉ IP đấu nối Internet 100.0.1.2 của R2 để đi Internet.

**Thực hiện:****Bước 1: Cấu hình ban đầu**

Học viên thực hiện đấu nối dây và cấu hình trên các thiết bị theo yêu cầu đặt ra.

Để giả lập việc cấp phát dải IP 200.0.0.0/29 cho mô hình đang xét, sử dụng một static route trên Router ISP:

```
ISP(config)#ip route 200.0.0.0 255.255.255.248 100.0.1.2
```

Cấu hình default route từ R2 chỉ về Router ISP:

```
R2(config)#ip route 0.0.0.0 0.0.0.0 100.0.1.1
```

**Bước 2: Cấu hình Static NAT****Cấu hình:**

```
R2(config)#ip nat inside source static 192.168.20.10 200.0.0.1
R2(config)#interface f0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#interface f0/1
```

```
R2(config-if)#ip nat outside
R2(config-if)#exit
```

### Kiểm tra:

Bảng NAT của R2:

```
R2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 200.0.0.1          192.168.10.10    ---              ---
```

Từ server, có thể đi được Internet:

```
C:\>ping 100.0.2.1

Pinging 100.0.2.1 with 32 bytes of data:
Reply from 100.0.2.1: bytes=32 time=36ms TTL=253
Reply from 100.0.2.1: bytes=32 time=40ms TTL=253
Reply from 100.0.2.1: bytes=32 time=38ms TTL=253
Reply from 100.0.2.1: bytes=32 time=45ms TTL=253
```

Từ Internet, có thể đi đến được server thông qua địa chỉ 200.0.0.1 của:

```
ISP#ping 200.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 26/28/30ms
```

### Bước 3: Cấu hình Dynamic NAT

#### Cấu hình:

Trên R2:

```
R2(config)#access-list 1 permit 192.168.10.0 0.0.0.7
R2(config)#ip nat pool ABC 200.0.0.2 200.0.0.6 prefix-length 29
R2(config)#ip nat inside source list 1 pool ABC
```

### Kiểm tra:

Thực hiện ping đi Internet:

```
R1#ping 100.0.2.1 source 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.0.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/34/42ms
```

Bảng NAT trên R2:

```
R2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 200.0.0.2:3        192.168.10.1:3    100.0.2.1:3        100.0.2.1:3
```

---	200.0.0.2	192.168.10.1	---	---
---	200.0.0.1	192.168.10.10	---	---

Thay đổi địa chỉ IP trên cổng F0/0.10 của R1 để kiểm tra việc đi Internet của các địa chỉ khác:

```
R1(config)#interface f0/0.10
R1(config-if)#ip address 192.168.10.2 255.255.255.0
R1(config-if)#end
R1#ping 100.0.2.1 source 192.168.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.0.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/23/31ms

R1(config)#interface f0/0.10
R1(config-if)#ip address 192.168.10.3 255.255.255.0
R1(config-if)#end
R1#ping 100.0.2.1 source 192.168.10.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.0.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/30/34ms

R1(config)#interface f0/0.10
R1(config-if)#ip address 192.168.10.4 255.255.255.0
R1(config-if)#end
R1#ping 100.0.2.1 source 192.168.10.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.0.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.4
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/63/88ms

R1(config)#interface f0/0.10
R1(config-if)#ip address 192.168.10.5 255.255.255.0
R1(config-if)#end
R1#ping 100.0.2.1 source 192.168.10.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.0.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.5
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/38/42ms
```

Các địa chỉ trong dải IP được yêu cầu đã đi được Internet.

Bảng NAT của R2:

R2#show ip nat translations				
Pro	Inside global	Inside local	Outside local	Outside global
---	200.0.0.2	192.168.10.1	---	---
---	200.0.0.3	192.168.10.2	---	---

---	200.0.0.4	192.168.10.3	---	---
---	200.0.0.5	192.168.10.4	---	---
---	200.0.0.6	192.168.10.5	---	---
---	200.0.0.1	192.168.10.10	---	---

#### Bước 4: Cấu hình NAT overload

##### Cấu hình:

Trên R2:

```
R2(config)#access-list 2 deny 192.168.20.10 0.0.0.0
R2(config)#access-list 2 permit 192.168.20.0 0.0.0.255
R2(config)#ip nat inside source list 2 interface f0/1 overload
```

##### Kiểm tra:

Kiểm tra rằng các địa chỉ khác nhau thuộc mạng 192.168.2.0/24 đi được Internet:

```
R2#ping 100.0.2.1 source 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.0.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/49/84ms

R2(config)#interface f0/0.20
R2(config-if)#ip address 192.168.20.2 255.255.255.0
R2(config-if)#end
R2#ping 100.0.2.1 source 192.168.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.0.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.20.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 18/23/28ms

R2(config)#interface f0/0
R2(config-if)#ip address 192.168.20.3 255.255.255.0
R2(config-if)#end
R2#ping 100.0.2.1 source 192.168.20.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.0.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.20.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 22/39/62ms
```

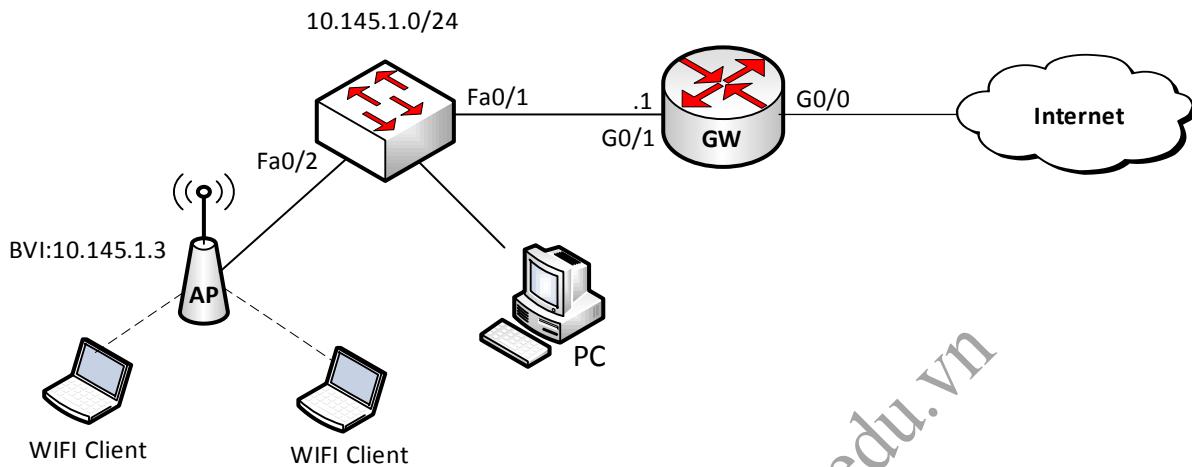
## Bảng NAT của R2:

<b>R2#show ip nat translations</b>				
Pro	Inside global	Inside local	Outside local	Outside global
---	200.0.0.2	192.168.1.1	---	---
---	200.0.0.3	192.168.1.2	---	---
---	200.0.0.4	192.168.1.3	---	---
---	200.0.0.5	192.168.1.4	---	---
---	200.0.0.6	192.168.1.5	---	---
icmp	100.0.1.2:7	192.168.20.1:7	100.0.2.1:7	100.0.2.1:7
icmp	100.0.1.2:8	192.168.20.2:8	100.0.2.1:8	100.0.2.1:8
icmp	100.0.1.2:9	192.168.20.3:9	100.0.2.1:9	100.0.2.1:9
---	200.0.0.1	192.168.10.10	---	---

# WIRELESS

## Lab 23 – Cấu hình Wireless AP với Single SSID

Sơ đồ:



Hình 23.1- Sơ đồ bài lab

Mô tả:

- Sơ đồ Lab gồm 1 Switch, 1 Router và 1 AP được đấu nối với nhau như hình 23.1.
- Trên sơ đồ này, học viên sẽ thực hiện cấu hình Cisco Wireless AP với 1 SSID.

Yêu cầu:

- Học viên thực hiện đấu nối các thiết bị, thực hiện một số cấu hình cơ bản trên Router và Switch.
- Cấu hình theo yêu cầu sau:
  - Tạo DHCP Pool trên Router GW để cấp địa chỉ IP cho người dùng
  - Cấu hình PAT trên Router GW để người dùng có thể truy cập được Internet
  - Tạo SSID trên với tên WAREN\_STAFF, dùng phương thức bảo vệ WPA2 và xác thực bằng PSK.

Cấu hình:

### 1. Cấu hình trên Router GW

Bước 1: Đặt địa chỉ IP cho cổng vật lý.

```

GW(config)#int gi0/0
GW(config-if)#ip add dhcp
GW(config)#int gi0/1
GW(config-if)#ip add 10.145.1.1 255.255.255.0
    
```

## Bước 2: Cấu hình PAT

```
GW(config)#access-list 1 permit 10.145.1.0 0.0.0.255
GW(config)#ip nat inside source list 1 int gi0/0 overload
GW(config)#int gi0/0
GW(config-if)#ip nat outside
GW(config)#int gi0/1
GW(config-subif)#ip nat inside
```

## Bước 3: Cấu hình DHCP Pool

```
GW(config)#ip dhcp excluded-address 10.145.1.1 10.145.1.4
GW(config)#ip dhcp pool LAB
GW(dhcp-config)#network 10.145.1.0 255.255.255.0
GW(dhcp-config)#default-router 10.145.1.1
GW(dhcp-config)#dns-server 8.8.8.8
```

## 2. Cấu hình trên Access-Point

### a. Cấu hình địa chỉ quản lý dùng CLI

Địa chỉ quản lý trên AP để cho phép thực hiện quản lý và cấu hình GUI

```
AP(config)#int bvi 1
AP(config-if)#ip add 10.145.1.3 255.255.255.0
```

### b. Cấu hình bằng giao diện GUI

Trước khi có thể cài đặt cấu hình cơ bản, AP và PC phải có địa chỉ IP

**Bước 1:** Mở trình duyệt trên PC và gõ địa chỉ của AP vào thanh tác vụ.

**Bước 2:** Gõ username *Cisco* và password *Cisco*



Hình 23.2 - Summary Status

**Bước 3:** Kích hoạt Radios Interface trên AP

Tại **NETWORK INTERFACES** chọn **Radio0-802.11G**, chọn tab **SETTINGS** sau đó chọn **Enable**.

Lưu ý: Lúc này trạng thái vẫn là Down do chưa có SSID được tạo.

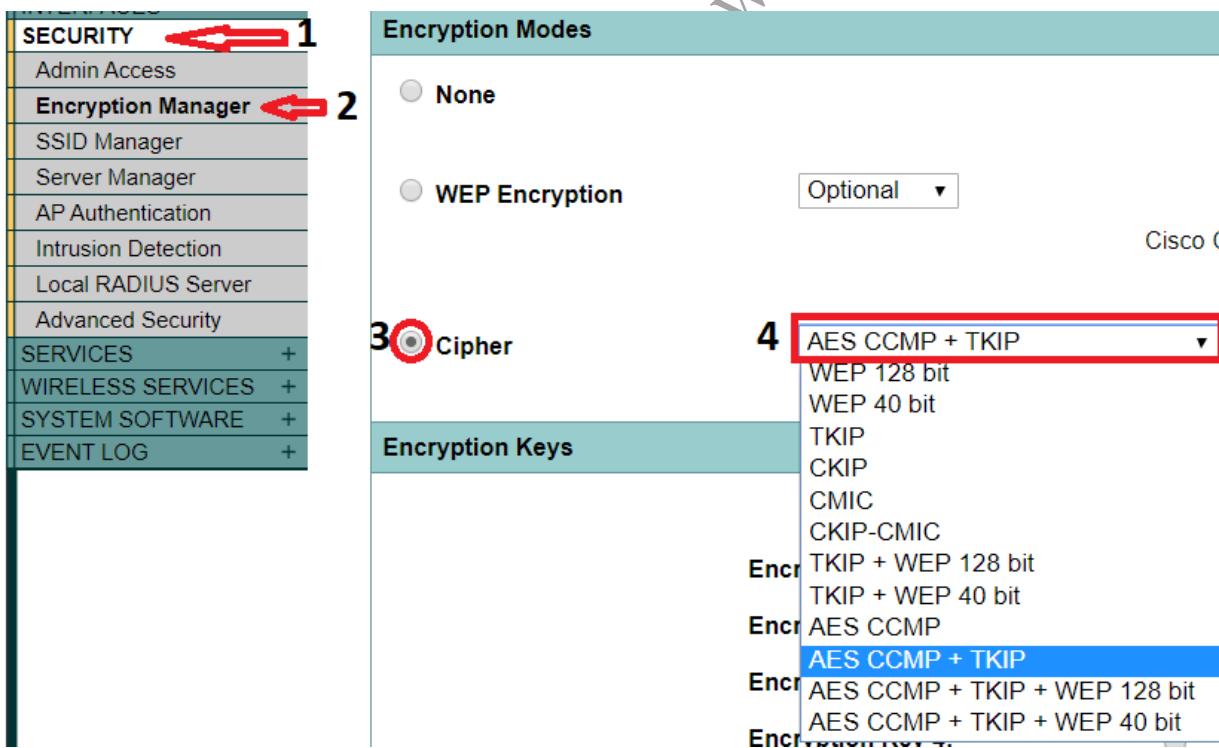


Hình 23.3 - Kích hoạt Radio Interface

#### Bước 4: Cấu hình tùy chọn bảo mật

##### Tại SECURITY chọn Encryption Manager

Chọn vào mục **Cipher**, sau đó chọn loại mã hóa. Loại mã hóa được sắp xếp theo mức độ an toàn, WEP bảo mật kém và AES CCMP bảo mật tốt nhất hiện tại nhưng chỉ có thể hỗ trợ các thiết bị sử dụng AES CCMP. Lựa chọn hỗ trợ TKIP để cho phép tương thích với thiết bị client không dây không hỗ trợ AES CCMP (hình 23.4).



Hình 23.4 - Encryption Manager

#### Bước 5: Thiết lập SSID mới:

Cũng trong **SECURITY** chọn **SSID Manager**, chọn **NEW** để tạo mới 1 SSID (hình 23.5).



Hình 23.5 - SSID Manager

#### Bước 6: Chọn phương thức xác thực.

Chọn Open Authentication (hình 23.6)

##### Client Authentication Settings

###### Methods Accepted:

- |  |                 |
|--|-----------------|
| <input checked="" type="checkbox"/> Open Authentication: | < NO ADDITION > |
| <input type="checkbox"/> Shared Authentication:          | < NO ADDITION > |
| <input type="checkbox"/> Network EAP:                    | < NO ADDITION > |

Hình 23.6: Client Authentication

#### Bước 7: Chọn phương thức bảo mật là WPA2 và xác định giá trị PSK (các thiết bị client không dây sẽ dùng giá trị này để xác thực với AP)(hình 23.7).

##### Client Authenticated Key Management

- |                     |                  |                               |  |  |
|---------------------|------------------|-------------------------------|--|--|
| Key Management:     | Mandatory        | <input type="checkbox"/> CCKM | <input checked="" type="checkbox"/> Enable WPA | WPAv2  |
| WPA Pre-shared Key: | •••••••••••••••• |                               |  | <input checked="" type="radio"/> ASCII <input type="radio"/> Hexadecimal |

Hình 23.7 - Client Authenticated Key Management

#### Bước 8: Broadcast SSID:

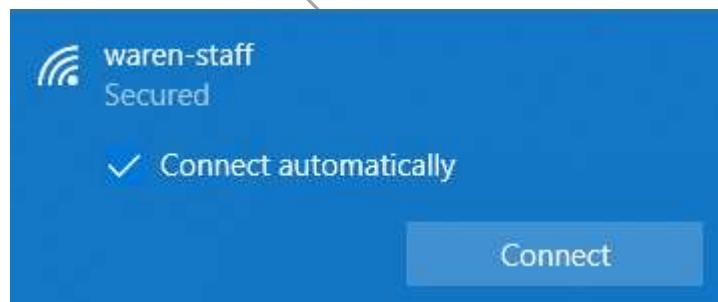
Tại mục Multiple BSSID Beacon, chọn Set SSID as Guest Mode và chọn tiếp Single BSSID trong mục Guest Mode/Infrastructure SSID Setting (hình 23.8)

Multiple BSSID Beacon Settings	
<b>Multiple BSSID Beacon</b> <input checked="" type="checkbox"/> Set SSID as Guest Mode	
<input type="checkbox"/> Set DataBeacon Rate (DTIM): <b>DISABLED</b> (1-100)	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
Guest Mode/Infrastructure SSID Settings	
Set Beacon Mode: <input checked="" type="radio"/> Single BSSID    Set Single Guest Mode SSID: <b>waren-staff</b> ▾	
<input type="radio"/> Multiple BSSID	
Set Infrastructure SSID: < NONE > ▾ <input type="checkbox"/> Force Infrastructure Devices to associate only to this SSID	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Hình 23.8 - BSSID Beacon Setting

### Kiểm tra

Thực hiện kết nối vào SSID: **waren-staff**, sau đó nhập PSK đã được định nghĩa trên AP (hình 23.9).



Hình 23.9

Sau khi kết nối thành công, máy tính sẽ nhận được IP từ DHCP Server.

```

SSID:      waren-staff
Protocol: 802.11g
Security type: WPA2-Personal
Network band: 2.4 GHz
Network channel: 12
IPv4 address: 10.145.1.5
IPv4 DNS servers: 8.8.8.8
               8.8.4.4
Manufacturer: Intel Corporation
Description: Intel(R) Wireless-AC 9560 160MHz
Driver version: 20.120.0.4
Physical address (MAC): A0-51-0B-D1-78-F1

```

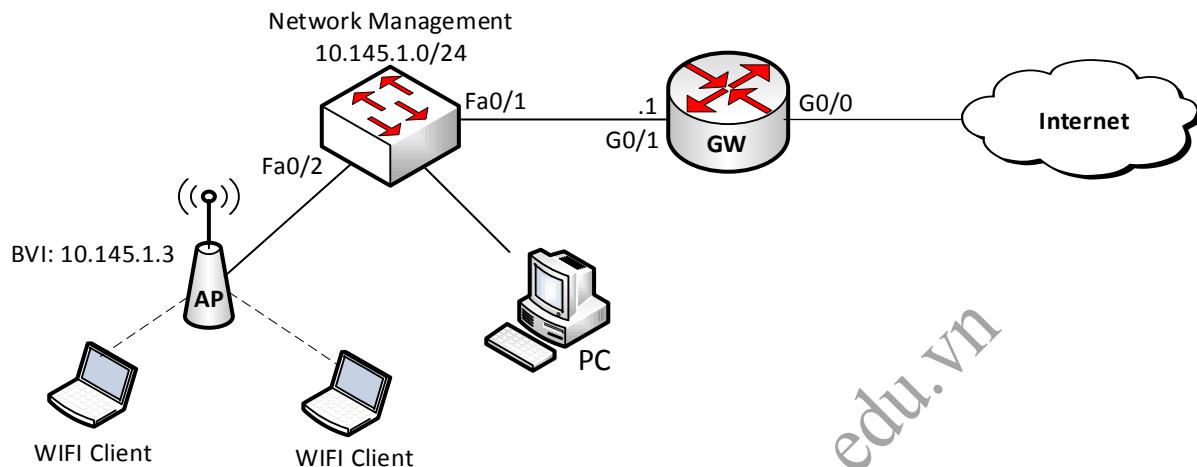
Có thể truy cập Internet thành công (hình 23.10):

```
Wireless LAN adapter Wi-Fi:  
  
    Connection-specific DNS Suffix . :  
    IPv4 Address . . . . . : 10.145.1.5  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . : 10.145.1.1  
  
C:\Users\Admin>ping waren.vn  
  
Pinging waren.vn [210.2.86.93] with 32 bytes of data:  
Reply from 210.2.86.93: bytes=32 time=3ms TTL=57  
Reply from 210.2.86.93: bytes=32 time=5ms TTL=57  
Reply from 210.2.86.93: bytes=32 time=7ms TTL=57  
Reply from 210.2.86.93: bytes=32 time=4ms TTL=57  
  
Ping statistics for 210.2.86.93:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 3ms, Maximum = 7ms, Average = 4ms
```

Hình 23.10

## Lab 24 – Cấu hình Wireless AP với Multiple SSID

### Sơ đồ



Hình 24.1 – Sơ đồ bài lab

### Mô tả:

- Sơ đồ Lab gồm 1 Switch, 1 Router và 1 AP được đấu nối với nhau như hình 24.1.
- Trên sơ đồ này, học viên sẽ thực hiện cấu hình Cisco Wireless AP với 2 SSID.

### Yêu cầu:

1. Học viên thực hiện đấu nối các thiết bị, thực hiện một số cấu hình cơ bản trên Router và Switch.
2. Cấu hình theo yêu cầu sau:
  - Tạo Vlan, cấu hình cổng trunk trên SW
  - Cấu hình IP và Sub-Interface trên Router GW
  - DHCP Pool trên Router GW để cấp địa chỉ IP cho người dùng
  - Cấu hình PAT trên Router GW để người dùng có thể truy cập được Internet
  - Tạo 2 SSID dùng phương thức bảo vệ WPA2 và xác thực bằng PSK.

SSID	VLAN	Network
	1 (Quản lý)	10.145.1.0/24
WAREN-GUEST	2	10.145.2.0/24
WAREN-STAFF	3	10.145.3.0/24

## Cấu hình:

### 1. Cấu hình trên Router GW

**Bước 1:** Đặt địa chỉ IP cho cổng vật lý.

```
GW(config)#int gi0/0
GW(config-if)#ip add dhcp
GW(config)#int gi0/1
GW(config-if)#ip add 10.145.1.1 255.255.255.0
GW(config)#int gi0/1.2
GW(config-subif)#encapsulation dot1Q 2
GW(config-subif)#ip add 10.145.2.1 255.255.255.0
GW(config)#int gi0/1.3
GW(config-subif)#encapsulation dot1Q 3
GW(config-subif)#ip add 10.145.3.1 255.255.255.0
```

**Bước 2: Cấu hình PAT**

```
GW(config)#access-list 1 permit 10.145.0.0 0.0.255.255
GW(config)#ip nat inside source list 1 int gi0/0 overload
GW(config)#int gi0/0
GW(config-if)#ip nat outside
GW(config)#int gi0/1
GW(config-subif)#ip nat inside
GW(config)#int gi0/1.2
GW(config-subif)#ip nat inside
GW(config)#int gi0/1.3
GW(config-subif)#ip nat inside
```

**Bước 3: Cấu hình DHCP Pool**

```
GW(config)#ip dhcp excluded-address 10.145.1.1 10.145.1.4
GW(config)#ip dhcp excluded-address 10.145.2.1 10.145.2.2
GW(config)#ip dhcp excluded-address 10.145.3.1 10.145.3.2
GW(config)#ip dhcp pool VLAN1
GW(dhcp-config)#network 10.145.1.0 255.255.255.0
GW(dhcp-config)#default-router 10.145.1.1
GW(dhcp-config)#dns-server 8.8.8.8
GW(config)#ip dhcp pool VLAN2
GW(dhcp-config)#network 10.145.2.0 255.255.255.0
GW(dhcp-config)#default-router 10.145.2.1
GW(dhcp-config)#dns-server 8.8.8.8
GW(config)#ip dhcp pool VLAN3
GW(dhcp-config)#network 10.145.3.0 255.255.255.0
GW(dhcp-config)#default-router 10.145.3.1
GW(dhcp-config)#dns-server 8.8.8.8
```

## 2. Cấu hình SW

```
Switch(config)#int f0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config)#int f0/2
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
```

## 3. Cấu hình trên Access-Point

### Cấu hình địa chỉ quản lý dùng CLI

Địa chỉ quản lý trên AP để cho phép thực hiện quản lý và cấu hình GUI

```
AP(config)#int bvi 1
AP(config-if)#ip add 10.145.1.3 255.255.255.0
```

### Cấu hình bằng giao diện GUI Express

Trước khi có thể cài đặt cấu hình cơ bản, AP và PC phải có địa chỉ IP

**Bước 1:** Mở trình duyệt trên PC và gõ địa chỉ của AP vào thanh tắc vụ.

**Bước 2:** Gõ username **Cisco** và password **Cisco**



Hình 24.2: Summary Status

**Bước 3:** Kích hoạt Radios Interface trên AP

Tại NETWORK INTERFACES chọn **Radio0-802.11G**, chọn tab SETTINGS sau đó chọn **Enable** (hình 24.3).

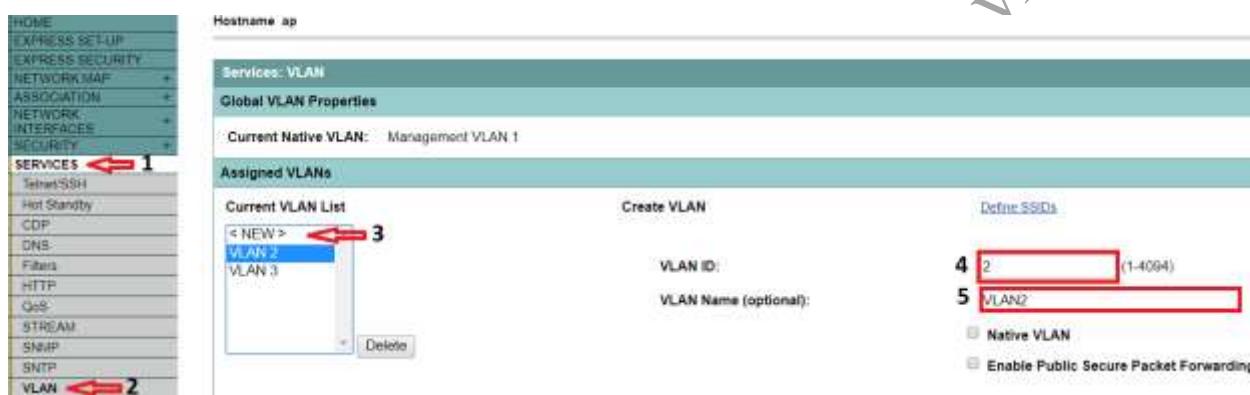
**Lưu ý:** Lúc này cổng vẫn sẽ bị Down vì chưa tạo SSID mới.



Hình 24.3 - Kích hoạt Radio Interface

#### Bước 4: Tạo VLAN

Trong mục **SERVICES** chọn **VLAN**, tiếp tục chọn **NEW**, nhập thông tin **VLAN ID** và **VLAN Name** (Hình 24.4).



Hình 24.4 - Tạo VLAN

#### Bước 5: Cấu hình tùy chọn bảo mật

Tại **SECURITY** chọn **Encryption Manager**, chọn tiếp **AES CCMP + TKIP** ở mục **Cipher** (Hình 24.5).



Hình 24.5 - Encryption Manager

### Bước 6: Tạo các SSID và gán VLAN tương ứng

Trong **SECURITY** chọn **SSID Manager** (hình 24.6):

- Chọn **NEW** để tạo mới 1 SSID
- SSID: Tên SSID
- VLAN: Gán SSID cho VLAN tạo ở bước trên



Hình 24.6 - SSID Manager

### Bước 7: Chọn phương thức xác thực

Tại mục **Client Authentication Setting**, chọn **Open Authentication** (hình 24.7).



Hình 24.7: Client Authentication

Tại mục **Client Authenticated Key Management** chọn **WPAv2** và xác định giá trị PSK cho mỗi SSID (hình 24.8).



Hình 24.8 - Client Authenticated Key Management

### Bước 8: Broadcast SSID

Tại mục **Multiple BSSID Beacon**, chọn **Set SSID as Guest Mode** (Hình 24.9).



Hình 24.9 - Multiple BSSID Beacon Settings

Sau đó tại mục **Guest Mode/Infrastructure SSID Settings**, chọn **Multiple BSSID**, để thiết lập chế độ Beacon dành cho nhiều SSID.

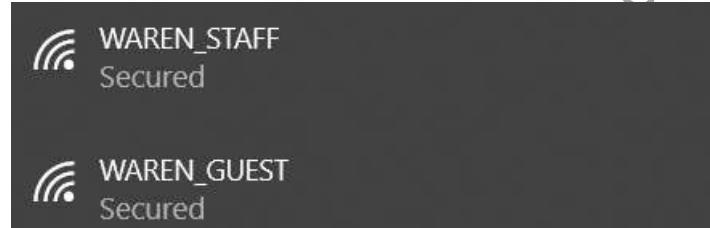


Hình 24.10 - Beacon Mode

Chọn **Apply** sau khi thiết lập cho từng SSID.

### Kiểm tra

Sau khi hoàn tất cấu hình, trên thiết bị Client không dây sẽ nhận được hai SSID (hình 24.11).



Hình 24.11

Địa chỉ IP được cấp khi kết nối vào SSID WAREN\_GUEST và ping thành công đến cisco.com.

SSID:	WAREN_GUEST
Protocol:	802.11g
Security type:	WPA2-Personal
Network band:	2.4 GHz
Network channel:	13
IPv4 address:	10.145.2.4
IPv4 DNS servers:	8.8.8.8 8.8.4.4

```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :
IPv4 Address . . . . . : 10.145.2.4
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.145.2.1

C:\Users\Admin>ping cisco.com

Pinging cisco.com [72.163.4.185] with 32 bytes of data:
Reply from 72.163.4.185: bytes=32 time=239ms TTL=236
Reply from 72.163.4.185: bytes=32 time=239ms TTL=236
Reply from 72.163.4.185: bytes=32 time=238ms TTL=236
Reply from 72.163.4.185: bytes=32 time=239ms TTL=236
```

Hình 24.12 – Kết nối thành công đến Cisco.com

Địa chỉ IP được cấp khi kết nối vào WAREN\_STAFF và ping thành công đến google.com

SSID:	WAREN_STAFF
Protocol:	802.11g
Security type:	WPA2-Personal
Network band:	2.4 GHz
Network channel:	13
IPv4 address:	10.145.3.3
IPv4 DNS servers:	8.8.8.8, 8.4.4

```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :
IPv4 Address . . . . . : 10.145.3.3
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.145.3.1

C:\Users\Admin>ping google.com

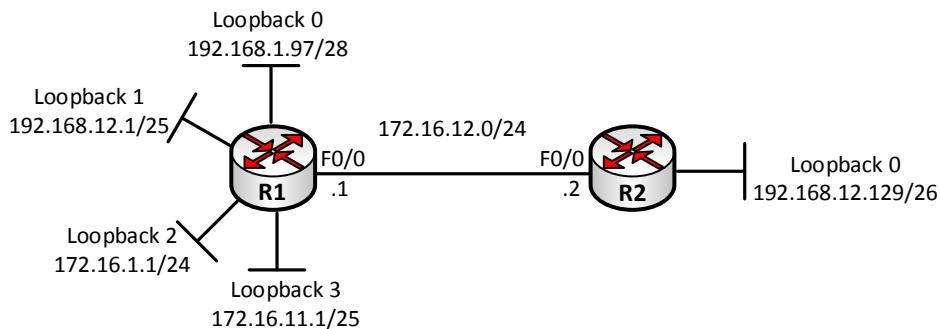
Pinging google.com [216.58.221.238] with 32 bytes of data:
Reply from 216.58.221.238: bytes=32 time=30ms TTL=55
Reply from 216.58.221.238: bytes=32 time=33ms TTL=55
Reply from 216.58.221.238: bytes=32 time=33ms TTL=55
Reply from 216.58.221.238: bytes=32 time=34ms TTL=55
```

Hình 24.13 – Kết nối thành công đến Google.com

# ROUTING

## Lab 25 – RIP

Sơ đồ:



Hình 25.1 - Sơ đồ bài Lab

Mô tả:

- Sơ đồ Lab gồm hai Router được đấu nối với nhau và đặt IP như hình vẽ.
- Trên sơ đồ này, học viên sẽ thực hiện khảo sát hoạt động của RIPv1 và RIPv2.

Yêu cầu:

1. Học viên đấu nối các thiết bị và đặt IP trên các interface như được chỉ ra trên sơ đồ.
2. Cấu hình các Router chạy định tuyến và thực hiện khảo sát hoạt động của RIPv1.
3. Cấu hình các Router chạy định tuyến và thực hiện khảo sát hoạt động của RIPv2.

Thực hiện:

**Bước 1:** Thiết lập cơ bản

Học viên thực hiện đấu nối dây và đặt địa chỉ IP trên các cổng Router như được chỉ ra trên hình 25.1.

**Bước 2:** Cấu hình và khảo sát hoạt động của RIPv1

Bật định tuyến RIPv1 trên các Router:

R1:

```

R1(config)#router rip
R1(config-router)#version 1
R1(config-router)#network 172.16.0.0
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.12.0
R1(config-router)#exit
  
```

R2:

```

R2(config)#router rip
R2(config-router)#version 1
R2(config-router)#network 172.16.0.0
R2(config-router)#network 192.168.12.0
  
```

```
R2 (config-router) #exit
```

Thực hiện lệnh “`debug ip rip`” trên các Router để quan sát hoạt động của RIP:

```
R1#debug ip rip
RIP protocol debugging is on

R2#debug ip rip
RIP protocol debugging is on
```

Quan sát thông tin về cập nhật định tuyến mà R1 gửi cho R2:

```
R1#
*Mar 1 00:07:40.975: RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0
(172.16.12.1)
*Mar 1 00:07:40.975: RIP: build update entries
*Mar 1 00:07:40.975: subnet 172.16.1.0 metric 1
*Mar 1 00:07:40.979: network 192.168.1.0 metric 1
*Mar 1 00:07:40.979: network 192.168.12.0 metric 1
```

Nhận xét về kết quả debug:

- R1 gửi cập nhật định tuyến cho láng giềng R2 bằng địa chỉ broadcast 255.255.255.255. Đây là địa chỉ được sử dụng mặc định cho hoạt động trao đổi thông tin của RIPv1.
- Các địa chỉ mạng được R1 gửi cho R2 đều không kèm theo subnet – mask. RIPv1 là một giao thức classful điển hình.
- Các subnet 192.168.1.96/28 trên loopback 0 và 192.168.12.0/25 trên loopback 1 được tự động tóm tắt về các mạng chính (major network hay classful network) 192.168.1.0 và 192.168.12.0 do các subnet này được R1 quảng bá đi qua một mạng chính khác (172.16.0.0/16). Hoạt động này được gọi là auto – summary.
- Các subnet 172.16.1.0/24 và 172.16.11.0/25 thuộc về cùng mạng chính với subnet 172.16.12.0/24 đầu nối giữa hai Router nên khi quảng bá qua R2 sẽ được R1 giữ nguyên địa chỉ mạng không auto – summary về mạng chính.

Tuy nhiên, trong hai subnet vừa nêu, chỉ subnet nào có subnet – mask giống với subnet – mask trên mạng đầu nối giữa R1 và R2 mới được quảng bá qua R2 nên trên kết quả debug chỉ thấy một subnet 172.16.1.0 của loopback 2 được quảng bá đi vì subnet này sử dụng subnet – mask 255.255.255.0 (/24) giống với subnet – mask của mạng 172.16.12.0 đầu nối giữa R1 và R2.

Quan sát hoạt động tiếp nhận cập nhật định tuyến RIPv1 trên Router R2:

```
R2#
*Mar 1 00:07:29.279: RIP: received v1 update from 172.16.12.1 on FastEthernet0/0
*Mar 1 00:07:29.279: 172.16.1.0 in 1 hops
*Mar 1 00:07:29.279: 192.168.1.0 in 1 hops
*Mar 1 00:07:29.283: 192.168.12.0 in 1 hops

R2#show ip route connected
```

```
192.168.12.0/26 is subnetted, 1 subnets
C      192.168.12.128 is directly connected, Loopback0
172.16.0.0/24 is subnetted, 2 subnets
C      172.16.12.0 is directly connected, FastEthernet0/0

R2#show ip route rip
172.16.0.0/24 is subnetted, 2 subnets
R      172.16.1.0 [120/1] via 172.16.12.1, 00:00:24, FastEthernet0/0
R      192.168.1.0/24 [120/1] via 172.16.12.1, 00:00:24, FastEthernet0/0
```

Nhận xét:

- R2 tiếp nhận được đầy đủ các địa chỉ mạng mà R1 đã quảng bá qua.
- Với các địa chỉ mạng nhận được mà là subnet, trong bài Lab này là 172.16.1.0, R2 sử dụng subnet – mask của mạng trên cổng tiếp nhận để gán cho chúng rồi đưa vào bảng định tuyến. Kết quả hiển thị trong bảng định tuyến cho thấy subnet 172.16.1.0 nhận được từ R1 được gán cho prefix – length là /24.
- Với các địa chỉ mạng nhận được mà là classful network, trong bài Lab này là 192.168.1.0, 192.168.12.0, R2 sẽ xem xét như sau:
  - Nếu trong bảng định tuyến tồn tại subnet của địa chỉ mạng nhận được, bỏ qua không cập nhật địa chỉ mạng này. Trong bài Lab này, địa chỉ mạng 192.168.12.0 mà R2 nhận được đã có một mạng con là 192.168.12.128/25 trong bảng định tuyến nên R2 sẽ bỏ qua không cập nhật route 192.168.12.0.
  - Nếu trong bảng định tuyến không tồn tại subnet nào của địa chỉ mạng nhận được, R2 sử dụng subnet – mask chuẩn của mạng classful lớp A, B hoặc C để gán cho các địa chỉ này rồi đưa chúng vào bảng định tuyến. Trong trường hợp bài Lab đang xét, R2 không có subnet nào của mạng 192.168.1.0 trong bảng định tuyến nên R2 sử dụng subnet – mask chuẩn lớp C là 255.255.255.0 (hay /24) cho mạng 192.168.1.0 rồi cài thông tin này vào bảng định tuyến.

Từ kết quả khảo sát ở trên có thể thấy được hai đặc điểm quan trọng của các giao thức định tuyến kiểu classful:

- Không gửi kèm theo subnet – mask trong các cập nhật định tuyến.
- Không hỗ trợ VLSM và mạng gián đoạn (discontiguous network).

### Bước 3: Cấu hình và khảo sát hoạt động của RIPv2

Thực hiện chuyển version của RIP trên các Router thành version 2:

```
R1(config)#router rip
R1(config-router)#version 2

R2(config)#router rip
R2(config-router)#version 2
```

Tiếp tục quan sát kết quả debug trên các router.

Trên R1:

R1#

```
*Mar 1 00:36:14.259: RIP: sending v2 update to 224.0.0.9 via FastEthernet0/0
(172.16.12.1)
*Mar 1 00:36:14.259: RIP: build update entries
*Mar 1 00:36:14.259: 172.16.1.0/24 via 0.0.0.0, metric 1, tag 0
*Mar 1 00:36:14.263: 172.16.11.0/25 via 0.0.0.0, metric 1, tag 0
*Mar 1 00:36:14.263: 192.168.1.0/24 via 0.0.0.0, metric 1, tag 0
*Mar 1 00:36:14.263: 192.168.12.0/24 via 0.0.0.0, metric 1, tag 0
```

Trên R2:

R2#

```
*Mar 1 00:36:02.515: RIP: received v2 update from 172.16.12.1 on FastEthernet0/0
*Mar 1 00:36:02.515: 172.16.1.0/24 via 0.0.0.0 in 1 hops
*Mar 1 00:36:02.515: 172.16.11.0/25 via 0.0.0.0 in 1 hops
*Mar 1 00:36:02.519: 192.168.1.0/24 via 0.0.0.0 in 1 hops
*Mar 1 00:36:02.519: 192.168.12.0/24 via 0.0.0.0 in 1 hops
```

Nhận xét:

- RIPv2 là một giao thức classless, các bản tin cập nhật đều bao gồm subnet – mask của các địa chỉ mạng được quảng bá.
- Luật auto – summary mặc định vẫn có tác dụng với RIPv2, các subnet 192.168.1.96/28 và 192.168.12.0/128 đều được summary về mạng chính khi được quảng bá qua biên giới của mạng chính khác.

Bảng định tuyến trên R2 cho các route RIP nhận được từ R1:

```
R2#show ip route rip
192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
R    192.168.12.0/24 [120/1] via 172.16.12.1, 00:00:14, FastEthernet0/0
172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
R    172.16.11.0/25 [120/1] via 172.16.12.1, 00:00:14, FastEthernet0/0
R    172.16.1.0/24 [120/1] via 172.16.12.1, 00:00:14, FastEthernet0/0
R    192.168.1.0/24 [120/1] via 172.16.12.1, 00:00:14, FastEthernet0/0
```

Để các subnet được quảng bá đúng giá trị của nó khi phải đi qua biên giới một mạng chính khác, cần phải thực hiện tắt auto – summary trên Router quảng bá. Thực hiện tắt trên R1:

```
R1(config)#router rip
R1(config-router)#no auto-summary
```

R2 sau đó, đã nhận được cập nhật chính xác về các subnet trên các loopback 0 và 1 của R1:

```
R2#show ip route rip
192.168.12.0/24 is variably subnetted, 3 subnets, 3 masks
R    192.168.12.0/25 [120/1] via 172.16.12.1, 00:00:02, FastEthernet0/0
R    192.168.12.0/24 [120/1] via 172.16.12.1, 00:00:29, FastEthernet0/0
```

```

172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
R      172.16.11.0/25 [120/1] via 172.16.12.1, 00:00:02, FastEthernet0/0
R      172.16.1.0/24 [120/1] via 172.16.12.1, 00:00:02, FastEthernet0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
R      192.168.1.96/28 [120/1] via 172.16.12.1, 00:00:02, FastEthernet0/0
R      192.168.1.0/24 [120/1] via 172.16.12.1, 00:00:29, FastEthernet0/0

```

Do ảnh hưởng của các timer được sử dụng bởi RIP, các địa chỉ classful 192.168.1.0/24 và 192.168.12.0/24 sẽ còn được giữ trong bảng định tuyến của R1 thêm một khoảng thời gian nữa (tối đa là 240s) rồi mới được xóa khỏi bảng định tuyến.

Kiểm tra rằng lúc này định tuyến đã thông suốt và các Router đã đi đến được các địa chỉ của nhau:

```

R1#ping 192.168.12.129
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.129, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/29/44ms

R2#ping 192.168.1.97
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.97, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/28/32ms

R2#ping 192.168.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/18/32ms

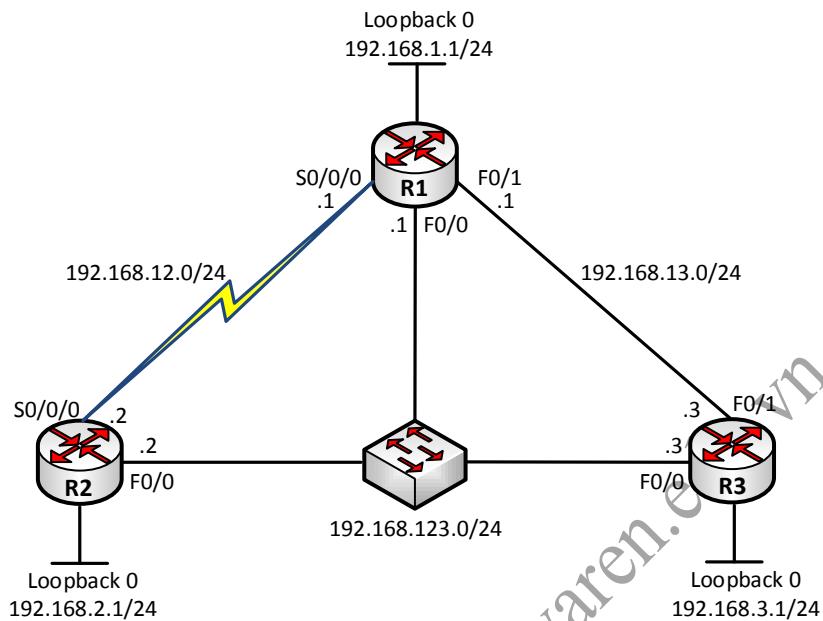
R2#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/29/36ms

R2#ping 172.16.11.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.11.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/23/32ms

```

## Lab 26 – OSPF

Sơ đồ:



Hình 26.1 – Sơ đồ bài Lab

Mô tả:

- Sơ đồ bài Lab gồm 3 Router và 1 Switch được đấu nối với nhau như hình 26.1.
- Trên sơ đồ này, học viên sẽ thực hiện chạy định tuyến OSPF đảm bảo mọi địa chỉ trên sơ đồ thấy nhau và khảo sát một vài đặc điểm hoạt động của OSPF.

Yêu cầu:

- Thực hiện đấu nối dây và đặt IP trên các thiết bị như được chỉ ra trên hình 26.1.
- Cấu hình định tuyến OSPF Area 0 trên các Router đảm bảo mọi địa chỉ IP trên sơ đồ thấy nhau.
- Hiệu chỉnh Router – ID của các Router như sau:  
R1: 1.1.1.1; R2: 2.2.2.2; R3: 3.3.3.3.
- Hiệu chỉnh bầu chọn DR và BDR theo yêu cầu sau:
  - Trên kết nối multiaccess giữa R1 – R2 – R3: R1 là DR, R2 là BDR và R3 là DROther.
  - Trên kết nối multiaccess giữa R1 và R3: đảm bảo R3 luôn là DR.
- Hiệu chỉnh cost trên các cổng thích hợp đảm bảo R2 đi đến loopback 0 của R1 chỉ theo đường Serial.

## Thực hiện:

### Bước 1: Kết nối thiết bị và đặt IP

Học viên thực hiện kết nối thiết bị và đặt IP theo sơ đồ hình 26.1.

### Bước 2: Cấu hình OSPF đơn vùng

#### Cấu hình:

R1:

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 192.168.12.0 0.0.0.255 area 0
R1(config-router)#network 192.168.13.0 0.0.0.255 area 0
R1(config-router)#network 192.168.123.0 0.0.0.255 area 0
R1(config-router)#exit
```

R2:

```
R2(config)#router ospf 1
R2(config-router)#network 192.168.2.0 0.0.0.255 area 0
R2(config-router)#network 192.168.12.0 0.0.0.255 area 0
R2(config-router)#network 192.168.123.0 0.0.0.255 area 0
R2(config-router)#exit
```

R3:

```
R3(config)#router ospf 1
R3(config-router)#network 192.168.3.0 0.0.0.255 area 0
R3(config-router)#network 192.168.13.0 0.0.0.255 area 0
R3(config-router)#network 192.168.123.0 0.0.0.255 area 0
R3(config-router)#exit
```

#### Kiểm tra:

Bảng neighbor của các router:

<b>R1#show ip ospf neighbor</b>					
Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.3.1	1	FULL/DR	00:00:32	192.168.13.3	FastEthernet0/1
192.168.2.1	1	FULL/BDR	00:00:34	192.168.123.2	FastEthernet0/0
192.168.3.1	1	FULL/DR	00:00:35	192.168.123.3	FastEthernet0/0
192.168.2.1	0	FULL/ -	00:00:30	192.168.12.2	Serial0/0/0

<b>R2#show ip ospf neighbor</b>					
Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.1	1	FULL/DROTHER	00:00:38	192.168.123.1	FastEthernet0/0
192.168.3.1	1	FULL/DR	00:00:31	192.168.123.3	FastEthernet0/0
192.168.1.1	0	FULL/ -	00:00:35	192.168.12.1	Serial0/0/0

<b>R3#show ip ospf neighbor</b>					
Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.1	1	FULL/DROTHER	00:00:35	192.168.123.1	FastEthernet0/0
192.168.2.1	1	FULL/BDR	00:00:36	192.168.123.2	FastEthernet0/0
192.168.1.1	1	FULL/BDR	00:00:36	192.168.13.1	FastEthernet0/1

## Bảng định tuyến của các router:

```
R1#show ip route ospf
 192.168.2.0/32 is subnetted, 1 subnets
O      192.168.2.1 [110/2] via 192.168.123.2, 00:09:33, FastEthernet0/0
 192.168.3.0/32 is subnetted, 1 subnets
O      192.168.3.1 [110/2] via 192.168.123.3, 00:09:33, FastEthernet0/0
                  [110/2] via 192.168.13.3, 00:08:25, FastEthernet0/1

R2#show ip route ospf
O      192.168.13.0/24 [110/2] via 192.168.123.3, 00:09:38, FastEthernet0/0
                  [110/2] via 192.168.123.1, 00:08:30, FastEthernet0/0
 192.168.1.0/32 is subnetted, 1 subnets
O      192.168.1.1 [110/2] via 192.168.123.1, 00:09:38, FastEthernet0/0
 192.168.3.0/32 is subnetted, 1 subnets
O      192.168.3.1 [110/2] via 192.168.123.3, 00:09:38, FastEthernet0/0

R3#show ip route ospf
O      192.168.12.0/24 [110/65] via 192.168.123.2, 00:09:42, FastEthernet0/0
                  [110/65] via 192.168.123.1, 00:09:42, FastEthernet0/0
                  [110/65] via 192.168.13.1, 00:08:34, FastEthernet0/1
 192.168.1.0/32 is subnetted, 1 subnets
O      192.168.1.1 [110/2] via 192.168.123.1, 00:09:42, FastEthernet0/0
                  [110/2] via 192.168.13.1, 00:08:34, FastEthernet0/1
 192.168.2.0/32 is subnetted, 1 subnets
O      192.168.2.1 [110/2] via 192.168.123.2, 00:09:42, FastEthernet0/0
```

## Bước 3: Hiệu chỉnh Router – ID

### Cấu hình:

R1:

```
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
Reload or use "clear ip ospf process" command, for this to take effect
R1(config-router)#end
R1#clear ip ospf process
Reset ALL OSPF processes? [no]: y
R1#
```

R2:

```
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
Reload or use "clear ip ospf process" command, for this to take effect
R2(config-router)#end
R2#clear ip ospf process
Reset ALL OSPF processes? [no]: y
R2#
```

R3:

```
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
Reload or use "clear ip ospf process" command, for this to take effect
R3(config-router)#end
R3#clear ip ospf process
Reset ALL OSPF processes? [no]: y
R3#
```

**Kiểm tra:**

```
R1#show ip ospf
Routing Process "ospf 1" with ID 1.1.1.1
(...)

R2#show ip ospf
Routing Process "ospf 1" with ID 2.2.2.2
(...)

R3#show ip ospf
Routing Process "ospf 1" with ID 3.3.3.3
(...)
```

**Bước 4:** Hiệu chỉnh bầu chọn DR/BDR

**Cấu hình:**

R1:

```
R1(config)#interface f0/0
R1(config-if)#ip ospf priority 255
R1(config)#interface f0/1
R1(config-if)#ip ospf priority 0
```

R2:

```
R2(config)#interface f0/0
R2(config-if)#ip ospf priority 254
```

**Kiểm tra:**

Do ảnh hưởng của luật non – preempt, để xúc tiến bầu chọn lại cho đúng kết quả yêu cầu, thực hiện reset tiến trình OSPF lần lượt trên R1, R2 và R3:

```
R1#clear ip ospf process
Reset ALL OSPF processes? [no]: y
R2#clear ip ospf process
Reset ALL OSPF processes? [no]: y
R3#clear ip ospf process
Reset ALL OSPF processes? [no]: y
```

Bảng neighbor trên 3 Router thể hiện kết quả bầu chọn:

R1#show ip ospf neighbor					
Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	1	FULL/DR	00:00:33	192.168.13.3	FastEthernet0/1
2.2.2.2	254	FULL/BDR	00:00:37	192.168.123.2	FastEthernet0/0
3.3.3.3	1	FULL/DROTHER	00:00:33	192.168.123.3	FastEthernet0/0
2.2.2.2	0	FULL/ -	00:00:37	192.168.12.2	Serial0/0/0

R2#show ip ospf neighbor					
Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.1.1	255	FULL/DR	00:00:35	192.168.123.1	FastEthernet0/0
3.3.3.3	1	FULL/DROTHER	00:00:38	192.168.123.3	FastEthernet0/0
1.1.1.1	0	FULL/ -	00:00:35	192.168.12.1	Serial0/0/0

R3#show ip ospf neighbor					
Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.1.1	255	FULL/DR	00:00:39	192.168.123.1	FastEthernet0/0
2.2.2.2	254	FULL/BDR	00:00:35	192.168.123.2	FastEthernet0/0
1.1.1.1	0	FULL/DROTHER	00:00:39	192.168.13.1	FastEthernet0/1

## Bước 5: Hiệu chỉnh cost

### Cấu hình:

```
R2(config)#interface s0/0/0
R2(config-if)#ip ospf cost 1
R2(config)#interface f0/0
R2(config-if)#ip ospf cost 2
```

### Kiểm tra:

Bảng định tuyến của R2 cho thấy đường đi đã được hiệu chỉnh lại theo yêu cầu:

R2#show ip route ospf					
O	192.168.13.0/24	[110/2]	via	192.168.12.1, 00:02:49,	Serial0/0/0
	192.168.1.0/32	is subnetted, 1 subnets			
O	192.168.1.1	[110/2]	via	192.168.12.1, 00:05:20,	Serial0/0/0
	192.168.3.0/32	is subnetted, 1 subnets			
O	192.168.3.1	[110/3]	via	192.168.123.3, 00:01:38,	FastEthernet0/0
				[110/3]	via 192.168.12.1, 00:01:38, Serial0/0/0

Traceroute từ R2 để xác nhận lộ trình đi đến loopback 0 của R1:

```
R2#traceroute 192.168.1.1

Type escape sequence to abort.
Tracing the route to 192.168.1.1

 1 192.168.12.1 28 msec 32 msec 28 msec
R2#
```

# **WAN – SERVICE – IPv6**

## Lab 27 – PPPoE

Sơ đồ:



Hình 27.1 – Sơ đồ bài Lab

Mô tả:

- Bài Lab gồm hai Router được kết nối với nhau như hình 27.1.
- Trong bài Lab này, học viên sẽ thực hiện cấu hình PPPoE với xác thực PAP.

Yêu cầu:

1. Học viên thực hiện đấu nối và cấu hình cơ bản như sơ đồ.
2. Thực hiện cấu hình PPPoE client với xác thực PAP
3. Cấu hình NAT đảm bảo mạng 1.1.1.1 ping thành công tới 8.8.8.8

Thực hiện:

Bước 1: Thiết lập ban đầu

Học viên thực hiện đấu nối giữa hai Router và và cấu hình cơ bản như hình 27.1.

Bước 2: PPPoE với xác thực PAP

Cấu hình:

Cấu hình PPPoE – Client:

```

PPPoE-Client(config)#interface dialer 0
PPPoE-Client(config-if)#encapsulation ppp ← Đóng gói PPP.
PPPoE-Client(config-if)#ip add negotiated ← Xin cấp ip tự động.
PPPoE-Client(config-if)#ppp pap sent-username user01 password waren01 ← Xác thực với pap.
PPPoE-Client(config-if)#dialer pool 1 ← Map vào interface vật lý.
PPPoE-Client(config-if)#exit
PPPoE-Client(config)#int g1
PPPoE-Client(config-if)#no shutdown
PPPoE-Client(config-if)#pppoe enable
PPPoE-Client(config-if)#pppoe-client dial-pool-number 1 ← Map với interface dialer được tạo ở trên.
  
```

Kiểm tra:

PPPoE-Client#sh ip int brief					
Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet1	unassigned	YES	unset	up	up
GigabitEthernet2	unassigned	YES	unset	administratively down	down
GigabitEthernet3	unassigned	YES	unset	administratively down	down
Dialer0	192.168.1.2	YES	IPCP	up	up
Virtual-Access1	unassigned	YES	unset	up	up
Virtual-Access2	unassigned	YES	manual	up	up

```

PPPoE-Client#sh pppoe session
  
```

1 client session

UniQ ID	PPPoE	RemMAC	Port	VA-st	VT	VA	Type	State
SID	LocMAC				Di0	Vi2		UP

N/A 1 000c.29fc.36fc Gil  
000c.29ab.74f5

Thiết lập session thành công tới PPPoE server và nhận được IP.

### Cấu hình PPPoE – Server (tham khảo):

```
PPPoE-Server(config-red) #bba-group pppoe warenprofile
PPPoE-Server(config-bba-group) # virtual-template 1
PPPoE-Server(config)#ip local pool pppoepool 192.168.1.2 192.168.1.254
PPPoE-Server(config)#username user01 password 0 waren01
PPPoE-Server(config)#interface Virtual-Template1
PPPoE-Server(config-if) # ip address 192.168.1.1 255.255.255.0
PPPoE-Server(config-if) # peer default ip address pool pppoepool
PPPoE-Server(config-if) # ppp authentication pap chap
PPPoE-Server(config-if) #interface GigabitEthernet1
PPPoE-Server(config-if) #no shutdown
PPPoE-Server(config-if) # pppoe enable group warenprofile
```

### Bước 3: Cấu hình NAT

#### NAT trên PPPoE – Client:

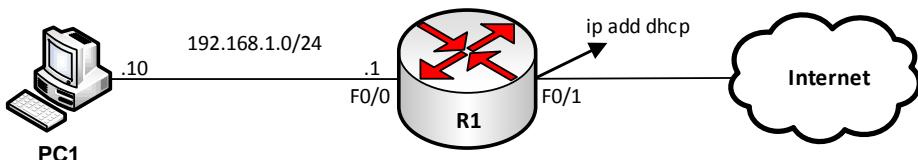
```
PPPoE-Client(config)#ip route 0.0.0.0 0.0.0.0 dialer 0
PPPoE-Client(config)#int dialer 0
PPPoE-Client(config-if) #ip nat out
PPPoE-Client(config-if) #int lo 0
PPPoE-Client(config-if) #ip add 1.1.1.1 255.255.255.0
PPPoE-Client(config-if) #ip nat inside
PPPoE-Client(config-if) #ex
PPPoE-Client(config)#access-list 1 permit 1.1.1.0 0.0.0.255
PPPoE-Client(config)#ip nat inside source list 1 interface dialer 0 overload
```

#### Kiểm tra:

```
PPPoE-Client#ping 8.8.8.8 source lo 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/5ms
PPPoE-Client#sh ip nat translations
Pro Inside global           Inside local          Outside local        Outside global
icmp 192.168.1.2:1         1.1.1.1:3           8.8.8.8:3          8.8.8.8:1
Total number of translations: 1
```

## Lab 28 – Syslog, NTP

Sơ đồ:



Hình 28.1 – Sơ đồ bài Lab

Mô tả:

- Bài Lab gồm 1 Router và 1 PC được đấu nối với nhau như hình 28.1. Router R1 có thêm một kết nối đi Internet.
- Trong bài Lab này học viên sẽ thực hiện cấu hình khảo sát hai kỹ thuật quan trọng trong quản lý mạng: Syslog và NTP.

Yêu cầu:

- Học viên thực hiện đấu nối các thiết bị, thực hiện một số cấu hình cơ bản.
- Cấu hình Syslog đưa thông tin log về Server lưu trữ, trong bài Lab này PC1 được sử dụng để làm Syslog server.
- Cấu hình Router làm NTP client đồng bộ thời gian với một NTP server trên Internet. Trong bài Lab này, học viên sử dụng NTP server có tên miền là “vn.pool.ntp.org”.

Thực hiện:

**Bước 1:** Kết nối và cấu hình cơ bản

Học viên thực hiện kết nối thiết bị và cấu hình cơ bản trên các thiết bị theo yêu cầu đặt ra.

**Bước 2:** Cấu hình Syslog

Bật tính năng logging:

```
R1(config)#logging on
```

Cấu hình địa chỉ syslog server mà các thông điệp syslog sẽ được gửi đến:

```
R1(config)#logging host 192.168.1.10
```

Chọn loại syslog sẽ được gửi:

```
R1(config)#logging trap debugging
```

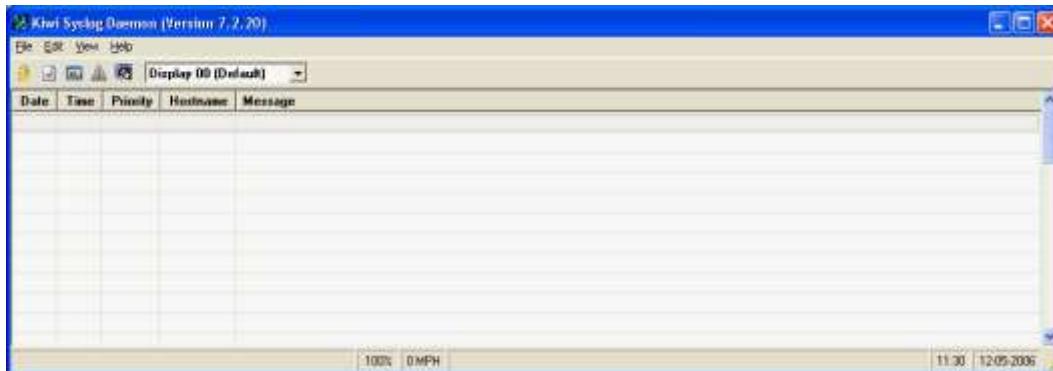
Mặc định, các thông điệp log sẽ không có nhãn thời gian. Nếu muốn gán thêm nhãn thời gian cho từng dòng log, thêm vào các lệnh sau:

```
R1(config)#service timestamps debug datetime localtime show-timezone msec
R1(config)#service timestamps log datetime localtime show-timezone msec
```

Các thông số của lệnh:

- debug: tất cả các thông tin debug sẽ được gán nhãn thời gian.
- log: tất cả các thông tin log sẽ được gán nhãn thời gian.
- datetime: ngày và giờ sẽ hiện trong thông điệp.
- localtime: thời gian được dùng là local.
- show-timezone: chỉ ra timezone.
- msec: thời gian chính xác đến từng mili giây.

Chạy phần mềm Kiwi Syslog Daemon, giao diện của chương trình (hình 28.2):



Hình 28.2 – Giao diện của chương trình Kiwi

Các thông điệp log (log message) của Router sẽ được gửi đến và xuất hiện trên cửa sổ phần mềm Kiwi Syslog Daemon của Syslog server.

### Bước 3: Cấu hình NTP client

Kiểm tra đảm bảo Router đi ra được internet:

```
Router#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/37/40ms
```

Thiết lập kết nối tới NTP server:

```
Router(config)#ip name-server 8.8.8.8
Router(config)#ntp server vn.pool.ntp.org
Translating "vn.pool.ntp.org"...domain server (192.168.4.6) (8.8.8.8) [OK]
```

Kiểm tra đồng bộ:

```
Router#show ntp status
Clock is synchronized, stratum 5, reference is 220.231.122.105
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
reference time is D9E1B0CB.58748896 (09:52:11.345 UTC Mon Nov 2 2018)
clock offset is -0.6651 msec, root delay is 366.35 msec
root dispersion is 92.30 msec, peer dispersion is 0.21 msec
```

Kiểm tra đồng hồ hệ thống trên Router:

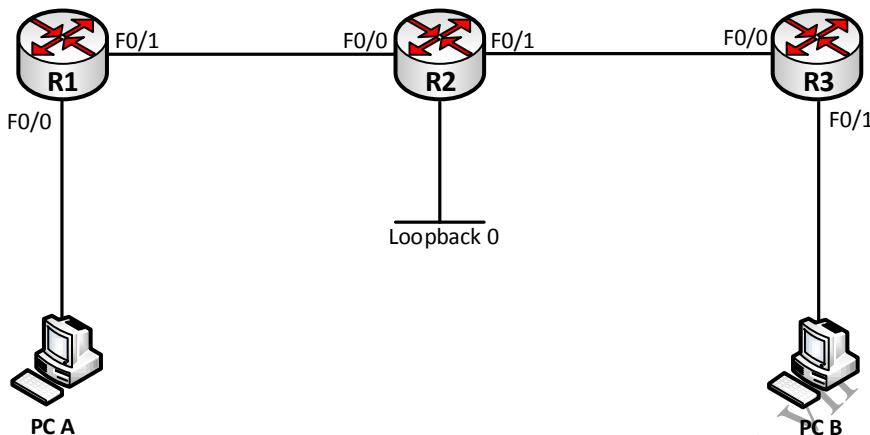
```
Router#show clock
09:53:17.485 UTC Mon Nov 2 2018
```

Hiệu chỉnh lại múi giờ theo múi giờ Việt Nam là UTC +7:

```
Router(config)#clock time zone +7
Nov  2 09:53:26.709: %SYS-6-CLOCKUPDATE: System clock has been updated from 09:53:26
UTC Mon Nov 2 2018 to 16:53:26 zone Mon Nov 2 2018, configured from console
Nov  2 09:53:27.913: %SYS-5-CONFIG_I: Configured from console by console
Router#show clock
16:53:34.461 zone Mon Nov 2 2018
```

## Lab 29 – Định tuyến IPv6

Sơ đồ:



Hình 29.1 – Sơ đồ bài Lab

Mô tả:

- Sơ đồ Lab gồm 3 Router đấu nối với nhau như hình 29.1.
- Trên sơ đồ này, học viên sẽ thực tập cấu hình định tuyến IPv6 đảm bảo các PC có thể ping được thấy nhau.
- Quy hoạch IP trên các cổng mạng của các thiết bị được chỉ ra theo bảng 1 dưới đây:

R1	Fa0/0: 2001:1::1/64
	Fa0/1: 2001:12::1/64
R2	Fa0/0: 2001:12::2/64
	Fa0/1: 2001:23::2/64
R3	Loopback 0: 2001:2::1/64
	Fa0/0: 2001:23::3/64
PC A	Fa0/1: 2001:3::1/64
	2001:1::2/64
PC B	2001:3::2/64

Bảng 1 – Quy hoạch IP cho sơ đồ Lab

Yêu cầu:

1. Học viên thực hiện đấu nối các thiết bị và đặt hostname cho các thiết bị như được chỉ ra trên hình 29.1.
2. Cấu hình các địa chỉ IPv6 trên các thiết bị theo quy hoạch IP được chỉ ra trên bảng 1.

3. Cấu hình định tuyến tĩnh đảm bảo các địa chỉ IPv6 đã cấu hình có thể đi đến được nhau.
4. Sau khi kiểm tra, gỡ bỏ cấu hình static route đã thực hiện ở yêu cầu 3, cấu hình định tuyến RIPng đảm bảo mọi địa chỉ thấy nhau.
5. Sau khi kiểm tra, gỡ bỏ cấu hình RIPng đã thực hiện ở yêu cầu 4, cấu hình định tuyến OSPFv3 đảm bảo mọi địa chỉ thấy nhau.

**Thực hiện:****Bước 1: Kết nối và cấu hình cơ bản**

Học viên thực hiện đấu nối dây giữa các thiết bị và đặt hostname cho các Router theo như sơ đồ hình 29.1.

**Bước 2: Cấu hình đặt địa chỉ IPv6**

Cấu hình chức năng định tuyến IPv6 và cấu hình IP các cổng giao tiếp trên các router.

```
R1(config)# ipv6 unicast-routing
R1(config)# int f0/0
R1(config-if)# ipv6 address 2001:1::1/64
R1(config)# int f0/1
R1(config-if)# ipv6 address 2001:12::1/64
R1(config-if)# exit

R2(config)# ipv6 unicast-routing
R2(config)# int f0/0
R2(config-if)# ipv6 address 2001:12::2/64
R2(config)# int f0/1
R2(config-if)# ipv6 address 2001:23::2/64
R2(config)# int loopback 0
R2(config-if)# ipv6 address 2001:2::2/64

R3(config)# ipv6 unicast-routing
R3(config)# int f0/0
R3(config-if)# ipv6 address 2001:23::3/64
R3(config)# int f0/1
R3(config-if)# ipv6 address 2001:3::1/64
```

**Bước 3: Cấu hình Static Route IPv6 trên các Router****Cấu hình:**

```
R1(config)# ipv6 route 2001:23::/64 2001:12::2
R1(config)# ipv6 route 2001:3::/64 2001:12::2
R1(config)# ipv6 route 2001:2::/64 2001:12::2

R2(config)# ipv6 route 2001:1::/64 2001:12::1
R2(config)# ipv6 route 2001:3::/64 2001:23::3

R3(config)# ipv6 route 2001:1::/64 2001:23::2
R3(config)# ipv6 route 2001:12::/64 2001:23::2
```

```
R3(config)# ipv6 route 2001:2::/64 2001:23::2
```

### Kiểm tra:

```
R1#show ipv6 route
(...)
C  2001:1::/64 [0/0]
    via ::, FastEthernet0/0
L  2001:1::1/128 [0/0]
    via ::, FastEthernet0/0
S  2001:2::/64 [1/0]
    via 2001:12::2
S  2001:3::/64 [1/0]
    via 2001:12::2
C  2001:12::/64 [0/0]
    via ::, FastEthernet0/1
L  2001:12::1/128 [0/0]
    via ::, FastEthernet0/1
S  2001:23::/64 [1/0]
    via 2001:12::2
L  FF00::/8 [0/0]
    via ::, Null0

R2# show ipv6 route
(...)
S  2001:1::/64 [1/0]
    via 2001:12::1
C  2001:2::/64 [0/0]
    via ::, Loopback0
L  2001:2::2/128 [0/0]
    via ::, Loopback0
S  2001:3::/64 [1/0]
    via 2001:23::3
C  2001:12::/64 [0/0]
    via ::, FastEthernet0/0
L  2001:12::2/128 [0/0]
    via ::, FastEthernet0/0
C  2001:23::/64 [0/0]
    via ::, FastEthernet0/1
L  2001:23::2/128 [0/0]
    via ::, FastEthernet0/1
L  FF00::/8 [0/0]
    via ::, Null0

R3#show ipv6 route
(...)
S  2001:1::/64 [1/0]
    via 2001:23::2
S  2001:2::/64 [1/0]
    via 2001:23::2
C  2001:3::/64 [0/0]
    via ::, FastEthernet0/1
```

```

L 2001:3::1/128 [0/0]
  via ::, FastEthernet0/1
s 2001:12::/64 [1/0]
  via 2001:23::2
C 2001:23::/64 [0/0]
  via ::, FastEthernet0/0
L 2001:23::3/128 [0/0]
  via ::, FastEthernet0/0
L FF00::/8 [0/0]
  via ::, Null0

```

Thực hiện ping kiểm tra từ PCA đến PCB (hình 29.2):

```

PC>ping 2001:3::2
Pinging 2001:3::2 with 32 bytes of data:

Reply from 2001:3::2: bytes=32 time=0ms TTL=125
Reply from 2001:3::2: bytes=32 time=0ms TTL=125
Reply from 2001:3::2: bytes=32 time=6ms TTL=125
Reply from 2001:3::2: bytes=32 time=1ms TTL=125

Ping statistics for 2001:3::2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms

PC>

```

Hình 29.2 – PCA ping kiểm tra PCB với Static Route

#### Bước 4: Cấu hình RIPng

##### Cấu hình:

Gỡ bỏ cấu hình Static Route trên các Router:

```

R1(config)#no ipv6 route 2001:23::/64 2001:12::2
R1(config)#no ipv6 route 2001:3::/64 2001:12::2
R1(config)#no ipv6 route 2001:2::/64 2001:12::2
R2(config)#no ipv6 route 2001:1::/64 2001:12::1
R2(config)#no ipv6 route 2001:3::/64 2001:23::3
R3(config)#no ipv6 route 2001:1::/64 2001:23::2
R3(config)#no ipv6 route 2001:12::/64 2001:23::2
R3(config)#no ipv6 route 2001:2::/64 2001:23::2

```

##### Cấu hình định tuyến RIPng:

```

R1(config)# interface f0/0
R1(config-if)# ipv6 rip RIP enable
R1(config-if)# exit
R1(config)# interface f0/1
R1(config-if)# ipv6 rip RIP enable
R1(config-if)# exit

R2(config)# interface f0/0
R2(config-if)# ipv6 rip RIP enable
R2(config-if)# exit

```

```
R2(config)# interface f0/1
R2(config-if)# ipv6 rip RIP enable
R2(config-if)# exit
R2(config)# interface loopback 0
R2(config-if)# ipv6 rip RIP enable
R2(config-if)# exit

R3(config)# interface f0/0
R3(config-if)# ipv6 rip RIP enable
R3(config-if)# exit
R3(config)# interface f0/1
R3(config-if)# ipv6 rip RIP enable
R3(config-if)# exit
```

### Kiểm tra:

Kiểm tra bảng định tuyến trên các Router:

```
R1# show ipv6 route
(...)
C 2001:1::/64 [0/0]
    via ::, FastEthernet0/0
L 2001:1::1/128 [0/0]
    via ::, FastEthernet0/0
R 2001:2::/64 [120/2]
    via FE80::230:A3FF:FE8D:401, FastEthernet0/1
R 2001:3::/64 [120/3]
    via FE80::230:A3FF:FE8D:401, FastEthernet0/1
C 2001:12::/64 [0/0]
    via ::, FastEthernet0/1
L 2001:12::1/128 [0/0]
    via ::, FastEthernet0/1
R 2001:23::/64 [120/2]
    via FE80::230:A3FF:FE8D:401, FastEthernet0/1
L FF00::/8 [0/0]
    via ::, Null0

R2# show ipv6 route
(...)
R 2001:1::/64 [120/2]
    via FE80::260:5CFF:FEA2:4B02, FastEthernet0/0
C 2001:2::/64 [0/0]
    via ::, Loopback0
L 2001:2::2/128 [0/0]
    via ::, Loopback0
R 2001:3::/64 [120/2]
    via FE80::20D:BDFF:FEB6:501, FastEthernet0/1
C 2001:12::/64 [0/0]
    via ::, FastEthernet0/0
L 2001:12::2/128 [0/0]
    via ::, FastEthernet0/0
C 2001:23::/64 [0/0]
    via ::, FastEthernet0/1
L 2001:23::2/128 [0/0]
    via ::, FastEthernet0/1
L FF00::/8 [0/0]
```

```

    via ::, Null0

R3#show ipv6 route
(...)
R  2001:1::/64 [120/3]
    via FE80::230:A3FF:FE8D:402, FastEthernet0/0
R  2001:2::/64 [120/2]
    via FE80::230:A3FF:FE8D:402, FastEthernet0/0
C  2001:3::/64 [0/0]
    via ::, FastEthernet0/1
L  2001:3::1/128 [0/0]
    via ::, FastEthernet0/1
R  2001:12::/64 [120/2]
    via FE80::230:A3FF:FE8D:402, FastEthernet0/0
C  2001:23::/64 [0/0]
    via ::, FastEthernet0/0
L  2001:23::3/128 [0/0]
    via ::, FastEthernet0/0
L  FF00::/8 [0/0]
    via ::, Null0

```

Ping kiểm tra từ PCA tới PCB (hình 29.3):

```

PC>ping 2001:3::2
Pinging 2001:3::2 with 32 bytes of data:
Reply from 2001:3::2: bytes=32 time=0ms TTL=125
Reply from 2001:3::2: bytes=32 time=0ms TTL=125
Reply from 2001:3::2: bytes=32 time=6ms TTL=125
Reply from 2001:3::2: bytes=32 time=1ms TTL=125

Ping statistics for 2001:3::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms
PC>

```

Hình 29.3 – Ping kiểm tra từ PCA đến PCB với định tuyến RIPng

### Bước 5: Cấu hình OSPFv3 trên các Router

#### Cấu hình:

Gỡ bỏ cấu hình RIPng trên các Router:

```
R1-2-3(config)#no ipv6 Router rip RIP
```

#### Cấu hình định tuyến OSPFv3:

```

R1(config)# ipv6 Router ospf 1
R1(config-rtr)# router-id 0.0.0.1
R1(config-rtr)# exit
R1(config)# interface f0/0
R1(config-if)# ipv6 ospf 1 area 0
R1(config-if)# exit
R1(config)# interface f0/1
R1(config-if)# ipv6 ospf 1 area 0
R1(config-if)# exit

```

```
R2(config)# ipv6 Router ospf 1
R2(config-rtr)# router-id 0.0.0.2
R2(config-rtr)# exit
R2(config)# interface f0/0
R2(config-if)# ipv6 ospf 1 area 0
R2(config-if)# exit
R2(config)# interface f0/1
R2(config-if)# ipv6 ospf 1 area 0
R2(config-if)# exit
R2(config)# interface loopback 0
R2(config-if)# ipv6 ospf 1 area 0
R2(config-if)# exit

R3(config)# ipv6 Router ospf 1
R3(config-rtr)# router-id 0.0.0.3
R3(config-rtr)# exit
R3(config)# interface f0/0
R3(config-if)# ipv6 ospf 1 area 0
R3(config-if)# exit
R3(config)# interface f0/1
R3(config-if)# ipv6 ospf 1 area 0
R3(config-if)# exit
```

### Kiểm tra:

Bảng định tuyến trên các Router:

```
R1# show ipv6 route
(...)
C  2001:1::/64 [0/0]
    via ::, FastEthernet0/0
L  2001:1::1/128 [0/0]
    via ::, FastEthernet0/0
O  2001:2::2/128 [110/1]
    via FE80::230:A3FF:FE8D:401, FastEthernet0/1
O  2001:3::/64 [110/3]
    via FE80::230:A3FF:FE8D:401, FastEthernet0/1
C  2001:12::/64 [0/0]
    via ::, FastEthernet0/1
L  2001:12::1/128 [0/0]
    via ::, FastEthernet0/1
O  2001:23::/64 [110/2]
    via FE80::230:A3FF:FE8D:401, FastEthernet0/1
L  FF00::/8 [0/0]
    via ::, Null0
R2# show ipv6 route
(...)
O  2001:1::/64 [110/2]
    via FE80::260:5CFF:FEA2:4B02, FastEthernet0/0
C  2001:2::/64 [0/0]
    via ::, Loopback0
L  2001:2::2/128 [0/0]
```

```

    via ::, Loopback0
o 2001:3::/64 [110/2]
    via FE80::20D:BDFF:FE86:501, FastEthernet0/1
C 2001:12::/64 [0/0]
    via ::, FastEthernet0/0
L 2001:12::2/128 [0/0]
    via ::, FastEthernet0/0
C 2001:23::/64 [0/0]
    via ::, FastEthernet0/1
L 2001:23::2/128 [0/0]
    via ::, FastEthernet0/1
L FF00::/8 [0/0]
    via ::, Null0
R3#show ipv6 route
(...)
o 2001:1::/64 [110/3]
    via FE80::230:A3FF:FE8D:402, FastEthernet0/0
o 2001:2::2/128 [110/1]
    via FE80::230:A3FF:FE8D:402, FastEthernet0/0
C 2001:3::/64 [0/0]
    via ::, FastEthernet0/1
L 2001:3::1/128 [0/0]
    via ::, FastEthernet0/1
o 2001:12::/64 [110/2]
    via FE80::230:A3FF:FE8D:402, FastEthernet0/0
C 2001:23::/64 [0/0]
    via ::, FastEthernet0/0
L 2001:23::3/128 [0/0]
    via ::, FastEthernet0/0
L FF00::/8 [0/0]
    via ::, Null0

```

Ping kiểm tra từ PC A tới PC B (hình 29.4):

```

PC>ping 2001:3::2
Pinging 2001:3::2 with 32 bytes of data:

Reply from 2001:3::2: bytes=32 time=0ms TTL=125
Reply from 2001:3::2: bytes=32 time=0ms TTL=125
Reply from 2001:3::2: bytes=32 time=6ms TTL=125
Reply from 2001:3::2: bytes=32 time=1ms TTL=125

Ping statistics for 2001:3::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms

PC>

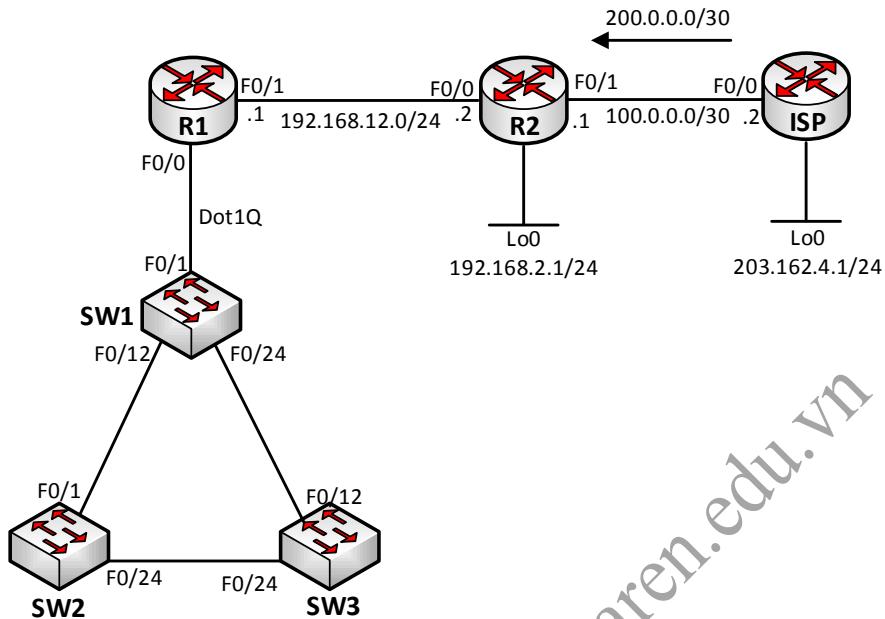
```

Hình 29.4 – Ping kiểm tra từ PCA đến PCB với OSPFv3

# LAB TỔNG HỢP

## Lab tổng hợp 1 – Switching – ACL – NAT

Sơ đồ:



Hình 1 – Sơ đồ bài Lab

Mô tả:

- Bài Lab gồm 3 Router và 3 Switch được đấu nối với nhau như hình 1.
- Các Router R1, R2 và các Switch đóng vai trò các thiết bị mạng của một doanh nghiệp, Router ISP giả lập gateway ISP cung cấp đường đi Internet cho các thiết bị bên trong.
- Quy hoạch IP trên các cổng mạng của các thiết bị được chỉ ra theo bảng 1 dưới đây:

Bảng 1 – Quy hoạch IP cho sơ đồ Lab

1	R1	Fa0/0.10 (VLAN 10): 192.168.10.1/24
		Fa0/0.20 (VLAN 20): 192.168.20.1/24
		Fa0/0.30 (VLAN 30): 192.168.30.1/24
		Fa0/1: 192.168.12.1/24
2	R2	Fa0/0: 192.168.12.2/24
		Lo0: 192.168.2.1/24
		Fa0/1: 100.0.0.1/30
3	ISP	Fa0/0: 100.0.0.2/24
		Lo0: 203.162.4.1/24

**Yêu cầu:****1. Cấu hình ban đầu:**

- Học viên thực hiện đấu nối dây và đặt IP trên cổng của các Router theo quy hoạch IP trên bảng 1.
- Cấu hình để ISP cấp về cho mạng doanh nghiệp dải IP 200.0.0.0/30.

**2. Cấu hình layer 2 switching:**

- Thiết lập trunking đấu nối giữa các switch.
- Cấu hình các VLAN thích hợp và sử dụng VTP để đồng bộ cấu hình VLAN trên các switch.
- SW1 làm root Switch cho VLAN 10, SW2 làm root Switch cho VLAN 20 và SW3 làm root Switch cho VLAN 30.
- Cấu hình R1 định tuyến giữa các VLAN.

**3. Cấu hình DHCP:**

- Cấu hình để R2 làm DHCP server cấp IP cho các user thuộc các VLAN 10, 20 và 30.

**4. Cấu hình NAT:**

- Địa chỉ 192.168.20.1 bên trong mạng được đại diện trên Internet bằng địa chỉ 200.0.0.1.
- Các VLAN 10, 20, 30 trong mạng doanh nghiệp đi Internet bằng địa chỉ đấu nối của R2 đến ISP.

**5. Cấu hình ACL:**

- Sử dụng Standard ACL để cấm các user thuộc VLAN 10 telnet đến R2, cho phép các địa chỉ khác.
- Sử dụng Extended ACL trên cổng F0/0 của R2 cấm VLAN 20 đi Internet bằng Web và cấm VLAN 30 ping đi Internet.

**Hướng dẫn:****Bước 1: Cấu hình ban đầu**

Học viên thực hiện đấu nối dây và đặt IP. Để cấp một dải IP từ ISP về mạng doanh nghiệp, sử dụng một static route trên ISP;

```
ISP(config)#ip route 200.0.0.0 255.255.255.252 100.0.0.1
```

**Bước 2: Cấu hình Layer 2 switching**

- Sử dụng các lệnh cấu hình trunking đã học để xây dựng các đường trunk theo yêu cầu.
- Sử dụng câu lệnh cấu hình một Switch trở thành root Switch để thực hiện hiệu chỉnh root Switch cho các VLAN tương ứng.

- Cấu hình một Switch làm VTP server, các Switch còn lại làm VTP client của cùng một domain VTP. Cấu hình VLAN 10, 20 và 30 trên server để cấu hình này lan truyền đến các Switch còn lại.
- Cấu hình Router định tuyến VLAN cho các VLAN 10, 20 và 30 sử dụng các sub – interface và encapsulation thích hợp.

#### Bước 3: Cấu hình DHCP

- Cấu hình định tuyến tĩnh trên hai Router đảm bảo các subnet trong mạng doanh nghiệp đi đến nhau được.
- Cấu hình pool DHCP trên R2 và cấu hình “ip helper-address” trên các cổng thích hợp của R1 để các user thuộc các VLAN 10, 20 và 30 có thể nhận được IP từ DHCP server R2.

#### Bước 4: Cấu hình NAT

- Thực hiện NAT tĩnh 192.168.2.1 thành 200.0.0.1.
- Thực hiện NAT overload các dải IP của các VLAN 10, 20, 30 thành địa chỉ cổng đầu nối của R2 đến ISP.

#### Bước 5: Cấu hình ACL

- Viết Standard ACL thích hợp và gán trên cổng VTY của R2 theo chiều in.
- Viết Extended ACL cấm lưu lượng TCP port 80 đến từ VLAN 20 và lưu lượng ICMP đến từ VLAN 30.

#### Kiểm tra:

#### Yêu cầu 2: Cấu hình layer 2 switching

Các đường trunk đã được thiết lập:

SW1#show interfaces trunk				
Port	Mode	Encapsulation	Status	Native vlan
Fa0/12	on	802.1q	trunking	1
Fa0/24	on	802.1q	trunking	1
SW2#show interfaces trunk				
Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1
Fa0/24	on	802.1q	trunking	1
SW3#show interfaces trunk				
Port	Mode	Encapsulation	Status	Native vlan
Fa0/12	on	802.1q	trunking	1
Fa0/24	on	802.1q	trunking	1

VTP được cấu hình đúng:

SW1#show vtp status	
VTP Version	: running VTP1 (VTP2 capable)
Configuration Revision	: 3
Maximum VLANs supported locally :	1005

```

Number of existing VLANs      : 8
VTP Operating Mode          : Server
VTP Domain Name             : waren

SW2#show vtp status
VTP Version capable         : 1 to 3
VTP version running          : 1
VTP Domain Name              : waren
VTP Pruning Mode             : Disabled
VTP Traps Generation         : Disabled
Device ID                   : 0024.51ed.d600
Configuration last modified by 0.0.0.0 at 3-1-93 00:27:41

Feature VLAN:
-----
VTP Operating Mode          : Client

SW3#show vtp status
VTP Version                  : 2
Configuration Revision        : 3
Maximum VLANs supported locally : 1005
Number of existing VLANs       : 8
VTP Operating Mode          : Client
VTP Domain Name              : waren

```

Cấu hình VLAN đã được đồng bộ:

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Gi0/1, Gi0/2
10 VLAN0010	active	
20 VLAN0020	active	
30 VLAN0030	active	

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Gi0/1, Gi0/2

10	VLAN0010	active
20	VLAN0020	active
30	VLAN0030	active

**SW3#show VLAN brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Gi0/1, Gi0/2
10	VLAN0010	active	
20	VLAN0020	active	
30	VLAN0030	active	

Spanning – tree đã được cấu hình đúng trên các switch:

**SW1#show spanning-tree VLAN 10**

VLAN0010					
Spanning tree enabled protocol ieee					
Root ID	Priority	24586			
	Address	c062.6b0a.fe80			
<b>This bridge is the root</b>					
	Hello Time	2 sec	Max Age 20 sec	Forward Delay 15 sec	
Bridge ID	Priority	24586 (priority 24576 sys-id-ext 10)			
	Address	c062.6b0a.fe80			
	Hello Time	2 sec	Max Age 20 sec	Forward Delay 15 sec	
	Aging Time	15 sec			
Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/12	Desg	FWD	19	128.14	P2p
Fa0/24	Desg	FWD	19	128.26	P2p

**SW2#show spanning-tree VLAN 20**

VLAN0020					
Spanning tree enabled protocol ieee					
Root ID	Priority	24596			
	Address	0024.51ed.d600			
<b>This bridge is the root</b>					
	Hello Time	2 sec	Max Age 20 sec	Forward Delay 15 sec	
Bridge ID	Priority	24596 (priority 24576 sys-id-ext 20)			
	Address	0024.51ed.d600			
	Hello Time	2 sec	Max Age 20 sec	Forward Delay 15 sec	
	Aging Time	300 sec			

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.1	P2p
Fa0/24	Desg	FWD	19	128.24	P2p

```
SW3#show spanning-tree VLAN 30

VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    24606
              Address     a40c.c304.9d80
This bridge is the root
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

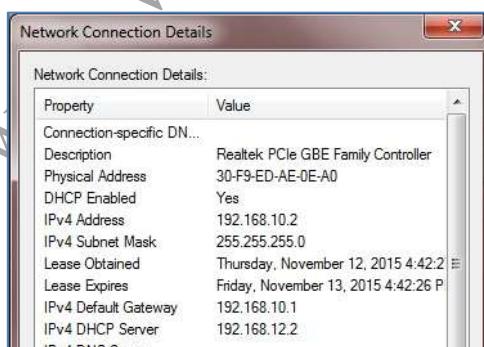
  Bridge ID  Priority    24606  (priority 24576 sys-id-ext 30)
  Address     a40c.c304.9d80
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time  300

Interface      Role Sts Cost      Prio.Nbr Type
-----
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/12	Desg	FWD	19	128.14	P2p
Fa0/24	Desg	FWD	19	128.26	P2p

### Yêu cầu 3: Cấu hình DHCP

Sau khi cấu hình xong DHCP, các user thuộc các VLAN phải nhận được IP từ DHCP, ví dụ với một PC thuộc VLAN 10 (hình 2):



Hình 2 – User thuộc VLAN 10 nhận được IP từ DHCP server

### Yêu cầu 4: Cấu hình NAT

ISP đi đến được địa chỉ 192.168.2.1 bằng IP Public 200.0.0.1:

```
ISP#ping 200.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4ms
```

User thuộc các VLAN đi được IP trên Internet:

```
C:\>ping 203.162.4.1

Pinging 203.162.4.1 with 32 bytes of data:
Reply from 203.162.4.1: bytes=32 time=2ms TTL=253
Reply from 203.162.4.1: bytes=32 time=1ms TTL=253
Reply from 203.162.4.1: bytes=32 time=1ms TTL=253
Reply from 203.162.4.1: bytes=32 time=1ms TTL=253

Ping statistics for 203.162.4.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Bảng NAT của R2:

Pro	Inside global	Inside local	Outside local	Outside global
---	200.0.0.1	192.168.2.1	---	---
icmp	100.0.0.1:1	192.168.10.2:1	203.162.4.1:1	203.162.4.1:1

### Yêu cầu 5: Cấu hình ACL

IP thuộc VLAN 10 không telnet được đến R2:

```
R1#telnet 192.168.12.2 /source-interface f0/0.10
Trying 192.168.12.2 ...
% Connection refused by remote host
```

IP thuộc VLAN khác telnet được R2:

```
R1#telnet 192.168.12.2 /source-interface f0/0.20
Trying 192.168.12.2 ... Open

User Access Verification

Password:
R2>
```

Bật HTTP server trên ISP để thực hiện kiểm tra tác dụng của extended ACL:

```
ISP(config)#ip http server
```

VLAN 10 có thể ping và đi Internet bằng web:

```
R1#ping 203.162.4.1 source 192.168.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.162.4.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4ms

R1#telnet 203.162.4.1 80 /source-interface f0/0.10
Trying 203.162.4.1, 80 ... Open
```

```
exit
HTTP/1.1 400 Bad Request
Date: Thu, 12 Nov 2015 10:28:59 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request
[Connection to 203.162.4.1 closed by foreign host]
```

VLAN 20 không đi Internet bằng web được:

```
R1#telnet 203.162.4.1 80 /source-interface f0/0.20
Trying 203.162.4.1, 80 ...
% Destination unreachable; gateway or host down
```

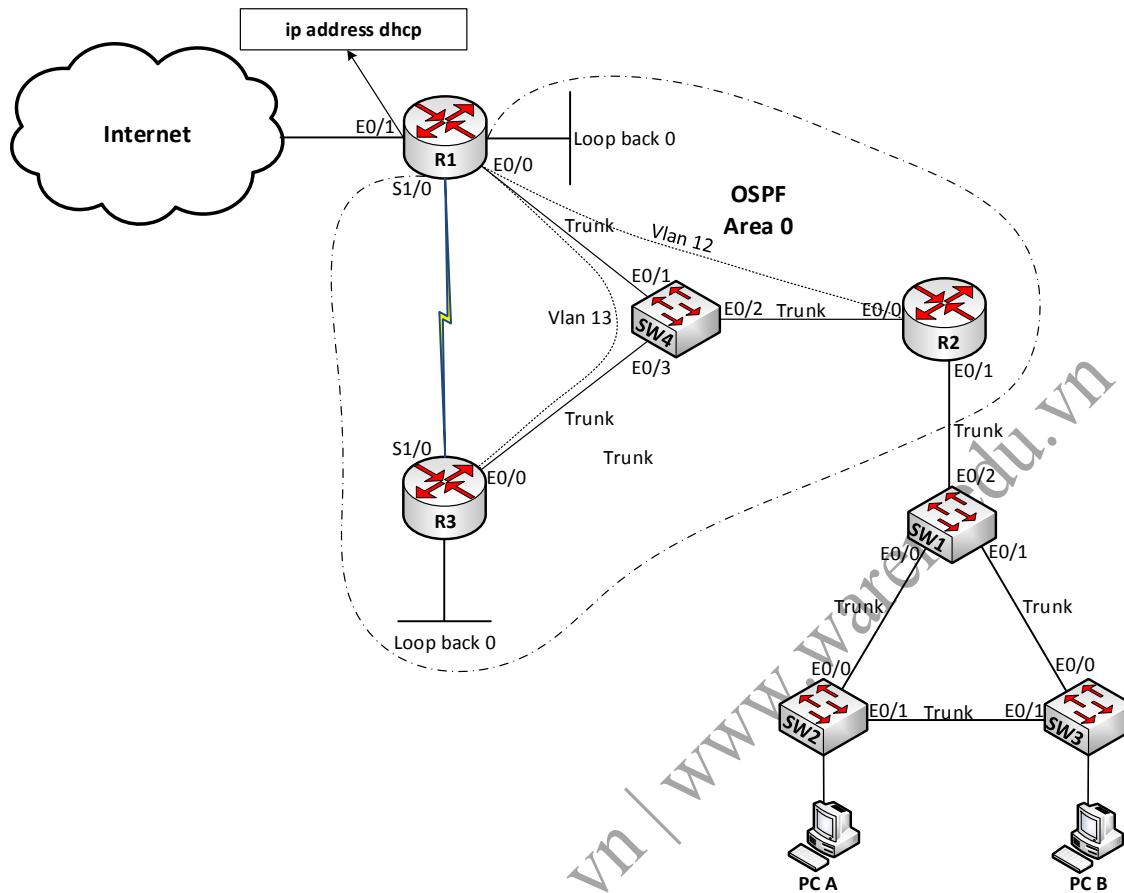
VLAN 30 không ping Internet được:

```
R1#ping 203.162.4.1 source 192.168.30.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.162.4.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.30.1
U.U.U

Success rate is 0 percent (0/5)
```

## Lab tổng hợp 2 – Routing & Switching

Sơ đồ:



Hình 1 – Sơ đồ bài Lab

Mô tả:

- Bài Lab gồm 3 Router và 4 Switch được đấu nối với nhau như hình 1.
- Quy hoạch IP trên các cổng mạng của các thiết bị được chỉ ra theo bảng 1 dưới đây:

Bảng 1 – Quy hoạch IP cho sơ đồ Lab

STT	Thiết bị	Cổng	IP	Chú thích
1	<b>R1</b>	e0/0.12 (VLAN 12)	172.16.12.1/24	
		e0/0.13 (VLAN 13)	172.16.13.1/24	
		S1/0	10.1.13.1/24	
		e0/1	DHCP	
		Lo 0	172.16.10.1/24	

STT	Thiết bị	Cổng	IP	Chú thích
2	<b>R2</b>	e0/0.12 (VLAN 12)	172.16.12.2/24	
		e0/1.10 (VLAN 10)	10.1.10.1/24	Gateway cho PC VLAN 10
		e0/1.20 (VLAN 20)	10.1.20.1/24	Gateway cho PC VLAN 20
		e0/1.30 (VLAN 30)	10.1.30.1/24	Gateway cho PC VLAN 30
3	<b>R3</b>	e0/0.13 (VLAN 13)	172.16.13.3/24	
		S1/0	10.1.13.3/24	
		Lo 0	172.16.30.1/24	
4	<b>SW1</b>	VLAN 10	10.1.10.251/24	Cổng quản lý
5	<b>SW2</b>	VLAN 10	10.1.10.252/24	Cổng quản lý
6	<b>SW3</b>	VLAN 10	10.1.10.253/24	Cổng quản lý
7	<b>SW4</b>	VLAN 123	172.16.123.4/24	Cổng quản lý
8	<b>PCA</b>	NIC (VLAN 20)	DHCP	
9	<b>PCB</b>	NIC (VLAN 30)	DHCP	

### Yêu cầu:

#### 1. Cấu hình cơ bản trên các thiết bị:

- Cấu hình cơ bản và đặt hostname cho các thiết bị như trên hình 1.
- Đặt enable password và console password cho các thiết bị là “waren”.
- Cấu hình đảm bảo thực hiện Telnet được đến các thiết bị.

#### 2. Cấu hình VTP:

- Cấu hình VTP trên các Switch theo yêu cầu sau:
  - Domain name: WAREN
  - Password: cisco
  - SW1: Server; SW2, SW3: Client

#### • Trên SW1, tạo các VLAN:

VLAN 10: CCNA

VLAN 20: Route

VLAN 30: Switch

Kiểm tra rằng cấu hình VLAN này đã lan truyền đến được tất cả các switch.

#### 3. Hiệu chỉnh STP:

Cấu hình đảm bảo:

- VLAN 10: Block port E0/1 – SW1

- VLAN 20: Block port E0/1 – SW2
- VLAN 30: Block port E0/1 – SW3

**4. Định tuyến giữa các VLAN:**

- Cấu hình Router R2 thực hiện định tuyến giữa các VLAN 10, 20 và 30.

**5. Point – to – point data link:**

- Cấu hình đường serial point – to – point nối giữa hai cổng S1/0 của hai Router R1 và R3 sử dụng giao thức lớp 2 PPP.

**6. Cấu hình định tuyến:**

- Cấu hình để R1 nhận IP cho cổng E0/1 từ gateway Internet thông qua DHCP.
- Thực hiện cấu hình định tuyến OSPF area 0 giữa các Router R1, R2 và R3 đảm bảo mọi subnet IP trên sơ đồ Lab có thể đi đến nhau.
- Hiệu chỉnh Router – ID của các Router như sau:
  - R1: 1.1.1.1; R2: 2.2.2.2; R3: 3.3.3.3.
- Hiệu chỉnh bầu chọn DR và BDR đảm bảo R3 luôn là DR.
- Cấu hình R1 quảng bá default – route vào sơ đồ Lab. Thực hiện cấu hình NAT trên R1 đảm bảo mọi địa chỉ của mạng doanh nghiệp có thể đi được Internet.

**7. ACL:**

- Cấu hình trên R2 sử dụng một Standard ACL để chỉ các IP chẵn của mạng 10.1.30.0/24 mới có thể truy nhập Telnet tới R2.
- Tại mạng 172.16.10.0/24 phía sau R1 có một server HTTP nội bộ. Cấu hình ACL đảm bảo chỉ các user thuộc VLAN 20 mới có thể truy nhập vào server HTTP này. ACL không được ảnh hưởng đến các hoạt động truyền dữ liệu khác.

**8. DHCP:**

- Cấu hình R1 làm DHCP server cấp IP cho các host thuộc các VLAN 10, 20, 30 và các user thuộc các subnet 172.16.10.0/24 và 172.16.30.0/24 của R1 và R3.

**9. IPv6:**

- Đặt địa chỉ IPv6 trên các cổng của các Router R1 và R3 theo yêu cầu sau:
  - Trên các cổng S1/0 của R1 và R3 sử dụng địa chỉ 2001:1:13::Y/64, trong đó Y là số hiệu của router.
- Trên các cổng Lo 0 của R1 và R3 sử dụng địa chỉ thuộc các subnet 2001:YYYY::1/64, trong đó Y là số hiệu của router.
- Thực hiện định tuyến tĩnh trên hai Router R1 và R3 đảm bảo mọi địa chỉ IPv6 thấy nhau.

## Hướng dẫn:

### Yêu cầu 1, 2:

**Bước 1:** Cấu hình cơ bản trên các thiết bị.

**Bước 2:** Cấu hình VTP Domain trên SW1.

**Bước 3:** Tạo các VLAN tương ứng trên SW1.

**Bước 4:** Gán cổng vào VLAN.

Đảm bảo kết quả như sau:

Trên SW1:

```
SW1#show vtp status
VTP Version : running VTP1 (VTP2 capable)
Configuration Revision : 4
Maximum VLANs supported locally : 1005
Number of existing VLANs : 9
VTP Operating Mode : Server
VTP Domain Name : WAREN
```

**Bước 5:** Cấu hình VTP mode client trên các thiết bị SW2, SW3

```
SW3#show vtp status
VTP Version capable : 1 to 3
VTP version running : 1
VTP Domain Name : WAREN
VTP Operating Mode : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs : 9
Configuration Revision : 4
```

### Yêu cầu 3:

**Bước 1:** Xác định Root Bridge cho STP VLAN 10, VLAN 20 và VLAN 30.

**Bước 2:** Cấu hình thay đổi priority trên thiết bị Switch phù hợp sao cho kết quả được hiển thị như sau:

SW1#show spanning-tree VLAN 10					
Interface	Role	Sts	Cost	Prio.Nbr	Type
E0/0	Root	FWD	12	128.160	P2p
E0/1	Altn	BLK	19	128.23	P2p

SW2#show spanning-tree VLAN 20					
Interface	Role	Sts	Cost	Prio.Nbr	Type
E0/0	Root	FWD	12	128.160	P2p
E0/1	Altn	BLK	19	128.23	P2p

SW3#show spanning-tree VLAN 30					
Interface	Role	Sts	Cost	Prio.Nbr	Type
E0/0	Root	FWD	12	128.160	P2p
E0/1	Altn	BLK	19	128.23	P2p

E0/0	Root FWD 12	128.160	P2p
E0/1	Altn BLK 19	128.23	P2p

#### Yêu cầu 4:

Cáu hình R2 thực hiện định tuyến giữa các VLAN 10, 20, 30.

Kiểm tra giao tiếp thành công từ PC thuộc VLAN 20 đến PC thuộc VLAN 30:

```
C:\>ping 10.1.30.30
Reply from 10.1.30.30: bytes=32 time<1ms TTL=127
Reply from 10.1.30.30: bytes=32 time<1ms TTL=127
```

#### Yêu cầu 5:

Thực hiện chuyển giao thức lớp 2 trên link serial giữa hai Router thành PPP và cáu hình xác thực PAP.

Các link đã chuyển sang PPP:

```
R1#show interfaces s1/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.13.1/24
  MTU 1500 bytes, BW 512 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
    Open: CDP/CP, IPCP, loopback not set
    Keepalive set (10 sec)
  (...)

R3#show interfaces s1/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.13.3/24
  MTU 1500 bytes, BW 512 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
    Open: IPCP, CDP/CP, loopback not set
    Keepalive set (10 sec)
  (...)
```

Sau khi xác thực thành công, link serial up/up, hai Router ping được nhau:

```
R1#show ip interface brief s1/0
Interface          IP-Address      OK? Method Status          Protocol
S1/0              192.168.12.1    YES NVRAM  up           up

R1#ping 10.1.13.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.13.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/10ms
```

## Yêu cầu 6:

Bảng neighbor trên 3 Router thể hiện kết quả bầu chọn:

R1#show ip ospf neighbor						
Neighbor ID	Pri	State	Dead Time	Address	Interface	
3.3.3.3	0	FULL/DROTHER	00:00:33	172.16.13.3	Ethernet0/0.13	
2.2.2.2	0	FULL/DROTHER	00:00:37	172.16.12.2	Ethernet0/0.13	
3.3.3.3	0	FULL/ -	00:00:37	10.1.13.3	Serial1/0	

Kiểm tra PC VLAN 20 đã đi ra được Internet:

```
C:\>ping 8.8.8.8
Reply from 8.8.8.8: bytes=32 time<1ms TTL=127
Reply from 8.8.8.8: bytes=32 time<1ms TTL=127
```

## Yêu cầu 7:

Cấu hình ACL thỏa yêu cầu

Chỉ có PC có IP chẵn thuộc mạng 10.1.30.0/24 mới có thể telnet tới R2:

```
C:\>ipconfig
Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . :
  IP Address . . . . . : 10.1.30.4
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.1.30.1
C:\>telnet 10.1.30.1
R2#
```

## Yêu cầu 8:

**Bước 1:** Cấu hình 5 DHCP pool trên R1 để cấp IP cho các PC thuộc VLAN 10, 20, 30 và users thuộc các subnet 172.16.10.0/24 và 172.16.30.0/24.

**Bước 2:** Cấu hình ip helper-address trên cổng phù hợp.

Kết quả đạt được sau các bước này:

PC VLAN 20 nhận được địa chỉ IP từ R1:

```
C:\>ipconfig
Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . :
  IP Address . . . . . : 10.1.20.3
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.1.20.1
```

PC VLAN 30 nhận được địa chỉ IP từ R1:

```
C:\>ipconfig
Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . :
  IP Address . . . . . : 10.1.30.3
```

```
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.1.30.1
```

Kiểm tra IP đã được R1 cấp phát:

R1#show ip dhcp binding			
Bindings from all pools not associated with VRF:			
IP address	Client-ID/ Hardware address/	Lease expiration	Type
10.1.20.3	0100.15f2.84b4.6b	Oct 28 2015 04:34 AM	Automatic
10.1.30.3	0100.e04c.b029.11	Oct 28 2015 04:21 AM	Automatic

### Yêu cầu 9:

**Bước 1:** Đặt địa chỉ IPv6 theo yêu cầu trên R1, R3.

**Bước 2:** Cấu hình static route

Ping thành công các Loopback giữa hai Router:

```
R3#ping ipv6 2001:1111::1 source 2001:3333::1
Sending 5, 100-byte ICMP Echos to 2001:1111::1, timeout is 2 seconds:
Packet sent with a source address of 2001:3333::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4ms
```



**TRUNG TÂM WAREN  
ĐÀO TẠO CHUYÊN GIA QUẢN TRỊ MẠNG & BẢO MẬT**

Địa chỉ:

Tầng 6, Tòa nhà 145 Lê Quang Định, Phường 14, Quận Bình Thạnh, Tp.Hồ Chí Minh.

Điện thoại: (028) 355 122 68 | HOTLINE: 0908 152 162

Website: [www.waren.vn](http://www.waren.vn) | [www.waren.edu.vn](http://www.waren.edu.vn)

Email: [waren@waren.vn](mailto:waren@waren.vn)

Facebook Fanpage: [www.facebook.com/waren.vn](https://www.facebook.com/waren.vn)

