

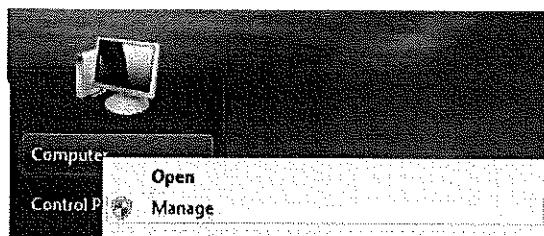
MỤC LỤC

Lab 1 – Đăng nhập vào giao diện dòng lệnh của Router.....	3
Lab 2 – Cấu hình cơ bản trên Router.....	6
Lab 3 – CDP, Telnet, SSH	11
Lab 4 – Tổng quan hoạt động của Switch.....	28
Lab 5 – Static Routing	31
Lab 6 – Static routing, DHCP	34
Lab 7 – Static routing, DHCP, Internet	40
Lab 8 – Dự phòng cho Static route.....	49
Lab 9 – VLAN, Trunking	53
Lab 10 – VTP, InterVLAN routing	60
Lab 11 – VLAN, Trunking, Static routing.....	71
Lab 12 – Spanning Tree Protocol.....	84
Lab 13 – Etherchannel.....	99
Lab 14 – Giao thức định tuyến RIPv2	110
Lab 15 – Giao thức định tuyến OSPF.....	120
Lab 16 – Layer 3 switch.....	133
Lab 17 – Access Control List (ACL).....	145
Lab 18 – Network Address Translation (NAT)	157
Lab 19 – PPPoE.....	166
Lab 20 – GRE VPN.....	172
Lab 21 – Cấu hình Access – Point một SSID	183
Lab 22 – Cấu hình Access – point nhiều SSID	194

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

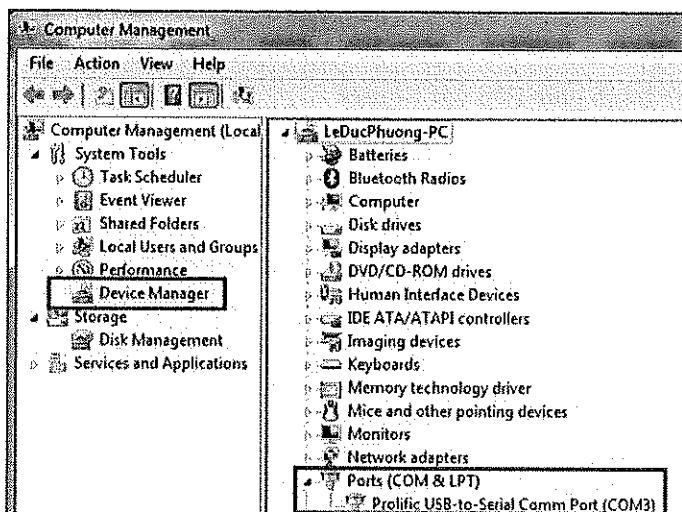
Phần này được hướng dẫn cho Win 7.

Click phải chuột vào phần “Computer” trên menu Start chọn “Manage” (hình 3):



Hình 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 4):



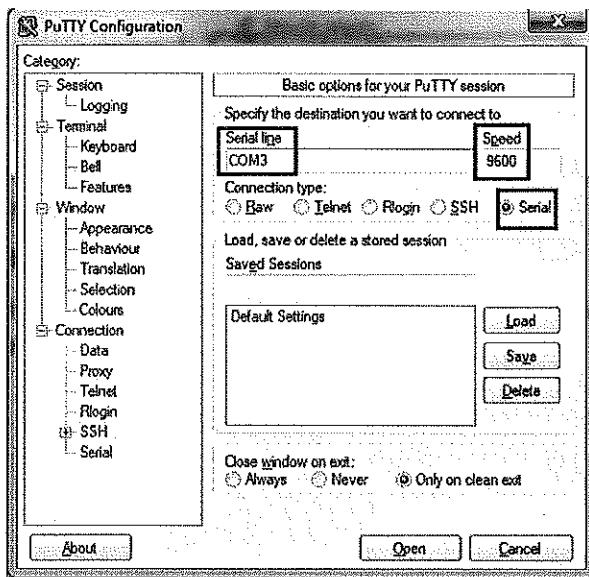
Hình 4 – Xác định cổng COM.

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 4).

Bước 4: Thiết lập PuTTY

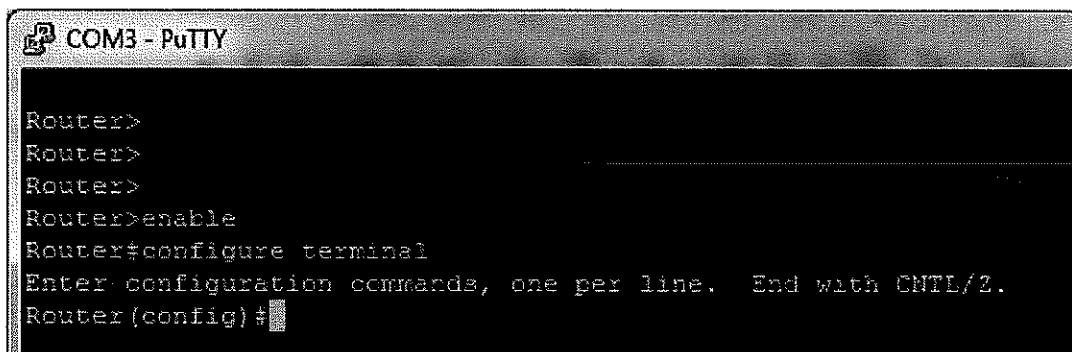
Học viên mở chương trình PuTTY đã chép trên PC và thực hiện chọn mục “Serial” và các thiết lập tương ứng như được chỉ ra trên hình 5. Trong đó:

- 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 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 6):



Hình 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.

```
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 di 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):

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Hình 2 – PC ping lên Router.

Bước 9: Lưu cấu hình

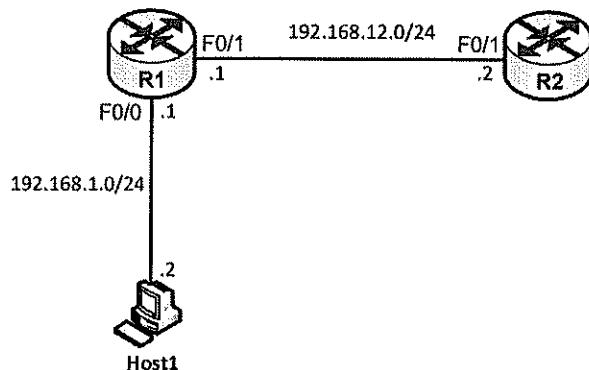
```
waren#copy running-config startup-config
Destination filename [startup-config]? <-Gõ Enter tại đây
Building configuration...
[OK]
waren#
```

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

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

Lab 3 – CDP, Telnet, SSH

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Bài lab gồm hai router và một host được kết nối với nhau theo sơ đồ hình 1.
- Trong bài lab này, các bạn học viên sẽ thực hành về các giao thức CDP, Telnet và SSH trên router.

Yêu cầu:

1. Cấu hình cơ bản:

- Các bạn học viên thực hiện cấu hình cơ bản trên các router R1 và R2 với các thông số được chỉ ra như trên sơ đồ (hostname, địa chỉ IP).
- Với yêu cầu này, các bạn thực hiện ôn tập lại một số lệnh cấu hình cơ bản đã thực hành trong buổi học trước.

2. CDP:

- Trên mỗi router, các bạn học viên thực hiện kiểm tra thông tin CDP mà router nhận được từ thiết bị láng giềng.
- Qua thao tác này, chúng ta sẽ nắm rõ hơn công dụng của giao thức CDP đã được đề cập trong bài giảng lý thuyết.

3. Telnet:

- Trên R1, các bạn học viên thực hiện cấu hình Telnet server để cho phép các thiết bị khác truy nhập đến router này bằng phương pháp Telnet. Password Telnet được sử dụng là “cisco”.
- Từ Host1 và R2, thực hiện telnet đến R1 để kiểm tra cấu hình đã thực hiện ở trên.

4. SSH:

- Trên R1, các bạn học viên thực hiện bổ sung thêm cấu hình SSH server. Tài khoản để SSH được lưu trữ nội bộ trên router R1: username là “cisco”, password là “waren”.
- Từ các thiết bị Host1 và R2, thực hiện truy nhập SSH đến R1 để kiểm tra cấu hình SSH đã thực hiện ở trên.

Thực hiện:**1. Cấu hình cơ bản:****Cấu hình:**

Ta thực hiện lại các thao tác cấu hình cơ bản trên hai router R1 và R2.

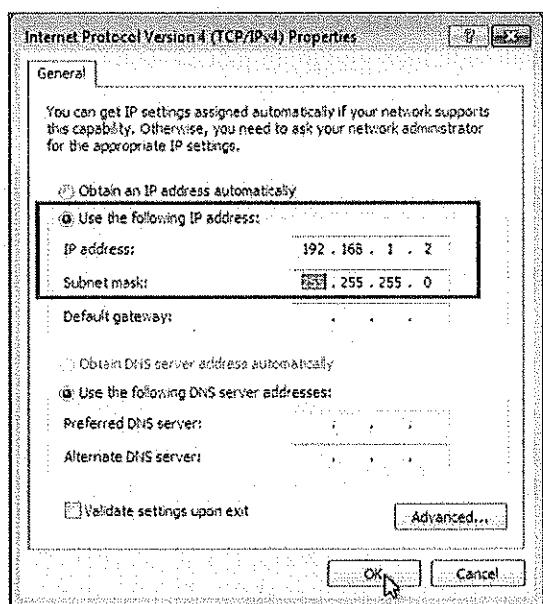
Trên R1:

```
Router(config)#hostname R1
R1(config)#interface e0/0
R1(config-if)#no shutdown
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface e0/1
R1(config-if)#no shutdown
R1(config-if)#ip address 192.168.12.1 255.255.255.0
R1(config-if)#exit
```

Trên R2:

```
Router(config)#hostname R2
R2(config)#interface e0/0
R2(config-if)#no shutdown
R2(config-if)#ip address 192.168.12.2 255.255.255.0
R2(config-if)#exit
```

Cấu hình IP trên card mạng của Host1 (hình 2):



Hình 2 – Cấu hình IP trên card mạng của Host1.

Kiểm tra:

Ta kiểm tra rằng kết nối IP giữa R1 và R2 đã thông suốt:

```
R1#ping 192.168.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Kết nối IP giữa R1 và Host1 cũng đã thông suốt:

```
R1#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 80 percent (4/5), round-trip min/avg/max = 2/3/8 ms
```

(Nhắc lại rằng, ta cần phải tắt Firewall Windows của Host 1 để R1 có thể ping được Host1.)

Ta thấy các lệnh ping đều bị timeout gói đầu. Điều này xảy ra là do ảnh hưởng của tiến trình phân giải địa chỉ ARP (Address Resolution Protocol). Giao thức ARP sẽ được đề cập trong chương 3 của giáo trình. Các lệnh ping sau này từ R1 đến Host1 và R2 sẽ không còn bị timeout gói đầu nữa:

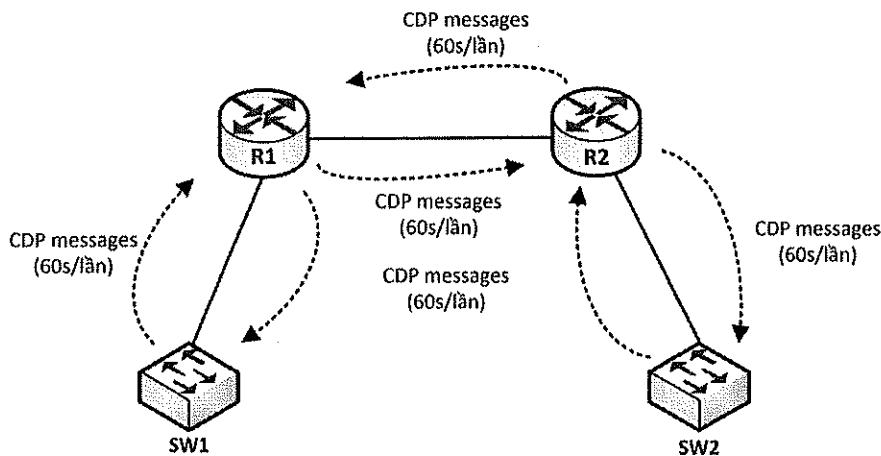
```
R1#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms

R1#ping 192.168.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

2. CDP:**Ghi chú:**

Một thao tác cơ bản mà các bạn học viên cần nắm khi bước đầu làm quen với thiết bị là hiểu và sử dụng được giao thức CDP.

CDP – Cisco Discovery Protocol là một giao thức đặc biệt của Cisco cho phép một thiết bị thu thập được thông tin về các thiết bị láng giềng kết nối trực tiếp với nó. Mặc định, một thiết bị Cisco sẽ gửi các thông điệp CDP liệt kê các thông tin về bản thân ra khỏi các cổng của nó đến các thiết bị láng giềng để từ đó các thiết bị láng giềng có thể nắm được thông tin về thiết bị. Các gói tin CDP này được gửi theo định kỳ mặc định là 60s/lần (xem hình 3).



Hình 3 – Các thiết bị trao đổi thông tin CDP.

CDP cho biết những thông tin như sau về thiết bị láng giềng kết nối trực tiếp:

- *Device ID*: Hostname của thiết bị láng giềng.
- *Local Interface*: Cổng nào đang được sử dụng để kết nối đến láng giềng.
- *Outgoing port*: Láng giềng đang dùng cổng nào để kết nối đến mình.
- *Capability*: Láng giềng có khả năng gì (Router, Switch , IGMP – một giao thức được sử dụng trong kỹ thuật Multicast,...).
- *Platform*: Chủng loại thiết bị của láng giềng. Ví dụ: láng giềng là Router 2811, Switch 3560,...
- *Địa chỉ IP của láng giềng*.
- *IOS version*: Hệ điều hành mà thiết bị láng giềng đang sử dụng.

Các lệnh cơ bản để thao tác với CDP:

- Xem thông tin về các láng giềng:

```
R#show cdp neighbors [detail]
R#show cdp entry *
```

- Bật/tắt CDP trên thiết bị:
 - Bật/tắt CDP trên toàn bộ thiết bị:

```
R(config)#[no] cdp run
```
 - Bật/tắt CDP trên một interface nào đó của thiết bị:

```
R(config-if)#[no] cdp enable
```

Kiểm tra CDP trên bài lab:

Chúng ta thực hiện “show cdp neighbor” trên router R1 để quan sát thông tin về láng giềng R2:

```
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

Từ kết quả show ở trên, chúng ta thấy rằng R1 có một thiết bị láng giềng kết nối trực tiếp với nó là thiết bị có hostname (“Device ID”) là R2. R1 kết nối cổng F0/1 của nó (“Local Intrfce” = “Fas 0/1”) đến cổng F0/0 (“Port ID” = “Fas 0/1”) của R2. Ta cũng thấy rằng R2 là một router dòng 2811 (“Platform” = “2811”).

Để xem thông tin chi tiết hơn, chúng ta có thể sử dụng tham số “detail” của câu lệnh show:

```
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
```

Ta thấy, trong kết quả show ở trên, bên cạnh những thông tin đã biết giống như kết quả rút gọn, ta còn thấy được địa chỉ IP của thiết bị láng giềng, version của IOS mà láng giềng này sử dụng.

Chúng ta cũng có thể đạt được kết quả show tương tự khi sử dụng lệnh “R#show cdp entry *”.

3. Telnet:

Cấu hình:

Thực hiện cấu hình trên R1 để các thiết bị khác có thể Telnet đến R1 bằng password “cisco”:

```
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#transport input telnet
```

Ghi chú:

Telnet là một phương thức truy nhập từ xa vào giao diện dòng lệnh của thiết bị thông qua mạng TCP/IP. Đó là một giao thức tầng Application hoạt động theo mô hình Client – Server, trong đó thiết bị được Telnet đến là Server (ví dụ: router) còn thiết bị thực hiện Telnet đó là Client (ví dụ: PC). Để truyền tải, các thông điệp Telnet trao đổi giữa client và server được đóng gói vào các segment TCP: Telnet chạy trên nền TCP, sử dụng port 23 tại phía server.

Như vậy, để có thể thực hiện Telnet để quản trị một thiết bị mạng, trên thiết bị ấy phải được cài đặt chương trình Telnet Server; tiếp theo, máy tính của người quản trị cần phải được cài đặt chương trình Telnet Client. Ngoài ra, địa chỉ IP của máy tính người quản trị cần phải đi đến được địa chỉ IP của thiết bị mạng mà người quản trị muốn Telnet đến (và để đảm bảo được điều này, hệ thống mạng TCP/IP nối giữa máy tính người quản trị và thiết bị mạng cần phải được cấu hình *định tuyến* đầy đủ).

Trong bài lab của chúng ta, Host1 kết nối trực tiếp đến router R1 bằng một địa chỉ IP cùng mạng với IP trên cổng F0/0 của router này nên Host1 đã có thể đi đến được R1 mà không cần phải thực hiện định tuyến gì thêm. Trên Cisco IOS đã tích hợp sẵn Telnet server nên ta chỉ cần sử dụng một chương trình Telnet client trên Host1 là có thể từ Host1 thực hiện Telnet đến được router R1. Với bài lab này, Host1 chạy hệ điều hành Windows có tích hợp sẵn chương trình Telnet client nên ta có thể bật chương trình này để sử dụng; ngoài ra ta cũng có thể sử dụng các phần mềm Terminal như PuTTY, Secure CRT, MobaXterm,... vì các phần mềm này đều có tích hợp Telnet client.

Riêng với router R2, ta có thể từ màn hình Console của R2 thực hiện Telnet sang router R1 vì bản thân Cisco IOS cũng tích hợp Telnet client.

Cuối cùng, để có thể Telnet thành công vào R1, trên router R1 ta cần phải cấu hình một password xác thực trên các cổng VTY và cấu hình để các cổng này cho phép các session Telnet được đi vào cổng:

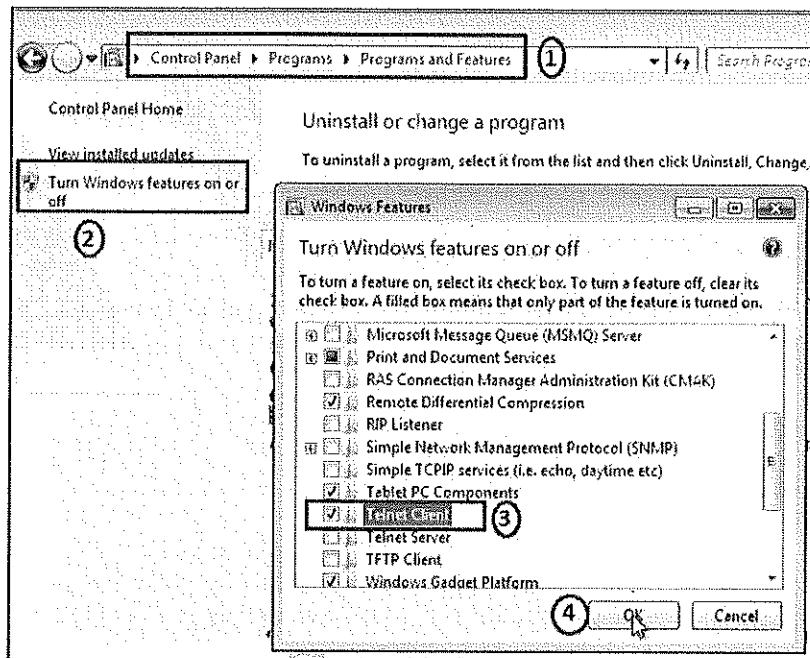
```
R1(config)#line vty 0 4
R1(config-line)#password cisco ] Đặt password Telnet
R1(config-line)#login
```

Các cổng VTY là các cổng ảo trên router. Mọi hoạt động truy nhập từ xa bằng Telnet hoặc SSH (sẽ cấu hình ở mục số 4) đều phải được tiến hành thông qua các cổng ảo này. Có 5 cổng VTY trên router được đánh số từ 0 đến 4, cho phép 5 user đồng thời truy nhập vào router để cấu hình router này.

Kiểm tra:

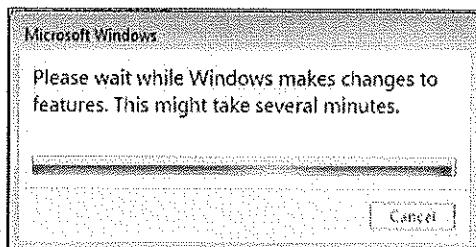
Trước hết, ta sử dụng tính năng Telnet client được tích hợp sẵn trên Windows của Host1 để thực hiện telnet đến R1. Mặc định, tính năng này bị tắt nên ta phải vào Control Panel của Windows để bật tính năng này lên (hình 4):

1. Chọn “Control Panel → Programs → Programs and Features”.
2. Chọn “Turn Windows features on or off”.
3. Click chọn vào “Telnet Client”.
4. Nhấn “OK”.



Hình 4 – Bật Telnet Client trên Windows.

Sau khi nhấn “OK”, các bạn học viên có thể phải chờ một khoảng thời gian ngắn để Windows active tính năng Telnet client (hình 5):



Hình 5 – Windows đang active Telnet client.

Sau khi đã bật Telnet client, chúng ta có thể từ cửa sổ CMD của Windows host thực hiện Telnet vào router bằng cách gõ lệnh “telnet” từ dấu nhắc hệ thống:

```
C:\> telnet 192.168.1.1
```

Cửa sổ của session Telnet hiện ra, chúng ta nhập password Telnet là “cisco” đã được cấu hình ở trên để truy nhập vào router R1:

```
User Access Verification
```

```
Password: <- Nhập password là "cisco"  
R1>enable  
% No password set  
R1>
```

Ta thấy rằng password Telnet chỉ cho phép user đi vào User mode của CLI trên R1, để đi sâu hơn nữa, IOS trên router R1 đòi hỏi user phải được tiếp tục xác thực bằng password Enable. Tuy nhiên, vì ta chưa cấu hình password Enable trên R1 nên user Telnet hiện nay chỉ có thể dừng lại tại User mode.

Như vậy, để người quản trị có thể Telnet vào được các mode sâu hơn của router, chúng ta cần phải cấu hình thêm Enable password cho R1:

```
R1(config)#enable password waren
```

Lúc này, ta có thể tiếp tục đi vào các mode sâu hơn của CLI trên cửa sổ Telnet của Host1:

```
User Access Verification
```

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

```
R1>enable
```

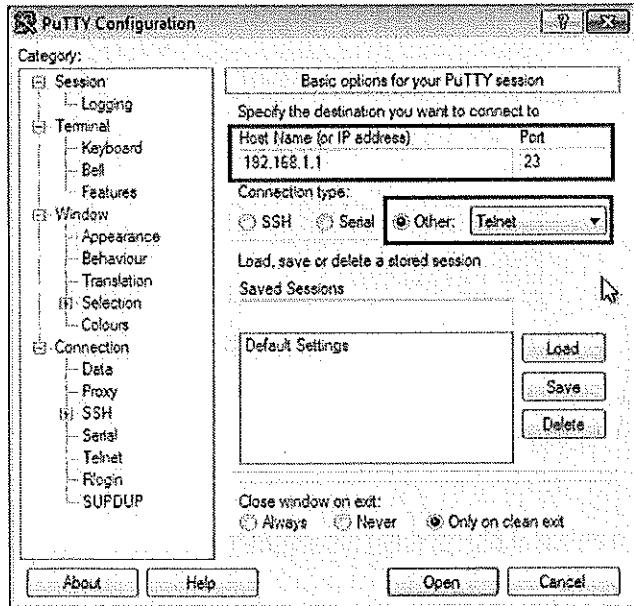
```
Password: <- Nhập password là "waren"
```

```
R1#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.1.1	YES	NVRAM	up	up
FastEthernet0/1	192.168.12.1	YES	NVRAM	up	up

```
R1#
```

Bên cạnh việc sử dụng chương trình Telnet client của Windows, chúng ta cũng có thể sử dụng một chương trình Terminal bất kỳ để Telnet, ví dụ, PuTTY (hình 6):



Hình 6 – Thực hiện Telnet đến R1 bằng PuTTY.

Tương tự như trên, sau khi mở session Telnet, giao diện dòng lệnh của router cũng hiện ra trên cửa sổ của chương trình PuTTY cho phép chúng ta cấu hình router thông qua session Telnet này.

Chúng ta đã thực hiện Telnet từ Windows host đến router. Ngoài ra, chúng ta cũng có thể thực hiện Telnet từ một router đến một router. Trong bài lab này, ta thực hiện Telnet từ màn hình console của R2 đến R1:

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

User Access Verification
Password: <- Nhập password Telnet là "cisco"
R1>enable
Password: <- Nhập password enable là "waren"
R1#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    192.168.1.1    YES NVRAM up           up
FastEthernet0/1    192.168.12.1   YES NVRAM up           up
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
```

Trên router R1, ta có thể kiểm tra rằng hiện nay đang những user nào đang đăng nhập vào CLI của router:

```
R1#show users
Line       User      Host(s)        Idle      Location
* 0 con 0    idle      00:00:00
  2 vty 0    idle      00:03:44 192.168.1.2
  3 vty 1    idle      00:00:42 192.168.12.2

Interface     User      Mode      Idle      Peer Address
```

Kết quả show cho thấy có 3 user đang đăng nhập vào router R1: một user qua cổng Console 0, hai user còn lại qua các cổng VTY 0 và VTY 1 với địa chỉ IP lần lượt là 192.168.1.2 (Host1) và 192.168.12.2 (R2). Dấu "*" được đặt trên dòng thông tin về user trên cổng Console cho biết kết quả show đang hiển thị là của màn hình Console.

Đến đây, chúng ta đã hoàn thành cấu hình Telnet trên router R1 và thực hiện kiểm tra cấu hình này.

4. SSH:

Cấu hình:

Trên router R1:

```
R1(config)#username cisco password waren
R1(config)#ip domain-name waren.vn
R1(config)#crypto key generate rsa
The name for the keys will be: R1.waren.vn
Choose the size of the key modulus in the range of 360 to 4096 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] (elapsed time was 4 seconds)
R1(config)#
*Jun 25 15:27:11.217: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

```
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#end
```

Ghi chú:

Giao thức Telnet là một giao thức truy nhập từ xa rất hiệu quả, tuy nhiên nhược điểm chính của giao thức này là mọi thông điệp Telnet trao đổi giữa Telnet client và Telnet server đều được để dưới dạng clear – text không mã hóa. Điều này đem lại nguy cơ bảo mật lớn cho Telnet.

Để khắc phục nhược điểm về bảo mật này của Telnet, ngày nay, giao thức SSH thường được sử dụng để thay thế. Có cùng công dụng như Telnet, nhưng SSH thực hiện mã hóa toàn bộ nội dung trao đổi giữa SSH client (trên thiết bị đầu cuối của người quản trị) và SSH server (trên thiết bị mạng cần truy nhập). SSH là một giao thức tầng Application, chạy trên nền TCP sử dụng port 22 tại phía SSH server.

Để cấu hình SSH server trên router Cisco, chúng ta tiến hành các bước như sau:

1. Cấu hình tài khoản cho hoạt động truy nhập. Nếu tài khoản này được đặt nội bộ trên router Cisco, chúng ta sử dụng lệnh khai báo tài khoản như sau:

```
R(config)#username username password password
```

2. Khai báo domain – name mà thiết bị router thuộc về. Domain – name này sẽ được kết hợp cùng Hostname của router để tạo thành *FQDN (Fully Qualified Domain Name)*. FQDN đến lượt nó, sẽ được Cisco IOS sử dụng để phát sinh các key RSA dùng cho hoạt động của SSH.

```
R(config)#ip domain-name Tên_miền
```

3. Yêu cầu IOS phát sinh một cặp key RSA cho SSH:

```
R(config)#crypto key generate rsa
```

Khi thi hành lệnh này, IOS sẽ yêu cầu chúng ta nhập chiều dài của key. Chiều dài càng cao, hoạt động của SSH càng bảo mật, tuy nhiên, tài nguyên của router sẽ càng bị tiêu tốn. Khi ta chọn chiều dài lớn hơn hoặc bằng 768 bit, SSH version 2 được tự động sử dụng.

4. Cấu hình để các cổng VTY cho phép các thông điệp SSH được phép đi vào router:

```
R(config)#line vty 0 4
R(config-line)#login local
R(config-line)#transport input ssh
R(config-line)#end
```

Khi ta sử dụng lệnh “*login local*”, các user truy nhập vào router qua đường VTY (kể cả Telnet và SSH) sẽ được xác thực dựa vào tài khoản gồm *username* và *password* đã lưu trên bộ nhớ nội bộ của router. Password trước đó nếu có cấu hình trên các đường VTY sẽ được bỏ qua.

SSH hiện nay có hai version là 1 và 2. Hai version này không tương thích với nhau, và ngày nay, SSH version 2 được khuyến nghị sử dụng vì có tính bảo mật cao hơn SSH version 1. Để có thể sử dụng SSH version 2, chiều dài key được phát sinh phải đạt tối thiểu là 768 bit. Câu lệnh để chuyển đổi giữa hai version sau khi đã phát sinh key trên router:

```
R(config)#ip ssh version {1|2}
```

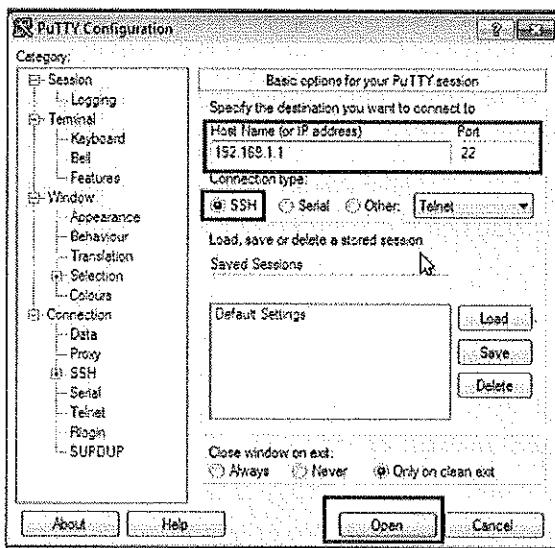
Để kiểm tra thông tin về tiến trình SSH đang chạy trên router, ta sử dụng lệnh show:

```
R#show ip ssh
```

Kiểm tra:

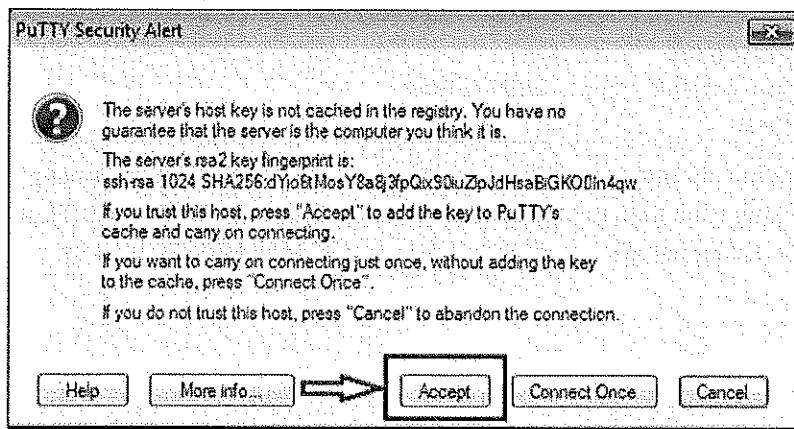
Trong bài lab này, ta thực hiện SSH từ Host1 đến router R1. Lưu ý rằng, Windows không tích hợp sẵn chương trình SSH Client nên ta phải sử dụng phần mềm PuTTY trên Host1 để thực hiện thao tác này. Trong thực tế, các phần mềm Terminal thông dụng đều có tích hợp SSH client nên bên cạnh PuTTY, chúng ta có rất nhiều sự lựa chọn khác để có thể thực thi SSH.

Ta nhập địa chỉ IP của R1, chọn phương thức kết nối là SSH, sau đó nhấn “Open” (hình 7):



Hình 7 – Nhập địa chỉ của router để SSH.

Sau khi nhấn “Open”, một cửa sổ hiện ra hỏi ý chúng ta có chấp nhận Public key RSA được gửi đến từ router không. Đây là một vấn đề liên quan đến bảo mật và mật mã hóa, là một chủ đề nằm ngoài chương trình, thuộc về các khóa học Security nên sẽ không được phân tích kỹ ở đây. Chúng ta chỉ cần nhấn “Accept” để chấp nhận key này (hình 8):



Hình 8 – Chấp nhận Public key gửi đến từ SSH server trên router.

Sau khi nhấn “Accept”, cửa sổ SSH hiện ra yêu cầu nhập username và password để đăng nhập vào CLI của thiết bị:

```
login as: cisco <- Nhập username là "cisco"  
Using keyboard-interactive authentication.  
Password: <- Nhập password là "waren"  
  
R1>enable  
Password:  
R1#
```

Sau khi nhập xong username và password đúng, chúng ta được đăng nhập vào mode User của thiết bị. Từ đây chúng ta nhập Enable password đi tiếp vào các mode bên trong để tiếp tục tương tác với thiết bị.

Trên đây là hoạt động SSH từ Windows host đến R1. Ta cũng có thể thực hiện SSH từ một router đến một router vì Cisco IOS của router cũng tích hợp chương trình SSH client. Trong bài lab này, từ console của R2, ta thực hiện SSH tới R1:

```
R2#ssh -l cisco 192.168.12.1  
Password: <- Nhập password của tài khoản SSH là "waren"  
  
R1>enable  
Password: <- Nhập password enable là "waren"  
R1#
```

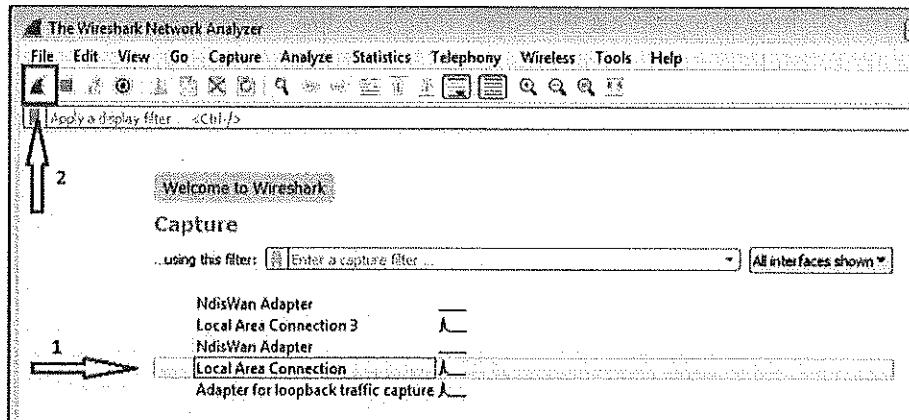
Như vậy, chúng ta đã hoàn thành cấu hình SSH server trên R1 và đã kiểm tra thử hoạt động SSH đến R1 từ Host1 và R2.

Tiếp theo, chúng ta sẽ thử thực hiện bắt gói trên Host1 để thấy được rằng Telnet sẽ không mã hóa dữ liệu còn SSH thì có thực hiện mã hóa dữ liệu. Chương trình bắt gói được sử dụng là Wireshark – một phần mềm bắt gói rất nổi tiếng hiện nay. Các bạn học viên có thể tải phần mềm Wireshark miễn phí từ đường link: <https://www.wireshark.org/download.html>

Trước hết, chúng ta cấu hình để R1 cho phép đồng thời cả hai phương thức Telnet và SSH đến nó:

```
R1(config)#line vty 0 4  
R1(config-line)#transport input telnet ssh  
R1(config-line)#end
```

Trên Host1, chúng ta mở chương trình Wireshark để thực hiện bắt gói trên card mạng LAN (hình 9). Khi cửa sổ giao diện của chương trình hiện ra, chúng ta chọn card mạng LAN của Host1 (“Local Area Connection”), sau đó nhấn vào biểu tượng bắt gói của chương trình để tiến hành bắt gói (hình 9).



Hình 9 – Giao diện chương trình Wireshark.

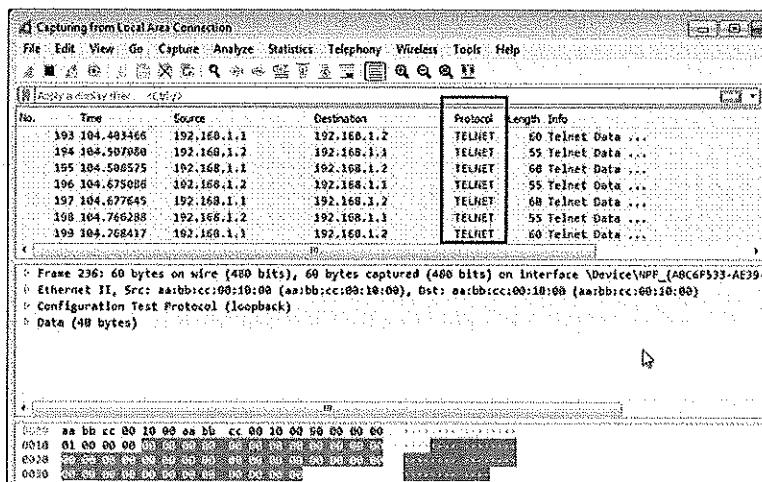
Tiếp theo, ta sử dụng PuTTY để mở một session Telnet đến router R1:

```
User Access Verification

Username: cisco <- Nhập username là "cisco"
Password: <- Nhập password là "waren"
R1>enable
Password: <- Nhập password là "waren"

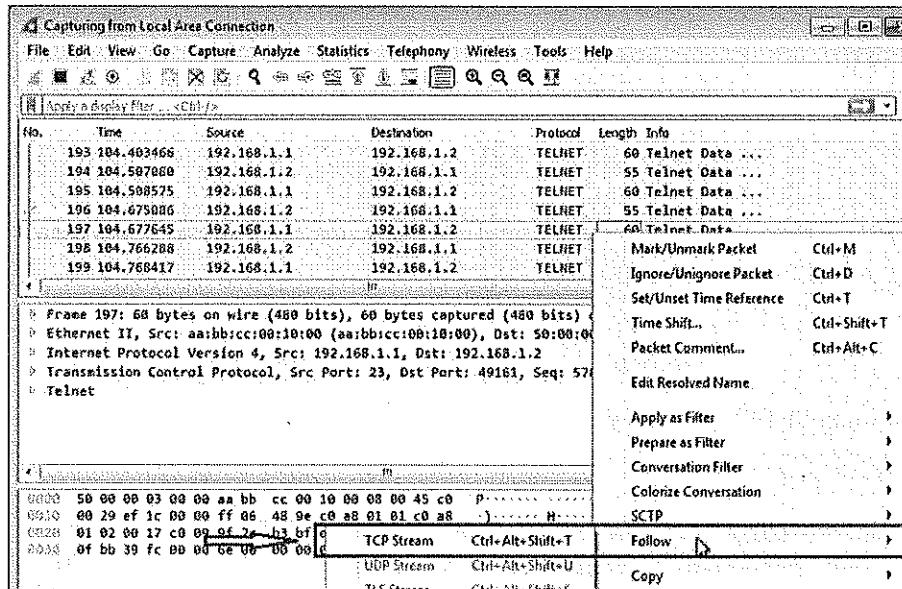
R1#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    192.168.1.1    YES NVRAM  up           up
FastEthernet0/1    192.168.12.1   YES NVRAM  up           up
```

Lưu ý rằng, lúc này để đăng nhập vào được router R1, chúng ta phải xác thực với router bằng username và password của tài khoản đã lưu trên R1 trước đó vì phương thức xác thực trên các cổng VTY đã được thiết lập lại là “`login local`”. Tiếp theo, chúng ta kiểm tra kết quả bắt gói trên Wireshark. Có thể thấy rằng, tất cả các gói Telnet của session Telnet vừa thực hiện đã được Wireshark bắt lại đầy đủ (hình 10):



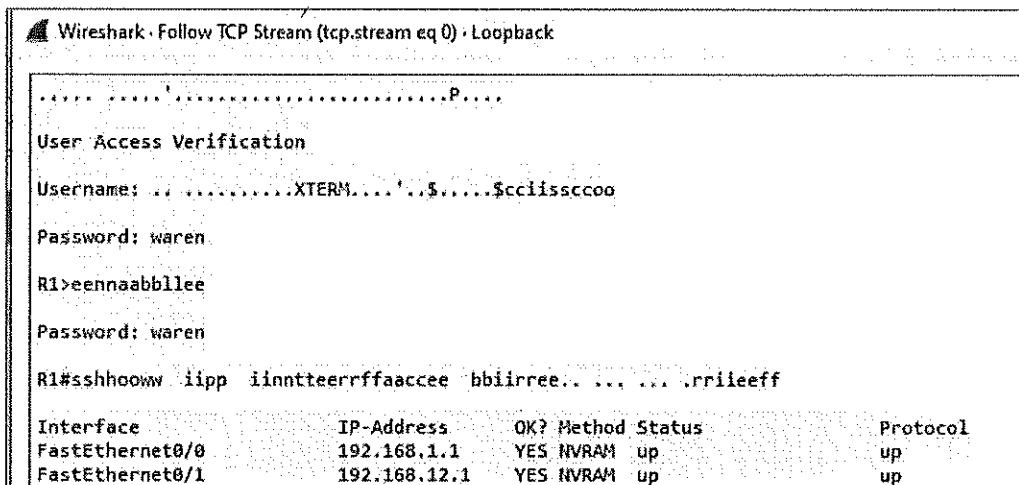
Hình 10 – Wireshark đã bắt được các gói Telnet.

Ta có thể kiểm tra nội dung thông tin mà Wireshark tổng hợp được từ các gói này bằng cách click phái vào một dòng “TELNET” bất kỳ rồi chọn “Follow”, sau đó là “TCP Stream” (hình 11):



Hình 11 – Xem nội dung thông tin Telnet bắt gói được.

Kết quả bắt gói của session Telnet được hiển thị (hình 12):

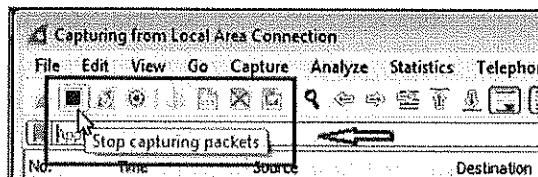


Hình 12 – Kết quả bắt gói Telnet.

Ta thấy rằng tất cả dữ liệu Telnet tương tác giữa Host1 và R1 đều đã được hiển thị trong kết quả bắt gói. Qua đây, ta có thể lấy được luôn cả username và password của tài khoản Telnet, biết được user này đã tương tác những gì với router. Điều này cho thấy Telnet không hề mã hóa dữ liệu của mình và khi bị capture, tất cả đều bị phơi bày một cách t胡ng minh. Telnet không có tính bảo mật.

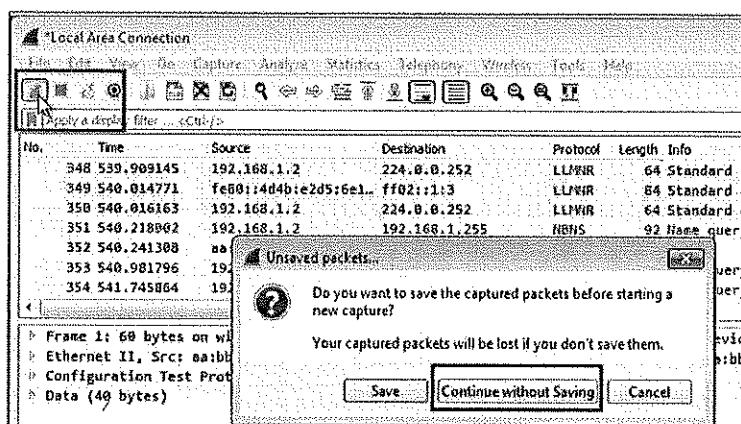
Tiếp theo, chúng ta thực hiện bắt các gói SSH để thấy rằng SSH có mã hóa thông tin được trao đổi, từ đó xác nhận rằng SSH có tính bảo mật cao hơn Telnet.

Trước hết, chúng ta tắt hoạt động bắt gói đang diễn ra ở trên bằng cách click vào biểu tượng “Stop” ở góc trái màn hình giao diện Wireshark (hình 13):



Hình 13 – Kết thúc bắt gói.

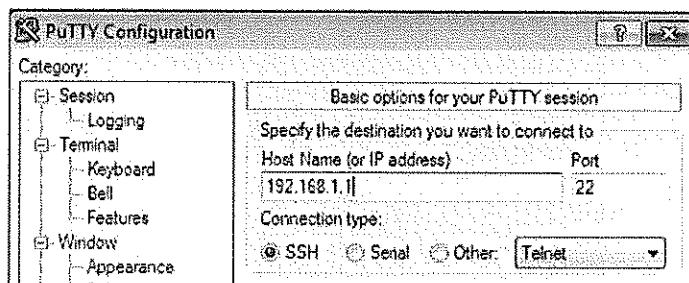
Tiếp theo, chúng ta nhấn vào biểu tượng khởi động bắt gói để thực hiện một lượt bắt gói mới; khi đó một cửa sổ hiện ra hỏi ý kiến, chúng ta chọn “Continue without Saving” (hình 14):



Hình 14 – Khởi tạo một lượt bắt gói mới.

Sau khi nhấn xong “Continue without Saving”, Wireshark bắt đầu thực hiện bắt gói trên card mạng của Host1.

Trên Host1, chúng ta sử dụng PuTTY mở một session SSH đến R1 (hình 15):



Hình 15 – Sử dụng PuTTY mở SSH đến R1.

Sau khi nhập username và password đăng nhập thiết bị, chúng ta cũng tương tác một số lệnh với R1 giống như đã làm với Telnet ở trên:

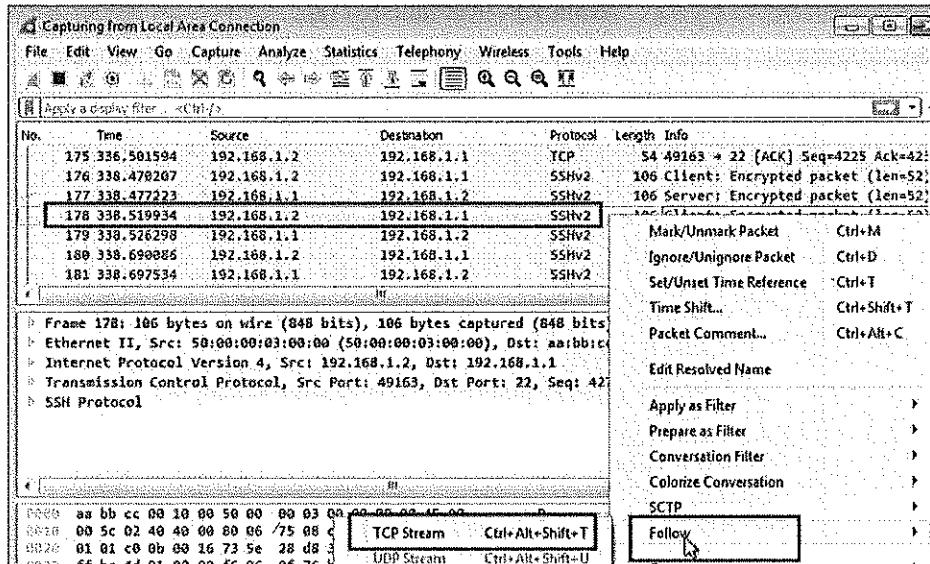
```
login as: cisco <- Nhập username là "cisco"
Using keyboard-interactive authentication.
Password: <- Nhập password là "waren"
R1>enable
```

Password: <- Nhập password là "waren"

R1#show ip interface brief

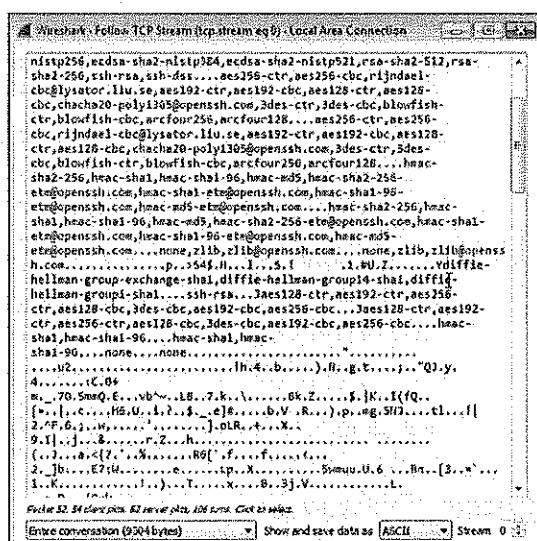
Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.1.1	YES	NVRAM	up	up
FastEthernet0/1	192.168.12.1	YES	NVRAM	up	up

Giống như đã làm với Telnet, chúng ta click phải vào một dòng SSHv2 bất kỳ trong cửa sổ Wireshark, chọn “Follow”, rồi chọn “TCP stream” để xem kết quả tổng hợp được từ việc bắt gói các gói SSH (hình 16):



Hình 16 – Xem thông tin bắt gói SSH.

Kết quả bắt gói SSH thu được (hình 17):

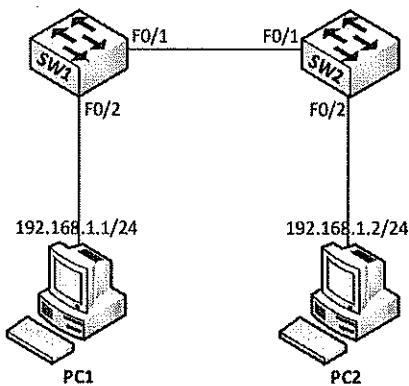


Hình 17 – Kết quả bắt gói SSH.

Ta thấy, lần bắt gói này, kết quả thu được chỉ là những kí tự đã được mã hóa, chúng ta không đọc được bất kỳ thông tin nào trong session SSH mà Host1 trao đổi với R1, SSH đã thực hiện mã hóa toàn bộ những thông tin này. Như vậy, SSH có tính bảo mật cao hơn Telnet rất nhiều và trong thực tế, SSH được khuyến nghị sử dụng để truy nhập từ xa đến thiết bị thay cho Telnet.

Lab 4 – Tổng quan hoạt động của Switch

Sơ đồ:



Hình 1 – Sơ đồ bài Lab.

Mô tả:

- Sơ đồ Lab gồm 2 Switch và 2 PC được đấu nối với nhau như hình 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, enable,... Đặt địa chỉ IP trên 2 PC được chỉ ra như trên hình 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-100	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 hình 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 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 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:

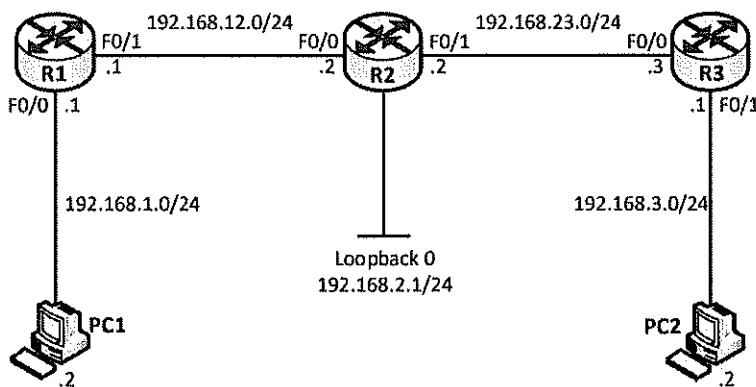
```
C:\Users\PC2>ipconfig/all
```

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . :  
Description . . . . . : Intel<R> PRO/100 VE Network Connnection  
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 . . . . . :
```

Lab 5 – Static Routing

Sơ đồ:



Hình 1 – Sơ đồ bài Lab.

Mô tả:

- Sơ đồ Lab gồm 3 Router và 2 PC được đấu nối với nhau như hình 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 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 Routing

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
```

Ta 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
```

Từ mỗi 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

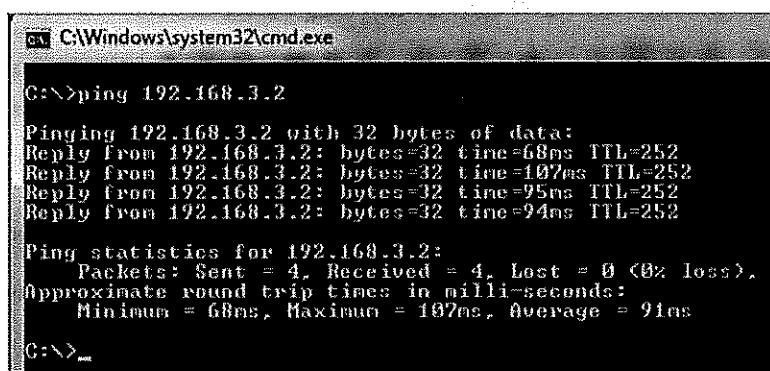
R2#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/43/60ms

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 kiểm tra giữa các host

Thực hiện ping từ PC1 đến PC2 (hình 2):



The screenshot shows a Windows Command Prompt window titled 'cmd C:\Windows\system32\cmd.exe'. The command 'ping 192.168.3.2' was entered, resulting in the following output:

```
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

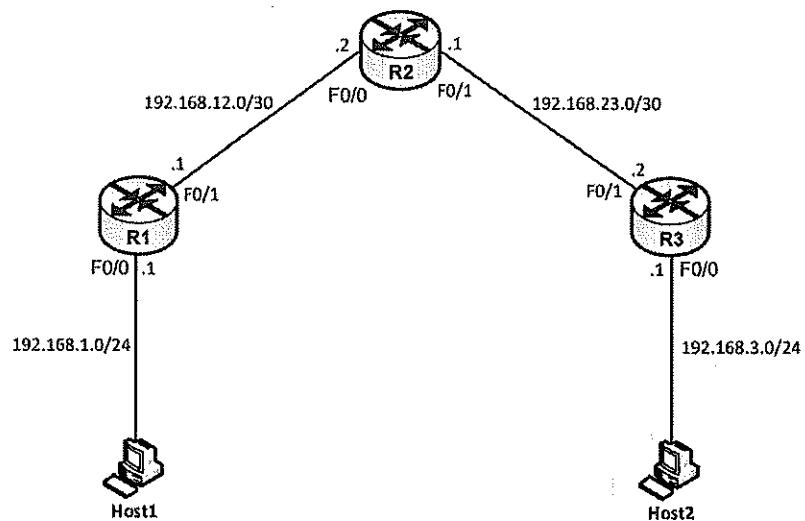
Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 68ms, Maximum = 107ms, Average = 91ms

C:\>
```

Hình 2 – PC1 ping PC2.

Lab 6 – Static routing, DHCP

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Bài lab gồm 3 router và 2 host được kết nối với nhau như hình 1.
- Trong bài lab này, các bạn học viên sẽ thực hiện cấu hình định tuyến tĩnh (static routing) đồng thời cấu hình dịch vụ cấp phát IP tự động cho các host bằng giao thức DHCP.

Yêu cầu:

1. Cấu hình cơ bản:

- Thực hiện cấu hình địa chỉ IP trên các interface của các router theo quy hoạch IP được chỉ ra trên hình 1.
- Các host không cần cấu hình IP mà sẽ được nhận IP tự động từ DHCP trong bước sau của bài lab.

2. Static routing:

- Thực hiện cấu hình static route trên các router đảm bảo mọi địa chỉ trên sơ đồ thấy nhau.

3. DHCP:

- Cấu hình R1 đảm nhận vai trò DHCP server cấp phát IP cho Host1. Các IP được cấp phát sẽ nằm trong dải từ 192.168.1.11 đến 192.168.1.199 của mạng 192.168.1.0/24.
- Cấu hình R2 đảm nhận vai trò DHCP server cấp phát IP cho Host2. Các IP được cấp phát sẽ nằm trong dải từ 192.168.3.11 đến 192.168.3.199 của mạng 192.168.3.0/24.

Thực hiện:

1. Cấu hình cơ bản:

Cấu hình:

Trên R1:

```
R1(config)#interface f0/0
R1(config-if)#no shutdown
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface f0/1
R1(config-if)#no shutdown
R1(config-if)#ip address 192.168.12.1 255.255.255.252
R1(config-if)#exit
```

Trên R2:

```
R2(config)#interface f0/0
R2(config-if)#no shutdown
R2(config-if)#ip address 192.168.12.2 255.255.255.252
R2(config-if)#exit
R2(config)#interface f0/1
R2(config-if)#no shutdown
R2(config-if)#ip address 192.168.23.1 255.255.255.252
R2(config-if)#exit
```

Trên R3:

```
R3(config)#interface f0/0
R3(config-if)#no shutdown
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#exit
R3(config)#interface f0/1
R3(config-if)#no shutdown
R3(config-if)#ip address 192.168.23.2 255.255.255.252
R3(config-if)#exit
```

Kiểm tra:

Ta kiểm tra rằng các đường link kết nối giữa các thiết bị đã thông suốt:

```
R1#ping 192.168.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

R2#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 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

2. Static routing:

Cấu hình:

Trên các router, chúng ta thực hiện cấu hình các static route để mọi địa chỉ trên sơ đồ thấy được nhau:

```
R1(config)#ip route 192.168.3.0 255.255.255.0 192.168.12.2
R1(config)#ip route 192.168.23.0 255.255.255.252 192.168.12.2

R2(config)#ip route 192.168.1.0 255.255.255.0 192.168.12.1
R2(config)#ip route 192.168.3.0 255.255.255.0 192.168.23.2

R3(config)#ip route 192.168.1.0 255.255.255.0 192.168.23.1
R3(config)#ip route 192.168.12.0 255.255.255.252 192.168.23.1
```

Kiểm tra:

Ta kiểm tra các static route trong bảng định tuyến của các router:

```
R1#show ip route static
(...)
S      192.168.3.0/24 [1/0] via 192.168.12.2
      192.168.23.0/30 is subnetted, 1 subnets
S          192.168.23.0 [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 192.168.23.2

R3#show ip route static
(...)
S      192.168.1.0/24 [1/0] via 192.168.23.1
      192.168.12.0/30 is subnetted, 1 subnets
S          192.168.12.0 [1/0] via 192.168.23.1
```

Ta kiểm tra rằng các mạng nội bộ của R1 và R3 đã có thể đi đến nhau:

```
R1#ping 192.168.3.1 source 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Từ router R2 có thể đi đến được các mạng nội bộ trên R1 và R3:

```
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 = 1/1/1 ms

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 = 1/1/1 ms
```

3. DHCP:

Cấu hình:

Ta cấu hình để R1 đảm nhận vai trò DHCP server tự cấp IP cho mạng LAN của mình:

```
R1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
R1(config)#ip dhcp excluded-address 192.168.1.200 192.168.1.254
R1(config)#ip dhcp pool LAN1
R1(dhcp-config)#network 192.168.1.0 /24
R1(dhcp-config)#default-router 192.168.1.1
R1(dhcp-config)#exit
```

Tiếp theo, ta cấu hình để R2 đảm nhận vai trò DHCP server cấp phát IP cho mạng LAN của R3:

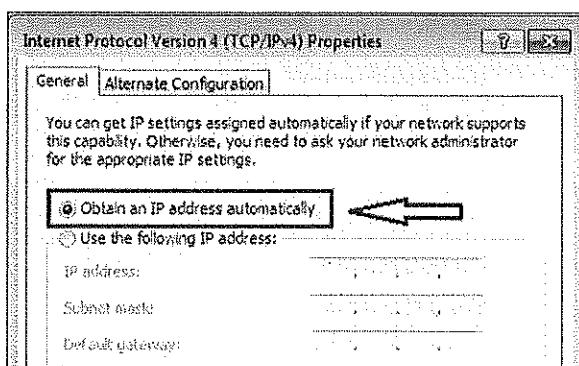
```
R2(config)#ip dhcp excluded-address 192.168.3.1 192.168.3.10
R2(config)#ip dhcp excluded-address 192.168.3.200 192.168.3.254
R2(config)#ip dhcp pool LAN3
R2(dhcp-config)#network 192.168.3.0 /24
R2(dhcp-config)#default-router 192.168.3.1
R2(dhcp-config)#exit
```

Ta còn phải cấu hình thêm R3 thành DHCP Relay Agent để mạng LAN của R3 có thể nhận được IP từ DHCP server R2:

```
R3(config)#interface f0/0
R3(config-if)#ip helper-address 192.168.23.1
R3(config-if)#exit
```

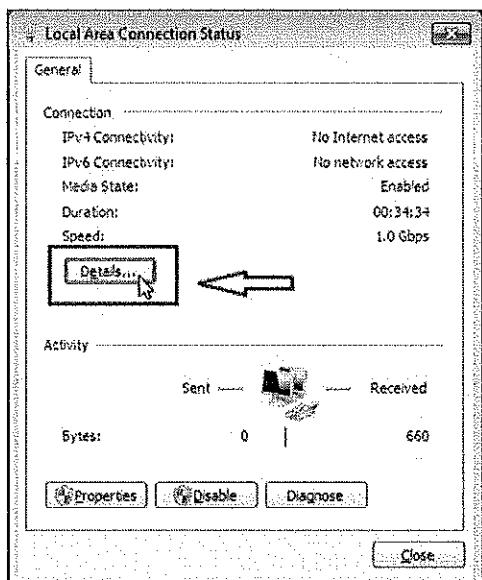
Kiểm tra:

Ta kiểm tra rằng Host1 đã có thể nhận IP động từ DHCP server R1. Trên cửa sổ cấu hình card mạng của Windows, ta hiệu chỉnh để card mạng Host1 nhận IP một cách tự động (hình 2):



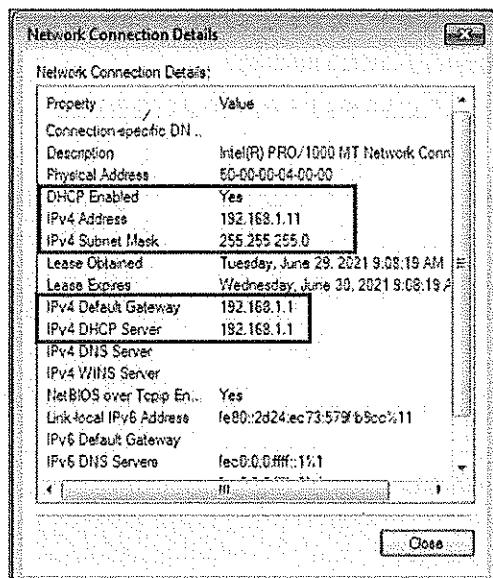
Hình 2 – Hiệu chỉnh card mạng nhận IP một cách tự động.

Lúc này, Windows trên Host1 sẽ tự xin cấp phát IP bằng DHCP, nếu DHCP cấp IP thành công, card mạng của Host1 sẽ nhận được IP trong dải địa chỉ cấp phát đã cấu hình trên R1. Ta kiểm tra điều này bằng cách nhấn phím “Details...” trong cửa sổ cấu hình card mạng của Windows (hình 3):



Hình 3 – Chọn xem thông tin chi tiết trên card mạng,

Thông tin IP trên card mạng của Host1 (hình 4):



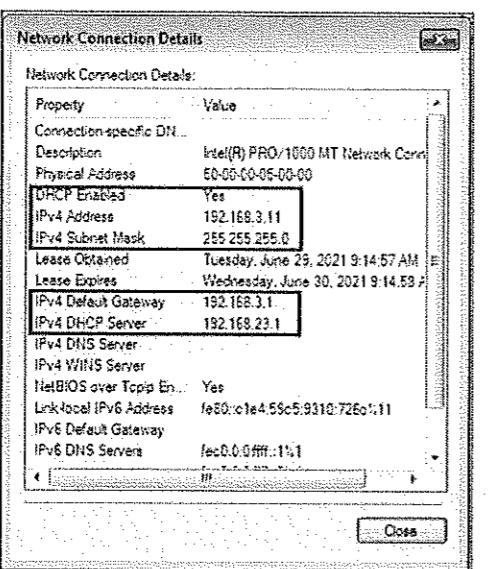
Hình 4 – Thông tin IP trên card mạng của Host1.

Ta thấy, Host1 đã nhận được cấu hình IP từ DHCP server R1.

Bên cạnh việc sử dụng giao diện đồ họa, ta cũng có thể sử dụng các lệnh sau trong cửa sổ CMD của Windows để cấu hình card mạng nhận IP từ DHCP:

```
C:\>ipconfig /release <- Xóa bỏ cấu hình IP cũ  
C:\>ipconfig /renew <- Xin cấp phát cấu hình IP mới
```

Ta kiểm tra rằng Host2 cũng đã nhận được IP từ DHCP server R2 (hình 5):



Hình 5 – Thông tin IP trên card mạng của Host2.

Như vậy cả Host1 và Host2 (đại diện cho mạng LAN của R1 và R3) đều đã nhận được cấu hình IP từ DHCP.

Ta kiểm tra dữ liệu trên hai DHCP server R1 và R2 để thấy rằng các thiết bị này đã thực hiện hoạt động cấp phát IP trong các pool của mình:

```
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       0150.0000.0400.00   Jun 30 2021 11:08 AM  Automatic

R2#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/          Lease expiration      Type
                  Hardware address/
                  User name
192.168.3.11       0150.0000.0500.00   Jun 30 2021 11:15 AM  Automatic
```

Trong DHCP, mỗi DHCP client (thiết bị xin IP) sẽ được định danh bằng một Client – ID. Client – ID sẽ có định dạng tùy vào hệ điều hành được sử dụng trên host đi xin IP. Với Windows, giá trị này sẽ được xây dựng bằng cách lấy prefix “01” gắn vào địa chỉ MAC trên card mạng của host. Ví dụ:

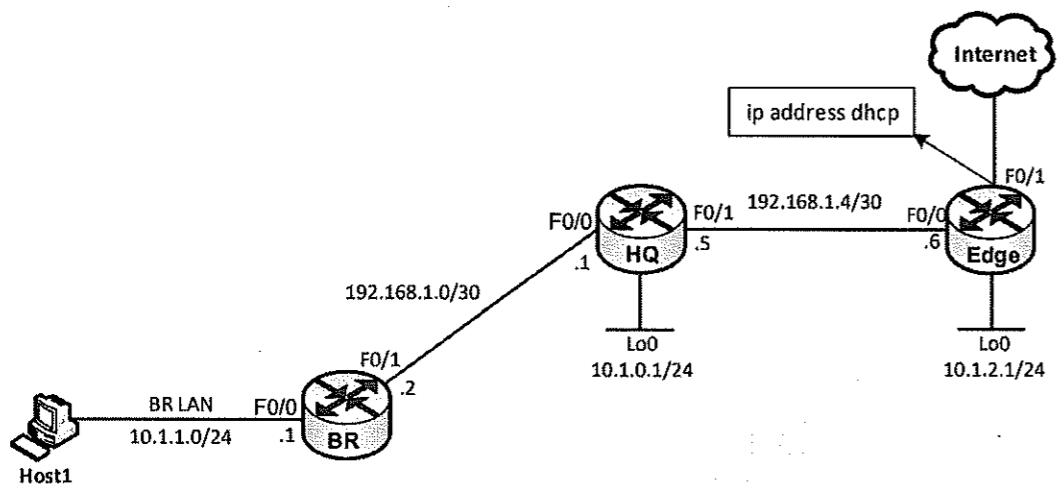
- Host1 có địa chỉ MAC là “50-00-00-04-00-00” thì Client – ID sẽ là “0150.0000.0400.00”.
- Host2 có địa chỉ MAC là “50-00-00-05-00-00” thì Client – ID sẽ là “0150.0000.0500.00”.

Trong kết quả show ở trên, ta thấy rõ ràng các DHCP server đã cấp phát được IP cho các host thuộc các mạng LAN mà chúng phụ trách.

Đến đây, chúng ta đã hoàn thành việc thiết lập và kiểm tra cấu hình DHCP trong bài lab.

Lab 7 – Static routing, DHCP, Internet

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Bài lab gồm 3 router và 1 PC được kết nối với nhau theo sơ đồ trên hình 1. Trong đó, các router đóng vai trò như các gateway của các chi nhánh của một mạng doanh nghiệp, gồm: HQ (Headquarters) – Trụ sở chính, BR (Branch) – Chi nhánh và Edge – router biên kết nối đi Internet. PC đóng vai trò như một host đại diện (Host1) của mạng LAN trên chi nhánh. Các mạng LAN của HQ và Edge được già lập bằng các interface loopback 0 của các router HQ và Edge.
- Trên sơ đồ lab này, các bạn học viên sẽ thực tập lại cấu hình static routing đảm bảo mọi địa chỉ trong mạng doanh nghiệp thấy nhau; cấu hình dịch vụ cấp phát IP tự động bằng DHCP và cấu hình để hệ thống mạng có thể cung cấp dịch vụ Internet đến người dùng doanh nghiệp.

Yêu cầu:

1. Cấu hình cơ bản:

- Các bạn học viên thực hiện xóa cấu hình cũ trên thiết bị và thực hiện kết nối thiết bị như sơ đồ lab trên hình 1.
- Thực hiện cấu hình cơ bản cho thiết bị: đặt hostname và đặt IP trên các cổng của các router như được chỉ ra trên hình vẽ. Các bạn học viên chưa cần cấu hình IP cho Host1, host này sẽ nhận IP từ dịch vụ cấp phát IP tự động DHCP.

2. Static routing:

Các bạn học viên thực hiện cấu hình static routing trên các router đảm bảo mọi địa chỉ IP Private trên sơ đồ có thể thấy được nhau.

3. DHCP:

Thực hiện cấu hình router HQ đảm nhận vai trò DHCP server cấp phát IP cho các host thuộc mạng LAN của BR (mạng 10.1.1.0/24).

4. Internet:

- Thực hiện cấu hình các router trên sơ đồ hình 1 để có thể cung cấp dịch vụ truy nhập Internet cho các user trong mạng doanh nghiệp.
- Hoạt động truy nhập Internet được kiểm tra bằng cách truy nhập Internet từ Host1.

Thực hiện:**1. Cấu hình cơ bản:****Cấu hình:**

Chúng ta thực hiện đặt hostname và cấu hình địa chỉ IP trên các router như được chỉ ra trên hình 1.

Trên HQ:

```
Router(config)#hostname HQ
HQ(config)#interface f0/0
HQ(config-if)#no shutdown
HQ(config-if)#ip address 192.168.1.1 255.255.255.252
HQ(config-if)#exit
HQ(config)#interface f0/1
HQ(config-if)#no shutdown
HQ(config-if)#ip address 192.168.1.5 255.255.255.252
HQ(config-if)#exit
HQ(config)#interface loopback 0
HQ(config-if)#ip address 10.1.0.1 255.255.255.0
HQ(config-if)#exit
```

Trên BR:

```
Router(config)#hostname BR
BR(config)#interface f0/0
BR(config-if)#no shutdown
BR(config-if)#ip address 10.1.1.1 255.255.255.0
BR(config-if)#exit
BR(config)#interface f0/1
BR(config-if)#no shutdown
BR(config-if)#ip address 192.168.1.2 255.255.255.252
BR(config-if)#exit
```

Trên Edge:

```
Router(config)#hostname Edge
Edge(config)#interface f0/0
Edge(config-if)#no shutdown
Edge(config-if)#ip address 192.168.1.6 255.255.255.252
```

```
Edge(config-if)#exit
Edge(config)#interface loopback 0
Edge(config-if)#ip address 10.1.2.1 255.255.255.0
Edge(config-if)#exit
```

Kiểm tra:

Chúng ta thực hiện kiểm tra rằng các cổng của các router đều đã được cấu hình địa chỉ IP đúng đắn và đều đã up/up:

```
HQ#show ip interface brief
Interface          IP-Address      OK? Method Status       Protocol
FastEthernet0/0    192.168.1.1    YES manual up        up
FastEthernet0/1    192.168.1.5    YES manual up        up
Serial0/0/0        unassigned     YES unset administratively down down
Serial0/0/1        unassigned     YES unset administratively down down
Loopback0          10.1.0.1      YES manual up        up

BR#show ip interface brief
Interface          IP-Address      OK? Method Status       Protocol
FastEthernet0/0    10.1.1.1      YES manual up        up
FastEthernet0/1    192.168.1.2    YES manual up        up
Serial0/0/0        unassigned     YES unset administratively down down

Edge#show ip interface brief
Interface          IP-Address      OK? Method Status       Protocol
FastEthernet0/0    192.168.1.6    YES manual up        up
FastEthernet0/1    unassigned     YES unset administratively down down
Serial0/0/0        unassigned     YES unset administratively down down
Serial0/0/1        unassigned     YES unset administratively down down
Loopback0          10.1.2.1      YES manual up        up
```

Các đường link kết nối giữa các router đã thông suốt IP:

```
HQ#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 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms

HQ#ping 192.168.1.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.6, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms
```

Đến đây, chúng ta đã hoàn thành yêu cầu cấu hình cơ bản trên các router.

2. Static routing:**Cấu hình:**

Chúng ta cấu hình các static route trên các router để đảm bảo các địa chỉ IP Private của mạng doanh nghiệp có thể thấy nhau:

```
HQ(config)#ip route 10.1.1.0 255.255.255.0 192.168.1.2
HQ(config)#ip route 10.1.2.0 255.255.255.0 192.168.1.6
BR(config)#ip route 10.1.0.0 255.255.255.0 192.168.1.1
BR(config)#ip route 10.1.2.0 255.255.255.0 192.168.1.1
BR(config)#ip route 192.168.1.4 255.255.255.252 192.168.1.1
Edge(config)#ip route 10.1.0.0 255.255.255.0 192.168.1.5
Edge(config)#ip route 10.1.1.0 255.255.255.0 192.168.1.5
Edge(config)#ip route 192.168.1.0 255.255.255.252 192.168.1.5
```

Kiểm tra:

Trước hết, chúng ta kiểm tra bảng định tuyến của các router:

```
HQ#show ip route static
 10.0.0.0/24 is subnetted, 3 subnets
 S   10.1.2.0 [1/0] via 192.168.1.2
 S   10.1.1.0 [1/0] via 192.168.1.6
BR#show ip route static
 10.0.0.0/24 is subnetted, 3 subnets
 S   10.1.2.0 [1/0] via 192.168.1.1
 S   10.1.0.0 [1/0] via 192.168.1.1
 192.168.1.0/30 is subnetted, 2 subnets
 S   192.168.1.4 [1/0] via 192.168.1.1
Edge#show ip route static
 10.0.0.0/24 is subnetted, 3 subnets
 S   10.1.1.0 [1/0] via 192.168.1.5
 S   10.1.0.0 [1/0] via 192.168.1.5
 192.168.1.0/30 is subnetted, 2 subnets
 S   192.168.1.0 [1/0] via 192.168.1.5
```

Tiếp theo, chúng ta kiểm tra rằng các mạng LAN đã có thể đi đến nhau được:

```
HQ#ping 10.1.1.1 source 10.1.0.1 <- HQ LAN thông suốt IP với BR LAN
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
HQ#ping 10.1.2.1 source 10.1.0.1 <- HQ LAN thông suốt IP với Edge LAN
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Đến đây, chúng ta đã hoàn tất yêu cầu về static routing của bài lab.

Tiếp theo, chúng ta di qua phần cấu hình dịch vụ DHCP.

3. DHCP:

Cấu hình:

Chúng ta thực hiện cấu hình router HQ trở thành DHCP server cấp phát IP cho các host thuộc BR LAN:

```
HQ(config)#ip dhcp excluded-address 10.1.1.1
HQ(config)#ip dhcp pool BR_LAN
HQ(dhcp-config)#network 10.1.1.0 /24
HQ(dhcp-config)#default-router 10.1.1.1
HQ(dhcp-config)#dns-server 8.8.8.8
HQ(dhcp-config)#exit
```

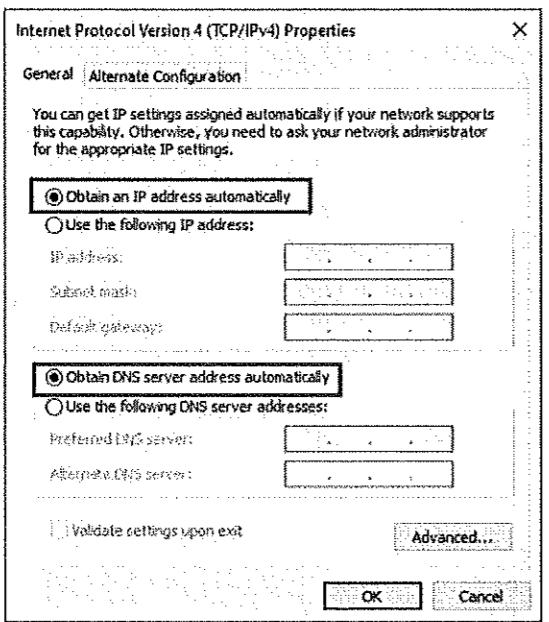
Các bạn đừng quên cấu hình router BR thành DHCP Relay Agent:

```
BR(config)#interface f0/0
BR(config-if)#ip helper-address 192.168.1.1
BR(config-if)#exit
```

Kiểm tra:

Trước hết, chúng ta kiểm tra rằng Host1 đã có thể nhận được IP từ DHCP.

Hiệu chỉnh card mạng của Host1 nhận IP tự động từ DHCP (hình 2):



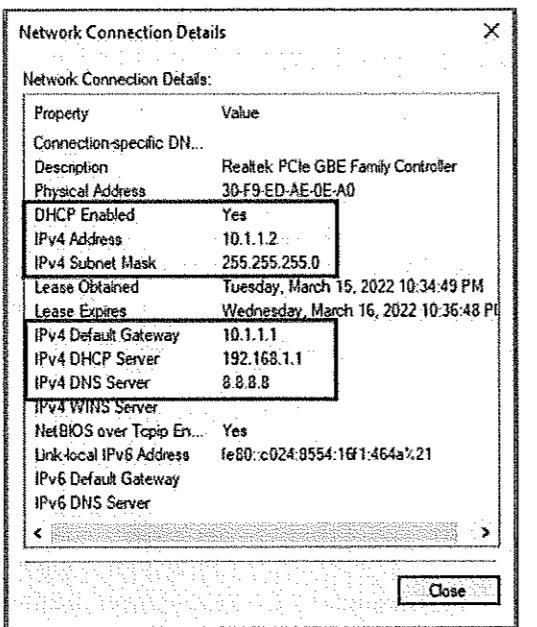
Hình 2 – Cấu hình Host1 nhận IP tự động từ DHCP.

Chúng ta cũng có thể vào cửa sổ CMD của Windows, sử dụng các lệnh:

```
C:>ipconfig /release
C:>ipconfig /renew
```

Các bạn học viên có thể xem lại bài lab 6 về vấn đề này.

Host1 đã nhận được IP tự động từ DHCP (hình 3):



Hình 3 – Host1 đã nhận được cấu hình IP từ DHCP.

Ta kiểm tra rằng router HQ đã thực sự cấp phát được IP xuống cho Host1:

```
HQ#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/          Lease expiration      Type
                  Hardware address/
                  User name
10.1.1.2        0130:f9ed,ae0e,a0    Jan 02 1970 12:19 AM  Automatic
```

(Ta có thể đối chiếu DHCP Client – ID trong kết quả show ở trên với địa chỉ MAC trên card mạng của Host1 để thấy rằng router HQ đã thực sự cấp phát IP xuống cho Host1.)

Đến đây, chúng ta đã hoàn thành yêu cầu về cấu hình DHCP.

4. Internet:

Cấu hình:

Trong mục tiếp theo, chúng ta sẽ cấu hình trên các router để các mạng LAN có thể truy nhập được Internet. Đây là một thao tác gần như bắt buộc mà người quản trị sẽ gặp trong các mạng doanh nghiệp. Để cung cấp được dịch vụ Internet đến các end – user, người quản trị cần phải thực hiện được hai vấn đề sau trên các router dẫn đường: *cấu hình default – route trên các router (default – routing)* và *thực hiện NAT trên router biên*.

Default – routing:

Ta cấu hình để cổng Internet F0/1 của router Edge nhận được IP từ DHCP:

```
Edge(config)#interface f0/1
Edge(config-if)#no shutdown
Edge(config-if)#ip address dhcp
Edge(config-if)#exit
```

Trong bài lab này, cổng F0/1 của router Edge sẽ được kết nối đến gateway Internet của Trung tâm. Khi thực hiện thao tác ở trên, gateway Internet của WAREN sẽ cấp phát xuống cổng F0/1 của router Edge một địa chỉ IP mặt ngoài, đồng thời cấp xuống luôn một default – gateway. Router Edge sẽ cập nhật IP cho cổng F0/1 và tự động phát sinh một default static route với next – hop IP chính là IP của default – gateway được cấp xuống.

Ta kiểm tra điều này trên router Edge:

```
Edge#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    192.168.1.6   YES NVRAM up           up
FastEthernet0/1    192.168.110.237 YES DHCP up           up
Serial0/0/0        unassigned     YES NVRAM administratively down down
Serial0/0/1        unassigned     YES NVRAM administratively down down
Loopback0          10.1.2.1      YES NVRAM up           up

Edge#show ip route static
 10.0.0.0/24 is subnetted, 3 subnets
S   10.1.1.0 [1/0] via 192.168.1.5
S   10.1.0.0 [1/0] via 192.168.1.5
  192.168.1.0/30 is subnetted, 2 subnets
S   192.168.1.0 [1/0] via 192.168.1.5
S*  0.0.0.0/0 [254/0] via 192.168.110.1
```

Lúc này, bản thân router Edge đã có thể truy nhập được Internet:

```
Edge#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 80 percent (4/5), round-trip min/avg/max = 28/28/28 ms
```

Tiếp theo, trên các router BR và HQ, chúng ta thực hiện cấu hình các static default – route chỉ hướng về router Edge:

```
BR(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
HQ(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.6
```

Đến đây, chúng ta đã hoàn thành thao tác thiết lập default – routing cho mạng doanh nghiệp.

NAT:

Network Address Translation – NAT là một kỹ thuật chuyển đổi địa chỉ, cho phép các địa chỉ Private được chuyển đổi thành địa chỉ Public để các host sử dụng IP Private bên trong mạng LAN có thể truy nhập được các tài nguyên trên Internet mà đặt tại các server sử dụng IP Public. NAT là một chuyên đề sẽ được đề cập

chi tiết trong chương 6 của chương trình.Tại thời điểm này, các bạn học viên tạm chấp nhận cấu hình như sau trên router biên để các host nội bộ có thể truy nhập được Internet:

```
Edge(config)#access-list 1 permit any
Edge(config)#ip nat inside source list 1 interface f0/1 overload
Edge(config)#interface f0/0
Edge(config-if)#ip nat inside
Edge(config-if)#exit
Edge(config)#interface f0/1
Edge(config-if)#ip nat outside
Edge(config-if)#exit
```

Kiểm tra:

Các router đều đã có default – route phục vụ truy nhập Internet:

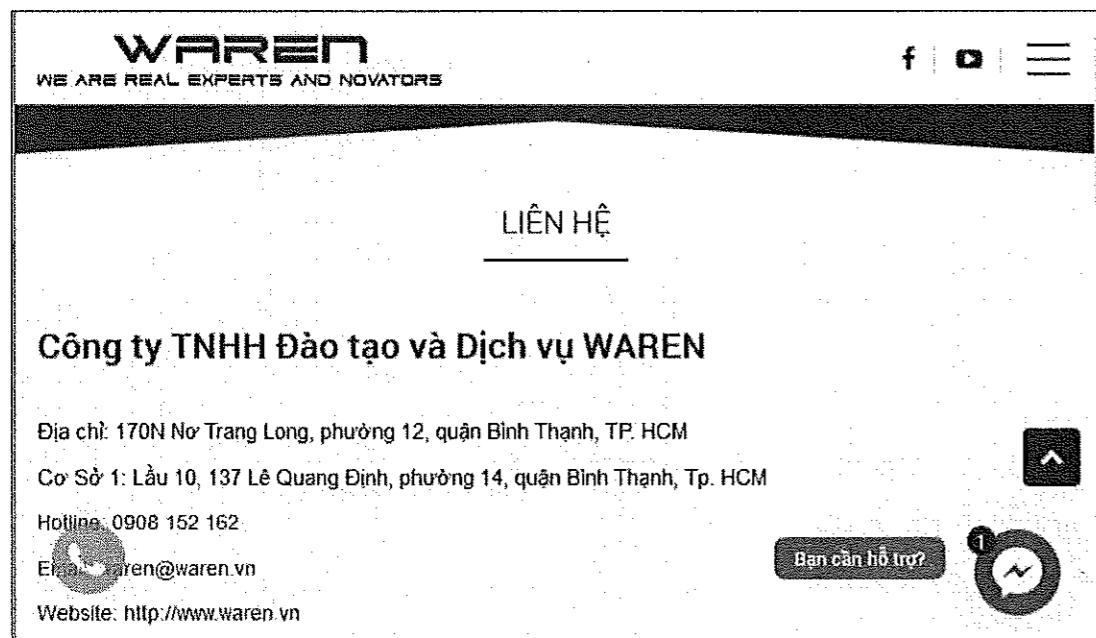
```
Edge#show ip route static
 10.0.0.0/24 is subnetted, 3 subnets
 S   10.1.1.0 [1/0] via 192.168.1.5
 S   10.1.0.0 [1/0] via 192.168.1.5
 192.168.1.0/30 is subnetted, 2 subnets
 S   192.168.1.0 [1/0] via 192.168.1.5
 S* 0.0.0.0/0 [254/0] via 192.168.110.1

HQ#show ip route static
 10.0.0.0/24 is subnetted, 3 subnets
 S   10.1.2.0 [1/0] via 192.168.1.6
 S   10.1.1.0 [1/0] via 192.168.1.2
 S* 0.0.0.0/0 [1/0] via 192.168.1.6

BR#show ip route static
 10.0.0.0/24 is subnetted, 3 subnets
 S   10.1.2.0 [1/0] via 192.168.1.1
 S   10.1.0.0 [1/0] via 192.168.1.1
 192.168.1.0/30 is subnetted, 2 subnets
 S   192.168.1.4 [1/0] via 192.168.1.1
 S* 0.0.0.0/0 [1/0] via 192.168.1.1
```

Trên các host, chúng ta sử dụng trình duyệt web để lướt một trang web bất kỳ để kiểm chứng rằng các host lúc này đã có thể truy nhập được Internet.

Truy nhập web trên Host1 (hình 4):

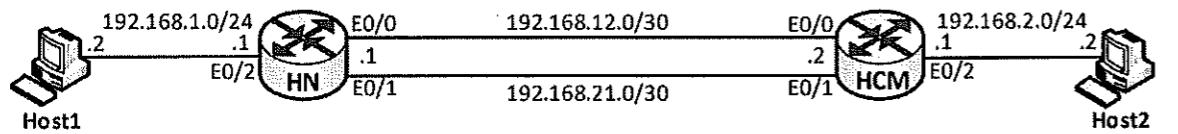


Hình 4 – Truy nhập web thành công trên Host1.

Đến đây, chúng ta đã hoàn thành yêu cầu đặt ra của bài lab.

Lab 8 – Dự phòng cho Static route

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Bài lab giả lập một mạng doanh nghiệp có hai chi nhánh tại Hà Nội (router HN) và TPHCM (router HCM) được kết nối với nhau bởi hai đường truyền WAN Ethernet (giữa các cặp cổng E0/0 và E0/1 của hai router).
- Trên sơ đồ lab này, các bạn học viên thực tập cấu hình dự phòng đường đi với static routing.

Yêu cầu:

Hãy sử dụng kỹ thuật static routing đảm bảo hoạt động di chuyển dữ liệu giữa hai chi nhánh của doanh nghiệp vừa nêu đạt yêu cầu như sau:

- Lưu lượng đi từ HN đến HCM sẽ sử dụng đường trên (nối giữa hai cổng E0/0) là đường chính, còn đường dưới (nối giữa hai cổng E0/1) chỉ để dự phòng.
- Lưu lượng đi từ HCM đến HN sẽ sử dụng đường dưới (nối giữa hai cổng E0/1) là đường chính, còn đường trên (nối giữa hai cổng E0/0) chỉ để dự phòng.

Thực hiện:

Cấu hình:

Để thực hiện yêu cầu đặt ra, chúng ta sử dụng tham số AD trong cấu hình static route, theo nguyên tắc: đường được gán AD nhỏ hơn sẽ là đường chính, còn đường được gán AD lớn hơn sẽ là đường dự phòng. Ngoài ra, ta còn kết hợp thêm hoạt động track với IP SLA vào static routing để các router có thể giám sát được tính thông suốt của đường truyền, từ đó có thể chuyển đổi từ đường chính sang đường dự phòng khi xảy ra sự cố.

Trước hết, ta thực hiện yêu cầu với chiều từ HN đến HCM.

Đầu tiên, ta cấu hình một IP SLA ping kiểm tra link chính bằng cách tự động ping liên tục từ địa chỉ 192.168.12.1 đến 192.168.12.2:

```
HN(config)#ip sla 1
HN(config-ip-sla)#icmp-echo 192.168.12.2 source-ip 192.168.12.1
HN(config-ip-sla)#frequency 5
HN(config-ip-sla)#exit

HN(config)#ip sla schedule 1 start-time now life forever
```

Ta cấu hình một track object theo dõi kết quả của IP SLA ping mới cấu hình; track object này sẽ trả kết quả là “Up” nếu ping thành công và “Down” nếu ping không thành công:

```
HN(config)#track 1 ip sla 1
HN(config-track)#exit
```

Cuối cùng, ta cấu hình các static route trên hai link chính và dự phòng và gắn track vào static route trên link chính:

```
HN(config)#ip route 192.168.2.0 255.255.255.0 192.168.12.2 5 track 1
HN(config)#ip route 192.168.2.0 255.255.255.0 192.168.21.2 10
```

(Trong cấu hình ở trên, static route trên đường chính có AD = 5 và trên đường dự phòng AD = 10.)

Ta thực hiện tương tự cho chiều từ HCM đến HN, với đường dưới là đường chính và đường trên là dự phòng:

```
HCM(config)#ip sla 1
HCM(config-ip-sla)#icmp-echo 192.168.21.1 source-ip 192.168.21.2
HCM(config-ip-sla-echo)#frequency 5
HCM(config-ip-sla-echo)#exit
HCM(config)#ip sla schedule 1 start-time now life forever

HCM(config)#track 1 ip sla 1
HCM(config-track)#exit

HCM(config)#ip route 192.168.1.0 255.255.255.0 192.168.21.1 5 track 1
HCM(config)#ip route 192.168.1.0 255.255.255.0 192.168.12.1 10
```

Kiểm tra:

Trước hết, ta kiểm tra cho chiều từ HN đến HCM.

Bảng định tuyến của router HN:

```
HN#show ip route static
(...)
S 192.168.2.0/24 [5/0] via 192.168.12.2
```

Ta thấy, router HN đang chọn next – hop 192.168.12.2 (đường trên) để đi đến mạng LAN 192.168.2.0/24 của HCM, đường này có AD = 5 đúng như đã cấu hình.

Kết quả trace từ Host1 trên LAN của HN đi đến Host2 trên LAN của HCM phản ánh rằng lưu lượng đi từ HN đến HCM được chuyển theo đường trên:

```
Host1> trace 192.168.2.2
trace to 192.168.2.2, 8 hops max, press Ctrl+C to stop
 1  192.168.1.1    0.811 ms  0.700 ms  0.831 ms
 2  192.168.12.2   1.750 ms  1.954 ms  1.804 ms
 3  *192.168.2.2   3.956 ms (ICMP type:3, code:3, Destination port unreachable)
```

Tiếp theo, ta thực hiện shutdown cổng E0/0 của router HCM để giả lập tình huống link chính cho chiều từ HN đến HCM bị sập:

```
HCM(config)#interface e0/0
HCM(config-if)#shutdown
```

Khi link chính down, kết quả track trên HN chuyển sang “Down” và router HN cập nhật lại bảng định tuyến, chuyển sang static route theo đường dưới:

```
*Aug 10 06:43:32.137: %TRACK-6-STATE: 1 ip sla 1 state Up -> Down
HN#show ip route static
(...)
S    192.168.2.0/24 [10/0] via 192.168.21.2
```

Ta thực hiện trace lại từ Host1 đến Host2 để xác nhận rằng lưu lượng từ HN đến HCM đã được chuyển sang đường dự phòng:

```
Host1> trace 192.168.2.2
trace to 192.168.2.2, 8 hops max, press Ctrl+C to stop
1  192.168.1.1    0.945 ms  0.680 ms  0.552 ms
2  192.168.21.2   1.191 ms  1.281 ms  0.910 ms
3  *192.168.2.2   1.073 ms (ICMP type:3, code:3, Destination port unreachable)
```

Ta no shutdown cổng E0/0 của HCM để mở lại đường link chính cho chiều HN đi HCM lại như cũ:

```
HCM(config)#interface e0/0
HCM(config-if)#no shutdown
```

Lúc này, kết quả track trên HN lại trở về "Up" và lưu lượng từ HN đi HCM lại được route theo link chính:

```
*Aug 10 06:51:17.425: %TRACK-6-STATE: 1 ip sla 1 state Down -> Up
HN#show ip route static
(...)
S    192.168.2.0/24 [5/0] via 192.168.12.2

Host1> trace 192.168.2.2
trace to 192.168.2.2, 8 hops max, press Ctrl+C to stop
1  192.168.1.1    0.724 ms  0.779 ms/ 1.268 ms
2  192.168.12.2   7.449 ms  3.574 ms  3.025 ms
3  *192.168.2.2   5.412 ms (ICMP type:3, code:3, Destination port unreachable)
```

Như vậy, hoạt động dự phòng static routing cho chiều từ HN đến HCM đã diễn ra đúng theo yêu cầu.

Ta có thể thực hiện kiểm tra tương tự cho chiều từ HCM đi HN.

Ghi chú:

Trong bài lab lần này, các host không sử dụng hệ điều hành Windows như các bài lab trước mà sử dụng một chương trình giả lập tích hợp sẵn trên EVE. Chương trình giả lập này chỉ tạo ra một PC ảo (VPC) với tính năng rất hạn chế và chỉ có giao diện dòng lệnh; tuy nhiên VPC rất nhẹ, giúp chúng ta tiết kiệm đáng kể tài nguyên thiết bị trong các bài lab. Trong các bài lab không yêu cầu gì cao về các host đầu cuối, chỉ ping, trace và chạy DHCP đơn giản, chúng ta nên sử dụng các VPC này làm host để tiết kiệm tài nguyên.

Một số lệnh cơ bản của VPC thường sử dụng:

- Đặt hostname cho VPC:

```
VPC>set pcname hostname
```

Ví dụ: VPC>set pcname Host1 -> Host1>

- Đặt IP cho VPC:

```
VPC>ip Địa_chi_IP/Prefix_length Default_gateway
```

Ví dụ:

```
Host1>ip 192.168.1.2/24 192.168.1.1
```

VPC này sẽ được gán địa chỉ IP là 192.168.1.2/24 và được thiết lập default – gateway là 192.168.1.1.
Để kiểm tra cấu hình IP đã thiết lập, ta sử dụng lệnh:

```
VPC>show ip
```

Ví dụ:

```
Host1> show ip
```

NAME	:	Host1{1}
IP/MASK	:	192.168.1.2/24
GATEWAY	:	192.168.1.1
DNS	:	
MAC	:	00:50:79:66:68:03
LPORT	:	20000
RHOST:PORT	:	127.0.0.1:30000
MTU	:	1500

- Ping:

```
VPC>ping Địa_chỉ_IP
```

Ví dụ:

```
Host1> ping 192.168.1.1
84 bytes from 192.168.1.1 icmp_seq=1 ttl=255 time=0.741 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=255 time=0.888 ms
(...)
```

- Trace:

```
VPC>trace Địa_chỉ_IP
```

Ví dụ: có thể xem trong bài lab ở trên.

- Sau khi thiết lập xong các thông số, các bạn học viên có thể lưu lại cấu hình đã thiết lập trên VPC:

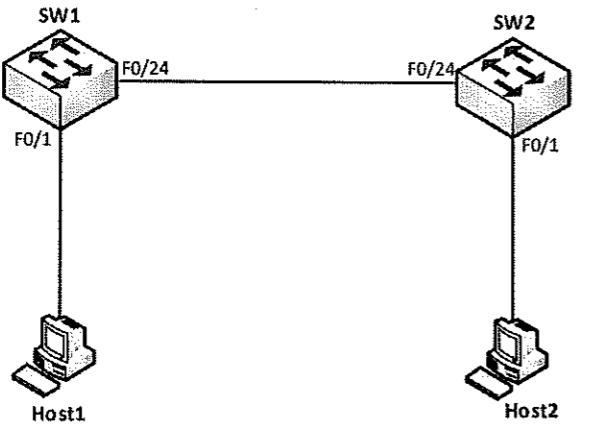
```
VPC>save
```

Ví dụ:

```
Host1> save
Saving startup configuration to startup.vpc
. done
```

Lab 9 – VLAN, Trunking

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Bài lab gồm hai switch và hai host được kết nối với nhau như trên sơ đồ hình 1.
- Trong bài lab này, các bạn học viên sẽ thực tập cấu hình VLAN trên switch và kiểm tra cấu hình VLAN này.

Yêu cầu:

1. Cấu hình VLAN:

Trên các switch SW1 và SW2 thực hiện tạo cấu hình VLAN như sau:

- VLAN 1:
 - Name: “default”.
 - Các port: F0/1 – F0/8.
- VLAN 2:
 - Name: “CCNA”.
 - Các port: F0/9 – F0/16.
- VLAN 3:
 - Name: “CCNP”.
 - Các port: F0/17 – F0/23.

2. Cấu hình Trunking:

- Thực hiện cấu hình đường link kết nối giữa hai switch trở thành đường trunk.
- Đường trunk này sử dụng phương pháp trunking IEEE 802.1Q.

3. Kiểm tra giao tiếp giữa hai host:

- Thực hiện cấu hình IP trên Host1 và Host2 lần lượt là 192.168.1.1/24 và 192.168.1.2/24.
- Kiểm tra rằng khi hai host được kết nối vào cùng một VLAN chúng có thể giao tiếp được với nhau và khi kết nối khác VLAN chúng không thể giao tiếp được với nhau.

Thực hiện:

1. Cấu hình VLAN:

Cấu hình:

Trên SW1 và SW2:

```
SW1-2(config)#vlan 2
SW1-2(config-vlan)#name CCNA
SW1-2(config-vlan)#exit
SW1-2(config)#vlan 3
SW1-2(config-vlan)#name CCNP
SW1-2(config-vlan)#exit

SW1-2(config)#interface range f0/9 - 16
SW1-2(config-if-range)#switchport mode access
SW1-2(config-if-range)#switchport access vlan 2
SW1-2(config-if-range)#exit

SW1-2(config)#interface range f0/17 - 23
SW1-2(config-if-range)#switchport mode access
SW1-2(config-if-range)#switchport access vlan 3
SW1-2(config-if-range)#exit
```

Ghi chú:

Các thao tác xây dựng cấu hình VLAN gồm các bước cơ bản như được trình bày dưới đây.

Tạo VLAN:

Sử dụng lệnh “vlan” trên mode Global configuration:

```
Switch(config)#vlan vlan-id
Switch(config-vlan)#

```

Mỗi VLAN được tạo ra sẽ được xác định bởi một *vlan – id*. Theo chuẩn 802.1Q của IEEE, dải giá trị của *vlan – id* chạy từ 0 đến 4095, bao gồm:

- 1 đến 1001*: Dải VLAN thông thường, chúng ta thường sử dụng các VLAN trong dải này.
- 1002 đến 1005*: Dải VLAN được dùng để giao tiếp với hệ thống mạng LAN kiểu Token Ring.
- 1006 đến 4094*: Dải VLAN mở rộng, dải này chỉ có thể sử dụng khi chuyển switch về mode hoạt động *Transparent*. Chúng ta sẽ nói về các mode này trong mục về giao thức VTP.
- 0 và 4095*: Dành riêng, không sử dụng cho các mục đích chia VLAN thông thường.
- Mặc định, các VLAN 1, 1002 đến 1005 luôn tồn tại trên switch, ta không thể xóa bỏ các VLAN này.

Đặt tên cho VLAN:

Ta thường đặt tên cho VLAN để hỗ trợ cho việc quản lý VLAN. Nếu không cấu hình đặt tên của VLAN, tên VLAN sẽ tự động được xây dựng dựa trên *vlan - id* của VLAN.

```
Switch(config-vlan)#name Tên_VLAN
```

Gán cổng vào VLAN:

Sau khi tạo xong các VLAN, chúng ta thường thực hiện gán các cổng trên switch vào các VLAN ấy. Để gán một cổng vào VLAN, chúng ta vào mode “config-if” của cổng ấy và sử dụng các lệnh:

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan vlan-id
```

Mặc định, tất cả các cổng của switch đều thuộc về VLAN 1.

Nếu phải gán một lúc nhiều cổng vào một VLAN, chúng ta sử dụng lệnh “interface range...” để có thể cấu hình cùng lúc trên các cổng này:

```
Switch(config)#interface range interface_list
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan vlan-id
```

Kiểm tra xác nhận cấu hình VLAN đã xây dựng:

Cấu hình VLAN sau khi thực hiện sẽ được lưu trên một file có tên là *vlan.dat* trên bộ nhớ Flash. Để quan sát cấu hình VLAN đã làm, ta cần phải hiển thị nội dung file này bằng lệnh “show vlan”:

```
Switch#show vlan [brief] <- Option “brief” sẽ giúp hiển thị gọn hơn kết quả show.
```

Khi cần phải xóa trắng cấu hình trên switch để thiết lập lại từ đầu, chúng ta nhớ phải xóa cả file *vlan.dat* trong tiến trình xóa vì nếu không cấu hình VLAN cũ sẽ vẫn còn được sử dụng trên switch. Nhóm lệnh xóa trắng cấu hình để thiết lập lại mọi thứ từ đầu trên switch:

```
Switch#erase startup-config
Switch#delete vlan.dat
Switch#reload
```

Kiểm tra:

Ta kiểm tra cơ sở dữ liệu VLAN trên hai switch, ví dụ, SW1:

```
SW1#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 Fa0/24, Fa0/25, Fa0/26, Fa0/27 Fa0/28, Fa0/29, Fa0/30, Fa0/31 Fa0/32, Fa0/33, Fa0/34, Fa0/35 Fa0/36, Fa0/37, Fa0/38, Fa0/39 Fa0/40, Fa0/41, Fa0/42, Fa0/43 Fa0/44, Fa0/45, Fa0/46, Fa0/47 Fa0/48, Gi0/1, Gi0/2, Gi0/3

		Gi0/4
2 CCNA	active	Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16
3 CCNP	active	Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Ta thấy, các VLAN và các cổng trực thuộc đã đạt được giống như yêu cầu của bài lab. Lưu ý rằng, chúng ra không cần phải thực hiện cấu hình name cho VLAN 1 vì mặc định VLAN 1 đã có tên là “default” và chúng ta không thể thay đổi được tên mặc định này. Bên cạnh đó, ban đầu tất cả các cổng đều thuộc VLAN 1 nên chúng ta không cần phải cấu hình gán các cổng F0/1 – F0/8, F0/24 – F0/48 vào VLAN 1. Cổng F0/24 hiện giờ vẫn là một cổng Access thuộc VLAN 1 nhưng trong bước sau ta sẽ chuyển cổng này thành cổng Trunk.

Ta có thể kiểm tra tương tự trên SW2.

2. Cấu hình Trunking:

Cấu hình:

Trên SW1 và SW2:

```
SW1-2(config)#interface f0/24
SW1-2(config-if)#switchport trunk encapsulation dot1q
SW1-2(config-if)#switchport mode trunk
SW1-2(config-if)#exit
```

Ghi chú:

Để thực hiện cấu hình một đường trunk, chúng ta phải vào mode cấu hình của hai cổng ở hai đầu đường trunk và tiến hành cấu hình các thông số như sau:

- Chọn chế độ trunking: Dot1Q hay ISL.

```
Switch(config-if)#switchport trunk encapsulation {dot1q|isl}
```

- Bật chế độ trunk trên cổng:

```
Switch(config-if)#switchport mode trunk
```

Mặc định, đường trunk được thiết lập sẽ cho qua tất cả các VLAN của switch, ta có thể giới hạn lại danh sách VLAN được phép đi qua đường trunk bằng cách sử dụng lệnh:

```
Switch(config-if)#switchport trunk allowed vlan {vlan-list | all | {add | except | remove} vlan-list}
```

Trong đó:

- vlan-list: là một danh sách các VLAN, được phân cách với nhau bởi các dấu phẩy hoặc dấu gạch ngang (“-”).
- all: Tất cả các VLAN từ 1 đến 4094 sẽ được phép đi qua đường trunk. Đây là chế độ mặc định trên một cổng trunk.
- add vlan-list: Thêm một danh sách VLAN mới vào danh sách VLAN hiện có đã được đi qua trên đường trunk.

- **except vlan-list:** Tất cả các VLAN đều được phép đi qua trên đường trunk này ngoại trừ các VLAN nằm trong *vlan-list*.
 - **remove vlan-list:** Gỡ bỏ các VLAN trong *vlan-list* ra khỏi danh sách các VLAN hiện đang được đi qua trên đường trunk.
- Ta cũng có thể hiệu chỉnh chọn Native VLAN trên một cổng trunk. Lưu ý rằng, việc chọn Native VLAN phải thống nhất trên hai cổng nằm ở hai đầu đường trunk. Câu lệnh:

```
Switch(config-if)#switchport trunk native vlan vlan-id
```
 - Sau khi cấu hình xong các đường trunk, chúng ta thường sử dụng các lệnh sau để kiểm tra lại kết quả cấu hình:

```
Switch#show interface [tên_interface] trunk
Switch#show interface switchport
```

Kiểm tra:

Trên các switch SW1 và SW2 thực hiện kiểm tra rằng đường link kết nối giữa hai switch đã được thiết lập trunking:

```
SW1#show interfaces trunk

Port      Mode          Encapsulation  Status        Native vlan
Fa0/24    on           802.1q        trunking     1

Port      Vlans allowed on trunk
Fa0/24    1-4094

Port      Vlans allowed and active in management domain
Fa0/24    1-3

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/24    1-3
```

Kết quả show cho thấy cổng F0/24 đã được thiết lập Trunking theo chuẩn Dot1Q đúng theo yêu cầu đặt ra. Ngoài ra ta cũng thấy có thêm một số thông số khác đáng chú ý:

- “**Vlans allowed on trunk**”:
Đây là danh sách VLAN được phép đi qua cổng Trunk này. Ta thấy danh sách này gồm các VLAN từ 1 đến 4094, đó là tất cả các VLAN có thể sử dụng trên switch Cisco. Như vậy, mặc định, một cổng trunk sẽ cho qua tất cả các VLAN có thể có được trên switch.
- “**Vlans allowed and active in management domain**”:
Đây là danh sách VLAN được phép và đang hoạt động thực sự trên switch mà có thể đi qua trên cổng Trunk. Ta thấy tuy rằng cổng trunk này cho phép 4094 VLAN trong dải VLAN được đi qua nó nhưng hiện tại cũng mới chỉ có 3 VLAN 1, 2, 3 là đang hoạt động và sử dụng đường trunk này mà thôi.
- “**Vlans in spanning tree forwarding state and not pruned**”:
Danh sách các VLAN đang hoạt động trên đường trunk mà không bị khóa bởi giao thức STP (Spanning Tree Protocol) hoặc tính năng VTP Pruning. STP và VTP Pruning sẽ được đề cập trong các phần khác của khóa học. Lúc này, cả 3 VLAN 1, 2, 3 đều không bị khóa trên cổng F0/24.

- Trong ba danh sách VLAN trên cổng trunk vừa nêu, danh sách thứ 3 là tập con của danh sách thứ 2, và danh sách thứ 2 là tập con của danh sách thứ nhất.

Chúng ta có thể kiểm tra tương tự trên SW2.

3. Kiểm tra giao tiếp giữa hai host:

Chúng ta thực hiện đặt IP trên hai host như được chỉ ra trên hình 1, trong đó Host1 nhận địa chỉ IP là 192.168.1.1/24 và Host2 nhận địa chỉ IP là 192.168.1.2/24.

Lúc này, cả hai host đang kết nối vào cổng F0/1 của hai switch nên chúng thuộc cùng VLAN 1, chúng có thể giao tiếp được với nhau:

```
C:\>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

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ta có thể chuyển hai host này sang các VLAN khác, miễn là hai host này thuộc cùng một VLAN thì chúng vẫn có thể giao tiếp với nhau. Ví dụ, trên cả hai switch, ta chuyển chúng sang VLAN 2:

```
SW1-2(config)#interface f0/1
SW1-2(config-if)#switchport access vlan 2
SW1-2(config-if)#exit
```

Hai host vẫn ping nhau thành công:

```
C:\>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

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ta thử chuyển Host2 sang VLAN khác, ví dụ, VLAN 3:

```
SW2(config)#interface f0/1
SW2(config-if)#switchport access vlan 3
SW2(config-if)#exit
```

Lúc này, Host1 và Host2 không còn giao tiếp được với nhau:

```
C:\>ping 192.168.1.2

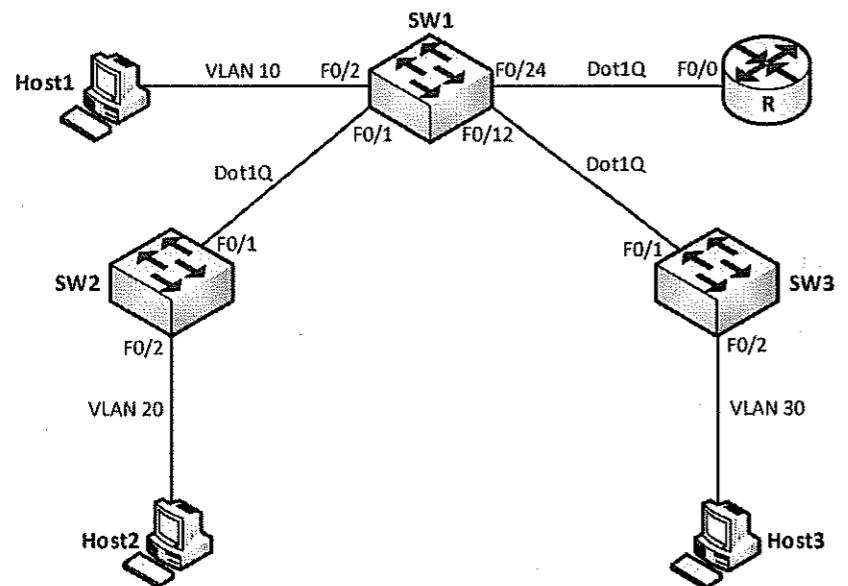
Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Như vậy, các host thuộc các VLAN khác nhau không thể giao tiếp được với nhau, chúng bị cô lập nhau về mặt layer 2.

Lab 10 – VTP, InterVLAN routing

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Bài lab gồm 1 router, 3 switch và 3 host được kết nối với nhau như sơ đồ hình 1.
- Trong bài lab này, các bạn học viên sẽ thực hành cấu hình đồng bộ thông tin VLAN giữa các switch sử dụng giao thức VTP và thực hiện định tuyến giữa các VLAN sử dụng router (giải pháp “Router on a Stick”).

Yêu cầu:

1. Trunking:

- Thực hiện cấu hình tất cả các đường link kết nối giữa các switch thành các đường trunk.
- Các đường trunk này sử dụng chuẩn trunking Dot1Q.

2. VTP, VLAN:

- Cấu hình để 3 switch tham gia VTP domain với các thông số như sau:
 - VTP domain: cisco, VTP password: waren.
 - SW1: server; SW2, SW3: client.
- Trên SW1 thực hiện tạo các VLAN 10, 20, 30. Kiểm tra xác nhận rằng cấu hình VLAN này sẽ được đồng bộ đến các switch SW2 và SW3.
- Trên các switch thực hiện kết nối các host vào các VLAN như được chỉ ra trên sơ đồ hình 1.

3. Định tuyến VLAN:

Cấu hình router R thực hiện định tuyến giữa các VLAN đã tạo trên hệ thống switch theo quy hoạch IP như trên bảng 1:

<i>Sub - interface</i>	<i>VLAN</i>	<i>Địa chỉ</i>	<i>Subnet</i>
F0/0.10	10	172.16.10.1	172.16.10.0/24
F0/0.20	20	172.16.20.1	172.16.20.0/24
F0/0.30	30	172.16.30.1	172.16.30.0/24

Bảng 1 – Quy hoạch IP cho định tuyến VLAN.

4. DHCP:

- Thực hiện cấu hình router R làm DHCP server cấp phát IP cho các host thuộc các VLAN theo quy hoạch IP trên bảng 1.
- Ping kiểm tra giữa các host để xác nhận rằng các host thuộc các VLAN đã có thể đi đến nhau.

Thực hiện:

1. Trunking:

Cấu hình:

Cấu hình:

Trên SW1:

```
SW1(config)#interface range f0/1,f0/12
SW1(config-if-range)#switchport trunk encapsulation dot1q
SW1(config-if-range)#switchport mode trunk
SW1(config-if-range)#exit
```

Trên SW2 và SW3:

```
SW2-3(config)#interface f0/1
SW2-3(config-if)#switchport trunk encapsulation dot1q
SW2-3(config-if)#switchport mode trunk
SW2-3(config-if)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng các đường trunk đã được thiết lập giữa các switch:

```
SW1#show interfaces trunk

Port      Mode          Encapsulation  Status      Native vlan
Fa0/1     on           802.1q        trunking    1
Fa0/12    on           802.1q        trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-4094
```

```
Fa0/12    1-4094

Port      Vlans allowed and active in management domain
Fa0/1     1
Fa0/12   1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1
Fa0/12   1

SW2-3#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
```

2. VTP, VLAN:

Cấu hình:

Thực hiện cấu hình để các switch tham gia VTP như yêu cầu đặt ra:

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

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

Trên SW1, thực hiện tạo các VLAN 10, 20, 30:

```
SW1(config)#vlan 10
SW1(config-vlan)#exit
SW1(config)#vlan 20
SW1(config-vlan)#exit
SW1(config)#vlan 30
SW1(config-vlan)#exit
```

Kiểm tra:

Ta kiểm tra các thông số VTP trên các switch mà chúng ta đã thiết lập.

Trên SW1:

```
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.abfa.0580
Configuration last modified by 0.0.0.0 at 3-1-93 00:13:24
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                : 0xC1 0x6B 0x97 0xF8 0x7D 0x6C 0xBD 0x1E
                           0xB2 0xD1 0x21 0xE7 0xB1 0x56 0xB1 0xC8

SW1#show vtp password
VTP Password: waren
```

Trên SW2, SW3

```
SW2-3#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 3-1-93 00:13:24

Feature VLAN:
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 8
Configuration Revision    : 3
MD5 digest                : 0xC1 0x6B 0x97 0xF8 0x7D 0x6C 0xBD 0x1E
                           0xB2 0xD1 0x21 0xE7 0xB1 0x56 0xB1 0xC8

SW2-3#show vtp password
VTP Password: waren
```

Kết quả kiểm tra cho thấy các thông số VTP trên các switch đã được thiết lập theo đúng yêu cầu đặt ra. Trong các thông số này, chúng ta chú ý đến tham số “Configuration Revision”. Có thể thấy giá trị Revision đã được đồng bộ giữa các switch (=3) và nếu giá trị này giống nhau trên tất cả các switch, chúng đã đồng bộ nhau về cấu hình VLAN. Chúng ta kiểm tra cấu hình VLAN trên các switch để xác nhận điều này:

SW1#show vlan brief		
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, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Fa0/25, Fa0/26 Fa0/27, Fa0/28, Fa0/29, Fa0/30 Fa0/31, Fa0/32, Fa0/33, Fa0/34 Fa0/35, Fa0/36, Fa0/37, Fa0/38 Fa0/39, Fa0/40, Fa0/41, Fa0/42 Fa0/43, Fa0/44, Fa0/45, Fa0/46 Fa0/47, Fa0/48, Gi0/1, Gi0/2 Gi0/3, Gi0/4
10 VLAN0010	active	
20 VLAN0020	active	
30 VLAN0030	active	
(...)		
SW2#show vlan brief		
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, Fa0/24, Fa0/25 Fa0/26, Fa0/27, Fa0/28, Fa0/29 Fa0/30, Fa0/31, Fa0/32, Fa0/33 Fa0/34, Fa0/35, Fa0/36, Fa0/37 Fa0/38, Fa0/39, Fa0/40, Fa0/41 Fa0/42, Fa0/43, Fa0/44, Fa0/45 Fa0/46, Fa0/47, Fa0/48, Gi0/1 Gi0/2, Gi0/3, Gi0/4
10 VLAN0010	active	
20 VLAN0020	active	
30 VLAN0030	active	
(...)		

Sau khi các switch đã được đồng bộ cấu hình VLAN, chúng ta thực hiện gán các cổng của chúng vào các VLAN như được chỉ ra trên hình 1:

```
SW1(config)#interface f0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#exit

SW2(config)#interface f0/2
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 20
SW2(config-if)#exit

SW3(config)#interface f0/2
SW3(config-if)#switchport mode access
SW3(config-if)#switchport access vlan 30
SW3(config-if)#exit
```

Ghi chú:

VTP – VLAN Trunking Protocol là giao thức của Cisco chạy trên các switch giúp chúng đồng bộ cấu hình VLAN với nhau. Thông tin VLAN được đồng bộ sẽ là VLAN – ID và tên của VLAN; các cổng trực thuộc các VLAN sẽ không được đồng bộ, các switch vẫn phải tự gán các cổng của mình vào các VLAN.

VTP có một số đặc điểm đáng chú ý như sau:

- Giữa các switch phải được thiết lập các đường dây nối trunking (Dot1Q hoặc ISL đều được) để chúng có thể chạy VTP với nhau.
- Các switch muốn đồng bộ VLAN bằng VTP phải tham gia chung một VTP domain và phải sử dụng cùng một VTP password (nếu có). Các câu lệnh để khai báo VTP domain và VTP password:

```
SW(config)#vtp domain Domain_name
SW(config)#vtp password Password
```

- Các switch khi tham gia VTP có thể hoạt động ở một trong 3 mode: *Server*, *Transparent*, *Client*.
 - Switch ở mode Server* được toàn quyền thay đổi cấu hình VLAN của nó (tạo VLAN, sửa thông tin của VLAN và xóa VLAN) và những thay đổi này sẽ được đồng bộ đến các switch khác trong domain.
 - Switch ở mode Client* hoàn toàn không được quyền thay đổi cấu hình VLAN của nó, mọi thông tin về VLAN trên switch này đều phải được đồng bộ từ một Server nào đó. Tuy vậy, switch Client vẫn có thể đồng bộ ngược lại cấu hình VLAN của nó đến các switch khác (kể cả Server switch) nếu cấu hình VLAN của nó mới hơn.
 - Switch ở mode Transparent* được quyền thay đổi cấu hình VLAN của nó nhưng hoàn toàn nội bộ. Một switch Transparent sẽ không đồng bộ cấu hình VLAN theo bất kỳ switch nào và cũng không gửi cấu hình VLAN của nó cho các switch khác. Switch Transparent được quyền độc lập về thông tin VLAN với các switch còn lại trong hệ thống. Tuy nhiên, switch Transparent sẽ vẫn chuyển tiếp thông tin VLAN của các switch khác đi ngang qua nó để các switch khác có thể đồng bộ cấu hình VLAN với nhau khi switch Transparent đứng giữa lô tuyễn trao đổi thông tin của các switch này.

- Câu lệnh để thiết lập mode cho switch khi tham gia VTP:

```
SW(config)#vtp mode {server | client | transparent}
```

Trong đó, “server” là mode mặc định của switch: nếu ta không cấu hình gì về mode, switch sẽ hoạt động ở mode server.

4. Để đo đạc “độ mới” của cấu hình VLAN, các switch trong VTP sẽ sử dụng một tham số gọi là *số Revision*. Ban đầu, mỗi switch sẽ đều có giá trị này bằng 0; cứ mỗi lần switch thay đổi cấu hình VLAN (tạo, sửa, xóa VLAN) giá trị này sẽ tăng lên 1 đơn vị. Do đó, switch nào thay đổi cấu hình VLAN nhiều hơn sẽ có giá trị revision lớn hơn và như vậy revision lớn hơn cũng phản ánh rằng cấu hình VLAN tương ứng có tính “cập nhật” hơn, “mới” hơn. Với nguyên tắc này, nếu hai switch tham gia VTP ở mode Server hoặc Client kết nối với nhau, cấu hình VLAN của switch nào có revision lớn hơn sẽ đè lên cấu hình VLAN của switch có revision nhỏ hơn.

Sau khi tất cả các switch trong một VTP domain đồng bộ cấu hình VLAN, giá trị revision trên chúng phải giống nhau. Ta có thể quan sát thông số này trong mục “Configuration Revision” của kết quả lệnh “show vtp status”.

5. Một vài điểm đáng chú ý khác:

- Switch ở mode Transparent được phép sử dụng dải VLAN mở rộng (1006 – 4094).
- Switch ở mode Transparent lưu cấu hình VLAN ở cả file *vlan.dat* và các file config (*running - config* và *startup - config*).
- Để xem VTP password đã cấu hình trên switch, chúng ta không sử dụng lệnh “SW#show vtp status” mà phải sử dụng lệnh show riêng: “SW3#show vtp password”.

3. Định tuyến VLAN:

Cấu hình:

Ta thực hiện cấu hình trên router R tạo các sub – interface như được chỉ ra trên bảng I để kết nối vào các VLAN 10, 20, 30, từ đó đảm nhận vai trò default – gateway cho các host thuộc các VLAN này:

```
R(config)#interface f0/0
R(config-if)#no shutdown
R(config-if)#exit

R(config)#interface f0/0.10
R(config-subif)#encapsulation dot1Q 10
R(config-subif)#ip address 172.16.10.1 255.255.255.0
R(config-subif)#exit

R(config)#interface f0/0.20
R(config-subif)#encapsulation dot1Q 20
R(config-subif)#ip address 172.16.20.1 255.255.255.0
R(config-subif)#exit

R(config)#interface f0/0.30
R(config-subif)#encapsulation dot1Q 30
R(config-subif)#ip address 172.16.30.1 255.255.255.0
R(config-subif)#exit
```

Trên SW1, thực hiện chuyển cổng kết nối đến router R thành cổng Trunk Dot1Q:

```
SW1(config)#interface f0/24
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
SW1(config-if)#exit
```

Kiểm tra:

Ta thực hiện kiểm tra rằng các sub – interface đã được tạo ra đầy đủ trên router R:

R#show ip interface brief				
Interface	IP-Address	OK?	Method	Status
FastEthernet0/0	unassigned	YES	unset	up
FastEthernet0/0.10	172.16.10.1	YES	manual	up
FastEthernet0/0.20	172.16.20.1	YES	manual	up
FastEthernet0/0.30	172.16.30.1	YES	manual	up
FastEthernet0/1	unassigned	YES	unset	administratively down
Serial0/0/0	unassigned	YES	unset	administratively down

Ngoài ra, cổng F0/24 của switch SW1 kết nối đến router R đã hoạt động ở chế độ trunking:

SW1#show interfaces trunk				
Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1
Fa0/12	on	802.1q	trunking	1
Fa0/24	on	802.1q	trunking	1

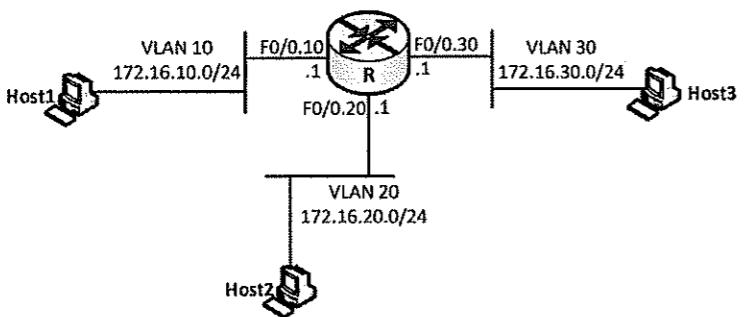
Port	Vlans allowed on trunk
Fa0/1	1-4094
Fa0/12	1-4094
Fa0/24	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,20,30
Fa0/12	1,10,20,30
Fa0/24	1,10,20,30

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1,10,20,30
Fa0/12	1,10,20,30
Fa0/24	1,10,20,30

Ghi chú:

Sau khi thực hiện cấu hình định tuyến VLAN như ở trên, sơ đồ lab của chúng ta có thể được vẽ lại theo góc nhìn layer 3 như trên hình 2:



Hình 2 – Sơ đồ layer 3.

4. DHCP:

Cấu hình:

Ta thực hiện cấu hình router làm DHCP server cấp phát IP cho các host thuộc các VLAN 10, 20, 30:

```
R(config)#ip dhcp excluded-address 172.16.10.1
R(config)#ip dhcp excluded-address 172.16.20.1
R(config)#ip dhcp excluded-address 172.16.30.1

R(config)#ip dhcp pool VLAN10
R(dhcp-config)#network 172.16.10.0 /24
R(dhcp-config)#default-router 172.16.10.1
R(dhcp-config)#exit

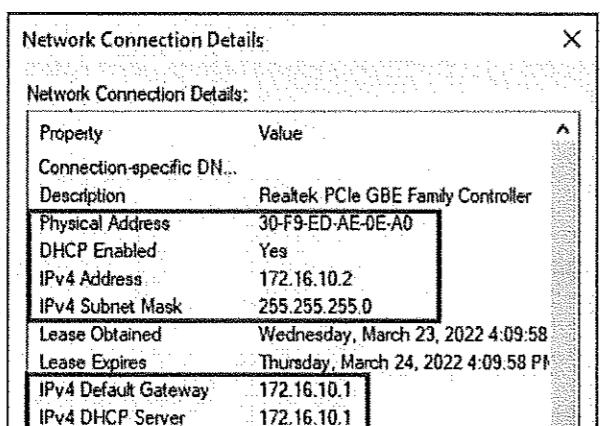
R(config)#ip dhcp pool VLAN20
R(dhcp-config)#network 172.16.20.0 /24
R(dhcp-config)#default-router 172.16.20.1
R(dhcp-config)#exit

R(config)#ip dhcp pool VLAN30
R(dhcp-config)#network 172.16.30.0 /24
R(dhcp-config)#default-router 172.16.30.1
R(dhcp-config)#exit
```

Kiểm tra:

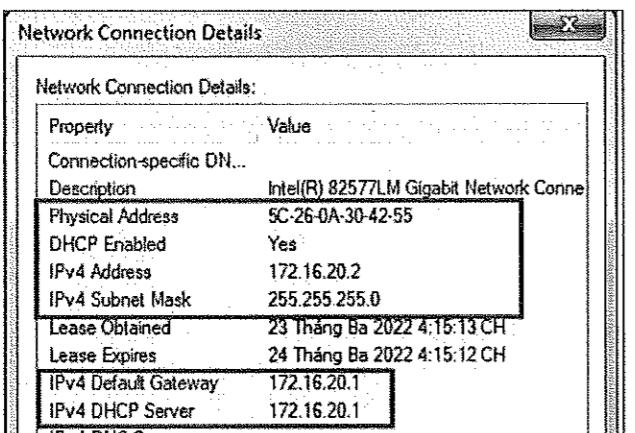
Chúng ta kiểm tra rằng các host đều đã nhận được IP từ DHCP.

Host1 đã nhận được cấu hình IP (hình 3):



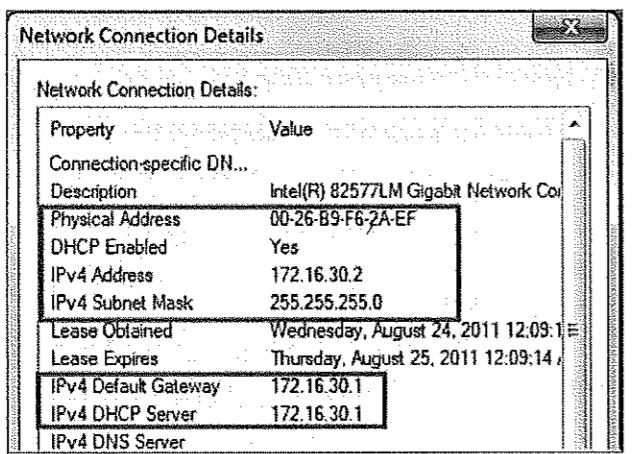
Hình 3 – Host1 nhận được cấu hình IP từ DHCP server.

Host2 đã nhận được cấu hình IP (hình 4):



Hình 4 – Host2 đã nhận được cấu hình IP.

Host 3 đã nhận được cấu hình IP (hình 5):



Hình 5 – Host3 đã nhận được cấu hình IP.

Bảng DHCP binding trên router R:

R#show ip dhcp binding			
Bindings from all pools not associated with VRF:			
IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
172.16.10.2	0130.f9ed.ae0e.a0	Jan 02 1970 01:05 AM	Automatic
172.16.20.2	015c.260a.3042.55	Jan 02 1970 01:10 AM	Automatic
172.16.30.2	0100.26b9.f62a.ef	Jan 02 1970 01:05 AM	Automatic

Cuối cùng, ta kiểm tra rằng các host trên các VLAN ping được nhau.

Host1 trên VLAN 10 ping thành công Host2 trên VLAN 20:

```
C:\>ping 172.16.20.2

Pinging 172.16.20.2 with 32 bytes of data:
Reply from 172.16.20.2: bytes=32 time=2ms TTL=127
Reply from 172.16.20.2: bytes=32 time=1ms TTL=127
Reply from 172.16.20.2: bytes=32 time=1ms TTL=127
Reply from 172.16.20.2: bytes=32 time=1ms TTL=127

Ping statistics for 172.16.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Host1 trên VLAN 10 ping thành công Host3 trên VLAN 30:

```
C:\>ping 172.16.30.2

Pinging 172.16.30.2 with 32 bytes of data:
Reply from 172.16.30.2: bytes=32 time=2ms TTL=127
Reply from 172.16.30.2: bytes=32 time=1ms TTL=127
Reply from 172.16.30.2: bytes=32 time=1ms TTL=127
Reply from 172.16.30.2: bytes=32 time=1ms TTL=127

Ping statistics for 172.16.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Host2 trên VLAN 20 ping thành công Host3 trên VLAN 30:

```
C:\>ping 172.16.30.2

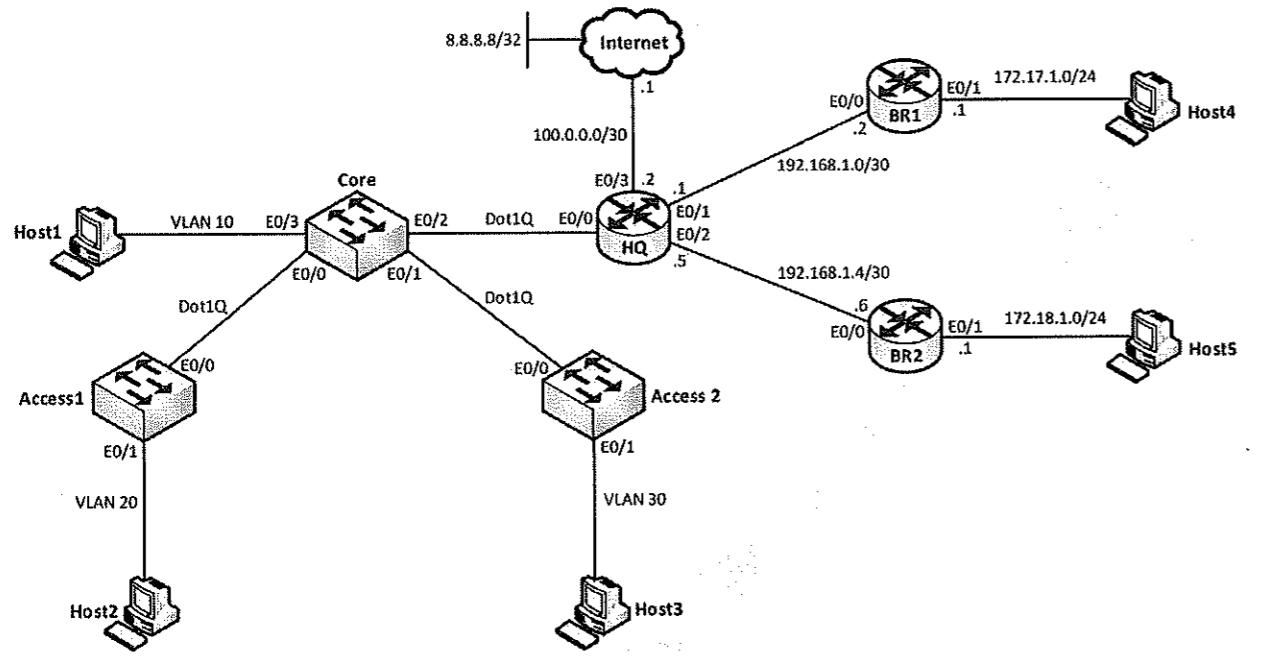
Pinging 172.16.30.2 with 32 bytes of data:
Reply from 172.16.30.2: bytes=32 time=2ms TTL=127
Reply from 172.16.30.2: bytes=32 time=1ms TTL=127
Reply from 172.16.30.2: bytes=32 time=1ms TTL=127
Reply from 172.16.30.2: bytes=32 time=1ms TTL=127

Ping statistics for 172.16.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Đến đây, chúng ta đã hoàn thành các yêu cầu đặt ra của bài lab.

Lab 11 – VLAN, Trunking, Static routing

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Sơ đồ bài lab gồm các thiết bị được kết nối với nhau như trên hình 1. Trong đó: các router và switch chạy hệ điều hành IOL và các host là các VPC tích hợp sẵn trên EVE.
- Bài lab giả lập kịch bản một mạng doanh nghiệp có 3 chi nhánh: Trụ sở chính (HQ – Headquaters) và 2 chi nhánh (Branch – BR) gồm BR1 và BR2. Tại HQ, router HQ còn kết nối xuống một hệ thống switch gồm một switch Core và hai switch Access. Chúng ta cần phải cấu hình các vấn đề về switching và static routing để mạng doanh nghiệp này được thông suốt.
- Trong bài lab này, các thiết bị đều đã được thiết lập sẵn hostname, các bạn học viên không cần phải cấu hình lại thông số này trên các thiết bị. Ngoài ra, trong suốt quá trình thực hiện bài lab, các bạn học viên không can thiệp vào cấu hình của thiết bị giả lập Internet.

Yêu cầu:

1. Trunking:

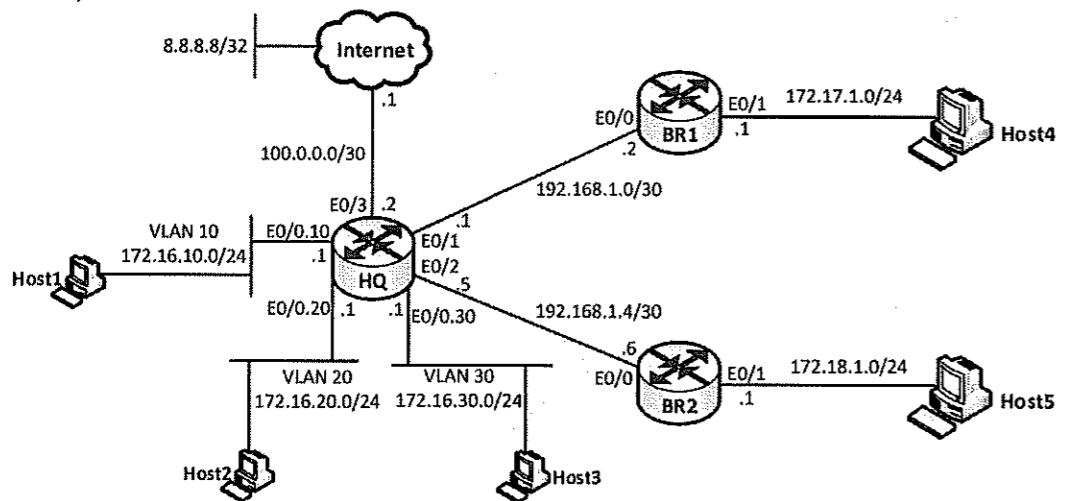
- Thực hiện cấu hình các đường link kết nối giữa các switch Core và Access1, Access2 thành các đường trunk.
- Các đường trunk này sử dụng chuẩn trunking IEEE 802.1Q.

2. VTP, VLAN:

- Cấu hình để 3 switch trên sơ đồ tham gia VTP với các thông số như sau:
 - VTP domain: *waren*, VTP password: *cisco*.
 - Core: server; Access1, Access2: client.
- Trên switch Core tạo các VLAN 10, 20, 30. Kiểm tra xác nhận rằng các VLAN này đã được đồng bộ xuống các switch access.
- Thực hiện gán các cổng trên các switch vào các VLAN như được chỉ ra trên hình 1.

3. Định tuyến VLAN:

- Cấu hình chia sub-interface trên router HQ thực hiện định tuyến VLAN cho các VLAN 10, 20, 30 như được chỉ ra trên hình 2:



Hình 2 – Sơ đồ layer 3.

- Ngoài ra, các bạn học viên cũng cần thực hiện cấu hình địa chỉ IP trên các cổng của các router theo quy hoạch IP trên hình 2.

4. Static routing:

- Thực hiện cấu hình static routing trên các router đảm bảo mọi địa chỉ IP trong mạng doanh nghiệp có thể đi đến nhau được (full-reachability).
- Các bạn học viên sử dụng sơ đồ hình 2 để thực hiện yêu cầu này.

5. DHCP:

Cấu hình để router HQ làm DHCP server cấp phát IP cho tất cả các host thuộc các VLAN và các LAN chi nhánh trên sơ đồ.

6. Internet:

- Thực hiện cấu hình đặt địa chỉ IP Public 100.0.0.2/30 lên cổng outside của router HQ.
- Thực hiện cấu hình trên các router đảm bảo mọi thiết bị trên sơ đồ truy nhập được Internet.
- Việc truy nhập Internet có thể được kiểm tra bằng cách ping đến địa chỉ 8.8.8.8.

Thực hiện:**1. Trunking:****Cấu hình:**

Chúng ta thực hiện thiết lập trunking Dot1Q giữa các switch của khối HQ:

```
Core(config)#interface range e0/0 - 1
Core(config-if-range)#switchport trunk encapsulation dot1q
Core(config-if-range)#switchport mode trunk
Core(config-if-range)#exit

Access1-2(config)#interface e0/0
Access1-2(config-if)#switchport trunk encapsulation dot1q
Access1-2(config-if)#switchport mode trunk
Access1-2(config-if)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng các đường trunk đã được thiết lập theo yêu cầu:

```
Core#show interfaces trunk

Port      Mode          Encapsulation  Status      Native vlan
Et0/0     on           802.1q        trunking    1
Et0/1     on           802.1q        trunking    1

Port      Vlans allowed on trunk
Et0/0     1-4094
Et0/1     1-4094

Port      Vlans allowed and active in management domain
Et0/0     1
Et0/1     1

Port      Vlans in spanning tree forwarding state and not pruned
Et0/0     1
Et0/1     1

Access1-2#show interfaces trunk

Port      Mode          Encapsulation  Status      Native vlan
Et0/0     on           802.1q        trunking    1

Port      Vlans allowed on trunk
Et0/0     1-4094

Port      Vlans allowed and active in management domain
Et0/0     1

Port      Vlans in spanning tree forwarding state and not pruned
Et0/0     1
```

2. VTP, VLAN:

Cấu hình:

Cấu hình để cho các switch tham gia VTP với các thông số đã được yêu cầu:

```
Core(config)#vtp domain waren
Core(config)#vtp password cisco
Access1-2(config)#vtp domain waren
Access1-2(config)#vtp password cisco
Access1-2(config)#vtp mode client
```

Trên switch Core tạo các VLAN 10, 20, 30:

```
Core(config)#vlan 10,20,30
Core(config-vlan)#exit
```

Kiểm tra:

Trước hết, chúng ta kiểm tra thông số VTP của các switch.

Trên switch Core:

```
Core#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                : aabb.cc80.5000
Configuration last modified by 0.0.0.0 at 7-6-21 09:06:54
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    : 1
MD5 digest               : 0xA2 0xD2 0xA8 0x3E 0x0B 0x29 0xBB 0x80
                           0x7C 0x9F 0xF9 0x1A 0x1B 0xF4 0xFC 0xCD

Core#show vtp password
VTP Password: cisco
```

Trên các switch access:

```
Access1-2#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                : aabb.cc80.6000
Configuration last modified by 0.0.0.0 at 7-6-21 09:06:54
```

Feature VLAN:

```
VTP Operating Mode : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs : 8
Configuration Revision : 1
MD5 digest : 0xA2 0xD2 0xA8 0x3E 0x0B 0x29 0xBB 0x80
              0x7C 0x9F 0xF9 0x1A 0x1B 0xF4 0xFC 0xCD
Access1#show vtp password
VTP Password: cisco
```

Các switch đã đồng bộ với nhau về cấu hình VLAN:

```
Core#show vlan brief
VLAN Name          Status    Ports
---- -----
1    default        active    Et0/2, Et0/3
10   VLAN0010       active
20   VLAN0020       active
30   VLAN0030       active
1002 fddi-default  act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default  act/unsup
1005 trnet-default  act/unsup

Access1-2#show vlan brief
VLAN Name          Status    Ports
---- -----
1    default        active    Et0/1, Et0/2, Et0/3
10   VLAN0010       active
20   VLAN0020       active
30   VLAN0030       active
1002 fddi-default  act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default  act/unsup
1005 trnet-default  act/unsup
```

Sau khi cấu hình VLAN đã được đồng bộ, trên các switch, chúng ta thực hiện gán các cổng vào các VLAN như đã được chỉ ra trên sơ đồ lab ở hình 1:

```
Core(config)#interface e0/3
Core(config-if)#switchport mode access
Core(config-if)#switchport access vlan 10
Core(config-if)#exit
```

```
Access1(config)#interface e0/1
Access1(config-if)#switchport mode access
Access1(config-if)#switchport access vlan 20
Access1(config-if)#exit

Access2(config)#interface e0/1
Access2(config-if)#switchport mode access
Access2(config-if)#switchport access vlan 30
Access2(config-if)#exit
```

Chúng ta kiểm tra lại cấu hình gán cổng vào VLAN đã thực hiện:

```
Core#show vlan brief
VLAN Name          Status    Ports
----- -----
1    default        active    Et0/2
10   VLAN0010       active    Et0/3
20   VLAN0020       active
30   VLAN0030       active
1002 fddi-default  act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default  act/unsup
1005 trnet-default  act/unsup

Access1#show vlan brief
VLAN Name          Status    Ports
----- -----
1    default        active    Et0/2, Et0/3
10   VLAN0010       active
20   VLAN0020       active
30   VLAN0030       active
1002 fddi-default  act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default  act/unsup
1005 trnet-default  act/unsup

Access2#show vlan brief
VLAN Name          Status    Ports
----- -----
1    default        active    Et0/2, Et0/3
10   VLAN0010       active
20   VLAN0020       active
30   VLAN0030       active
1002 fddi-default  act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default  act/unsup
1005 trnet-default  act/unsup
```

Đến đây, chúng ta đã hoàn thành phần cấu hình VLAN, Trunking và VTP.

3. Định tuyến VLAN:

Cấu hình:

Ta thực hiện chia sub-interface trên cổng E0/0 của router HQ để định tuyến giữa các VLAN 10, 20, 30 trên hệ thống switch (các bạn học viên tham khảo sơ đồ hình 2 để làm câu lab này):

```
HQ(config)#interface e0/0
HQ(config-if)#no shutdown
HQ(config-if)#exit
HQ(config)#interface e0/0.10
HQ(config-subif)#encapsulation dot1q 10
HQ(config-subif)#ip address 172.16.10.1 255.255.255.0
HQ(config-subif)#exit
HQ(config)#interface e0/0.20
HQ(config-subif)#encapsulation dot1q 20
HQ(config-subif)#ip address 172.16.20.1 255.255.255.0
HQ(config-subif)#exit
HQ(config)#interface e0/0.30
HQ(config-subif)#encapsulation dot1q 30
HQ(config-subif)#ip address 172.16.30.1 255.255.255.0
HQ(config-subif)#exit
```

Thực hiện bật chế độ trunking Dot1Q trên cổng E0/2 của switch Core đầu nối đến router HQ:

```
Core(config)#interface e0/2
Core(config-if)#switchport trunk encapsulation dot1q
Core(config-if)#switchport mode trunk
Core(config-if)#exit
```

Sau khi thực hiện xong thao tác định tuyến VLAN như ở trên, chúng ta cấu hình địa chỉ IP nội bộ trên các cổng còn lại của router HQ và các router BR1, BR2:

```
HQ(config)#interface e0/1
HQ(config-if)#no shutdown
HQ(config-if)#ip address 192.168.1.1 255.255.255.252
HQ(config-if)#exit
HQ(config)#interface e0/2
HQ(config-if)#no shutdown
HQ(config-if)#ip address 192.168.1.5 255.255.255.252
HQ(config-if)#exit
BR1(config)#interface e0/0
BR1(config-if)#no shutdown
BR1(config-if)#ip address 192.168.1.2 255.255.255.252
BR1(config-if)#exit
BR1(config)#interface e0/1
BR1(config-if)#no shutdown
BR1(config-if)#ip address 172.17.1.1 255.255.255.0
BR1(config-if)#exit
```

```
BR2(config)#interface e0/0
BR2(config-if)#no shutdown
BR2(config-if)#ip address 192.168.1.6 255.255.255.252
BR2(config-if)#exit
BR2(config)#interface e0/1
BR2(config-if)#no shutdown
BR2(config-if)#ip address 172.18.1.1 255.255.255.0
BR2(config-if)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng các sub – interface trên router HQ đã được tạo ra một cách đầy đủ:

```
HQ#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
Ethernet0/0        unassigned     YES NVRAM up           up
Ethernet0/0.10      172.16.10.1   YES manual up          up
Ethernet0/0.20      172.16.20.1   YES manual up          up
Ethernet0/0.30      172.16.30.1   YES manual up          up
Ethernet0/1         192.168.1.1   YES manual up          up
Ethernet0/2         192.168.1.5   YES manual up          up
Ethernet0/3         unassigned    YES NVRAM administratively down down
```

Cổng E0/2 đầu nối đến router HQ của switch Core đã hoạt động ở chế độ Trunking Dot1Q:

```
Core#show interfaces e0/2 trunk
Port      Mode          Encapsulation  Status      Native vlan
Et0/2     on            802.1q        trunking    1

Port      Vlans allowed on trunk
Et0/2     1-4094

Port      Vlans allowed and active in management domain
Et0/2     1,10,20,30

Port      Vlans in spanning tree forwarding state and not pruned
Et0/2     1,10,20,30
```

Các đường link kết nối giữa các router đã thông suốt IP:

```
HQ#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 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms

HQ#ping 192.168.1.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.6, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms
```

4. Static routing:

Cấu hình:

Để thực hiện các yêu cầu về định tuyến và cấu hình các dịch vụ mạng, các bạn học viên nên dựa vào sơ đồ layer 3 ở hình 2 để tiến hành các thao tác cấu hình.

Cấu hình định tuyến tĩnh trên các router:

```
HQ(config)#ip route 172.17.1.0 255.255.255.0 192.168.1.2
HQ(config)#ip route 172.18.1.0 255.255.255.0 192.168.1.6

BR1(config)#ip route 172.16.10.0 255.255.255.0 192.168.1.1
BR1(config)#ip route 172.16.20.0 255.255.255.0 192.168.1.1
BR1(config)#ip route 172.16.30.0 255.255.255.0 192.168.1.1
BR1(config)#ip route 172.18.1.0 255.255.255.0 192.168.1.1

BR2(config)#ip route 172.16.10.0 255.255.255.0 192.168.1.5
BR2(config)#ip route 172.16.20.0 255.255.255.0 192.168.1.5
BR2(config)#ip route 172.16.30.0 255.255.255.0 192.168.1.5
BR2(config)#ip route 172.17.1.0 255.255.255.0 192.168.1.5
```

Kiểm tra:

Chúng ta kiểm tra bảng định tuyến của các router để xác nhận rằng các static route đã được khai báo đầy đủ:

```
HQ#show ip route static
(...)
    172.17.0.0/24 is subnetted, 1 subnets
S        172.17.1.0 [1/0] via 192.168.1.2
    172.18.0.0/24 is subnetted, 1 subnets
S        172.18.1.0 [1/0] via 192.168.1.6

BR1#show ip route static
(...)
    172.16.0.0/24 is subnetted, 3 subnets
S        172.16.10.0 [1/0] via 192.168.1.1
S        172.16.20.0 [1/0] via 192.168.1.1
S        172.16.30.0 [1/0] via 192.168.1.1
    172.18.0.0/24 is subnetted, 1 subnets
S        172.18.1.0 [1/0] via 192.168.1.1

BR2#show ip route static
(...)
    172.16.0.0/24 is subnetted, 3 subnets
S        172.16.10.0 [1/0] via 192.168.1.5
S        172.16.20.0 [1/0] via 192.168.1.5
S        172.16.30.0 [1/0] via 192.168.1.5
    172.17.0.0/24 is subnetted, 1 subnets
S        172.17.1.0 [1/0] via 192.168.1.5
```

Các VLAN của HQ và các mạng LAN của các chi nhánh đã đi đến nhau được:

```
HQ#ping 172.17.1.1 source 172.16.10.1 <- VLAN 10 của HQ và BR1 LAN di đến nhau được
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.1.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
HQ#ping 172.18.1.1 source 172.16.10.1 <- VLAN 10 của HQ và BR2 LAN di đến nhau được
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.18.1.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
HQ#ping 172.17.1.1 source 172.16.20.1 <- VLAN 20 của HQ và BR1 LAN di đến nhau được
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.1.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
HQ#ping 172.18.1.1 source 172.16.20.1 <- VLAN 20 của HQ và BR2 LAN di đến nhau được
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.18.1.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
HQ#ping 172.17.1.1 source 172.16.30.1 <- VLAN 30 của HQ và BR1 LAN di đến nhau được
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.1.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.30.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
HQ#ping 172.18.1.1 source 172.16.30.1 <- VLAN 30 của HQ và BR2 LAN di đến nhau được
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.18.1.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.30.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
BR1#ping 172.18.1.1 source 172.17.1.1 <- BR1 LAN và BR2 LAN di đến nhau được
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.18.1.1, timeout is 2 seconds:
Packet sent with a source address of 172.17.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

5. DHCP:

Cấu hình:

Cấu hình DHCP server trên router HQ để cấp phát IP cho các VLAN và các LAN:

```
HQ(config)#ip dhcp excluded-address 172.16.10.1
HQ(config)#ip dhcp excluded-address 172.16.20.1
HQ(config)#ip dhcp excluded-address 172.16.30.1
HQ(config)#ip dhcp excluded-address 172.17.1.1
HQ(config)#ip dhcp excluded-address 172.18.1.1

HQ(config)#ip dhcp pool HQ_VLAN10
HQ(dhcp-config)#network 172.16.10.0 /24
HQ(dhcp-config)#default-router 172.16.10.1
HQ(dhcp-config)#exit
HQ(config)#ip dhcp pool HQ_VLAN20
HQ(dhcp-config)#network 172.16.20.0 /24
HQ(dhcp-config)#default-router 172.16.20.1
HQ(dhcp-config)#exit
HQ(config)#ip dhcp pool HQ_VLAN30
HQ(dhcp-config)#network 172.16.30.0 /24
HQ(dhcp-config)#default-router 172.16.30.1
HQ(dhcp-config)#exit

HQ(config)#ip dhcp pool BR1_LAN
HQ(dhcp-config)#network 172.17.1.0 /24
HQ(dhcp-config)#default-router 172.17.1.1
HQ(dhcp-config)#exit

HQ(config)#ip dhcp pool BR2_LAN
HQ(dhcp-config)#network 172.18.1.0 /24
HQ(dhcp-config)#default-router 172.18.1.1
HQ(dhcp-config)#exit
```

Cấu hình để các router BR1 và BR2 trở thành DHCP Relay Agent:

```
BR1(config)#interface e0/1
BR1(config-if)#ip helper-address 192.168.1.1
BR1(config-if)#exit

BR2(config)#interface e0/1
BR2(config-if)#ip helper-address 192.168.1.5
BR2(config-if)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng các host thuộc các VLAN và các LAN đều đã có thể nhận được IP từ DHCP:

```
Host1> dhcp -r
DDORA IP 172.16.10.2/24 GW 172.16.10.1

Host2> dhcp -r
DDORA IP 172.16.20.2/24 GW 172.16.20.1

Host3> dhcp -r
DDORA IP 172.16.30.2/24 GW 172.16.30.1
```

```
Host4> dhcp -r
DDORA IP 172.17.1.2/24 GW 172.17.1.1

Host5> dhcp -r
DDORA IP 172.18.1.2/24 GW 172.18.1.1
```

Bảng DHCP binding trên router HQ:

HQ#show ip dhcp binding				
Bindings from all pools not associated with VRF:				
IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type	
172.16.10.2	0100.5079.6668.08	Jul 08 2021 05:59 AM	Automatic	
172.16.20.2	0100.5079.6668.09	Jul 08 2021 06:00 AM	Automatic	
172.16.30.2	0100.5079.6668.0a	Jul 08 2021 06:00 AM	Automatic	
172.17.1.2	0100.5079.6668.0b	Jul 08 2021 06:00 AM	Automatic	
172.18.1.2	0100.5079.6668.0c	Jul 08 2021 06:00 AM	Automatic	

Đến đây, việc cấu hình dịch vụ DHCP cho mạng doanh nghiệp trong bài lab đã hoàn tất.

6. Internet:

Cấu hình:

Ta thực hiện đặt IP Public mặt ngoài trên cổng E0/3 của router HQ:

```
HQ(config)#interface e0/3
HQ(config-if)#no shutdown
HQ(config-if)#ip address 100.0.0.2 255.255.255.252
HQ(config-if)#exit
```

Tiếp theo, ta thực hiện thao tác *default – routing* trên các router:

```
HQ(config)#ip route 0.0.0.0 0.0.0.0 100.0.0.1
BR1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
BR2(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.5
```

Cuối cùng, ta thực hiện cấu hình NAT trên router biên HQ đảm bảo mọi địa chỉ trên sơ đồ có thể truy nhập được Internet:

```
HQ(config)#access-list 1 permit any
HQ(config)#ip nat inside source list 1 interface e0/3 overload
HQ(config)#interface e0/3
HQ(config-if)#ip nat outside
HQ(config-if)#exit
HQ(config)#interface e0/0.10
HQ(config-subif)#ip nat inside
HQ(config-subif)#exit
HQ(config)#interface e0/0.20
HQ(config-subif)#ip nat inside
HQ(config-subif)#exit
```

```
HQ(config)#interface e0/0.30
HQ(config-subif)#ip nat inside
HQ(config-subif)#exit
HQ(config)#interface range e0/1 - 2
HQ(config-if-range)#ip nat inside
HQ(config-if-range)#exit
```

Kiểm tra:

Chúng ta thực hiện kiểm tra hoạt động truy nhập Internet bằng cách ping đi 8.8.8.8 từ các host:

```
Host1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=1.826 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=3.544 ms

Host2> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=1.821 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=4.195 ms

Host3> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=2.027 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=3.859 ms

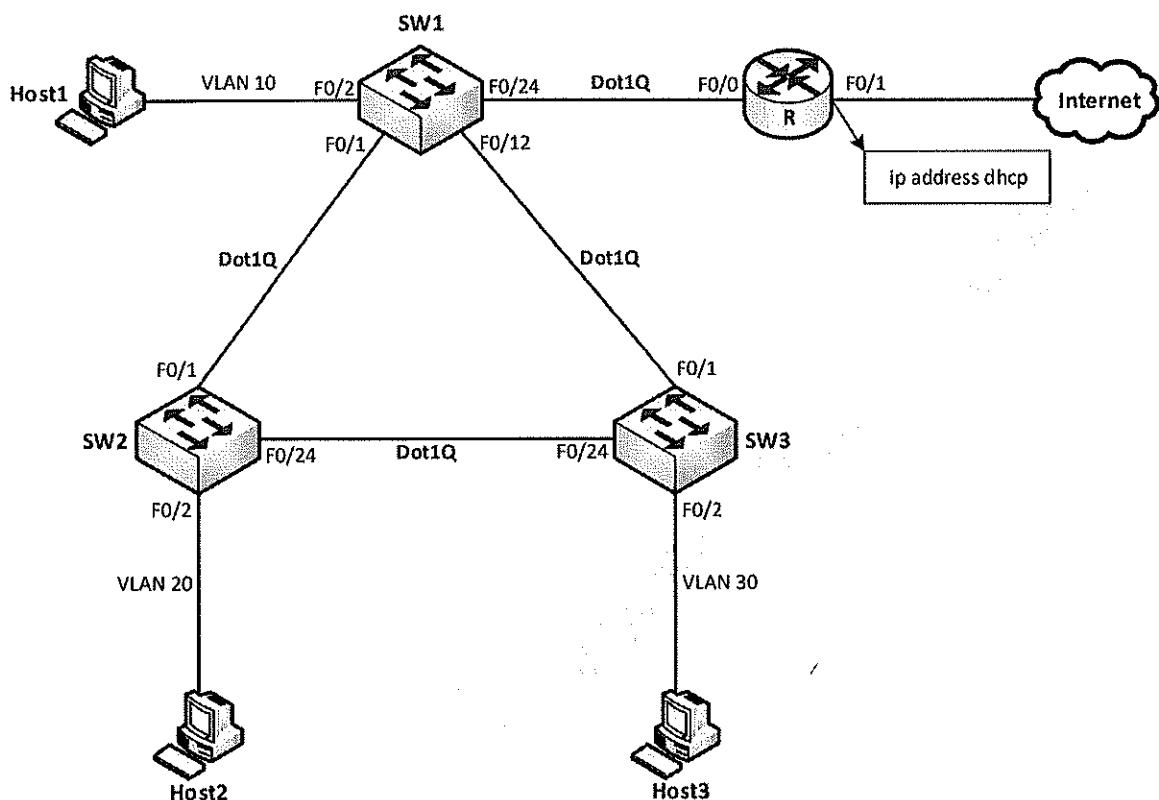
Host4> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=1.570 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=1.578 ms

Host5> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=3.384 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=1.993 ms
```

Tất cả các host thuộc các VLAN và các LAN đều đã có thể truy nhập được Internet. Chúng ta đã hoàn tất yêu cầu đặt ra.

Lab 12 – Spanning Tree Protocol

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Bài lab gồm các thiết bị được kết nối với nhau theo sơ đồ hình 1.
- Trong bài lab này, các bạn học viên sẽ thực hành cấu hình hiệu chỉnh STP trên các switch từ đó ôn tập và củng cố các kiến thức về giao thức STP đã được học.

Yêu cầu:

1. Trunking:

- Cấu hình các đường link nối giữa các switch thành các đường trunk.
- Các đường trunk này sử dụng chuẩn trunking Dot1Q.

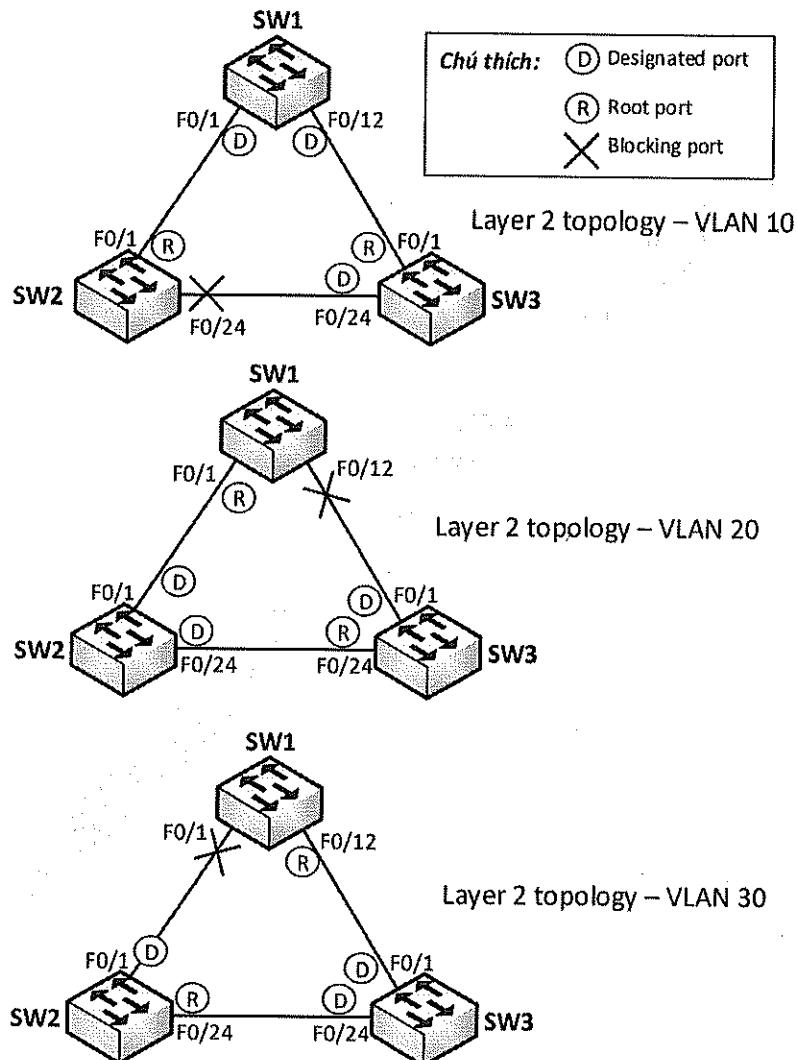
2. VTP, VLAN:

- Cấu hình 3 switch tham gia VTP với các thông số như sau:
 - VTP domain: *waren*, VTP password: *cisco*.
 - SW1: server; SW2, SW3: client.

- Trên SW1, tạo các VLAN 10, 20, 30, kiểm tra xác nhận rằng cấu hình VLAN này đã được lan truyền đến các SW2 và SW3.
 - Thực hiện gán các cổng của các switch vào các VLAN như được chỉ ra trên hình 1.

3. STP;

- Cấu hình hiệu chỉnh STP trên các switch đảm bảo rằng tất cả các đường link kết nối giữa các switch đều phải được tận dụng để truyền dữ liệu.
 - Cụ thể, vai trò của các cổng của các switch trên các VLAN phải đạt được như sau (hình 2):



Hình 2 – Kết quả hội tụ STP trên các VLAN.

4. Định tuyến VLAN:

Cấu hình router R thực hiện định tuyến giữa các VLAN đã tạo trên hệ thống switch theo quy hoạch IP như trên bảng 1:

<i>Sub-interface</i>	<i>VLAN</i>	<i>Địa chỉ</i>	<i>Subnet</i>
F0/0.10	10	172.16.10.1	172.16.10.0/24
F0/0.20	20	172.16.20.1	172.16.20.0/24
F0/0.30	30	172.16.30.1	172.16.30.0/24

Bảng 1 – Quy hoạch IP cho định tuyến VLAN.

5. DHCP:

- Thực hiện cấu hình router R làm DHCP server cấp phát IP cho các host thuộc các VLAN theo quy hoạch IP trên bảng 1.
- Ping kiểm tra giữa các host để xác nhận rằng các host thuộc các VLAN đã có thể đón nhau.

6. Internet:

- Cấu hình router R đảm bảo các host đều có thể truy nhập được Internet.
- Hoạt động truy nhập Internet được kiểm tra bằng cách truy nhập Internet từ các host.

Thực hiện:

1. Trunking:

Cấu hình:

Trên SW1:

```
SW1(config)#interface range f0/1,f0/12
SW1(config-if-range)#switchport trunk encapsulation dot1q
SW1(config-if-range)#switchport mode trunk
SW1(config-if-range)#exit
```

Trên SW2 và SW3:

```
SW2-3(config)#interface range f0/1,f0/24
SW2-3(config-if-range)#switchport trunk encapsulation dot1q
SW2-3(config-if-range)#switchport mode trunk
SW2-3(config-if-range)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng các đường trunk đã được thiết lập giữa các switch:

SW1#show interfaces trunk					
Port	Mode	Encapsulation	Status	Native vlan	
Fa0/1	on	802.1q	trunking	1	
Fa0/12	on	802.1q	trunking	1	

```
Port      Vlans allowed on trunk
Fa0/1    1-4094
Fa0/12   1-4094

Port      Vlans allowed and active in management domain
Fa0/1    1
Fa0/12   1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    1
Fa0/12   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

```
Port      Vlans allowed on trunk
Fa0/1    1-4094
Fa0/24   1-4094
```

```
Port      Vlans allowed and active in management domain
Fa0/1    1
Fa0/24   1
```

```
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    none
Fa0/24   1
```

SW3#show interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1
Fa0/24	on	802.1q	trunking	1

```
Port      Vlans allowed on trunk
Fa0/1    1-4094
Fa0/24   1-4094
```

```
Port      Vlans allowed and active in management domain
Fa0/1    1
Fa0/24   1
```

```
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    1
Fa0/24   1
```

2. VTP, VLAN:

Cấu hình:

Chúng ta thực hiện cấu hình VTP giữa các switch như được yêu cầu:

```
SW1(config)#vtp domain waren
SW1(config)#vtp password cisco
SW2-3(config)#vtp domain waren
SW2-3(config)#vtp password cisco
SW2-3(config)#vtp mode client
```

Trên SW1, thực hiện tạo các VLAN 10, 20, 30 để lan truyền đến các switch khác:

```
SW1(config)#vian 10,20,30
SW1(config-vlan)#exit
```

Sau khi cấu hình VLAN đã được đồng bộ, trên các switch chúng ta thực hiện gán các cổng vào các VLAN như được chỉ ra trên sơ đồ lab:

```
SW1(config)#interface f0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#exit

SW2(config)#interface f0/2
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 20
SW2(config-if)#exit

SW3(config)#interface f0/2
SW3(config-if)#switchport mode access
SW3(config-if)#switchport access vlan 30
SW3(config-if)#exit
```

Kiểm tra:

Các thông số VTP trên các switch:

```
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           : 0023.5ecd.1400
Configuration last modified by 0.0.0.0 at 3-1-93 00:14:25
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 : 1
```

```
MD5 digest : 0xA2 0xD2 0xA8 0x3E 0x0B 0x29 0xBB 0x80
              0x7C 0x9F 0xF9 0x1A 0x1B 0xF4 0xFC 0xCD

SW1#show vtp password
VTP Password: cisco

SW2-3#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 : 0023.abfa.0580
Configuration last modified by 0.0.0.0 at 3-1-93 00:14:25
Feature VLAN:
-----
VTP Operating Mode : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs : 8
Configuration Revision : 1
MD5 digest : 0xA2 0xD2 0xA8 0x3E 0x0B 0x29 0xBB 0x80
              0x7C 0x9F 0xF9 0x1A 0x1B 0xF4 0xFC 0xCD

SW2-3#show vtp password
VTP Password: cisco
```

Cấu hình VLAN trên các switch:

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, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Fa0/25, Fa0/26, Fa0/27 Fa0/28, Fa0/29, Fa0/30, Fa0/31 Fa0/32, Fa0/33, Fa0/34, Fa0/35 Fa0/36, Fa0/37, Fa0/38, Fa0/39 Fa0/40, Fa0/41, Fa0/42, Fa0/43 Fa0/44, Fa0/45, Fa0/46, Fa0/47 Fa0/48, Gi0/1, Gi0/2, Gi0/3 Gi0/4	/
10 VLAN0010	active	Fa0/2	
20 VLAN0020	active		
30 VLAN0030	active		
1002 fddi-default	act/unsup		
1003 token-ring-default	act/unsup		
1004 fddinet-default	act/unsup		
1005 trnet-default	act/unsup		

```
SW2#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, Fa0/25, Fa0/26, Fa0/27 Fa0/28, Fa0/29, Fa0/30, Fa0/31 Fa0/32, Fa0/33, Fa0/34, Fa0/35 Fa0/36, Fa0/37, Fa0/38, Fa0/39 Fa0/40, Fa0/41, Fa0/42, Fa0/43 Fa0/44, Fa0/45, Fa0/46, Fa0/47 Fa0/48, Gi0/1, Gi0/2, Gi0/3 Gi0/4
10 VLAN0010	active	
20 VLAN0020	active	Fa0/2
30 VLAN0030	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	
SW3#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, Fa0/25, Fa0/26, Fa0/27 Fa0/28, Fa0/29, Fa0/30, Fa0/31 Fa0/32, Fa0/33, Fa0/34, Fa0/35 Fa0/36, Fa0/37, Fa0/38, Fa0/39 Fa0/40, Fa0/41, Fa0/42, Fa0/43 Fa0/44, Fa0/45, Fa0/46, Fa0/47 Fa0/48, Gi0/1, Gi0/2, Gi0/3 Gi0/4
10 VLAN0010	active	
20 VLAN0020	active	
30 VLAN0030	active	Fa0/2
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

3. STP:

Cấu hình:

Để đạt được yêu cầu về hội tụ STP như trên hình 2, chúng ta cần thực hiện hiệu chỉnh STP trên các VLAN như sau:

- Trên VLAN 10, SW1 là Primary Root switch và SW3 là Secondary Root switch.
- Trên VLAN 20, SW2 là Primary Root switch và SW3 là Secondary Root switch.
- Trên VLAN 30, SW3 là Primary Root switch và SW2 là Secondary Root switch.

Cấu hình trên các switch cho yêu cầu 1:

```
SW1(config)#spanning-tree vlan 10 root primary
SW3(config)#spanning-tree vlan 10 root secondary
```

Cấu hình trên các switch cho yêu cầu 2:

```
SW2(config)#spanning-tree vlan 20 root primary
SW3(config)#spanning-tree vlan 20 root secondary
```

Cấu hình trên các switch cho yêu cầu 3:

```
SW3(config)#spanning-tree vlan 30 root primary
SW2(config)#spanning-tree vlan 30 root secondary
```

Kiểm tra:

Chúng ta kiểm tra rằng STP trên các switch đã hội tụ đúng theo yêu cầu.

Chúng ta kiểm tra cho VLAN 10.

Trên SW1:

```
SW1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
              Address     0023.5ecd.1400
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24586  (priority 24576 sys-id-ext 10)
              Address     0023.5ecd.1400
              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        128.3    P2p
  Fa0/2          Desg FWD 19        128.4    P2p
  Fa0/12         Desg FWD 19        128.14   P2p
```

Kết quả kiểm tra cho thấy trên VLAN 10, SW1 đang là root switch. Khi SW1 là root switch, tất cả các cổng của nó đều là *Designated port*.

Ta kiểm tra thông số STP VLAN 10 trên SW2:

```
SW2#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
              Address     0023.5ecd.1400
              Cost         19
              Port        3 (FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
              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       128.3    P2p
  Fa0/24         Altn BLK 19       128.26   P2p
```

Ta thấy cổng E0/0 của SW2 là root port và cổng E0/1 của SW2 bị khóa đúng như yêu cầu.

Cuối cùng, chúng kiểm tra thông số STP của SW3 trên VLAN 10:

```
SW3#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
              Address     0023.5ecd.1400
              Cost         19
              Port        3 (FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28682  (priority 28672 sys-id-ext 10)
              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          Root FWD 19       128.3    P2p
  Fa0/24         Desg FWD 19       128.26   P2p
```

Các cổng trên SW3 cũng hội tụ STP trên VLAN 10 đúng như yêu cầu.

Ta cũng có thể kiểm tra trạng thái khóa hay không khóa các VLAN trên các cổng bằng cách quan sát kết quả của lệnh “show interfaces trunk”:

```
SW1#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1
Fa0/12	on	802.1q	trunking	1

Port Vlans allowed on trunk

Fa0/1	1-4094
Fa0/12	1-4094

Port Vlans allowed and active in management domain

Fa0/1	1,10,20,30
Fa0/12	1,10,20,30

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1	1,10,20 <- Cả hai cổng trunk đều cho qua VLAN 10
Fa0/12	1,10,30

```
SW2#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1
Fa0/24	on	802.1q	trunking	1

Port Vlans allowed on trunk

Fa0/1	1-4094
Fa0/24	1-4094

Port Vlans allowed and active in management domain

Fa0/1	1,10,20,30
Fa0/24	1,10,20,30

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1	10,20,30 <- Chỉ có cổng trunk F0/1 cho qua VLAN 10
Fa0/24	1,20,30

```
SW3#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1
Fa0/24	on	802.1q	trunking	1

Port Vlans allowed on trunk

Fa0/1	1-4094
Fa0/24	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,20,30
Fa0/24	1,10,20,30
Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1,10,20,30 <- Cả hai cổng trunk đều cho qua VLAN 10
Fa0/24	1,10,20,30

Kết quả show ở trên cho thấy cổng F0/24 của SW2 không cho qua VLAN 10 (trong danh sách các VLAN ở trạng thái “spanning tree forwarding” trên cổng không có VLAN 10), các cổng của các switch khác đều cho qua VLAN 10. Điều này một lần nữa xác nhận lại kết quả hội tụ STP đã đạt được.

Chúng ta có thể kiểm tra tương tự cho các VLAN 20 và 30.

4. Định tuyến VLAN:

Cấu hình:

Trên router R:

```
R(config)#interface f0/0
R(config-if)#no shutdown
R(config-if)#exit
R(config)#interface f0/0.10
R(config-subif)#encapsulation dot1Q 10
R(config-subif)#ip address 172.16.10.1 255.255.255.0
R(config-subif)#exit
R(config)#interface f0/0.20
R(config-subif)#encapsulation dot1Q 20
R(config-subif)#ip address 172.16.20.1 255.255.255.0
R(config-subif)#exit
R(config)#interface f0/0.30
R(config-subif)#encapsulation dot1Q 30
R(config-subif)#ip address 172.16.30.1 255.255.255.0
R(config-subif)#exit
```

Trên SW1:

```
SW1(config)#interface f0/24
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
SW1(config-if)#exit
```

Kiểm tra:

Trên router R:

```
R#show ip interface brief
Interface          IP-Address      OK? Method Status        Protocol
FastEthernet0/0    unassigned     YES NVRAM up           up
FastEthernet0/0.10  172.16.10.1   YES manual up          up
FastEthernet0/0.20  172.16.20.1   YES manual up          up
FastEthernet0/0.30  172.16.30.1   YES manual up          up
FastEthernet0/1     unassigned     YES manual administratively down down
```

Trên SW1:

```
SW1#show interfaces trunk

Port      Mode          Encapsulation  Status      Native vlan
Fa0/1     on           802.1q        trunking   1
Fa0/12    on           802.1q        trunking   1
Fa0/24    on           802.1q        trunking   1

Port      Vlans allowed on trunk
Fa0/1     1-4094
Fa0/12    1-4094
Fa0/24    1-4094

Port      Vlans allowed and active in management domain
Fa0/1     1,10,20,30
Fa0/12    1,10,20,30
Fa0/24    1,10,20,30

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,10,20
Fa0/12    1,10,30
Fa0/24    1,10,20,30
```

5. DHCP:

Cấu hình:

Thực hiện cấu hình router R làm DHCP server cấp phát IP xuống các host thuộc các VLAN:

```
R(config)#ip dhcp excluded-address 172.16.10.1
R(config)#ip dhcp excluded-address 172.16.20.1
R(config)#ip dhcp excluded-address 172.16.30.1

R(config)#ip dhcp pool VLAN10
R(dhcp-config)#network 172.16.10.0 /24
R(dhcp-config)#default-router 172.16.10.1
R(dhcp-config)#dns-server 8.8.8.8
R(dhcp-config)#exit

R(config)#ip dhcp pool VLAN20
R(dhcp-config)#network 172.16.20.0 /24
R(dhcp-config)#default-router 172.16.20.1
R(dhcp-config)#dns-server 8.8.8.8
R(dhcp-config)#exit

R(config)#ip dhcp pool VLAN30
R(dhcp-config)#network 172.16.30.0 /24
R(dhcp-config)#default-router 172.16.30.1
R(dhcp-config)#dns-server 8.8.8.8
R(dhcp-config)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng các host đều đã nhận được IP từ DHCP.

Host1 đã nhận được cấu hình IP (hình 3):

Network Connection Details:	
Connection-specific DN...	
Description	
Property	Value
Physical Address	30-F9-ED-AE-0E-A0
DHCP Enabled	Yes
IPv4 Address	172.16.10.2
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Wednesday, March 23, 2022 4:09:58 PM
Lease Expires	Thursday, March 24, 2022 4:09:58 PM
IPv4 Default Gateway	172.16.10.1
IPv4 DHCP Server	172.16.10.1

Hình 3 – Host1 nhận được cấu hình IP từ DHCP server.

Host2 đã nhận được cấu hình IP (hình 4):

Network Connection Details:	
Connection-specific DN...	
Description	
Property	Value
Physical Address	5C-26-0A-30-42-55
DHCP Enabled	Yes
IPv4 Address	172.16.20.2
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	23 Tháng Ba 2022 4:15:13 CH
Lease Expires	24 Tháng Ba 2022 4:15:12 CH
IPv4 Default Gateway	172.16.20.1
IPv4 DHCP Server	172.16.20.1

Hình 4 – Host2 đã nhận được cấu hình IP.

Host 3 đã nhận được cấu hình IP (hình 5):

Network Connection Details:	
Connection-specific DN...	
Description	
Property	Value
Physical Address	00-26-B9-F6-2A-EF
DHCP Enabled	Yes
IPv4 Address	172.16.30.2
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Wednesday, August 24, 2011 12:09:15 PM
Lease Expires	Thursday, August 25, 2011 12:09:14 PM
IPv4 Default Gateway	172.16.30.1
IPv4 DHCP Server	172.16.30.1
IPv4 DNS Server	

Hình 5 – Host3 đã nhận được cấu hình IP.

Bảng DHCP binding trên router R:

R#show ip dhcp binding				
Bindings from all pools not associated with VRF:				
IP address	Client-ID/ Hardware address/	Lease expiration	Type	
	User name			
172.16.10.2	0130.f9ed.ae0e.a0	Jan 02 1970 01:05 AM	Automatic	
172.16.20.2	015c.260a.3042.55	Jan 02 1970 01:10 AM	Automatic	
172.16.30.2	0100.26b9.f62a.ef	Jan 02 1970 01:05 AM	Automatic	

Cuối cùng, ta kiểm tra rằng các host trên các VLAN ping được nhau.

Host1 trên VLAN 10 ping thành công Host2 trên VLAN 20:

```
C:\>ping 172.16.20.2

Pinging 172.16.20.2 with 32 bytes of data:
Reply from 172.16.20.2: bytes=32 time=2ms TTL=127
Reply from 172.16.20.2: bytes=32 time=1ms TTL=127
Reply from 172.16.20.2: bytes=32 time=1ms TTL=127
Reply from 172.16.20.2: bytes=32 time=1ms TTL=127

Ping statistics for 172.16.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Host1 trên VLAN 10 ping thành công Host3 trên VLAN 30:

```
C:\>ping 172.16.30.2

Pinging 172.16.30.2 with 32 bytes of data:
Reply from 172.16.30.2: bytes=32 time=2ms TTL=127
Reply from 172.16.30.2: bytes=32 time=1ms TTL=127
Reply from 172.16.30.2: bytes=32 time=1ms TTL=127
Reply from 172.16.30.2: bytes=32 time=1ms TTL=127

Ping statistics for 172.16.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Host2 trên VLAN 20 ping thành công Host3 trên VLAN 30:

```
C:\>ping 172.16.30.2

Pinging 172.16.30.2 with 32 bytes of data:
Reply from 172.16.30.2: bytes=32 time=2ms TTL=127
Reply from 172.16.30.2: bytes=32 time=1ms TTL=127
Reply from 172.16.30.2: bytes=32 time=1ms TTL=127
Reply from 172.16.30.2: bytes=32 time=1ms TTL=127
```

```
Ping statistics for 172.16.30.2:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

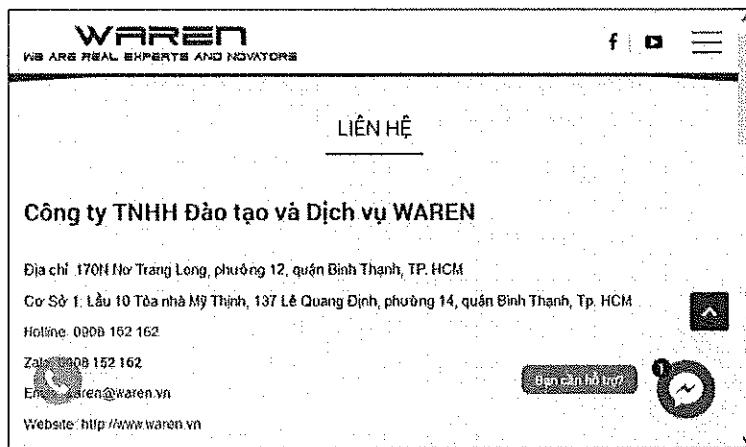
6. Internet:

Cấu hình:

```
R(config)#interface f0/1  
R(config-if)#no shutdown  
R(config-if)#ip address dhcp  
R(config-if)#exit  
  
R(config)#access-list 1 permit any  
R(config)#ip nat inside source list 1 interface f0/1 overload  
  
R(config)#interface f0/0.10  
R(config-subif)#ip nat inside  
R(config-subif)#exit  
R(config)#interface f0/0.20  
R(config-subif)#ip nat inside  
R(config-subif)#exit  
R(config)#interface f0/0.30  
R(config-subif)#ip nat inside  
R(config-subif)#exit  
  
R(config)#interface f0/1  
R(config-if)#ip nat outside  
R(config-if)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng các host thuộc các VLAN đều đã truy nhập được Internet. Ví dụ, Host1 (hình 6):



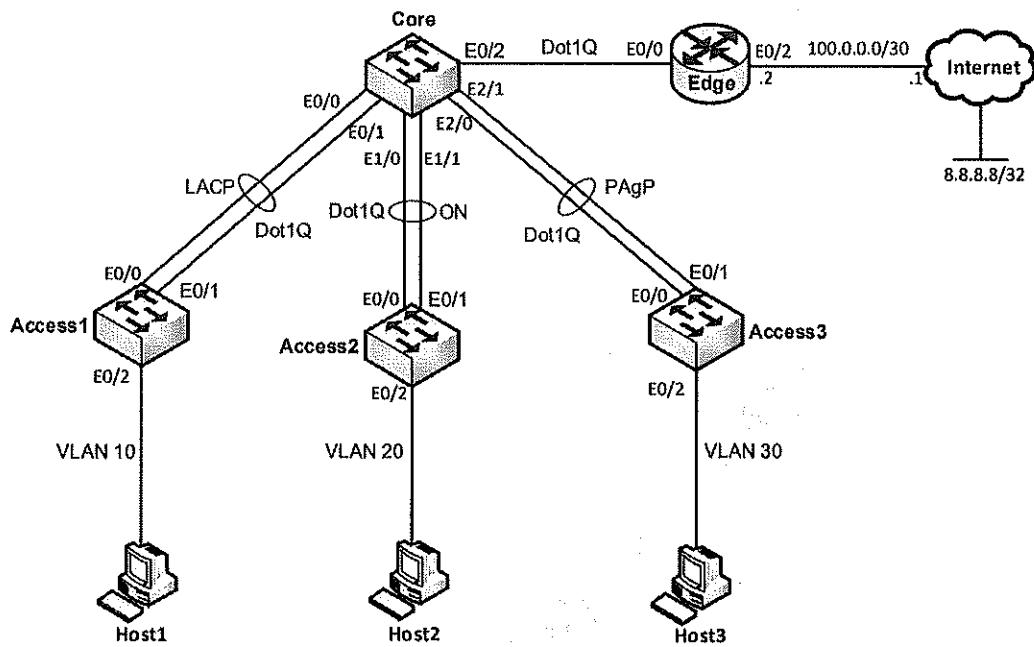
Hình 6 – Truy nhập web thành công trên Host1.

Chúng ta có thể kiểm tra tương tự trên Host2 và Host3.

Đến đây, chúng ta đã hoàn thành tất cả các yêu cầu của bài lab.

Lab 13 – Etherchannel

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

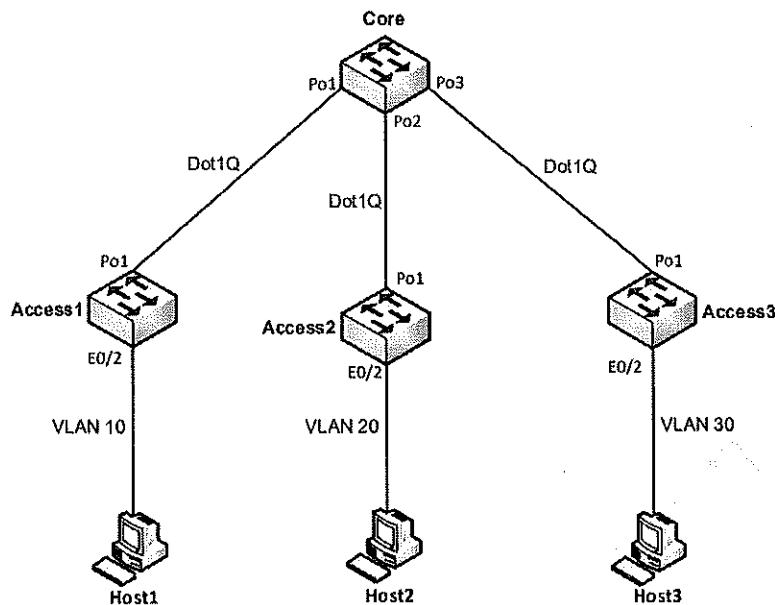
Mô tả:

- Sơ đồ bài lab gồm các thiết bị được kết nối với nhau như trên hình 1. Trong đó: các router và các switch (bao gồm cả thiết bị giả lập Internet) chạy hệ điều hành IOL, các host là các VPC được tích hợp sẵn trên EVE.
- Trong bài lab này, các bạn học viên sẽ thực hiện cấu hình Etherchannel theo các phương thức cấu hình đã được trình bày trong phần lý thuyết.
- Các thiết bị đã được cấu hình sẵn hostname, các bạn không cần phải thiết lập lại thông số này. Ngoài ra, các bạn không can thiệp vào thiết bị giả lập Internet trong suốt quá trình thực hiện bài lab.

Yêu cầu:

1. Cấu hình Etherchannel:

- Thực hiện thiết lập các đường Etherchannel như được mô tả trong hình 1.
- Trong đó:
 - Link Etherchannel nối giữa Core và Access1 sử dụng phương thức LACP.
 - Link Etherchannel nối giữa Core và Access2 sử dụng phương thức cấu hình tĩnh (ON).
 - Link Etherchannel nối giữa Core và Access3 sử dụng phương thức PAgP.
- Kết quả thiết lập Etherchannel giữa các switch được mô tả trong hình 2:

*Hình 2 – Sơ đồ Etherchannel.***2. Cấu hình Trunking:**

- Thực hiện cấu hình các đường Etherchannel nối giữa các switch thành các đường trunk.
- Các đường trunk này sử dụng kỹ thuật Trunking Dot1Q.

3. VTP, VLAN:

- Cấu hình để các switch tham gia VTP với các thông số như sau:
 - VTP domain: *waren*, VTP password: *cisco*.
 - Core: Server; Access1, Access2, Access3: Client.
- Trên switch Core thực hiện tạo các VLAN 10, 20, 30, sau đó thực hiện kiểm tra xác nhận rằng cấu hình VLAN này đã lan truyền xuống các switch access.
- Trên các switch access, thực hiện gán các cổng nối đến các host vào các VLAN như được chỉ ra trên sơ đồ lan ở các hình 1 và 2.

4. Định tuyến VLAN:

Trên router Edge, thực hiện định tuyến giữa các VLAN theo các thông số được chỉ ra trong bảng 1:

<i>Sub - interface</i>	<i>VLAN</i>	<i>Địa chỉ</i>	<i>Subnet</i>
E0/0.10	10	10.1.10.1	10.1.10.0/24
E0/0.20	20	10.1.20.1	10.1.20.0/24
E0/0.30	30	10.1.30.1	10.1.30.0/24

Bảng 1 – Quy hoạch IP cho định tuyến VLAN.

5. DHCP:

- Thực hiện cấu hình router Edge làm DHCP server cấp phát IP cho các host thuộc các VLAN theo quy hoạch IP trên bảng 1.
- Ping kiểm tra giữa các host để xác nhận rằng các host thuộc các VLAN đã có thể đi đến nhau.

6. Internet:

- Cấu hình router Edge đảm bảo các host đều có thể truy nhập được Internet.
- Hoạt động truy nhập Internet được kiểm tra bằng cách ping đến địa chỉ 8.8.8.8 từ các host.

Thực hiện:**1. Cấu hình Etherchannel:****Cấu hình:**

Chúng ta thực hiện cấu hình các đường Etherchannel giữa các cặp switch theo yêu cầu đặt ra.

Etherchannel giữa Core và Access1 (LACP):

```
Core(config)#interface range e0/0 - 1
Core(config-if-range)#shutdown
Core(config-if-range)#channel-group 1 mode active
Core(config-if-range)#no shutdown
Core(config-if-range)#exit

Access1(config)#interface range e0/0 - 1
Access1(config-if-range)#shutdown
Access1(config-if-range)#channel-group 1 mode active
Access1(config-if-range)#no shutdown
Access1(config-if-range)#exit
```

Etherchannel giữa Core và Access2 (ON):

```
Core(config)#interface range e1/0 - 1
Core(config-if-range)#shutdown
Core(config-if-range)#channel-group 2 mode on
Core(config-if-range)#no shutdown
Core(config-if-range)#exit

Access2(config)#interface range e0/0 - 1
Access2(config-if-range)#shutdown
Access2(config-if-range)#channel-group 1 mode on
Access2(config-if-range)#no shutdown
Access2(config-if-range)#exit
```

Etherchannel giữa Core và Access3 (PAgP):

```
Core(config)#interface range e2/0 - 1
Core(config-if-range)#shutdown
Core(config-if-range)#channel-group 3 mode desirable
Core(config-if-range)#no shutdown
Core(config-if-range)#exit
```

```
Access3(config)#interface range e0/0 - 1
Access3(config-if-range)#shutdown
Access3(config-if-range)#channel-group 1 mode desirable
Access3(config-if-range)#no shutdown
Access3(config-if-range)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng Etherchannel đã được thiết lập giữa các cặp switch như yêu cầu đặt ra.

Giữa Core và Access1:

```
Core#show etherchannel 1 summary
(...)
Group Port-channel Protocol Ports
-----+-----+-----+
1 Po1(SU) LACP Et0/0(P) Et0/1(P)

Access1#show etherchannel summary
(...)
Group Port-channel Protocol Ports
-----+-----+-----+
1 Po1(SU) LACP Et0/0(P) Et0/1(P)
```

Giữa Core và Access2:

```
Core#show etherchannel 2 summary
(...)
Group Port-channel Protocol Ports
-----+-----+-----+
2 Po2(SU) - Et1/0(P) Et1/1(P)

Access2#show etherchannel summary
(...)
Group Port-channel Protocol Ports
-----+-----+-----+
1 Po1(SU) - Et0/0(P) Et0/1(P)
```

Giữa Core và Access3:

```
Core#show etherchannel 3 summary
(...)
Group Port-channel Protocol Ports
-----+-----+-----+
3 Po3(SU) PAgP Et2/0(P) Et2/1(P)

Access3#show etherchannel summary
(...)
Group Port-channel Protocol Ports
-----+-----+-----+
1 Po1(SU) PAgP Et0/0(P) Et0/1(P)
```

2. Cấu hình Trunking:

Cấu hình:

Chúng ta dựa vào sơ đồ ở hình 2 để thực hiện cấu hình lab này.

Trên Core:

```
Core(config)#interface range po1,po2,po3
Core(config-if-range)#switchport trunk encapsulation dot1q
Core(config-if-range)#switchport mode trunk
Core(config-if-range)#exit
```

Trên các switch access:

```
Access1-2-3(config)#interface po 1
Access1-2-3(config-if)#switchport trunk encapsulation dot1q
Access1-2-3(config-if)#switchport mode trunk
Access1-2-3(config-if)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng các đường trunk Etherchannel đã được thiết lập đầy đủ giữa các switch:

```
Core#show interfaces trunk
Port      Mode          Encapsulation  Status      Native vlan
Po1       on           802.1q        trunking    1
Po2       on           802.1q        trunking    1
Po3       on           802.1q        trunking    1

Port      Vlans allowed on trunk
Po1       1-4094
Po2       1-4094
Po3       1-4094

Port      Vlans allowed and active in management domain
Po1       1
Po2       1
Po3       1

Port      Vlans in spanning tree forwarding state and not pruned
Po1       1
Po2       1
Po3       1

Access1-2-3#show interfaces trunk
Port      Mode          Encapsulation  Status      Native vlan
Po1       on           802.1q        trunking    1

Port      Vlans allowed on trunk
Po1       1-4094

Port      Vlans allowed and active in management domain
Po1       1

Port      Vlans in spanning tree forwarding state and not pruned
Po1       1
```

3. VTP, VLAN:

Cấu hình:

Ta cấu hình các switch tham gia VTP với các thông số theo yêu cầu đặt ra.

Trên Core:

```
Core(config)#vtp domain waren
Core(config)#vtp password cisco
```

Trên các switch access:

```
Access1-2-3(config)#vtp domain waren
Access1-2-3(config)#vtp password cisco
Access1-2-3(config)#vtp mode client
```

Trên switch Core, chúng ta tạo các VLAN 10, 20, 30:

```
Core(config)#vlan 10,20,30
Core(config-vlan)#exit
```

Nhờ có VTP, cấu hình VLAN này sẽ được đồng bộ xuống các switch access.

Tiếp theo, trên các switch access, chúng ta thực hiện gán cổng vào các VLAN như yêu cầu đặt ra:

```
Access1(config)#interface e0/2
Access1(config-if)#switchport mode access
Access1(config-if)#switchport access vlan 10
Access2(config-if)#exit

Access2(config)#interface e0/2
Access2(config-if)#switchport mode access
Access2(config-if)#switchport access vlan 20
Access2(config-if)#exit

Access3(config)#interface e0/2
Access3(config-if)#switchport mode access
Access3(config-if)#switchport access vlan 30
Access3(config-if)#exit
```

Kiểm tra:

Ta kiểm tra thông số VTP trên các switch:

```
Core#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                 : aabb.cc80.1000
Configuration last modified by 0.0.0.0 at 7-15-21 03:19:16
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 : 1
MD5 digest : 0xA2 0xD2 0xA8 0x3E 0x0B 0x29 0xBB 0x80
              0x7C 0x9F 0xF9 0x1A 0x1B 0xF4 0xFC 0xCD
```

```
Core#show vtp password
```

```
VTP Password: cisco
```

```
Access1-2-3#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 : aabb.cc80.2000
Configuration last modified by 0.0.0.0 at 7-15-21 03:19:16
```

Feature VLAN:

```
VTP Operating Mode : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs : 8
Configuration Revision : 1
MD5 digest : 0xA2 0xD2 0xA8 0x3E 0x0B 0x29, 0xBB 0x80
              0x7C 0x9F 0xF9 0x1A 0x1B 0xF4 0xFC 0xCD
```

```
Access1-2-3#show vtp password
```

```
VTP Password: cisco
```

Cấu hình VLAN trên các switch:

```
Core#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Et0/2, Et0/3, Et1/2, Et1/3 Et2/2, Et2/3
10 VLAN0010	active	
20 VLAN0020	active	
30 VLAN0030	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Access1#show vlan brief

VLAN Name	Status	Ports
1 default	active	Et0/3
10 VLAN0010	active	Et0/2
20 VLAN0020	active	
30 VLAN0030	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Access2#show vlan brief

VLAN Name	Status	Ports
1 default	active	Et0/3
10 VLAN0010	active	
20 VLAN0020	active	Et0/2
30 VLAN0030	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Access3#show vlan brief

VLAN Name	Status	Ports
1 default	active	Et0/3
10 VLAN0010	active	
20 VLAN0020	active	
30 VLAN0030	active	Et0/2
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

4. Định tuyến VLAN:

Cấu hình:

Ta cấu hình router Edge thực hiện định tuyến VLAN theo các thông số đã được chỉ ra trên bảng 1:

```
Edge(config)#interface e0/0
Edge(config-if)#no shutdown
Edge(config-if)#exit
Edge(config)#interface e0/0.10
Edge(config-subif)#encapsulation dot1q 10
Edge(config-subif)#ip address 10.1.10.1 255.255.255.0
Edge(config-subif)#exit
```

```
Edge(config)#interface e0/0.20
Edge(config-subif)#encapsulation dot1q 20
Edge(config-subif)#ip address 10.1.20.1 255.255.255.0
Edge(config-subif)#exit
Edge(config)#interface e0/0.30
Edge(config-subif)#encapsulation dot1q 30
Edge(config-subif)#ip address 10.1.30.1 255.255.255.0
Edge(config-subif)#exit
```

Cấu hình cổng đầu nối đến Edge của switch Core thành cổng trunk:

```
Core(config)#interface e0/2
Core(config-if)#switchport trunk encapsulation dot1q
Core(config-if)#switchport mode trunk
Core(config-if)#exit
```

Kiểm tra:

Các sub-interface đã được tạo ra đầy đủ trên router Edge:

```
Edge#show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
Ethernet0/0        unassigned     YES NVRAM up           up
Ethernet0/0.10      10.1.10.1    YES manual up          up
Ethernet0/0.20      10.1.20.1    YES manual up          up
Ethernet0/0.30      10.1.30.1    YES manual up          up
Ethernet0/1         unassigned     YES NVRAM administratively down down
Ethernet0/2         unassigned     YES NVRAM administratively down down
Ethernet0/3         unassigned     YES NVRAM administratively down down
```

Cổng đầu nối đến router Edge của switch Core đã được chuyển thành cổng trunk:

```
Core#show interfaces e0/2 trunk
Port      Mode          Encapsulation  Status      Native vlan
Et0/2    on           802.1q        trunking    1

Port      Vlans allowed on trunk
Et0/2    1-4094

Port      Vlans allowed and active in management domain
Et0/2    1,10,20,30

Port      Vlans in spanning tree forwarding state and not pruned
Et0/2    1,10,20,30
```

5. DHCP:

Cấu hình:

Chúng ta thực hiện cấu hình router Edge trở thành DHCP server cấp phát IP cho các host thuộc các VLAN:

```
Edge(config)#ip dhcp excluded-address 10.1.10.1
Edge(config)#ip dhcp excluded-address 10.1.20.1
Edge(config)#ip dhcp excluded-address 10.1.30.1
```

```
Edge(config)#ip dhcp pool VLAN10
Edge(dhcp-config)#network 10.1.10.0 /24
Edge(dhcp-config)#default-router 10.1.10.1
Edge(dhcp-config)#exit
Edge(config)#ip dhcp pool VLAN20
Edge(dhcp-config)#network 10.1.20.0 /24
Edge(dhcp-config)#default-router 10.1.20.1
Edge(dhcp-config)#exit
Edge(config)#ip dhcp pool VLAN30
Edge(dhcp-config)#network 10.1.30.0 /24
Edge(dhcp-config)#default-router 10.1.30.1
Edge(dhcp-config)#exit
```

Kiểm tra:

Thực hiện kiểm tra rằng các host thuộc các VLAN đều đã có thể nhận được cấu hình IP:

```
Host1> dhcp -r
DDORA IP 10.1.10.2/24 GW 10.1.10.1
Host2> dhcp -r
DDORA IP 10.1.20.2/24 GW 10.1.20.1
Host3> dhcp -r
DDORA IP 10.1.30.2/24 GW 10.1.30.1
```

Bảng DHCP binding trên router Edge:

Edge#show ip dhcp binding			
Bindings from all pools not associated with VRF:			
IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
10.1.10.2	0100.5079.6668.07	Jul 16 2021 05:41 AM	Automatic
10.1.20.2	0100.5079.6668.08	Jul 16 2021 05:42 AM	Automatic
10.1.30.2	0100.5079.6668.09	Jul 16 2021 05:42 AM	Automatic

Ta kiểm tra rằng các host đã có thể giao tiếp được với nhau:

```
Host1> ping 10.1.20.2
84 bytes from 10.1.20.2 icmp_seq=1 ttl=63 time=5.712 ms
84 bytes from 10.1.20.2 icmp_seq=2 ttl=63 time=5.689 ms
Host1> ping 10.1.30.2
84 bytes from 10.1.30.2 icmp_seq=1 ttl=63 time=9.415 ms
84 bytes from 10.1.30.2 icmp_seq=2 ttl=63 time=5.974 ms
Host2> ping 10.1.30.2
84 bytes from 10.1.30.2 icmp_seq=1 ttl=63 time=2.502 ms
84 bytes from 10.1.30.2 icmp_seq=2 ttl=63 time=5.141 ms
```

6. Internet:

Cấu hình:

Đặt địa chỉ IP mặt ngoài và cấu hình default – route trên router Edge:

```
Edge(config)#interface e0/1
Edge(config-if)#no shutdown
Edge(config-if)#ip address 100.0.0.2 255.255.255.252
Edge(config-if)#exit
Edge(config)#ip route 0.0.0.0 0.0.0.0 100.0.0.1
```

Cấu hình NAT trên router biên:

```
Edge(config)#access-list 1 permit any
Edge(config)#ip nat inside source list 1 interface e0/1 overload
Edge(config)#interface e0/1
Edge(config-if)#ip nat outside
Edge(config-if)#exit
Edge(config)#interface e0/0.10
Edge(config-subif)#ip nat inside
Edge(config-subif)#exit
Edge(config)#interface e0/0.20
Edge(config-subif)#ip nat inside
Edge(config-subif)#exit
Edge(config)#interface e0/0.30
Edge(config-subif)#ip nat inside
Edge(config-subif)#exit
```

Kiểm tra:

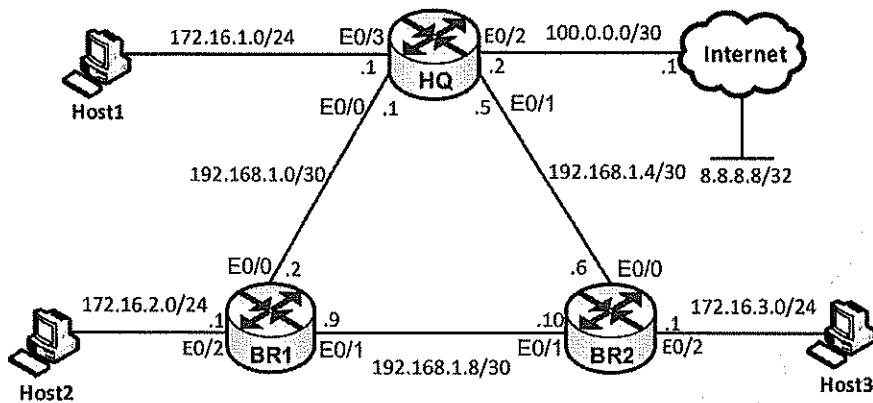
Chúng ta kiểm tra rằng các host thuộc các VLAN đều đã truy nhập được Internet:

```
Host1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=6.619 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=2.012 ms
Host2> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=1.902 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=4.275 ms
Host3> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=2.340 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=4.343 ms
```

Đến đây, chúng ta đã hoàn thành các yêu cầu đặt ra của bài lab.

Lab 14 – Giao thức định tuyến RIPv2

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Sơ đồ bài lab gồm các thiết bị được kết nối với nhau như trên hình 1. Trong đó: các router sử dụng hệ điều hành IOL, các host là các VPC được tích hợp sẵn trên EVE.
- Bài lab giả lập một mạng doanh nghiệp gồm 3 chi nhánh (một Trụ sở chính – Headquarters – HQ cùng hai chi nhánh – Branch – BR1 và BR2). Trên sơ đồ này, các bạn học viên cấu hình giao thức định tuyến RIPv2 đảm bảo mọi địa chỉ nội bộ của mạng doanh nghiệp này thấy nhau. Ngoài ra, các bạn thực hiện cấu hình thêm các dịch vụ DHCP và Internet cho các user trên mạng này.
- Các thiết bị đều đã được thiết lập sẵn hostname, các bạn không cần phải cấu hình lại thông số này. Trong quá trình làm lab, các bạn không can thiệp vào thiết bị giả lập Internet.

Yêu cầu:

1. Cấu hình cơ bản:

- Các bạn học viên thực hiện cấu hình địa chỉ IP trên các cổng nội bộ của các router theo quy hoạch IP được chỉ ra trên sơ đồ hình 1.
- Sau khi cấu hình xong, các bạn kiểm tra rằng các đường link kết nối giữa các router đã thông suốt IP.

2. Cấu hình RIPv2:

- Thực hiện cấu hình định tuyến RIPv2 trên các router đảm bảo tất cả các địa chỉ trên sơ đồ có thể thấy được nhau.
- Sau khi cấu hình xong, các bạn học viên thực hiện kiểm tra bảng định tuyến của các router và ping kiểm tra để xác nhận rằng các subnet LAN trên các router đã có thể đi đến nhau.

3. DHCP:

Thực hiện cấu hình router HQ thành DHCP server cấp phát IP cho các host trên sơ đồ.

4. Internet:

- Trên router HQ thực hiện cấu hình đảm bảo tất cả các địa chỉ IP nội bộ trong mạng doanh nghiệp có thể truy nhập được Internet.
- Việc truy nhập Internet có thể được kiểm tra bằng cách ping đến địa chỉ 8.8.8.8.

Thực hiện:**1. Cấu hình cơ bản:****Cấu hình:**

Trên HQ:

```
HQ(config)#interface e0/0
HQ(config-if)#no shutdown
HQ(config-if)#ip address 192.168.1.1 255.255.255.252
HQ(config-if)#exit
HQ(config)#interface e0/1
HQ(config-if)#no shutdown
HQ(config-if)#ip address 192.168.1.5 255.255.255.252
HQ(config-if)#exit
HQ(config)#interface e0/3
HQ(config-if)#no shutdown
HQ(config-if)#ip address 172.16.1.1 255.255.255.0
HQ(config-if)#exit
```

Trên BR1:

```
BR1(config)#interface e0/0
BR1(config-if)#no shutdown
BR1(config-if)#ip address 192.168.1.2 255.255.255.252
BR1(config-if)#exit
BR1(config)#interface e0/1
BR1(config-if)#no shutdown
BR1(config-if)#ip address 192.168.1.9 255.255.255.252
BR1(config-if)#exit
BR1(config)#interface e0/2
BR1(config-if)#no shutdown
BR1(config-if)#ip address 172.16.2.1 255.255.255.0
BR1(config-if)#exit
```

Trên BR2:

```
BR2(config)#interface e0/0
BR2(config-if)#no shutdown
BR2(config-if)#ip address 192.168.1.6 255.255.255.252
BR2(config-if)#exit
BR2(config)#interface e0/1
BR2(config-if)#no shutdown
BR2(config-if)#ip address 192.168.1.10 255.255.255.252
BR2(config-if)#exit
```

```
BR2(config)#interface e0/2
BR2(config-if)#no shutdown
BR2(config-if)#ip address 172.16.3.1 255.255.255.0
BR2(config-if)#exit
```

Kiểm tra:

Ta kiểm tra rằng các đường link đã thông suốt IP:

```
HQ#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 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

HQ#ping 192.168.1.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.6, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

BR1#ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

2. Cấu hình RIPv2:**Cấu hình:**

Trên cả 3 router, thực hiện cấu hình RIPv2 để các địa chỉ nội bộ thấy nhau:

```
router rip
version 2
network 172.16.0.0
network 192.168.1.0
no auto-summary
```

Ghi chú:

Giao thức định tuyến RIP có hai version là 1 và 2, hai version này không tương thích với nhau. Mặc định, tiến trình RIP trên các router sẽ phát đi các gói tin RIP theo cấu trúc gói của version 1 và tiếp nhận cả hai loại gói tin RIPv1 và RIPv2. Chúng ta nên cấu hình để tiến trình RIP trên router chỉ sử dụng version 2, điều này được thực hiện bằng câu lệnh “version” trong mode cấu hình của tiến trình định tuyến:

```
R(config)#router rip
R(config-router)#version 2
```

Khi bật định tuyến trên một router, chúng ta thực hiện bật trên từng cổng của router. Khi một cổng được bật định tuyến, router sẽ bắt đầu trao đổi thông tin định tuyến trên cổng này đồng thời quảng bá địa chỉ mạng trên cổng đến các router kết nối ở các cổng khác. Với Cisco IOS, để cho một cổng tham gia định tuyến, chúng ta sử dụng lệnh “network” tham chiếu đến một dải IP có chứa địa chỉ IP trên cổng; và riêng với cấu hình

định tuyến cho RIP, dải IP tham chiếu luôn là *major – network* chứa địa chỉ IP của cổng. Do đó, trên các router của bài lab, cấu hình add các cổng router vào tiến trình định tuyến RIP sẽ là:

```
R(config-router) #network 192.168.1.0
R(config-router) #network 172.16.0.0
```

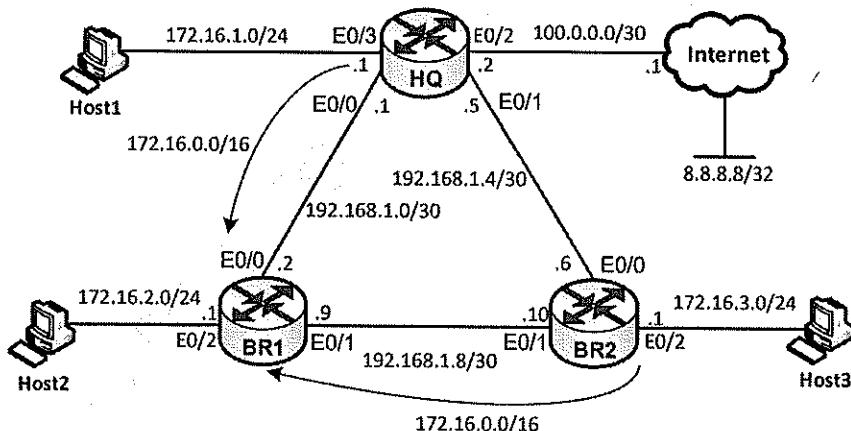
Nhắc lại rằng, một địa chỉ mạng được xem là *major network* hay *classful network* nếu đây là một địa chỉ mạng nguyên bản lớp A, B hoặc C chưa bị chia nhỏ ra bởi kỹ thuật subnetting. *Ví dụ:*

- 10.0.0.0/8 là một major network lớp A.
- 172.16.0.0/16 là một major network lớp B.
- 192.168.1.0/24 là một major network lớp C.

Ngược lại với khái niệm major network là khái niệm *subnet*, đó là một mạng con đã được chia ra từ một major nào đó. *Ví dụ:*

- 10.1.1.0/24 là một *subnet*, được chia ra từ *major* 10.0.0.0/8.
- 172.16.1.0/24 là một *subnet*, được chia ra từ *major* 172.16.0.0/16
- 192.168.1.96/28 là một *subnet*, được chia ra từ *major* 192.168.1.0/24.

Một đặc điểm nữa cần lưu ý với RIP nói riêng và các giao thức họ distance – vector nói chung là các router thường tự động thực hiện một tính năng gọi là *auto – summary*. Với tính năng này, router sẽ thực hiện chuyển một subnet thành major network khi quảng bá subnet này đi xuyên qua một major network khác; điều này sẽ khiến cho hoạt động định tuyến sẽ cập nhật không chính xác các địa chỉ mạng trên sơ đồ. Ta xem xét ví dụ:



Hình 2 – Ví dụ về “auto – summary”.

Trong ví dụ trên hình 2 (cũng là sơ đồ bài lab đang thực hiện), nếu tính năng “auto – summary” được chạy, router HQ vì phải quảng bá subnet 172.16.1.0/24 thuộc về major network 172.16.0.0/16 đi qua một subnet thuộc về một major khác (192.168.1.0/30 của 192.168.1.0/24) nên nó sẽ tự động thay đổi địa chỉ được quảng bá thành địa chỉ 172.16.0.0/16 rồi quảng bá đi đến BR1. Tương tự, router BR2 thay vì quảng bá chính xác địa chỉ 172.16.3.0/24 thì lại quảng bá thành 172.16.0.0/16 qua cho BR1. Từ đó, dẫn đến router BR1 sẽ không phân biệt được các địa chỉ mạng đích thuộc các router HQ và BR2 mà xem cả hai mạng đích này như một mạng duy nhất là mạng 172.16.0.0/16 từ đó dẫn đến sự sai lệch về thông tin trong bảng định tuyến.

Để tránh xảy ra hiện tượng “auto – summary” như mô tả ở trên, trên các router chạy RIP, ta cần tắt tính năng này bằng lệnh:

```
R(config-router) #no auto-summary
```

Kiểm tra:

Chúng ta thực hiện kiểm tra các route được học bởi giao thức RIPv2 trong bảng định tuyến các router:

```
HQ#show ip route rip
(...)
  172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
R      172.16.2.0/24 [120/1] via 192.168.1.2, 00:00:11, Ethernet0/0
R      172.16.3.0/24 [120/1] via 192.168.1.6, 00:00:08, Ethernet0/1
  192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
R      192.168.1.8/30 [120/1] via 192.168.1.6, 00:00:08, Ethernet0/1
                  [120/1] via 192.168.1.2, 00:00:11, Ethernet0/0

BR1#show ip route rip
(...)
  172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
R      172.16.1.0/24 [120/1] via 192.168.1.1, 00:00:14, Ethernet0/0
R      172.16.3.0/24 [120/1] via 192.168.1.10, 00:00:10, Ethernet0/1
  192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
R      192.168.1.4/30 [120/1] via 192.168.1.10, 00:00:10, Ethernet0/1
                  [120/1] via 192.168.1.1, 00:00:14, Ethernet0/0

BR2#show ip route rip
(...)
  172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
R      172.16.1.0/24 [120/1] via 192.168.1.5, 00:00:21, Ethernet0/0
R      172.16.2.0/24 [120/1] via 192.168.1.9, 00:00:21, Ethernet0/1
  192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
R      192.168.1.0/30 [120/1] via 192.168.1.9, 00:00:21, Ethernet0/1
                  [120/1] via 192.168.1.5, 00:00:21, Ethernet0/0
```

Từ kết quả show, chúng ta thấy rằng, các router đều đã được cập nhật tất cả các địa chỉ mạng trên sơ đồ. Ta phân tích một dòng thông tin trong số này:

```
HQ#show ip route rip
(...)
  172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
R      172.16.2.0/24 [120/1] via 192.168.1.2, 00:00:11, Ethernet0/0
(...)
```

Trong route này:

- Ký hiệu “R”: cho biết đường đi này được cập nhật bởi giao thức RIP.
- “172.16.2.0/24”: địa chỉ mạng đích.
- “[120/1]”: giá trị bên trái dấu “/” chính là giá trị AD mặc định của các route RIP và giá trị bên phải dấu “/” là metric để đến mạng đích tính từ router đang xét. Thật vậy, nếu quan sát sơ đồ, ta thấy, từ router HQ để đến mạng 172.16.2.0/24 theo hướng cổng E0/0, cần phải bước qua một router

(router BR1). Metric của một route RIP tính bằng hop – count, là tổng số router trên đường đi đến đích, nên metric của route đi đến 172.16.2.0/24 từ HQ là 1.

- “via 192.168.1.2”: địa chỉ IP next – hop của route. Chính là địa chỉ của router láng giềng đã quảng bá route tốt nhất cho router đang xét, hay địa chỉ của router kế tiếp trên đường đi đến đích.
- “00:00:11”: thời gian tính từ lúc route này được cập nhật vào bảng định tuyến – 11giây (định dạng hiện đang hiển thị là hh:mm:ss). Với RIP, vì các route được router quảng bá gửi đi gửi lại liên tục theo định kỳ 30s/lần nên khoảng thời gian này không bao giờ vượt quá 30s trong các trường hợp thông thường không xảy ra lỗi.
- “Ethernet0/0”: cổng ra (output interface) của route. Đây chính là cổng mà router HQ sẽ đẩy dữ liệu đi ra để đi đến mạng đích 172.16.2.0/24.

Với bảng định tuyến đã được cập nhật thông tin đầy đủ, lúc này các mạng LAN của các router đã có thể đi đến nhau được:

```
HQ#ping 172.16.2.1 source 172.16.1.1 <- HQ LAN đi đến được BR1 LAN
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

HQ#ping 172.16.3.1 source 172.16.1.1 <- HQ LAN đi đến được BR2 LAN
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

BR1#ping 172.16.3.1 source 172.16.2.1 <- BR1 LAN đi đến được BR2 LAN
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Ta có thể kiểm tra tính dự phòng đường đi được thực hiện một cách tự động bởi giao thức định tuyến. Ví dụ, hiện tại, HQ đang đi đến mạng 172.16.2.0/24 của BR1 bằng đường link nối trực tiếp đến router này:

```
HQ#show ip route rip
(...)
    172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
R        172.16.2.0/24 [120/1] via 192.168.1.2, 00:00:11, Ethernet0/0
(...)
```

Ta thực hiện shutdown cổng E0/0 của router BR1 để già lập tình huống đường link nối giữa BR1 và HQ bị lỗi kết nối:

```
BR1(config)#interface e0/0
BR1(config-if)#shutdown
```

Lúc này, chúng ta thấy khoảng thời gian cập nhật route của mạng 172.16.2.0/24 đã vượt quá 30s:

```
HQ#show ip route rip
(...)
  172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
R    172.16.2.0/24 [120/1] via 192.168.1.2, 00:01:22, Ethernet0/0
R    172.16.3.0/24 [120/1] via 192.168.1.6, 00:00:18, Ethernet0/1
      192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
R      192.168.1.8/30 [120/1] via 192.168.1.6, 00:00:18, Ethernet0/1
          [120/1] via 192.168.1.2, 00:01:22, Ethernet0/0
```

Tuy nhiên, đường đi này vẫn được giữ lại trong bảng định tuyến của router và HQ vẫn lái dữ liệu đi đến mạng 172.16.2.0/24 theo đường này dẫn đến dữ liệu bị mất:

```
HQ#ping 172.16.2.1 source 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.1.1
.....
Success rate is 0 percent (0/5)
```

Phái sau khoảng thời gian 240s, route bị lỗi mới được gỡ hoàn toàn khỏi bảng định tuyến và route mới được cập nhật để thay thế:

```
HQ#show ip route rip
(...)
  172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
R    172.16.2.0/24 [120/2] via 192.168.1.6, 00:00:06, Ethernet0/1
R    172.16.3.0/24 [120/1] via 192.168.1.6, 00:00:06, Ethernet0/1
      192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
R      192.168.1.8/30 [120/1] via 192.168.1.6, 00:00:06, Ethernet0/1
```

Lúc này dữ liệu đi đến mạng 172.16.2.0/24 được lái theo route mới, không còn xảy ra tình trạng mất dữ liệu:

```
HQ#ping 172.16.2.1 source 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Ví dụ vừa trình bày ở trên cho thấy rằng khi chạy định tuyến động, việc chuyển đổi đường đi được diễn ra một cách hoàn toàn tự động và không cần phải sử dụng thêm các cơ chế phụ trợ như IP SLA và track như với định tuyến tĩnh. Tuy nhiên, với RIP, việc thay đổi tuyến đường diễn ra rất chậm (tới 240s), và điều này không thể chấp nhận được trong các mạng ngày nay. Trong các mạng doanh nghiệp hiện nay, giao thức định tuyến RIP ít khi được sử dụng.

Sau khi kiểm tra xong, chúng ta nhớ no shutdown cổng E0/0 của BR1 lại như cũ:

```
BR1(config)#interface e0/0
BR1(config-if)#no shutdown
```

Router HQ lại cập nhật lại đường đi cũ khi link đầu nối đã được khôi phục:

```
HQ#show ip route rip
(...)
  172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
R*   172.16.2.0/24 [120/1] via 192.168.1.2, 00:00:00, Ethernet0/0
R     172.16.3.0/24 [120/1] via 192.168.1.6, 00:00:16, Ethernet0/1
      192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
R     192.168.1.8/30 [120/1] via 192.168.1.6, 00:00:16, Ethernet0/1
          [120/1] via 192.168.1.2, 00:00:00, Ethernet0/0
```

3. DHCP:

Cấu hình:

Chúng ta cấu hình router HQ làm DHCP server cấp phát IP cho các host thuộc các mạng LAN trên sơ đồ:

```
HQ(config)#ip dhcp excluded-address 172.16.1.1
HQ(config)#ip dhcp excluded-address 172.16.2.1
HQ(config)#ip dhcp excluded-address 172.16.3.1

HQ(config)#ip dhcp pool HQ_LAN
HQ(dhcp-config)#network 172.16.1.0 /24
HQ(dhcp-config)#default-router 172.16.1.1
HQ(dhcp-config)#exit

HQ(config)#ip dhcp pool BR1_LAN
HQ(dhcp-config)#network 172.16.2.0 /24
HQ(dhcp-config)#default-router 172.16.2.1
HQ(dhcp-config)#exit

HQ(config)#ip dhcp pool BR2_LAN
HQ(dhcp-config)#network 172.16.3.0 /24
HQ(dhcp-config)#default-router 172.16.3.1
HQ(dhcp-config)#exit
```

Bên cạnh đó, chúng ta cũng cấu hình để các router BR1 và BR2 làm DHCP Relay Agent:

```
BR1(config)#interface e0/2
BR1(config-if)#ip helper-address 192.168.1.1
BR1(config-if)#exit

BR2(config)#interface e0/2
BR2(config-if)#ip helper-address 192.168.1.5
BR2(config-if)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng các host đã nhận được cấu hình IP thông qua DHCP:

```
Host1> dhcp -r
DDORA IP 172.16.1.2/24 GW 172.16.1.1

Host2> dhcp -r
DDORA IP 172.16.2.2/24 GW 172.16.2.1

Host3> dhcp -r
DDORA IP 172.16.3.2/24 GW 172.16.3.1
```

Bảng DHCP binding của router HQ:

HQ#show ip dhcp binding			
Bindings from all pools not associated with VRF:			
IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
172.16.1.2	0100.5079.6668.05	Jul 20 2021 05:13 PM	Automatic
172.16.2.2	0100.5079.6668.06	Jul 20 2021 05:13 PM	Automatic
172.16.3.2	0100.5079.6668.07	Jul 20 2021 05:13 PM	Automatic

Ta kiểm tra rằng các host có thể đi đến nhau được:

```
Host1> ping 172.16.2.2
84 bytes from 172.16.2.2 icmp_seq=1 ttl=62 time=2.792 ms
84 bytes from 172.16.2.2 icmp_seq=2 ttl=62 time=3.072 ms

Host1> ping 172.16.3.2
84 bytes from 172.16.3.2 icmp_seq=1 ttl=62 time=2.440 ms
84 bytes from 172.16.3.2 icmp_seq=2 ttl=62 time=2.018 ms

Host2> ping 172.16.3.2
84 bytes from 172.16.3.2 icmp_seq=1 ttl=62 time=1.118 ms
84 bytes from 172.16.3.2 icmp_seq=2 ttl=62 time=2.774 ms
```

4. Internet:

Cấu hình:

Trước hết, chúng ta cấu hình IP mặt ngoài trên cổng E0/2 của router HQ:

```
HQ(config)#interface e0/2
HQ(config-if)#no shutdown
HQ(config-if)#ip address 100.0.0.2 255.255.255.252
HQ(config-if)#exit
```

Tiếp theo, chúng ta thực hiện cấu hình default – route đi Internet trên router HQ và sử dụng giao thức RIPv2 để lan truyền default – route này vào các router còn lại:

```
HQ(config)#ip route 0.0.0.0 0.0.0.0 100.0.0.1
HQ(config)#router rip
HQ(config-router)#default-information originate
HQ(config-router)#exit
```

Cuối cùng, chúng ta cấu hình NAT overload trên router HQ đảm bảo mọi địa chỉ trong mạng doanh nghiệp có thể truy nhập được Internet:

```
HQ(config)#access-list 1 permit any
HQ(config)#ip nat inside source list 1 interface e0/2 overload
HQ(config)#interface range e0/0 - 1,e0/3
HQ(config-if-range)#ip nat inside
HQ(config-if-range)#exit
```

```
HQ(config)#interface e0/2
HQ(config-if)#ip nat outside
HQ(config-if)#exit
```

Ghi chú:

Khác với các bài lab static routing, lần này các router chạy giao thức định tuyến động với nhau, có giao tiếp với nhau. Do đó, chúng ta chỉ cần thiết lập một default – route trên router biên đi Internet rồi cấu hình để router biên này sử dụng giao thức định tuyến để lan truyền default – route vào các router còn lại. Với giao thức RIPv2, câu lệnh để router biên thực hiện lan truyền default – route vào trong là:

```
R(config)#router rip
R(config-router)#default-information originate
```

Kiểm tra:

Chúng ta kiểm tra xác nhận rằng tất cả các router đều đã có default – route cho hoạt động truy nhập Internet:

```
HQ#show ip route static
(...)
Gateway of last resort is 100.0.0.1 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 100.0.0.1

BR1#show ip route rip
(...)
Gateway of last resort is 192.168.1.1 to network 0.0.0.0

R*      0.0.0.0/0 [120/1] via 192.168.1.1, 00:00:24, Ethernet0/0
(...)

BR2#show ip route rip
(...)
Gateway of last resort is 192.168.1.5 to network 0.0.0.0

R*      0.0.0.0/0 [120/1] via 192.168.1.5, 00:00:00, Ethernet0/0
(...)
```

Các host đã có thể truy nhập được Internet:

```
Host1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=0.931 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=1.161 ms

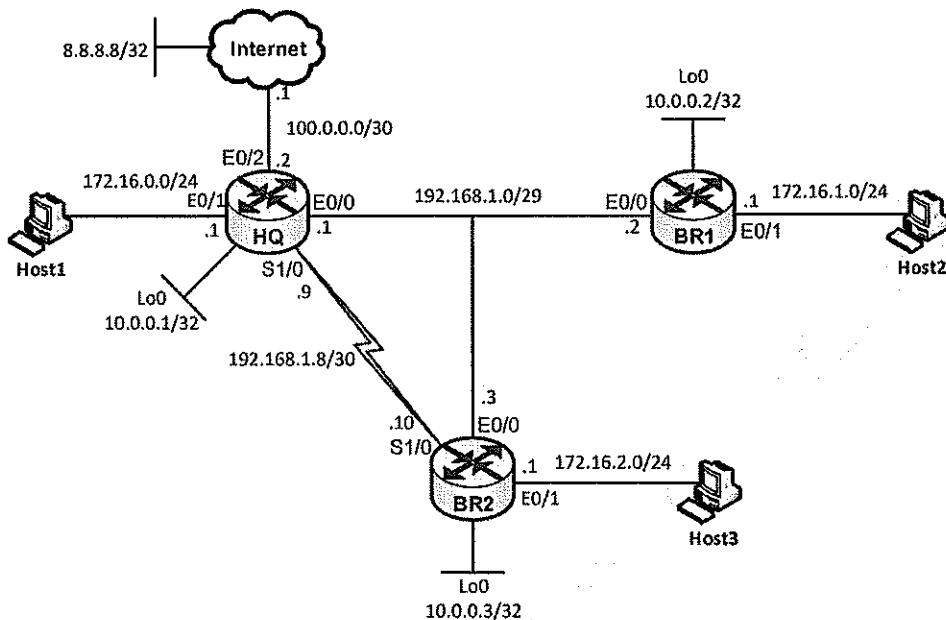
Host2> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=1.574 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=1.487 ms

Host3> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=1.316 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=1.855 ms
```

Đến đây, chúng ta đã hoàn thành các yêu cầu đặt ra của bài lab.

Lab 15 – Giao thức định tuyến OSPF

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Bài lab gồm các thiết bị được kết nối với nhau như trên sơ đồ hình 1. Trong đó: các router sử dụng hệ điều hành IOL và các host là các VPC được tích hợp sẵn trên EVE.
 - Bài lab giả lập một sơ đồ mạng doanh nghiệp gồm 3 chi nhánh: một Trụ sở chính – Headquaters – HQ và hai chi nhánh – Branch – BR1 và BR2; các host trên sơ đồ đại diện cho các mạng LAN của từng chi nhánh. Trong bài lab này, các bạn học viên sẽ thực tập cấu hình giao thức định tuyến OSPF đảm bảo mọi địa chỉ trong mạng doanh nghiệp này thấy nhau.
 - Các thiết bị đều đã được thiết lập sẵn hostname, các bạn học viên không cần phải cấu hình lại thông số này. Ngoài ra, các bạn cũng không can thiệp vào cấu hình của thiết bị giả lập Internet trong suốt quá trình thực hiện bài lab.

Yêu cầu:

1. Cấu hình cơ bản:

- Thực hiện cấu hình địa chỉ IP trên các cổng nội bộ của các router theo quy hoạch IP đã được chỉ ra trên sơ đồ ở hình 1.
 - Trên các router thực hiện tạo các interface loopback 0 với địa chỉ IP là 10.0.0.1/32 (HQ), 10.0.0.2/32 (BR1) và 10.0.0.3/32 (BR2).
 - Sau khi cấu hình xong, các bạn kiểm tra rằng các đường link kết nối giữa các router đã thông suốt kết nối IP.

2. Cấu hình OSPF:

- Cấu hình định tuyến OSPF trên các router của sơ đồ, đảm bảo mọi địa chỉ của mạng doanh nghiệp ở trên có thể đi đến nhau được.
- Sau khi cấu hình xong, các bạn học viên thực hiện kiểm tra bằng định tuyến của các router và kiểm tra rằng các mạng LAN đã có thể đi đến nhau được.

3. DHCP:

Cấu hình router HQ đảm nhận vai trò DHCP server cấp phát IP cho các host thuộc các mạng LAN.

4. Internet:

- Cấu hình router HQ đảm bảo tất cả các host trên mạng doanh nghiệp có thể truy nhập được Internet.
- Hoạt động truy nhập Internet có thể được kiểm tra bằng cách ping đến địa chỉ 8.8.8.8.

5. Hiệu chỉnh OSPF:

- Cấu hình hiệu chỉnh router – id của các router HQ, BR1, BR2 lần lượt thành: 1.1.1.1, 2.2.2.2, 3.3.3.3.
- Cấu hình đảm bảo trên đường link multiaccess, router HQ luôn đảm nhận vai trò DR.
- Cấu hình để router BR2 chọn đường đi đến mạng LAN của HQ (172.16.0.0/24) thông qua link serial kết nối giữa hai router thay vì sử dụng link Ethernet.

Thực hiện:

1. Cấu hình cơ bản:

Cấu hình:

Trên HQ:

```
HQ(config)#interface e0/0
HQ(config-if)#no shutdown
HQ(config-if)#ip address 192.168.1.1 255.255.255.248
HQ(config-if)#exit
HQ(config)#interface e0/1
HQ(config-if)#no shutdown
HQ(config-if)#ip address 172.16.0.1 255.255.255.0
HQ(config-if)#exit
HQ(config)#interface s1/0
HQ(config-if)#no shutdown
HQ(config-if)#ip address 192.168.1.9 255.255.255.252
HQ(config-if)#exit
HQ(config)#interface loopback 0
HQ(config-if)#ip address 10.0.0.1 255.255.255.255
HQ(config-if)#exit
```

Trên BR1:

```
BR1(config)#interface e0/0
BR1(config-if)#no shutdown
BR1(config-if)#ip address 192.168.1.2 255.255.255.248
BR1(config-if)#exit
```

```
BR1(config)#interface e0/1
BR1(config-if)#no shutdown
BR1(config-if)#ip address 172.16.1.1 255.255.255.0
BR1(config-if)#exit
BR1(config)#interface loopback 0
BR1(config-if)#ip address 10.0.0.2 255.255.255.255
BR1(config-if)#exit
```

Trên BR2:

```
BR2(config)#interface e0/0
BR2(config-if)#no shutdown
BR2(config-if)#ip address 192.168.1.3 255.255.255.248
BR2(config-if)#exit
BR2(config)#interface e0/1
BR2(config-if)#no shutdown
BR2(config-if)#ip address 172.16.2.1 255.255.255.0
BR2(config-if)#exit
BR2(config)#interface s1/0
BR2(config-if)#no shutdown
BR2(config-if)#ip address 192.168.1.10 255.255.255.252
BR2(config-if)#exit
BR2(config)#interface loopback 0
BR2(config-if)#ip address 10.0.0.3 255.255.255.255
BR2(config-if)#exit
```

Kiểm tra:

Ta kiểm tra rằng các đường link giữa các router đã thông suốt kết nối IP:

```
HQ#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 80 percent (4/5), round-trip min/avg/max = 1/1/3 ms
HQ#ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
HQ#ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
.!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/9/11 ms
BR1#ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

2. Cấu hình OSPF:

Cấu hình:

Trên HQ:

```
HQ(config)#router ospf 1
HQ(config-router)#network 192.168.1.0 0.0.0.7 area 0
HQ(config-router)#network 192.168.1.8 0.0.0.3 area 0
HQ(config-router)#network 172.16.0.0 0.0.0.255 area 0
HQ(config-router)#network 10.0.0.1 0.0.0.0 area 0
HQ(config-router)#exit
```

Trên BR1:

```
BR1(config)#router ospf 1
BR1(config-router)#network 192.168.1.0 0.0.0.7 area 0
BR1(config-router)#network 172.16.1.0 0.0.0.255 area 0
BR1(config-router)#network 10.0.0.2 0.0.0.0 area 0
BR1(config-router)#exit
```

Trên BR2:

```
BR2(config)#router ospf 1
BR2(config-router)#network 192.168.1.0 0.0.0.7 area 0
BR2(config-router)#network 192.168.1.8 0.0.0.3 area 0
BR2(config-router)#network 172.16.2.0 0.0.0.255 area 0
BR2(config-router)#network 10.0.0.3 0.0.0.0 area 0
BR2(config-router)#exit
```

Ghi chú:

Tương tự với các giao thức định tuyến khác, để bật định tuyến OSPF trên router, chúng ta cần thực hiện bật theo từng cổng. Để bật định tuyến trên cổng, chúng ta sử dụng lệnh “network” tham chiếu đến một dải địa chỉ IP có chứa địa chỉ IP của cổng mà chúng ta muốn bật định tuyến. Với OSPF, khi tham chiếu đến một dải IP, ta sử dụng phương pháp kết hợp một IP tham chiếu với một wildcard – mask; ngoài ra, khi cấu hình để một cổng tham gia OSPF ta còn phải chỉ ra cổng này tham gia Area nào. Do đó, cấu hình bật OSPF trên các cổng của các router phải tuân theo cú pháp sau:

```
R(config)#router ospf process-id
R(config-router)#network Reference_IP wildcard_mask area area-id
```

Ví dụ:

Để router HQ cho cổng E0/0 với địa chỉ 192.168.1.1/29 được tham gia OSPF Area 0, chúng ta có thể gõ một trong các lệnh như sau:

```
HQ(config)#router ospf 1
HQ(config-router)#network 192.168.1.0 0.0.0.7 area 0
```

Hoặc:

```
HQ(config)#router ospf 1
HQ(config-router)#network 192.168.1.0 0.0.0.3 area 0
```

Hoặc:

```
HQ(config)#router ospf 1
HQ(config-router)#network 192.168.1.1 0.0.0.0 area 0
```

.V.V...

Với lệnh đầu, cú pháp “192.168.1.0 0.0.0.7” sẽ lấy được toàn bộ các IP thuộc dải 192.168.1.0/29 và dải này có chứa địa chỉ IP 192.168.1.1 của cổng E0/0 nên cổng E0/0 được tham gia OSPF Area 0.

Với lệnh thứ hai, cú pháp “192.168.1.0 0.0.0.3” sẽ lấy được toàn bộ các IP thuộc dải 192.168.1.0/30 và dải này có chứa địa chỉ IP 192.168.1.1 của cổng E0/0 nên cổng E0/0 cũng sẽ được tham gia OSPF Area 0.

Với lệnh cuối cùng, cú pháp “192.168.1.1 0.0.0.0” sẽ lấy chính xác địa chỉ IP 192.168.1.1 của cổng E0/0 nên cổng E0/0 được tham gia OSPF Area 0.

Tóm lại, chúng ta có quyền chọn bất kỳ biểu thức nào miễn là cách viết này lấy được địa chỉ IP trên cổng là cổng sẽ được tham gia định tuyến. Nhắc lại rằng, khi một cổng của router được tham gia định tuyến, tiến trình định tuyến sẽ bắt đầu trao đổi thông tin định tuyến trên cổng và thực hiện quảng bá thông tin về cổng (trong đó có địa chỉ mạng trên cổng) đến các router khác.

Kiểm tra:

Chúng ta kiểm tra các route OSPF trong bảng định tuyến của các router:

```
HQ#show ip route ospf
(...)
  10.0.0.0/32 is subnetted, 3 subnets
O      10.0.0.2 [110/11] via 192.168.1.2, 00:06:18, Ethernet0/0
O      10.0.0.3 [110/11] via 192.168.1.3, 00:06:18, Ethernet0/0
  172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O      172.16.1.0/24 [110/20] via 192.168.1.2, 00:06:18, Ethernet0/0
O      172.16.2.0/24 [110/20] via 192.168.1.3, 00:06:18, Ethernet0/0
BR1#show ip route ospf
(...)
  10.0.0.0/32 is subnetted, 3 subnets
O      10.0.0.1 [110/11] via 192.168.1.1, 00:06:23, Ethernet0/0
O      10.0.0.3 [110/11] via 192.168.1.3, 00:06:33, Ethernet0/0
  172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O      172.16.0.0/24 [110/20] via 192.168.1.1, 00:06:23, Ethernet0/0
O      172.16.2.0/24 [110/20] via 192.168.1.3, 00:06:33, Ethernet0/0
  192.168.1.0/24 is variably subnetted, 3 subnets, 3 masks
O      192.168.1.8/30 [110/74] via 192.168.1.3, 00:06:33, Ethernet0/0
                  [110/74] via 192.168.1.1, 00:06:23, Ethernet0/0
BR2#show ip route ospf
(...)
  10.0.0.0/32 is subnetted, 3 subnets
O      10.0.0.1 [110/11] via 192.168.1.1, 00:06:27, Ethernet0/0
O      10.0.0.2 [110/11] via 192.168.1.2, 00:06:37, Ethernet0/0
  172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O      172.16.0.0/24 [110/20] via 192.168.1.1, 00:06:27, Ethernet0/0
O      172.16.1.0/24 [110/20] via 192.168.1.2, 00:06:37, Ethernet0/0
```

Các mạng LAN của các chi nhánh lúc này đã có thể đi đến nhau:

```
HQ#ping 172.16.1.1 source 172.16.0.1 <- HQ LAN di đến được BR1 LAN
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

HQ#ping 172.16.2.1 source 172.16.0.1 <- HQ LAN di đến được BR2 LAN
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

BR1#ping 172.16.2.1 source 172.16.1.1 <- BR1 LAN di đến được BR2 LAN
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Chúng ta kiểm tra thêm một số thông số khác.

Bảng neighbor của router HQ:

HQ#show ip ospf neighbor					
Neighbor ID	Pri	State	Dead Time	Address	Interface
10.0.0.3	0	FULL/ -	00:00:33	192.168.1.10	Serial1/0
10.0.0.2	1	FULL/BDR	00:00:31	192.168.1.2	Ethernet0/0
10.0.0.3	1	FULL/DR	00:00:32	192.168.1.3	Ethernet0/0

Trong kết quả show, chúng ta có thể thấy, bảng neighbor của router HQ liệt kê ra các neighbor mà nó đã thiết lập được quan hệ trên từng interface chạy OSPF. Với OSPF, các neighbor này được định danh bởi router-id của chúng. Ta thấy:

- Trên cổng Serial 1/0 (S1/0), router HQ có một neighbor là router có router-id là 10.0.0.3 (chính là BR2). Như đã đề cập trong bài giảng lý thuyết, trên link serial, không xảy ra bầu chọn DR/BDR nên quan hệ láng giềng trên link này được ký hiệu là “Full/ -”.
- Trên cổng Ethernet 0/0 (E0/0), router HQ thấy hai láng giềng là 10.0.0.2 (BR1) và 10.0.0.3 (BR2) (neighbor BR2 được thấy lại một lần nữa trên link Ethernet). Vì Ethernet là một môi trường data link multiaccess nên trên link này xảy ra hoạt động bầu chọn DR, BDR; trong hoạt động bầu chọn này, router BR2 (10.0.0.3) đang đảm nhận vai trò DR và router BR1 (10.0.0.2) đang đảm nhận vai trò BDR; từ đó suy ra router HQ đang đảm nhận vai trò DROther trên link này.

Ta có thể kiểm tra tương tự với bảng neighbor của các router còn lại.

Một câu lệnh show thông dụng khác thường được sử dụng để kiểm tra các thông số của một tiến trình định tuyến trên router là lệnh “show ip protocols”:

```
HQ#show ip protocols
(...)
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.0.0.1 <- Router-ID của router HQ
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.0.0.1 0.0.0.0 area 0
    172.16.0.0 0.0.0.255 area 0
    192.168.1.0 0.0.0.7 area 0
    192.168.1.8 0.0.0.3 area 0
  Routing Information Sources:
    Gateway          Distance      Last Update
    10.0.0.2          110          00:19:18
    10.0.0.3          110          00:19:18
  Distance: (default is 110)
```

Các biểu thức đã sử dụng để đưa các cổng vào OSPF

Để kiểm tra thông số OSPF trên một cổng đang chạy định tuyến, chúng ta sử dụng lệnh “show ip ospf interface [interface]”:

```
HQ#show ip ospf interface e0/0
Ethernet0/0 is up, line protocol is up Cổng E0/0 tham gia Area 0
  Internet Address 192.168.1.1/29, Area 0, Attached via Network Statement
  Process ID 1, Router ID 10.0.0.1, Network Type BROADCAST, Cost: 10 <- Cổng có cost=10
  Topology-MTID   Cost     Disabled     Shutdown     Topology Name
    0           10       no           no           Base
  Transmit Delay is 1 sec, State DROTHER, Priority 1 <- HQ là DROther, Priority=1
  Designated Router (ID) 10.0.0.3, Interface address 192.168.1.3 <- Thông tin của DR
  Backup Designated router (ID) 10.0.0.2, Interface address 192.168.1.2 <- Thông tin
của BDR
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40   Hello timer và Dead timer trên cổng E0/0
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 10.0.0.2 (Backup Designated Router)
    Adjacent with neighbor 10.0.0.3 (Designated Router)] Các neighbor trên E0/0
  Suppress hello for 0 neighbor(s)
```

3. DHCP:

Cấu hình:

Chúng ta cấu hình router HQ làm DHCP server cấp phát IP xuống cho các host thuộc các mạng LAN:

```
HQ(config)#ip dhcp excluded-address 172.16.0.1
HQ(config)#ip dhcp excluded-address 172.16.1.1
HQ(config)#ip dhcp excluded-address 172.16.2.1

HQ(config)#ip dhcp pool HQ_LAN
HQ(dhcp-config)#network 172.16.0.0 /24
HQ(dhcp-config)#default-router 172.16.0.1
HQ(dhcp-config)#exit

HQ(config)#ip dhcp pool BR1_LAN
HQ(dhcp-config)#network 172.16.1.0 /24
HQ(dhcp-config)#default-router 172.16.1.1
HQ(dhcp-config)#exit

HQ(config)#ip dhcp pool BR2_LAN
HQ(dhcp-config)#network 172.16.2.0 /24
HQ(dhcp-config)#default-router 172.16.2.1
HQ(dhcp-config)#exit
```

Bên cạnh đó, chúng ta cấu hình để các router BR1 và BR2 làm DHCP Relay Agent:

```
BR1-2(config)#interface e0/1
BR1-2(config-if)#ip helper-address 10.0.0.1
BR1-2(config-if)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng các host đều đã có thể nhận được cấu hình IP từ DHCP:

```
Host1> dhcpc -r
DDORA IP 172.16.0.2/24 GW 172.16.0.1

Host2> dhcpc -r
DDORA IP 172.16.1.2/24 GW 172.16.1.1

Host3> dhcpc -r
DDORA IP 172.16.2.2/24 GW 172.16.2.1
```

Bảng DHCP binding của router HQ:

```
HQ#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/           Lease expiration      Type
                  Hardware address/
                  User name
172.16.0.2          0100.5079.6668.05    Jul 21 2021 10:39 AM  Automatic
172.16.1.2          0100.5079.6668.06    Jul 21 2021 10:39 AM  Automatic
172.16.2.2          0100.5079.6668.07    Jul 21 2021 10:39 AM  Automatic
```

Với cấu hình IP nhận được, các host có thể đi đến nhau được:

```
Host1> ping 172.16.1.2
84 bytes from 172.16.1.2 icmp_seq=1 ttl=62 time=3.070 ms
84 bytes from 172.16.1.2 icmp_seq=2 ttl=62 time=1.551 ms

Host1> ping 172.16.2.2
84 bytes from 172.16.2.2 icmp_seq=1 ttl=62 time=4.574 ms
84 bytes from 172.16.2.2 icmp_seq=2 ttl=62 time=1.502 ms

Host2> ping 172.16.2.2
84 bytes from 172.16.2.2 icmp_seq=1 ttl=62 time=2.471 ms
84 bytes from 172.16.2.2 icmp_seq=2 ttl=62 time=2.024 ms
```

4. Internet:

Cấu hình:

Trước hết, chúng ta cấu hình IP mặt ngoài cho cổng đi Internet của router HQ:

```
HQ(config)#interface e0/2
HQ(config-if)#no shutdown
HQ(config-if)#ip address 100.0.0.2 255.255.255.252
HQ(config-if)#exit
```

Tiếp theo, chúng ta cấu hình default – route trên HQ cho hoạt động truy nhập Internet và thực hiện lan truyền default – route này vào mạng bên trong bằng OSPF:

```
HQ(config)#ip route 0.0.0.0 0.0.0.0 100.0.0.1
HQ(config)#router ospf 1
HQ(config-router)#default-information originate
HQ(config-router)#exit
```

Cuối cùng, chúng ta cấu hình NAT trên router HQ để đảm bảo mọi địa chỉ IP trên mạng doanh nghiệp đều có thể truy nhập được Internet:

```
HQ(config)#access-list 1 permit any
HQ(config)#ip nat inside source list 1 interface e0/2 overload
HQ(config)#interface e0/2
HQ(config-if)#ip nat outside
HQ(config-if)#exit
HQ(config)#interface range e0/0 - 1
HQ(config-if-range)#ip nat inside
HQ(config-if-range)#exit
HQ(config)#interface s1/0
HQ(config-if)#ip nat inside
HQ(config-if)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng các router đều đã có default – route cho hoạt động truy nhập Internet:

```
HQ#show ip route static
(...)
Gateway of last resort is 100.0.0.1 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 100.0.0.1

BR1#show ip route ospf
(...)
Gateway of last resort is 192.168.1.1 to network 0.0.0.0
O*E2 0.0.0.0/0 [110/1] via 192.168.1.1, 00:09:04, Ethernet0/0
    10.0.0.0/32 is subnetted, 3 subnets
O      10.0.0.1 [110/11] via 192.168.1.1, 01:10:00, Ethernet0/0
O      10.0.0.3 [110/11] via 192.168.1.3, 01:10:10, Ethernet0/0
    172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O      172.16.2.0/24 [110/20] via 192.168.1.3, 01:10:10, Ethernet0/0
    192.168.1.0/24 is variably subnetted, 3 subnets, 3 masks
O      192.168.1.8/30 [110/74] via 192.168.1.3, 01:10:10, Ethernet0/0
                    [110/74] via 192.168.1.1, 01:10:00, Ethernet0/0

BR2#show ip route ospf
(...)
Gateway of last resort is 192.168.1.1 to network 0.0.0.0
O*E2 0.0.0.0/0 [110/1] via 192.168.1.1, 00:09:08, Ethernet0/0
    10.0.0.0/32 is subnetted, 3 subnets
O      10.0.0.1 [110/11] via 192.168.1.1, 01:10:04, Ethernet0/0
O      10.0.0.2 [110/11] via 192.168.1.2, 01:10:14, Ethernet0/0
    172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O      172.16.1.0/24 [110/20] via 192.168.1.2, 01:10:14, Ethernet0/0
```

Chúng ta kiểm tra rằng các host thuộc các mạng LAN đều đã có thể truy nhập được Internet:

```
Host1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=2.714 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=1.939 ms

Host2> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=3.177 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=3.026 ms

Host3> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=2.580 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=2.741 ms
```

5. Hiệu chỉnh OSPF:**Cấu hình:**

Trước hết, chúng ta kiểm tra giá trị router – id của các router OSPF trong bài lab:

```
HQ#show ip ospf | inc ID
Routing Process "ospf 1" with ID 10.0.0.1
```

```
BR1#show ip ospf | inc ID
Routing Process "ospf 1" with ID 10.0.0.2
BR2#show ip ospf | inc ID
Routing Process "ospf 1" with ID 10.0.0.3
```

Ta thấy hiện nay router – id của các router OSPF được lấy là địa chỉ IP trên các interface loopback 0 của chúng. Điều này hoàn toàn phù hợp với lý thuyết.

Để hiệu chỉnh lại router – id của router OSPF, chúng ta sử dụng lệnh “router-id” sau đó khởi động lại tiến trình OSPF trên router:

```
HQ(config)#router ospf 1
HQ(config-router)#router-id 1.1.1.1
% OSPF: Reload or use "clear ip ospf process" command, for this to take effect
HQ(config-router)#end
HQ#clear ip ospf process
Reset ALL OSPF processes? [no]: y
BR1(config)#router ospf 1
BR1(config-router)#router-id 2.2.2.2
% OSPF: Reload or use "clear ip ospf process" command, for this to take effect
BR1(config-router)#end
BR1#clear ip ospf process
Reset ALL OSPF processes? [no]: y
BR2(config)#router ospf 1
BR2(config-router)#router-id 3.3.3.3
% OSPF: Reload or use "clear ip ospf process" command, for this to take effect
BR2(config-router)#end
BR2#clear ip ospf process
Reset ALL OSPF processes? [no]: y
```

Để hiệu chỉnh đảm bảo router HQ luôn là DR trên link multi – access, chúng ta cấu hình giá trị OSPF priority trên các cổng của các router khác nhận giá trị là 0:

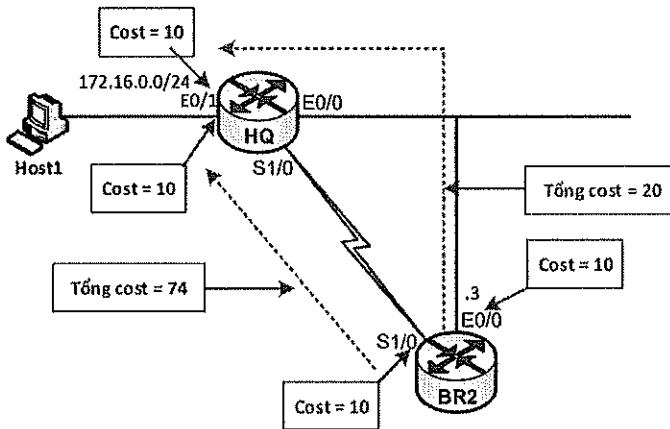
```
BR1-2(config)#interface e0/0
BR1-2(config-if)#ip ospf priority 0
BR1-2(config-if)#exit
```

Cuối cùng, chúng ta thực hiện yêu cầu hiệu chỉnh đường đi của bài lab.

Hiện nay, router BR2 đang chọn hướng để đi đến mạng LAN của HQ là theo link Ethernet trên cổng E0/0:

```
BR2#show ip route 172.16.0.0 255.255.255.0
Routing entry for 172.16.0.0/24
Known via "ospf 1", distance 110, metric 20, type intra area
Last update from 192.168.1.1 on Ethernet0/0, 00:24:38 ago
Routing Descriptor Blocks:
* 192.168.1.1, from 1.1.1.1, 00:24:38 ago, via Ethernet0/0
  Route metric is 20, traffic share count is 1
```

Ta có thể giải thích điều này như dưới đây.



Hình 2 – Tính cost từ router BR2 đi đến mạng 172.16.0.0/24.

Từ hình 2, ta có thể thấy:

- Từ BR2, nếu đi theo link Ethernet, tổng cost tích lũy sẽ bao gồm hai giá trị cost của cổng E0/1 trên HQ và E0/0 trên BR2. Giá trị cost mặc định của các cổng Ethernet là 10 nên ta sẽ có tổng cost là 20.
- Bên cạnh đó, nếu đi theo link serial, tổng cost tích lũy sẽ bao gồm hai giá trị cost của cổng E0/1 trên HQ và S1/0 trên BR2. Giá trị cost mặc định của cổng Ethernet là 10 và của cổng serial là 64 nên ta sẽ có tổng cost theo hướng này là 74.

Vì tổng cost tích lũy theo hướng Ethernet link nhỏ hơn tổng cost tích lũy theo hướng serial link nên tiến trình OSPF trên BR2 sẽ chọn hướng Ethernet đưa vào bảng định tuyến để sử dụng làm đường đi chính thức đến mạng 172.16.0.0/24 của HQ.

Để router BR2 đổi lại đường đi theo hướng serial, chúng ta cần hiệu chỉnh giá trị cost trên các cổng phù hợp sao cho tổng cost theo hướng serial nhỏ hơn tổng cost theo hướng Ethernet. Ta có thể hiệu chỉnh lại cost trên cổng serial của BR2 để đáp ứng được yêu cầu này như sau:

```
BR2(config)#interface s1/0
BR2(config-if)#ip ospf cost 1
BR2(config-if)#exit
```

Khi cost trên cổng S1/0 của BR2 đã được đổi lại thành 1, tổng cost theo hướng serial sẽ là: 11, nhỏ hơn hướng Ethernet, router BR2 sẽ cập nhật lại hướng đi mới là serial vào trong bảng định tuyến thay cho hướng đi cũ theo đường Ethernet.

Kiểm tra:

Trước hết, chúng ta kiểm tra rằng giá trị router – id trên các router đã được cập nhật lại theo yêu cầu:

```
HQ#show ip ospf | inc ID
Routing Process "ospf 1" with ID 1.1.1.1
BR1#show ip ospf | inc ID
Routing Process "ospf 1" with ID 2.2.2.2
BR2#show ip ospf | inc ID
Routing Process "ospf 1" with ID 3.3.3.3
```

Trên đường link Ethernet, lúc này, HQ đã là DR, các router còn lại vì priority = 0 nên luôn là DROther:

```
HQ#show ip ospf interface e0/0
Ethernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/29, Area 0, Attached via Network Statement
  Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 10
  Topology-MTID    Cost    Disabled    Shutdown    Topology Name
    0          10        no         no           Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, Interface address 192.168.1.1
(...)

HQ#show ip ospf neighbor

Neighbor ID      Pri   State       Dead Time     Address          Interface
3.3.3.3          0     FULL/ -     00:00:36     192.168.1.10    Serial1/0
2.2.2.2          0     FULL/DROTHER 00:00:33     192.168.1.2     Ethernet0/0
3.3.3.3          0     FULL/DROTHER 00:00:37     192.168.1.3     Ethernet0/0
```

Bảng định tuyến của router BR2 cũng chỉ ra rằng, lúc này router BR2 chọn đường đi đến mạng LAN 172.16.0.0/24 của HQ theo hướng serial:

```
BR2#show ip route 172.16.0.0 255.255.255.0
Routing entry for 172.16.0.0/24
  Known via "ospf 1", distance 110, metric 11, type intra area
  Last update from 192.168.1.9 on Serial1/0, 00:08:14 ago
  Routing Descriptor Blocks:
    * 192.168.1.9, from 1.1.1.1, 00:08:14 ago, via Serial1/0
      Route metric is 11, traffic share count is 1
```

Kết quả show cũng cho thấy, giá trị cost tích lũy lúc này của hướng serial đã được cập nhật lại là 11 đúng như phân tích ở trên.

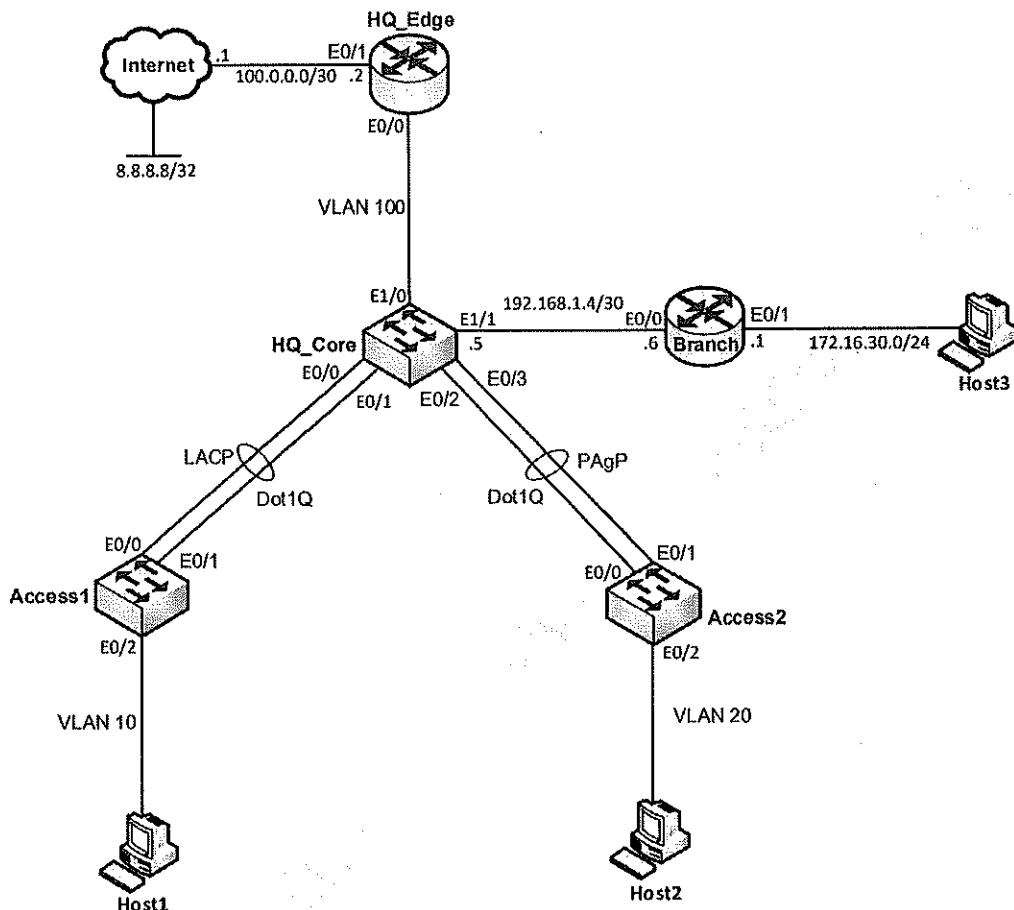
Ta có thể thực hiện trace từ Host3 đến Host1 để xác nhận lại lộ tuyến di chuyển từ BR2 LAN đến HQ LAN đã được chuyển đổi thành hướng serial:

```
Host3> trace 172.16.0.2
trace to 172.16.0.2, 8 hops max, press Ctrl+C to stop
  1  172.16.2.1  0.845 ms  0.937 ms  0.971 ms
  2  192.168.1.9  6.554 ms  4.794 ms  6.056 ms
  3  *172.16.0.2  9.171 ms (ICMP type:3, code:3, Destination port unreachable)
```

Đến đây, chúng ta đã hoàn thành tất cả các yêu cầu đặt ra của bài lab.

Lab 16 – Layer 3 switch

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Bài lab gồm các thiết bị được kết nối với nhau theo sơ đồ được chỉ ra trên hình 1. Trong sơ đồ này, các thiết bị router và switch sử dụng IOL, các host là các VPC tích hợp sẵn trên EVE.
- Bài lab giả lập một mạng doanh nghiệp có hai chi nhánh: HQ (Headquarters – Trụ sở chính) và Branch – Chi nhánh. Trong đó mạng LAN bên trụ sở chính sử dụng mô hình 2 lớp gồm có một switch Core (HQ_Core) và 2 switch access (Access1, Access2).
- Trong bài lab này, các bạn học viên sẽ thực hành thao tác với layer 3 switch cũng như ôn tập lại một số chủ đề đã học trong chương trình.
- Các thiết bị đều đã được cấu hình sẵn hostname, các bạn không cần phải thiết lập lại thông số này. Ngoài ra, các bạn không cần thiệp vào thiết bị giả lập Internet trong suốt quá trình thực hiện bài lab.

Yêu cầu:**1. Etherchannel:**

- Cấu hình thiết lập Etherchannel giữa Core và Access1. Đường Etherchannel này phải được thiết lập theo phương thức LACP.
- Cấu hình thiết lập Etherchannel giữa Core và Access2. Đường Etherchannel này phải được thiết lập theo phương thức PAgP.

2. Trunking:

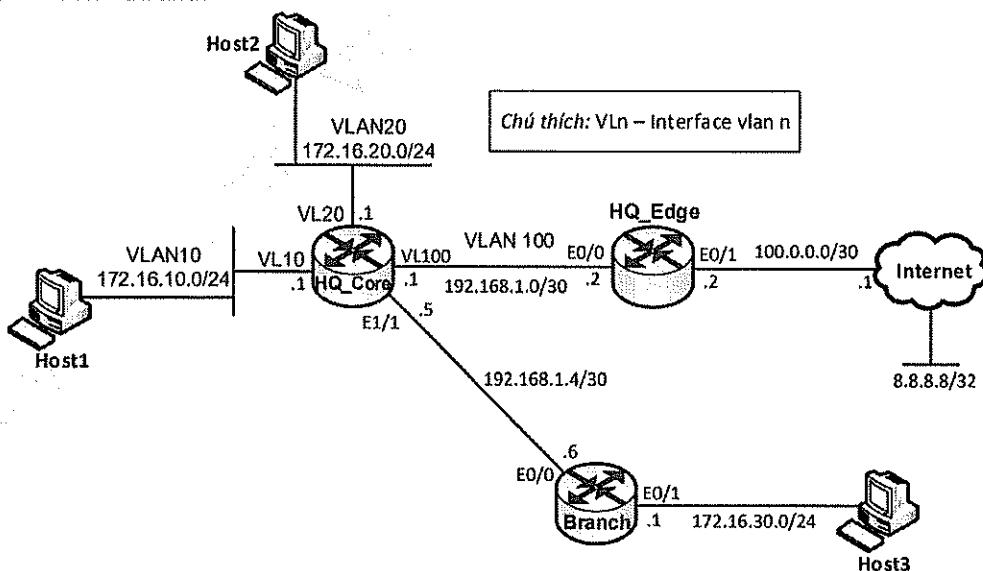
- Cấu hình các đường Etherchannel đã thiết lập ở trên hoạt động ở chế độ trunking.
- Các đường trunk này sử dụng chuẩn trunking Dot1Q.

3. VTP, VLAN:

- Cấu hình các switch của HQ tham gia VTP với các thông số như sau:
 - VTP domain: *waren*, VTP password: *cisco*.
 - Core: Server; Access1, Access2: Client.
- Trên switch Core cấu hình các VLAN 10, 20. Thực hiện kiểm tra rằng cấu hình VLAN này đã được lan truyền đến các switch Access.
- Trên các switch Access, thực hiện gán các cổng vào các VLAN mới tạo như được chỉ ra trên hình 1.

4. Layer 3 switching:

- Trên switch Core, thực hiện tạo các interface vlan cũng như chuyển cổng E1/1 thành cổng layer 3 và thực hiện đặt IP trên các interface layer 3 này theo quy hoạch IP như trong hình 2.
- Bên cạnh đó, các bạn học viên cũng thực hiện cấu hình địa chỉ IP cho các router như được chỉ ra trong sơ đồ hình 2 vừa nêu.

*Hình 2 – Sơ đồ layer 3.*

5. Định tuyến OSPF:

- Cấu hình định tuyến OSPF Area 0 trên các router và switch layer 3 đảm bảo mọi địa chỉ nội bộ trên sơ đồ thấy nhau.
- Các bạn học viên dựa vào sơ đồ layer 3 ở hình 2 để thực hiện yêu cầu này.

6. DHCP và Internet:

- Cấu hình để router HQ_Edge đảm nhận vai trò DHCP server cấp phát IP cho các VLAN 10, 20 và mạng LAN của Branch.
- Bên cạnh đó, các bạn học viên cũng thực hiện cấu hình để tất cả các IP trong mạng doanh nghiệp có thể truy nhập được Internet. Việc truy nhập Internet có thể được kiểm tra bằng cách ping đến 8.8.8.8 từ các host.

Thực hiện:

1. Etherchannel:

Cấu hình:

Thực hiện cấu hình Etherchannel LACP giữa Core và Access1:

```
HQ_Core(config)#interface range e0/0 - 1
HQ_Core(config-if-range)#shutdown
HQ_Core(config-if-range)#channel-group 1 mode active
HQ_Core(config-if-range)#no shutdown
HQ_Core(config-if-range)#exit

Access1(config)#interface range e0/0 - 1
Access1(config-if-range)#shutdown
Access1(config-if-range)#channel-group 1 mode active
Access1(config-if-range)#no shutdown
Access1(config-if-range)#exit
```

Thực hiện cấu hình Etherchannel PAgP giữa Core và Access2:

```
HQ_Core(config)#interface range e0/2 - 3
HQ_Core(config-if-range)#shutdown
HQ_Core(config-if-range)#channel-group 2 mode desirable
HQ_Core(config-if-range)#no shutdown
HQ_Core(config-if-range)#exit

Access2(config)#interface range e0/0 - 1
Access2(config-if-range)#shutdown
Access2(config-if-range)#channel-group 1 mode desirable
Access2(config-if-range)#no shutdown
Access2(config-if-range)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng các đường Etherchannel đã được thiết lập giữa các switch:

```
HQ_Core#show etherchannel summary
```

```
(...)
Group Port-channel Protocol Ports
-----+-----+-----+
1 Po1 (SU) LACP Et0/0 (P) Et0/1 (P)
2 Po2 (SU) PAgP Et0/2 (P) Et0/3 (P)
```

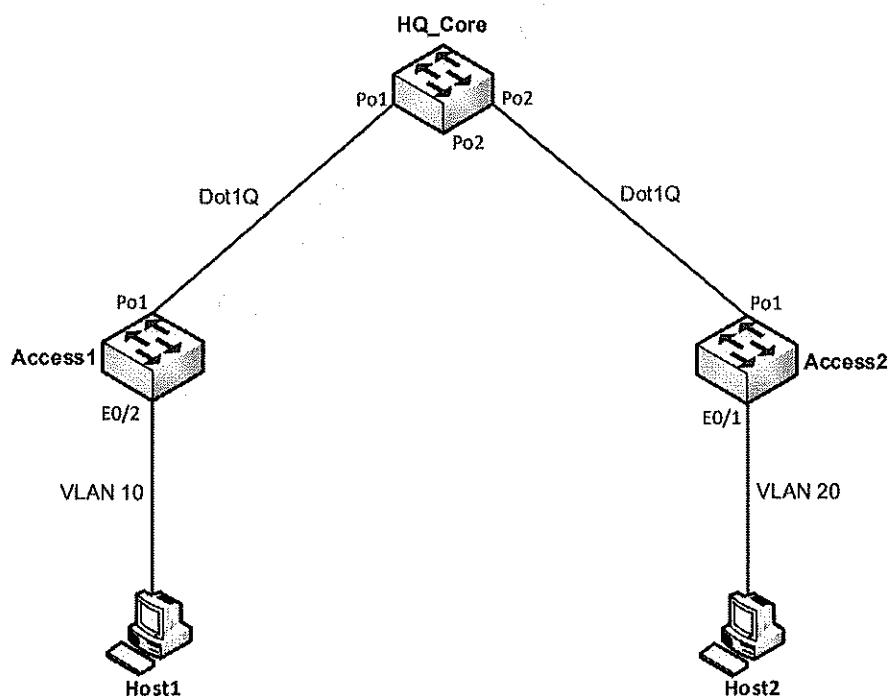
```
Access1#show etherchannel summary
```

```
(...)
Group Port-channel Protocol Ports
-----+-----+-----+
1 Po1 (SU) LACP Et0/0 (P) Et0/1 (P)
```

```
Access2#show etherchannel summary
```

```
(...)
Group Port-channel Protocol Ports
-----+-----+-----+
1 Po1 (SU) PAgP Et0/0 (P) Et0/1 (P)
```

Sau khi các đường Etherchannel đã được thiết lập, chúng ta có thể vẽ lại phần layer 2 của sơ đồ lab như sau:



Hình 3 – Sơ đồ layer 2 với Etherchannel.

2. Trunking:

Cấu hình:

Chúng ta thực hiện cấu hình trunking cho các đường Etherchannel:

```
HQ_Core(config)#interface range po1,po2
HQ_Core(config-if-range)#switchport trunk encapsulation dot1q
HQ_Core(config-if-range)#switchport mode trunk
HQ_Core(config-if-range)#exit

Access1-2(config)#interface po 1
Access1-2(config-if)#switchport trunk encapsulation dot1q
Access1-2(config-if)#switchport mode trunk
Access1-2(config-if)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng các đường Etherchannel đã lên Trunk:

```
HQ_Core#show interfaces trunk

Port      Mode          Encapsulation  Status      Native vlan
Po1       on           802.1q        trunking    1
Po2       on           802.1q        trunking    1

Port      Vlans allowed on trunk
Po1       1-4094
Po2       1-4094

Port      Vlans allowed and active in management domain
Po1       1
Po2       1

Port      Vlans in spanning tree forwarding state and not pruned
Po1       1
Po2       1

Access1-2#show interfaces trunk

Port      Mode          Encapsulation  Status      Native vlan
Po1       on           802.1q        trunking    1

Port      Vlans allowed on trunk
Po1       1-4094

Port      Vlans allowed and active in management domain
Po1       1

Port      Vlans in spanning tree forwarding state and not pruned
Po1       1
```

3. VTP, VLAN:

Cấu hình:

Cấu hình VTP trên các switch:

```
HQ_Core(config)#vtp domain waren
HQ_Core(config)#vtp password cisco
Access1-2(config)#vtp domain waren
Access1-2(config)#vtp password cisco
Access1-2(config)#vtp mode client
```

Cấu hình tạo VLAN 10, 20 trên switch Core:

```
HQ_Core(config)#vlan 10,20
HQ_Core(config-vlan)#exit
```

Sau khi cấu hình VLAN đã được đồng bộ giữa các switch, thực hiện gán các cổng vào các VLAN này trên các switch Access:

```
Access1(config)#interface e0/2
Access1(config-if)#switchport mode access
Access1(config-if)#switchport access vlan 10
Access1(config-if)#exit

Access2(config)#interface e0/2
Access2(config-if)#switchport mode access
Access2(config-if)#switchport access vlan 20
Access2(config-if)#exit
```

Kiểm tra:

Ta kiểm tra các thông số VTP của các switch:

```
HQ_Core#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                    : aabb.cc80.1000
Configuration last modified by 0.0.0.0 at 7-22-21 09:03:10
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      : 7
Configuration Revision        : 1
MD5 digest                   : 0x17 0x36 0xF1 0x13 0xAE 0xAB 0xB2 0x88
                                0xF8 0x52 0x28 0x7A 0xE2 0x17 0x2F 0x09
```

```
Access1-2#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 : aabb.cc80.2000
Configuration last modified by 0.0.0.0 at 7-22-21 09:03:10
```

Feature VLAN:

```
VTP Operating Mode : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs : 7
Configuration Revision : 1
MD5 digest : 0x17 0x36 0xF1 0x13 0xAE 0xAB 0xB2 0x88
             0xF8 0x52 0x28 0x7A 0xE2 0x17 0x2F 0x09
```

Cấu hình VLAN đã được đồng bộ trên các switch, các switch Access cũng đã gán các cổng vào các VLAN một cách phù hợp:

```
HQ_Core#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Et1/0, Et1/1, Et1/2, Et1/3
10 VLAN0010	active	
20 VLAN0020	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

```
Access1#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Et0/3
10 VLAN0010	active	Et0/2
20 VLAN0020	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

```
Access2#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Et0/3
10 VLAN0010	active	
20 VLAN0020	active	Et0/2
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

4. Layer 3 switching:

Cấu hình:

Dựa vào sơ đồ layer 3 trên hình 2, chúng ta thực hiện cấu hình các interface layer 3 trên switch Core_HQ để định tuyến VLAN cho các VLAN người dùng (VLAN 10 và 20):

```
HQ_Core(config)#interface vlan 10
HQ_Core(config-if)#no shutdown
HQ_Core(config-if)#ip address 172.16.10.1 255.255.255.0
HQ_Core(config-if)#exit

HQ_Core(config)#interface vlan 20
HQ_Core(config-if)#no shutdown
HQ_Core(config-if)#ip address 172.16.20.1 255.255.255.0
HQ_Core(config-if)#exit
```

Tiếp theo, chúng ta tạo kết nối layer 3 đến router HQ_Edge:

```
HQ_Core(config)#vlan 100
HQ_Core(config-vlan)#exit
HQ_Core(config)#interface e1/0
HQ_Core(config-if)#switchport mode access
HQ_Core(config-if)#switchport access vlan 100
HQ_Core(config-if)#exit

HQ_Core(config)#interface vlan 100
HQ_Core(config-if)#no shutdown
HQ_Core(config-if)#ip address 192.168.1.1 255.255.255.252
HQ_Core(config-if)#exit
```

Trên Core, cuối cùng, chúng ta chuyển cổng E1/1 thành cổng layer 3 để kết nối layer 3 đến router Branch:

```
HQ_Core(config)#interface e1/1
HQ_Core(config-if)#no switchport
HQ_Core(config-if)#ip address 192.168.1.5 255.255.255.252
HQ_Core(config-if)#exit
```

Trên các router, chúng ta thực hiện cấu hình các địa chỉ IP như được chỉ ra trên sơ đồ layer 3 ở hình 2:

```
HQ_Edge(config)#interface e0/0
HQ_Edge(config-if)#no shutdown
HQ_Edge(config-if)#ip address 192.168.1.2 255.255.255.252
HQ_Edge(config-if)#exit
HQ_Edge(config)#interface e0/1
HQ_Edge(config-if)#no shutdown
HQ_Edge(config-if)#ip address 100.0.0.2 255.255.255.252
HQ_Edge(config-if)#exit

Branch(config)#interface e0/0
Branch(config-if)#ip address 192.168.1.6 255.255.255.252
Branch(config-if)#exit
```

```
Branch(config)#interface e0/1
Branch(config-if)#no shutdown
Branch(config-if)#ip address 172.16.30.1 255.255.255.0
Branch(config-if)#exit
```

Kiểm tra:

Chúng ta kiểm tra danh sách các interface trên switch Core:

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	unassigned	YES	unset	up	up
Ethernet0/1	unassigned	YES	unset	up	up
Ethernet0/2	unassigned	YES	unset	up	up
Ethernet0/3	unassigned	YES	unset	up	up
Ethernet1/0	unassigned	YES	unset	up	up
Ethernet1/1	192.168.1.5	YES	manual	up	up
Ethernet1/2	unassigned	YES	unset	up	up
Ethernet1/3	unassigned	YES	unset	up	up
Port-channel1	unassigned	YES	unset	up	up
Port-channel2	unassigned	YES	unset	up	up
Vlan10	172.16.10.1	YES	manual	up	up
Vlan20	172.16.20.1	YES	manual	up	up
Vlan100	192.168.1.1	YES	manual	up	up

Chúng ta kiểm tra rằng các đường layer 3 kết nối giữa switch Core với các router đã thông suốt IP:

```
HQ_Core#ping 192.168.1.2 <- Switch Core và router Edge đã thông suốt IP
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/3 ms
HQ_Core#ping 192.168.1.6 <- Switch Core và router Branch đã thông suốt IP
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.6, timeout is 2 seconds:
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms
```

5. Định tuyến OSPF:**Cấu hình:**

Chúng ta thực hiện chạy định tuyến OSPF Area 0 trên Core switch:

```
HQ_Core(config)#ip routing
HQ_Core(config)#router ospf 1
HQ_Core(config-router)#network 172.16.10.0 0.0.0.255 area 0
HQ_Core(config-router)#network 172.16.20.0 0.0.0.255 area 0
HQ_Core(config-router)#network 192.168.1.0 0.0.0.3 area 0
HQ_Core(config-router)#network 192.168.1.4 0.0.0.3 area 0
HQ_Core(config-router)#exit
```

Việc cấu hình định tuyến trên switch layer 3 hoàn toàn giống với router, tuy nhiên, trước khi thực hiện cấu hình định tuyến, chúng ta cần bật chế độ routing trên switch bằng lệnh “ip routing” ở mode config.

Cấu hình OSPF Area 0 trên các router của bài lab:

```
HQ_Edge(config)#router ospf 1
HQ_Edge(config-router)#network 192.168.1.0 0.0.0.3 area 0
HQ_Edge(config-router)#exit

Branch(config)#router ospf 1
Branch(config-router)#network 172.16.30.0 0.0.0.255 area 0
Branch(config-router)#network 192.168.1.4 0.0.0.3 area 0
Branch(config-router)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng switch Core đã thiết lập quan hệ láng giềng OSPF với các router:

```
HQ_Core#show ip ospf neighbor

Neighbor ID      Pri   State        Dead Time     Address          Interface
192.168.1.6       1     FULL/BDR    00:00:37     192.168.1.6    Ethernet1/1
192.168.1.2       1     FULL/BDR    00:00:32     192.168.1.2    Vlan100
```

Bảng định tuyến trên switch Core và các router:

```
HQ_Core#show ip route ospf
(...)
  172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O      172.16.30.0/24 [110/20] via 192.168.1.6, 00:02:38, Ethernet1/1

HQ_Edge#show ip route ospf
(...)
  172.16.0.0/24 is subnetted, 3 subnets
O      172.16.10.0 [110/11] via 192.168.1.1, 00:03:23, Ethernet0/0
O      172.16.20.0 [110/11] via 192.168.1.1, 00:03:23, Ethernet0/0
O      172.16.30.0 [110/30] via 192.168.1.1, 00:02:39, Ethernet0/0
  192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
O      192.168.1.4/30 [110/20] via 192.168.1.1, 00:03:23, Ethernet0/0

Branch#show ip route ospf
(...)
  172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O      172.16.10.0/24 [110/11] via 192.168.1.5, 00:02:52, Ethernet0/0
O      172.16.20.0/24 [110/11] via 192.168.1.5, 00:02:52, Ethernet0/0
  192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
O      192.168.1.0/30 [110/11] via 192.168.1.5, 00:02:52, Ethernet0/0
```

Ta thấy, các subnet nội bộ đã được học đầy đủ thông qua OSPF vào bảng định tuyến của switch và các router.

Ta kiểm tra rằng, từ các VLAN người dùng của HQ có thể đi đến được mạng LAN của chi nhánh:

```
HQ_Core#ping 172.16.30.1 source 172.16.10.1 <- VLAN 10 di đến được Branch LAN
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.30.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
```

```
HQ_Core#ping 172.16.30.1 source 172.16.20.1 <- VLAN 20 đi đến được Branch LAN
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.30.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/5 ms
```

6. DHCP và Internet:

Cấu hình:

Ta thực hiện cấu hình dịch vụ DHCP trên hệ thống mạng theo yêu cầu đặt ra:

```
HQ_Edge(config)#ip dhcp excluded-address 172.16.10.1
HQ_Edge(config)#ip dhcp excluded-address 172.16.20.1
HQ_Edge(config)#ip dhcp excluded-address 172.16.30.1
HQ_Edge(config)#ip dhcp pool HQ_VLAN10
HQ_Edge(dhcp-config)#network 172.16.10.0 /24
HQ_Edge(dhcp-config)#default-router 172.16.10.1
HQ_Edge(dhcp-config)#exit
HQ_Edge(config)#ip dhcp pool HQ_VLAN20
HQ_Edge(dhcp-config)#network 172.16.20.0 /24
HQ_Edge(dhcp-config)#default-router 172.16.20.1
HQ_Edge(dhcp-config)#exit
HQ_Edge(config)#ip dhcp pool Branch_LAN
HQ_Edge(dhcp-config)#network 172.16.30.0 /24
HQ_Edge(dhcp-config)#default-router 172.16.30.1
HQ_Edge(dhcp-config)#exit

HQ_Core(config)#interface vlan 10
HQ_Core(config-if)#ip helper-address 192.168.1.2
HQ_Core(config-if)#exit
HQ_Core(config)#interface vlan 20
HQ_Core(config-if)#ip helper-address 192.168.1.2
HQ_Core(config-if)#exit

Branch(config)#interface e0/1
Branch(config-if)#ip helper-address 192.168.1.2
Branch(config-if)#exit
```

Cấu hình DHCP Server

Cấu hình DHCP Relay Agent

Cấu hình DHCP Relay Agent

Tiếp theo, chúng ta thực hiện cấu hình dịch vụ Internet:

```
HQ_Edge(config)#ip route 0.0.0.0 0.0.0.0 100.0.0.1
HQ_Edge(config)#router ospf 1
HQ_Edge(config-router)#default-information originate
HQ_Edge(config-router)#exit

HQ_Edge(config)#access-list 1 permit any
HQ_Edge(config)#ip nat inside source list 1 interface e0/1 overload
HQ_Edge(config)#interface e0/0
HQ_Edge(config-if)#ip nat inside
HQ_Edge(config-if)#exit
```

Cấu hình Default - routing

Cấu hình NAT

```
HQ_Edge(config)#interface e0/1
HQ_Edge(config-if)#ip nat outside
HQ_Edge(config-if)#exit
```

Cấu hình NAT

Kiểm tra:

Chúng ta kiểm tra rằng các host thuộc các VLAN và LAN đã nhận được cấu hình IP từ DHCP:

```
Host1> dhcp -r
DDORA IP 172.16.10.2/24 GW 172.16.10.1

Host2> dhcp -r
DDORA IP 172.16.20.2/24 GW 172.16.20.1

Host3> dhcp -r
DDORA IP 172.16.30.2/24 GW 172.16.30.1
```

Bảng DHCP binding của router HQ_Edge:

HQ_Edge#show ip dhcp binding			
Bindings from all pools not associated with VRF:			
IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
172.16.10.2	0100.5079.6668.07	Jul 24 2021 06:11 AM	Automatic
172.16.20.2	0100.5079.6668.08	Jul 24 2021 06:11 AM	Automatic
172.16.30.2	0100.5079.6668.09	Jul 24 2021 06:14 AM	Automatic

Các host có thể đi đến nhau được:

```
Host1> ping 172.16.20.2
84 bytes from 172.16.20.2 icmp_seq=1 ttl=63 time=3.282 ms
84 bytes from 172.16.20.2 icmp_seq=2 ttl=63 time=2.297 ms

Host1> ping 172.16.30.2
84 bytes from 172.16.30.2 icmp_seq=1 ttl=62 time=3.085 ms
84 bytes from 172.16.30.2 icmp_seq=2 ttl=62 time=2.374 ms

Host2> ping 172.16.30.2
84 bytes from 172.16.30.2 icmp_seq=1 ttl=62 time=1.891 ms
84 bytes from 172.16.30.2 icmp_seq=2 ttl=62 time=4.658 ms
```

Các host đã có thể truy nhập Internet:

```
Host1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=1.784 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=3.890 ms

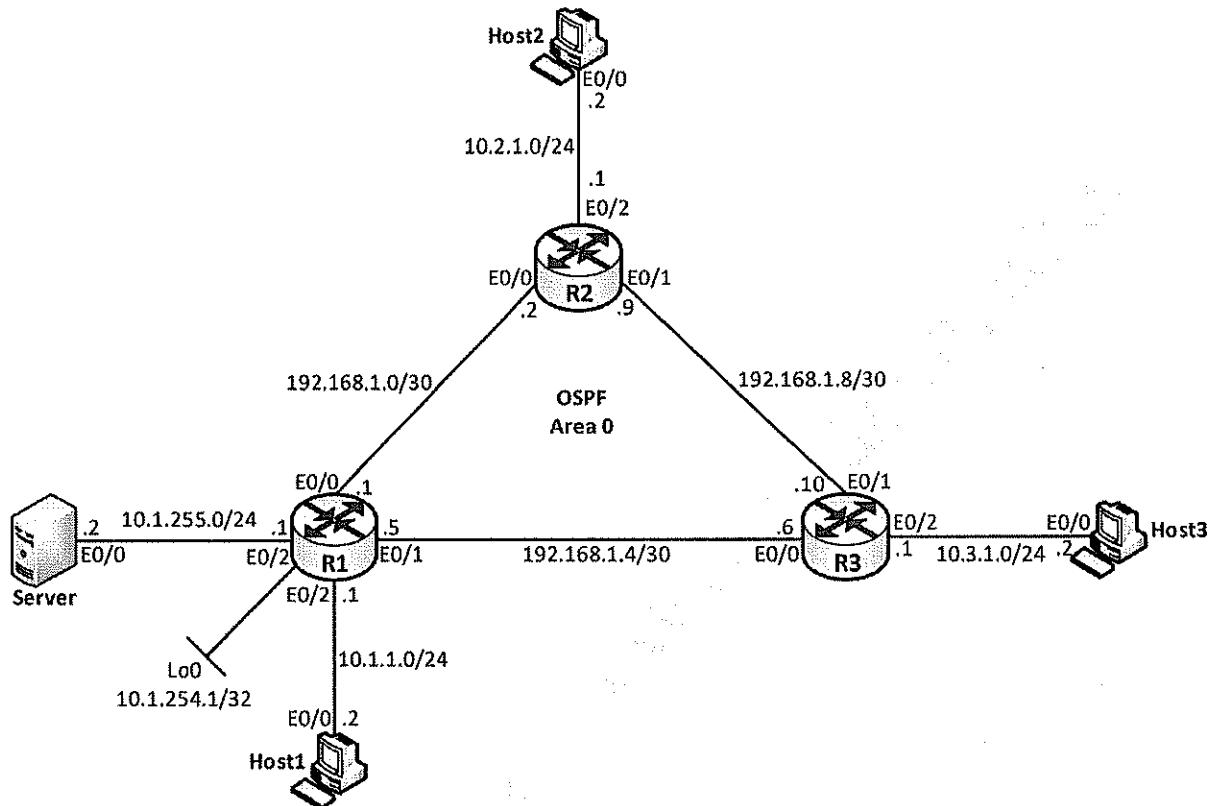
Host2> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=1.746 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=5.315 ms

Host3> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=252 time=2.151 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=252 time=2.358 ms
```

Đến đây, chúng ta đã hoàn thành tất cả các yêu cầu đặt ra của bài lab.

Lab 17 – Access Control List (ACL)

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Bài lab gồm các thiết bị được đấu nối với nhau như trên hình 1. Trên sơ đồ lab này, các bạn học viên sẽ thực hành ôn tập các vấn đề về kỹ thuật access control list (ACL) trên router Cisco.
- Trong bài lab này, các thiết bị đều đã được cấu hình thiết lập sẵn hostname và địa chỉ IP trên các cổng, các bạn học viên không cần phải cấu hình lại các thông số này.
- Các thiết bị: Server, Host1, Host2 và Host3 được giả lập bởi router Cisco chạy IOS, Khi thao tác trên các thiết bị này, các bạn sử dụng tập lệnh của Cisco IOS của router. Như đã nêu ở trên, các host và server đều đã được thiết lập cấu hình ban đầu, chúng ta chỉ cần thiệp thay đổi cấu hình trên chúng khi được yêu cầu trong bài lab; riêng thiết bị Server, các bạn học viên không thao tác trong suốt quá trình thực hiện bài lab.

Yêu cầu:**1. Cấu hình OSPF:**

- Các bạn học viên thực hiện cấu hình OSPF trên các router đảm bảo mọi địa chỉ trên sơ đồ thấy nhau.
- Các cổng của các router đều tham gia Area 0 và sử dụng tiến trình OSPF 1.

2. Standard ACL (1):

Trên R1 thực hiện cấu hình một standard ACL và đặt vào vị trí thích hợp để đáp ứng các yêu cầu sau:

- Chỉ cho phép các user thuộc dải IP 10.1.1.0/24 được quyền telnet đến R1.
- Mọi địa chỉ khác đều bị cấm thực hiện hoạt động telnet vừa nêu.

3. Extended ACL (1):

Trên cổng E0/2 của R1 hãy cấu hình một Extended ACL theo chiều out đáp ứng các yêu cầu sau:

- Chỉ cho phép các user thuộc mạng 10.2.1.0/24 được truy nhập web đến thiết bị Server.
- Chỉ cho phép các user thuộc mạng 10.3.1.0/24 được thực hiện DNS query đến thiết bị Server. Tên miền được sử dụng để test ở câu này là “testhost.com”.
- Chỉ cho phép các user thuộc mạng 10.1.1.0/24 được ping đến thiết bị Server.

4. Standard ACL (2):

Trên R2 và R3 thực hiện cấu hình các standard ACL ở các vị trí thích hợp để đáp ứng các yêu cầu sau:

- Chỉ cho phép các user thuộc dải IP từ 10.1.1.32 đến 10.1.1.35 được quyền telnet đến R2.
- Chỉ cho phép các user thuộc dải IP từ 10.1.1.96 đến 10.1.1.97 được quyền telnet đến R3.

5. Extended ACL (2):

Thực hiện bổ sung cấu hình cho extended ACL đã làm trên R1 để đáp ứng yêu cầu sau:

- Thiết bị Server ping được đến các user thuộc hai dải IP 10.2.1.0/24 và 10.3.1.0/24.
- Tuy nhiên, các user thuộc hai dải vừa nêu không ping được Server.

6. Named ACL:

- Thực hiện thay đổi standard ACL trên R1 thành một named – ACL với tên là “TELNET”, và vẫn giữ nguyên công dụng như của ACL đã cấu hình trước đó.
- Thực hiện thay đổi extended ACL trên R1 thành một named – ACL với tên là “FIREWALL”, và vẫn giữ nguyên công dụng như của ACL đã cấu hình trước đó.

Thực hiện:**1. Cấu hình OSPF:****Cấu hình:**

Trên R1:

```
R1(config)#router ospf 1
R1(config-router)#network 10.1.1.1 0.0.0.0 area 0
R1(config-router)#network 10.1.254.1 0.0.0.0 area 0
R1(config-router)#network 10.1.255.1 0.0.0.0 area 0
```

```
R1(config-router)#network 192.168.1.1 0.0.0.0 area 0
R1(config-router)#network 192.168.1.5 0.0.0.0 area 0
R1(config-router)#exit
```

Trên R2:

```
R2(config)#router ospf 1
R2(config-router)#network 10.2.1.1 0.0.0.0 area 0
R2(config-router)#network 192.168.1.2 0.0.0.0 area 0
R2(config-router)#network 192.168.1.9 0.0.0.0 area 0
R2(config-router)#exit
```

Trên R3:

```
R3(config)#interface range e0/0 - 2
R3(config-if-range)#ip ospf 1 area 0
R3(config-if-range)#exit
```

Kiểm tra:

Ta kiểm tra rằng quan hệ láng giềng OSPF đã được thiết lập đầy đủ giữa các router:

R1#show ip ospf neighbor					
Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.10	1	FULL/BDR	00:00:37	192.168.1.6	Ethernet0/1
192.168.1.9	1	FULL/BDR	00:00:31	192.168.1.2	Ethernet0/0

R2#show ip ospf neighbor					
Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.10	1	FULL/DR	00:00:35	192.168.1.10	Ethernet0/1
10.1.254.1	1	FULL/DR	00:00:34	192.168.1.1	Ethernet0/0

R3#show ip ospf neighbor					
Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.9	1	FULL/BDR	00:00:33	192.168.1.9	Ethernet0/1
10.1.254.1	1	FULL/DR	00:00:34	192.168.1.5	Ethernet0/0

Bảng định tuyến trên các router đều đã được OSPF cập nhật đầy đủ các subnet không kết nối trực tiếp:

R1#show ip route ospf					
(...)	10.0.0.0/8	is variably subnetted, 7 subnets, 2 masks			
O	10.2.1.0/24	[110/20]	via 192.168.1.2, 00:06:09,	Ethernet0/0	
O	10.3.1.0/24	[110/20]	via 192.168.1.6, 00:05:40,	Ethernet0/1	
	192.168.1.0/24	is variably subnetted, 5 subnets, 2 masks			
O	192.168.1.8/30	[110/20]	via 192.168.1.6, 00:05:40,	Ethernet0/1	
		[110/20]	via 192.168.1.2, 00:02:49,	Ethernet0/0	
R2#show ip route ospf					
(...)	10.0.0.0/8	is variably subnetted, 6 subnets, 2 masks			
O	10.1.1.0/24	[110/20]	via 192.168.1.1, 00:06:09,	Ethernet0/0	
O	10.1.254.1/32	[110/11]	via 192.168.1.1, 00:06:09,	Ethernet0/0	
O	10.1.255.0/24	[110/20]	via 192.168.1.1, 00:06:09,	Ethernet0/0	
O	10.3.1.0/24	[110/20]	via 192.168.1.10, 00:02:53,	Ethernet0/1	
	192.168.1.0/24	is variably subnetted, 5 subnets, 2 masks			

```
O      192.168.1.4/30 [110/20] via 192.168.1.10, 00:02:53, Ethernet0/1
                  [110/20] via 192.168.1.1, 00:06:09, Ethernet0/0
R3#show ip route ospf
(...)
  10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
O      10.1.1.0/24 [110/20] via 192.168.1.5, 00:05:43, Ethernet0/0
O      10.1.254.1/32 [110/11] via 192.168.1.5, 00:05:43, Ethernet0/0
O      10.1.255.0/24 [110/20] via 192.168.1.5, 00:05:43, Ethernet0/0
O      10.2.1.0/24 [110/20] via 192.168.1.9, 00:02:57, Ethernet0/1
  192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O      192.168.1.0/30 [110/20] via 192.168.1.9, 00:02:57, Ethernet0/1
                  [110/20] via 192.168.1.5, 00:05:43, Ethernet0/0
```

Ta có thể kiểm tra rằng trước khi áp các access – list, mọi host trên sơ đồ đều đã có thể đi đến được nhau:

```
Host1#ping 10.2.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
Host1#ping 10.3.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms
Host1#ping 10.1.255.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.255.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
Host1#ping 10.1.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.254.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Host2#ping 10.3.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Host2#ping 10.1.255.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.255.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

```
Host2#ping 10.1.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.254.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

Host3#ping 10.1.255.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.255.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

Host3#ping 10.1.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.254.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

2. Standard ACL (I):

Cấu hình:

Truờc khi cấu hình ACL, mọi user trên mọi subnet đều có thể Telnet được đến R1:

```
Host1#telnet 10.1.254.1
Trying 10.1.254.1 ... Open

R1#
Host2#telnet 10.1.254.1
Trying 10.1.254.1 ... Open

R1#
Host3#telnet 10.1.254.1
Trying 10.1.254.1 ... Open

R1#
```

Ta cấu hình ACL trên R1 để chỉ cho phép các user thuộc subnet 10.1.1.0/24 được telnet vào R1:

```
R1(config)#access-list 1 permit 10.1.1.0 0.0.0.255
R1(config)#line vty 0 4
R1(config-line)#access-class 1 in
R1(config-line)#exit
```

Kiểm tra:

Ta kiểm tra nội dung ACL vừa cấu hình:

```
R1#show access-lists 1
Standard IP access list 1
    10 permit 10.1.1.0, wildcard bits 0.0.0.255
```

ACL này đã được đặt vào các cổng VTY của R1:

```
R1#show run | sec vty
line vty 0 4
access-class 1 in
privilege level 15
no login
transport input telnet
```

Lúc này, Host1 vẫn có thể telnet được đến R1 nhưng Host2 và Host3 đã không còn có thể telnet được R1:

```
Host1#telnet 10.1.254.1
Trying 10.1.254.1 ... Open
R1#
Host2#telnet 10.1.254.1
Trying 10.1.254.1 ...
% Connection refused by remote host
Host3#telnet 10.1.254.1
Trying 10.1.254.1 ...
% Connection refused by remote host
```

3. Extended ACL (1):

Cấu hình:

Trước khi cấu hình ACL, tất cả các host đều có thể truy nhập web đến Server:

```
Host1>telnet 10.1.255.2 80
Trying 10.1.255.2, 80 ... Open
exit
HTTP/1.1 400 Bad Request
Date: Thu, 23 Jul 2020 08:19:59 GMT
Server: cisco-IOS
Accept-Ranges: none
400 Bad Request
[Connection to 10.1.255.2 closed by foreign host]

Host2>telnet 10.1.255.2 80
Trying 10.1.255.2, 80 ... Open
exit
HTTP/1.1 400 Bad Request
Date: Thu, 23 Jul 2020 08:20:13 GMT
Server: cisco-IOS
Accept-Ranges: none
400 Bad Request
[Connection to 10.1.255.2 closed by foreign host]

Host3>telnet 10.1.255.2 80
Trying 10.1.255.2, 80 ... Open
exit
HTTP/1.1 400 Bad Request
Date: Thu, 23 Jul 2020 08:20:21 GMT
Server: cisco-IOS
Accept-Ranges: none
400 Bad Request
[Connection to 10.1.255.2 closed by foreign host]
```

Ở trên ta kiểm tra việc truy nhập web đến thiết bị Server bằng cách telnet đến địa chỉ của thiết bị này với port đích được đổi thành port 80. Ta thấy rằng các host sau khi truy nhập đều được trả về một hồi đáp HTTP với code 400 – Bad request; điều này cho thấy hiện tại, cả 3 host đều đang truy nhập web được đến Server. Theo yêu cầu đặt ra, ta cấu hình ACL để chỉ cho các user thuộc subnet 10.2.1.0/24 (Host2) được phép truy nhập web đến Server vừa nêu. Trên R1:

```
R1(config)#access-list 100 permit tcp 10.2.1.0 0.0.0.255 host 10.1.255.2 eq 80
```

Hiện tại, cả 3 host thuộc 3 subnet đều có thể sử dụng DNS server trên 10.1.255.2. Ta phải viết một “rule” ACL để chỉ cho phép subnet 10.3.1.0/24 được sử dụng DNS server này.

Trước hết, ta kiểm tra rằng các host đều có thể query DNS đến thiết bị 10.1.255.2:

```
Host1-2-3(config)#ip domain-lookup
Host1-2-3(config)#ip name-server 10.1.255.2
Host1-2-3(config)#exit

Host1-2-3#ping testhost.com
Translating "testhost.com"...domain server (10.1.255.2) [OK]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.254.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Ta viết tiếp một “rule” ACL chỉ cho phép các user thuộc subnet 10.3.1.0/24 được query DNS đến Server:

```
R1(config)#access-list 100 permit udp 10.3.1.0 0.0.0.255 host 10.1.255.2 eq 53
```

Cuối cùng, ta viết một dòng ACL để chỉ cho phép các host thuộc mạng 10.1.1.0/24 được phép ping đến Server. Lưu ý rằng, trước đó, trong yêu cầu 1, ta đã kiểm tra xác nhận rằng hiện nay mọi host đều có thể ping đến Server. Trên R1:

```
R1(config)#access-list 100 permit icmp 10.1.1.0 0.0.0.255 host 10.1.255.2
```

Sau khi hoàn tất các “rule”, ta thực hiện áp ACL 100 vừa cấu hình vào cổng E0/2 theo chiều out:

```
R1(config)#interface e0/2
R1(config-if)#ip access-group 100 out
R1(config-if)#exit
```

Kiểm tra:

Ta kiểm tra rằng ACL vừa nêu đã phát huy tác dụng.

Đầu tiên, chỉ còn Host2 (thuộc mạng 10.2.1.0/24) có thể truy nhập web đến Server:

```
Host1#telnet 10.1.255.2 80
Trying 10.1.255.2, 80 ...
% Destination unreachable; gateway or host down

Host2#telnet 10.1.255.2 80
Trying 10.1.255.2, 80 ... Open
exit
HTTP/1.1 400 Bad Request
Date: Thu, 23 Jul 2020 08:48:44 GMT
```

```
Server: cisco-IOS
Accept-Ranges: none
400 Bad Request
[Connection to 10.1.255.2 closed by foreign host]

Host3#telnet 10.1.255.2 80
Trying 10.1.255.2, 80 ...
% Destination unreachable; gateway or host down
```

Tiếp theo, chỉ Host3 (thuộc mạng 10.3.1.0/24) được query DNS đến Server:

```
Host1#ping testhost.com
Translating "testhost.com"...domain server (10.1.255.2)
% Unrecognized host or address, or protocol not running.

Host2#ping testhost.com
Translating "testhost.com"...domain server (10.1.255.2)
% Unrecognized host or address, or protocol not running.

Host3#ping testhost.com
Translating "testhost.com"...domain server (10.1.255.2) [OK]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.254.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Cuối cùng, chỉ Host1 (thuộc mạng 10.1.1.0/24) ping được Server:

```
Host1#ping 10.1.255.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.255.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

Host2#ping 10.1.255.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.255.2, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)

Host3#ping 10.1.255.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.255.2, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
```

4. Standard ACL (2):

Cấu hình:

Trên R2, ta cấu hình một standard ACL và đặt vào các cổng VTY để chỉ cho phép các IP từ 10.1.1.32 đến 10.1.1.35 được phép telnet vào R2:

```
R2(config)#access-list 1 permit 10.1.1.32 0.0.0.3
R2(config)#line vty 0 4
R2(config-line)#access-class 1 in
```

```
R2(config-line)#exit
```

Tiếp theo, trên R3, ta cấu hình một standard ACL và đặt vào các cổng VTY để chỉ cho phép các IP 10.1.1.96 và 10.1.1.97 được phép telnet vào R2:

```
R3(config)#access-list 1 permit 10.1.1.96 0.0.0.1
R3(config)#line vty 0 4
R3(config-line)#access-class 1 in
R3(config-line)#exit
```

Kiểm tra:

Hiện nay Host1 đang sử dụng địa chỉ IP 10.1.1.2 và như vậy, theo các dòng ACL vừa mới cấu hình ở trên, Host1 không thể telnet được đến R2 và R3:

```
Host1#telnet 192.168.1.2
Trying 192.168.1.2 ...
% Connection refused by remote host

Host1#telnet 192.168.1.6
Trying 192.168.1.6 ...
% Connection refused by remote host
```

Ta thực hiện thay đổi IP của Host1 thành 10.1.1.32, là một địa chỉ có thể telnet đến R2 và thử lại telnet:

```
Host1(config)#interface e0/0
Host1(config-if)#ip address 10.1.1.32 255.255.255.0
Host1(config-if)#end

Host1#telnet 192.168.1.2
Trying 192.168.1.2 ... Open <-Telnet R2 thành công
R2#
```

Ta tiếp tục thay đổi IP của Host1 thành 10.1.1.96, là một địa chỉ có thể telnet đến R3 và thử lại telnet:

```
Host1(config)#interface e0/0
Host1(config-if)#ip address 10.1.1.96 255.255.255.0
Host1(config-if)#end

Host1#telnet 192.168.1.6
Trying 192.168.1.6 ... Open <-Telnet R3 thành công
R3#
```

5. Extended ACL (2):

Cấu hình:

Trước hết, ta kiểm tra rằng hiện nay các thiết bị Host2 và Host3 không ping được Server nhưng Server cũng không ping được các host này:

```
Host2#ping 10.1.255.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.255.2, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)

Host3#ping 10.1.255.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.255.2, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)

Server#ping 10.2.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Server#ping 10.3.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Để Server có thể ping được thành công đến các host ở các mạng 10.2.1.0/24 và 10.3.1.0/24, ta bổ sung thêm một dòng vào ACL 100 cho phép các gói ICMP Echo Reply trả về từ các host thuộc hai mạng này:

```
R1(config)#access-list 100 permit icmp 10.2.1.0 0.0.0.255 host 10.1.255.2 echo-reply
R1(config)#access-list 100 permit icmp 10.3.1.0 0.0.0.255 host 10.1.255.2 echo-reply
```

Kiểm tra:

Ta kiểm tra rằng, lúc này các thiết bị Host2 và Host3 vẫn không ping được Server nhưng Server đã có thể ping được các host:

```
Host2#ping 10.1.255.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.255.2, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)

Host3#ping 10.1.255.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.255.2, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)

Server#ping 10.2.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

```
Server#ping 10.3.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

6. Named ACL:

Cấu hình:

Ta thực hiện chuyển đổi các access – list đã cấu hình trên R1 thành dạng Named – ACL.

Trước hết, ta kiểm tra lại các ACL đã cấu hình:

```
R1#show access-lists
Standard IP access list 1
    10 permit 10.1.1.0, wildcard bits 0.0.0.255
Extended IP access list 100
    10 permit tcp 10.2.1.0 0.0.0.255 host 10.1.255.2 eq www (10 matches)
    20 permit udp 10.3.1.0 0.0.0.255 host 10.1.255.2 eq domain (1 match)
    30 permit icmp 10.1.1.0 0.0.0.255 host 10.1.255.2 (5 matches)
    40 permit icmp 10.2.1.0 0.0.0.255 host 10.1.255.2 echo-reply (5 matches)
    50 permit icmp 10.3.1.0 0.0.0.255 host 10.1.255.2 echo-reply (5 matches)
```

Ta thực hiện gỡ bỏ Standard ACL số 1 và thay bằng một Standard Named ACL có tên là “TELNET”:

```
R1(config)#no access-list 1
R1(config)#ip access-list standard TELNET
R1(config-std-nacl)#permit 10.1.1.0 0.0.0.255
R1(config-std-nacl)#exit
R1(config)#line vty 0 4
R1(config-line)#no access-class 1 in
R1(config-line)#access-class TELNET in
R1(config-line)#exit
```

Tiếp theo, ta thực hiện gỡ bỏ Extended ACL số 100 và thay bằng một Extended Named ACL có tên là “FIREWALL”:

```
R1(config)#no access-list 100
R1(config)#ip access-list extended FIREWALL
R1(config-ext-nacl)#permit tcp 10.2.1.0 0.0.0.255 host 10.1.255.2 eq 80
R1(config-ext-nacl)#permit udp 10.3.1.0 0.0.0.255 host 10.1.255.2 eq 53
R1(config-ext-nacl)#permit icmp 10.1.1.0 0.0.0.255 host 10.1.255.2
R1(config-ext-nacl)#permit icmp 10.2.1.0 0.0.0.255 host 10.1.255.2 echo-reply
R1(config-ext-nacl)#permit icmp 10.3.1.0 0.0.0.255 host 10.1.255.2 echo-reply
R1(config-ext-nacl)#exit
R1(config)#interface e0/2
R1(config-if)#no ip access-group 100 out
R1(config-if)#ip access-group FIREWALL out
R1(config-if)#exit
```

Kiểm tra:

Ta kiểm tra lại các ACL mới được thay thế và vị trí đặt chúng:

```
R1#show access-lists
Standard IP access list TELNET
  10 permit 10.1.1.0, wildcard bits 0.0.0.255
Extended IP access list FIREWALL
  10 permit tcp 10.2.1.0 0.0.0.255 host 10.1.255.2 eq www
  20 permit udp 10.3.1.0 0.0.0.255 host 10.1.255.2 eq domain
  30 permit icmp 10.1.1.0 0.0.0.255 host 10.1.255.2
  40 permit icmp 10.2.1.0 0.0.0.255 host 10.1.255.2 echo-reply
  50 permit icmp 10.3.1.0 0.0.0.255 host 10.1.255.2 echo-reply

R1#show run | sec vty
line vty 0 4
  access-class TELNET in
  privilege level 15
  no login
  transport input telnet

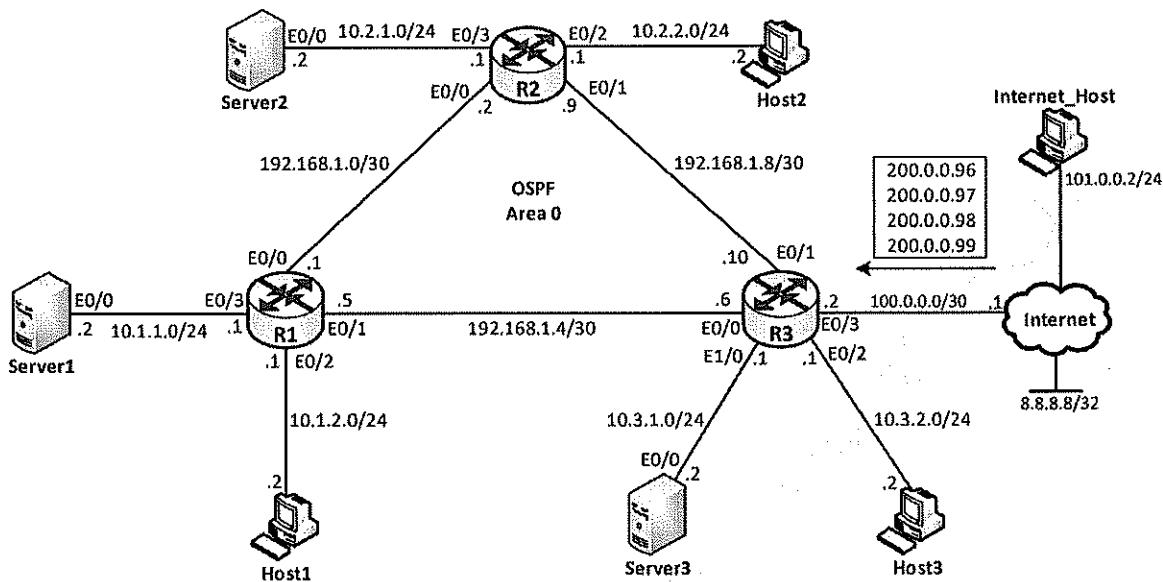
R1#show run interface e0/2
Building configuration...

Current configuration : 96 bytes
!
interface Ethernet0/2
  ip address 10.1.255.1 255.255.255.0
  ip access-group FIREWALL out
end
```

Các bạn có thể thực hiện lại các thao tác kiểm tra giống như đã thực hiện ở các bước trên để xác nhận rằng các ACL vẫn hoạt động đúng đắn.

Lab 18 – Network Address Translation (NAT)

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Bài lab gồm các thiết bị đấu nối với nhau như trên hình 1. Sơ đồ này giả lập một mạng doanh nghiệp gồm 3 chi nhánh (R1, R2, R3); mỗi chi nhánh có một mạng kết nối đến khối server ($10.x.1.0/24$) và một mạng kết nối đến khái end – user ($10.x.2.0/24$), với x là số hiệu của router. Mạng doanh nghiệp này đi Internet thông qua gateway R3, sử dụng phương thức leased – line Internet. Với gói dịch vụ Internet đang sử dụng, ngoại IP mặt ngoài ($100.0.0.2$), doanh nghiệp này còn được cấp thêm 4 IP Public gồm các IP từ $200.0.0.96$ đến $200.0.0.99$. Trên nền kịch bản này, các bạn học viên sẽ thực hành các kỹ thuật NAT cơ bản thường được sử dụng trong mạng doanh nghiệp ngày nay.
- Các thiết bị trên bài lab đều đã được cấu hình sẵn hostname và địa chỉ IP trên các cổng, các bạn học viên không phải thiết lập lại các thông số này. Ngoài ra, các bạn cũng không can thiệp vào các thiết bị Server (Server1, Server2, Server3), các thiết bị giả lập Internet và Internet_Host trong suốt quá trình thực hiện bài lab.

Yêu cầu:

1. Cấu hình định tuyến:

- Trên các router thực hiện cấu hình OSPF Area 0 đảm bảo mọi địa chỉ trong mạng nội bộ có thể đi đến nhau được.
- Trên router biên R3 thực hiện cấu hình một static default – route trả về gateway $100.0.0.1$ và sử dụng OSPF để lan truyền default – route này vào các router bên trong.

2. NAT (1):

- Cấu hình NAT một cách thích hợp trên router biên R3 đảm bảo các user thuộc các mạng LAN 2 (10.2.2.0/24) và LAN 3 (10.3.2.0/24) sử dụng IP public mặt ngoài trên cổng E0/3 của R3 để truy nhập Internet.
- Việc kiểm tra được thực hiện bằng cách ping đi 8.8.8.8 từ các host Host2 và Host3.

3. NAT (2):

- Trên router biên R3, thực hiện cấu hình NAT một cách thích hợp để hosting Server2 của R2 lên Internet.
- Các user trên Internet sẽ phải đi đến được Server2 bằng địa chỉ IP Public 200.0.0.96 trong dải IP mà ISP đã cấp phát cho doanh nghiệp.

4. NAT (3):

- Trên router biên R3, thực hiện cấu hình NAT một cách thích hợp để hosting dịch vụ web trên Server1 của R1 lên Internet.
- Các user trên Internet chỉ có thể truy nhập web đến Server1 thông qua port 80 của địa chỉ IP Public 200.0.0.97 trong dải IP mà ISP đã cấp phát cho doanh nghiệp.

5. NAT (4):

- Cấu hình NAT một cách thích hợp trên router biên R3 đảm bảo các user thuộc mạng LAN 1 (10.1.2.0/24) sử dụng IP public 200.0.0.98 trong dải IP mà ISP đã cấp phát cho doanh nghiệp để truy nhập Internet.
- Việc kiểm tra được thực hiện bằng cách ping đi 8.8.8.8 từ Host1.

6. NAT (5):

- Trên router biên R3, thực hiện cấu hình NAT một cách thích hợp để hosting dịch vụ *Telnet* trên *Server3* của R3 lên Internet. Các user trên Internet phải telnet đến Server3 thông qua port 2323 của địa chỉ public 200.0.0.99 mà ISP đã cấp phát cho doanh nghiệp.
- Trên router biên R3, thực hiện cấu hình NAT một cách thích hợp để hosting dịch vụ *web* trên *Server3* của R3 lên Internet. Các user trên Internet phải truy nhập web đến Server3 thông qua port 8080 của địa chỉ public 200.0.0.99 mà ISP đã cấp phát cho doanh nghiệp.
- Ngoài ra, trên router biên R3 cũng thực hiện NAT một cách thích hợp để hosting dịch vụ *Telnet* trên *Server1* của R1 lên Internet. Các user trên Internet phải telnet đến Server1 thông qua port 2321 của địa chỉ public 200.0.0.99 mà ISP đã cấp phát cho doanh nghiệp.

Thực hiện:**1. Cấu hình định tuyến:****Cấu hình:**

Trên R1 và R2:

```
interface range e0/0 - 3
 ip ospf 1 area 0
```

Trên R3:

```
R3(config)#interface range e0/0 - 2,e1/0
R3(config-if-range)#ip ospf 1 area 0
R3(config-if-range)#exit

R3(config)#ip route 0.0.0.0 0.0.0.0 100.0.0.1
R3(config)#router ospf 1
R3(config-router)#default-information originate
R3(config-router)#exit
```

Kiểm tra:

Các router OSPF đã thiết lập quan hệ láng giềng đầy đủ:

R1#show ip ospf neighbor					
Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.10	1	FULL/DR	00:00:34	192.168.1.6	Ethernet0/1
192.168.1.9	1	FULL/DR	00:00:34	192.168.1.2	Ethernet0/0

R2#show ip ospf neighbor					
Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.10	1	FULL/DR	00:00:31	192.168.1.10	Ethernet0/1
192.168.1.5	1	FULL/BDR	00:00:38	192.168.1.1	Ethernet0/0

R3#show ip ospf neighbor					
Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.9	1	FULL/BDR	00:00:38	192.168.1.9	Ethernet0/1
192.168.1.5	1	FULL/BDR	00:00:34	192.168.1.5	Ethernet0/0

Bảng định tuyến của các router đã có đầy đủ thông tin định tuyến, các router bên trong R1 và R2 đã có default – route phục vụ cho mục đích truy nhập Internet:

R1#show ip route ospf					
(...)					
Gateway of last resort is 192.168.1.6 to network 0.0.0.0					
O*E2	0.0.0.0/0	[110/1]	via	192.168.1.6, 00:07:14, Ethernet0/1	
	10.0.0.0/8	is variably subnetted, 8 subnets, 2 masks			
O	10.2.1.0/24	[110/20]	via	192.168.1.2, 00:02:39, Ethernet0/0	
O	10.2.2.0/24	[110/20]	via	192.168.1.2, 00:02:39, Ethernet0/0	
O	10.3.1.0/24	[110/20]	via	192.168.1.6, 00:02:17, Ethernet0/1	
O	10.3.2.0/24	[110/20]	via	192.168.1.6, 00:02:17, Ethernet0/1	
	192.168.1.0/24	is variably subnetted, 5 subnets, 2 masks			
O	192.168.1.8/30	[110/20]	via	192.168.1.6, 00:07:31, Ethernet0/1	
		[110/20]	via	192.168.1.2, 00:07:31, Ethernet0/0	
R2#show ip route ospf					
(...)					
Gateway of last resort is 192.168.1.10 to network 0.0.0.0					
O*E2	0.0.0.0/0	[110/1]	via	192.168.1.10, 00:07:16, Ethernet0/1	
	10.0.0.0/8	is variably subnetted, 8 subnets, 2 masks			
O	10.1.1.0/24	[110/20]	via	192.168.1.1, 00:02:42, Ethernet0/0	
O	10.1.2.0/24	[110/20]	via	192.168.1.1, 00:02:42, Ethernet0/0	

```
O      10.3.1.0/24 [110/20] via 192.168.1.10, 00:02:19, Ethernet0/1
O      10.3.2.0/24 [110/20] via 192.168.1.10, 00:02:19, Ethernet0/1
    192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O      192.168.1.4/30 [110/20] via 192.168.1.10, 00:07:33, Ethernet0/1
                  [110/20] via 192.168.1.1, 00:07:33, Ethernet0/0
R3#show ip route ospf
(...)
Gateway of last resort is 100.0.0.1 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O      10.1.1.0/24 [110/20] via 192.168.1.5, 00:02:42, Ethernet0/0
O      10.1.2.0/24 [110/20] via 192.168.1.5, 00:02:42, Ethernet0/0
O      10.2.1.0/24 [110/20] via 192.168.1.9, 00:02:42, Ethernet0/1
O      10.2.2.0/24 [110/20] via 192.168.1.9, 00:02:42, Ethernet0/1
    192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O      192.168.1.0/30 [110/20] via 192.168.1.9, 00:07:43, Ethernet0/1
                  [110/20] via 192.168.1.5, 00:07:43, Ethernet0/0
```

Ta có thể kiểm tra rằng các host đã có thể đi đến các server và có thể đi đến nhau một cách đầy đủ:

```
Host1> ping 10.1.1.2 <- Host1 ping thành công Server1
84 bytes from 10.1.1.2 icmp_seq=1 ttl=254 time=1.745 ms
84 bytes from 10.1.1.2 icmp_seq=2 ttl=254 time=1.039 ms

Host1> ping 10.2.1.2 <- Host1 ping thành công Server2
84 bytes from 10.2.1.2 icmp_seq=1 ttl=253 time=4.225 ms
84 bytes from 10.2.1.2 icmp_seq=2 ttl=253 time=2.630 ms

Host1> ping 10.3.1.2 <- Host1 ping thành công Server3
84 bytes from 10.3.1.2 icmp_seq=1 ttl=253 time=7.266 ms
84 bytes from 10.3.1.2 icmp_seq=2 ttl=253 time=2.964 ms

Host1> ping 10.2.2.2 <- Host1 ping thành công Host2
84 bytes from 10.2.2.2 icmp_seq=1 ttl=62 time=4.042 ms
84 bytes from 10.2.2.2 icmp_seq=2 ttl=62 time=2.245 ms

Host1> ping 10.3.2.2 <- Host1 ping thành công Host3
84 bytes from 10.3.2.2 icmp_seq=1 ttl=62 time=5.031 ms
84 bytes from 10.3.2.2 icmp_seq=2 ttl=62 time=2.561 ms

Host2> ping 10.2.1.2 <- Host2 ping thành công Server2
84 bytes from 10.2.1.2 icmp_seq=1 ttl=254 time=1.886 ms
84 bytes from 10.2.1.2 icmp_seq=2 ttl=254 time=2.090 ms

Host2> ping 10.3.1.2 <- Host2 ping thành công Server3
84 bytes from 10.3.1.2 icmp_seq=1 ttl=253 time=1.581 ms
84 bytes from 10.3.1.2 icmp_seq=2 ttl=253 time=2.867 ms

Host2> ping 10.3.2.2 <- Host2 ping thành công Host3
84 bytes from 10.3.2.2 icmp_seq=1 ttl=62 time=2.009 ms
84 bytes from 10.3.2.2 icmp_seq=2 ttl=62 time=2.517 ms

Host3> ping 10.3.1.2 <- Host3 ping thành công Server3
84 bytes from 10.3.1.2 icmp_seq=1 ttl=254 time=1.366 ms
84 bytes from 10.3.1.2 icmp_seq=2 ttl=254 time=0.781 ms
```

2. NAT (1):

Cấu hình:

Ta thực hiện cấu hình NAT overload trên R3 để NAT các địa chỉ thuộc hai subnet 10.2.2.0/24 và 10.3.2.0/24 thành IP mặt ngoài của router R3 khi các user thuộc hai subnet này truy nhập Internet:

```
R3(config)#ip access-list standard LAN2_LAN3
R3(config-std-nacl)#permit 10.2.2.0 0.0.0.255
R3(config-std-nacl)#permit 10.3.2.0 0.0.0.255
R3(config-std-nacl)#exit

R3(config)#ip nat inside source list LAN2_LAN3 interface e0/3 overload
R3(config)#interface range e0/0 - 2,e1/0
R3(config-if-range)#ip nat inside
R3(config-if-range)#exit

R3(config)#interface e0/3
R3(config-if)#ip nat outside
R3(config-if)#exit
```

Kiểm tra:

Ta kiểm tra xác nhận rằng, lúc này các user thuộc hai mạng LAN 2(10.2.2.0/24) và LAN 3(10.3.2.0/24) đều đã truy nhập được Internet:

```
Host2> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=3.773 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=1.458 ms

Host3> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=2.193 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=1.364 ms
```

Hoạt động truy nhập Internet của các user này được thực hiện thông qua NAT địa chỉ thành IP mặt ngoài của router biên R3:

R3#show ip nat translations				
Protocol	Inside global	Inside local	Outside local	Outside global
icmp	100.0.0.2:58504	10.2.2.2:58504	8.8.8.8:58504	8.8.8.8:58504
icmp	100.0.0.2:58760	10.2.2.2:58760	8.8.8.8:58760	8.8.8.8:58760
icmp	100.0.0.2:60040	10.3.2.2:60040	8.8.8.8:60040	8.8.8.8:60040
icmp	100.0.0.2:60296	10.3.2.2:60296	8.8.8.8:60296	8.8.8.8:60296

Như vậy, hoạt động NAT phục vụ việc truy nhập Internet của các user trên LAN 2 và LAN 3 đã diễn ra đúng theo yêu cầu đặt ra.

3. NAT (2):

Cấu hình:

Ta cấu hình NAT tĩnh trên router R3 thực hiện NAT địa chỉ định địa chỉ của Server2 10.2.1.2 thành IP Public 200.0.0.96 để đáp ứng yêu cầu đặt ra:

```
R3(config)#ip nat inside source static 10.2.1.2 200.0.0.96
```

Kiểm tra:

Ta kiểm tra bảng NAT của router biên R3 để xác nhận rằng một entry NAT tĩnh cho cặp địa chỉ 10.2.1.2 – 200.0.0.96 đã được lưu cố định vào bảng NAT:

R3#show ip nat translations			
Pro	Inside global	Inside local	Outside local
---	200.0.0.96	10.2.1.2	---

Các user trên Internet hiện đã có thể truy nhập đến Server2 của mạng doanh nghiệp thông qua địa chỉ public 200.0.0.96. Ta kiểm tra điều này từ thiết bị Internet_Host:

```
Internet_Host#ping 200.0.0.96 <- Ping được đến Server2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.0.0.96, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
Internet_Host#telnet 200.0.0.96 <- Telnet được đến Server2
Trying 200.0.0.96 ... Open
```

User Access Verification

Password:
Server2>

Bảng NAT của R3 khi Internet_Host truy nhập đến Server2:

R3#show ip nat translations			
Pro	Inside global	Inside local	Outside local
icmp	200.0.0.96:1	10.2.1.2:1	101.0.0.2:1
tcp	200.0.0.96:23	10.2.1.2:23	101.0.0.2:45345
---	200.0.0.96	10.2.1.2	---

Các entry NAT phát sinh thêm cho thấy các hoạt động truy nhập Server2 bằng Ping và Telnet đã thực hiện được thành công là nhờ NAT trên R3. Ta đã public thành công Server2 lên Internet bằng NAT tĩnh.

4. NAT (3):**Cấu hình:**

Ta thực hiện NAT tĩnh TCP port 80 của Server1 thành port 80 của địa chỉ IP public 200.0.0.97 để đáp ứng yêu cầu đặt ra:

```
R3(config)#ip nat inside source static tcp 10.1.1.2 80 200.0.0.97 80
```

Kiểm tra:

Ta kiểm tra bảng NAT của router R3 để xác nhận rằng entry NAT tĩnh này đã được cập nhật:

R3#show ip nat translations			
Pro	Inside global	Inside local	Outside local
tcp	200.0.0.97:80	10.1.1.2:80	---
---	200.0.0.96	10.2.1.2	---

Từ Internet_Host, ta thực hiện truy nhập web vào Server1 thông qua port 80 của địa chỉ public 200.0.0.97 để kiểm chứng hoạt động NAT vừa cấu hình:

```
Internet_Host>telnet 200.0.0.97 80
Trying 200.0.0.97...80 ... Open
exit
HTTP/1.1 400 Bad Request
Date: Mon, 10 Aug 2020 03:20:00 GMT
Server: cisco-IOS
Accept-Ranges: none
400 Bad Request
[Connection to 200.0.0.97 closed by foreign host]
```

} HTTP Response từ Server1, code: 400

Internet_Host nhận được hồi đáp HTTP từ Server1, điều này cho thấy hoạt động NAT đã diễn ra thành công.

5. NAT (4):

Cấu hình:

Để đáp ứng yêu cầu này, chúng ta thực hiện NAT overload toàn bộ các IP thuộc dải 10.1.2.0/24 (LAN 1) thành địa chỉ IP Public 200.0.0.98 được cấp phát bởi ISP. Địa chỉ 200.0.0.98 không phải là IP mặt ngoài nên chúng ta sẽ tạo một pool riêng cho địa chỉ này để thực hiện NAT.

Trên R3:

```
R3(config)#ip access-list standard LAN1
R3(config-std-nacl)#permit 10.1.2.0 0.0.0.255
R3(config-std-nacl)#exit
R3(config)#ip nat pool IP_200_0_0_98 200.0.0.98 200.0.0.98 prefix-length 24
R3(config)#ip nat inside source list LAN1 pool IP_200_0_0_98 overload
```

Kiểm tra:

Ta thực hiện ping kiểm tra đến địa chỉ 8.8.8.8 trên Internet từ Host1:

```
Host1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=3.514 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=2.650 ms
```

Bảng NAT trên router R3 cho thấy địa chỉ của Host1 lúc này đã được NAT thành IP public 200.0.0.98:

R3#show ip nat translations				
Protocol	Inside global	Inside local	Outside local	Outside global
tcp	200.0.0.97:80	10.1.1.2:80	---	---
icmp	200.0.0.98:54207	10.1.2.2:54207	8.8.8.8:54207	8.8.8.8:54207
icmp	200.0.0.98:54463	10.1.2.2:54463	8.8.8.8:54463	8.8.8.8:54463
---	200.0.0.96	10.2.1.2	---	---

Như vậy hoạt động NAT cho LAN1 để đi Internet đã diễn ra đúng theo yêu cầu đặt ra.

6. NAT (5):

Cấu hình:

Ta thực hiện lần lượt các yêu cầu đặt ra của câu 6.

Đầu tiên, thực hiện hosting dịch vụ Telnet của Server3 lên Internet thông qua port 2323 của địa chỉ IP public 200.0.0.99:

```
R3(config)#ip nat inside source static tcp 10.3.1.2 23 200.0.0.99 2323
```

Tiếp theo, ta thực hiện hosting dịch vụ Web của Server3 lên Internet thông qua port 8080 của địa chỉ IP public 200.0.0.99:

```
R3(config)#ip nat inside source static tcp 10.3.1.2 80 200.0.0.99 8080
```

Cuối cùng, ta tiến hành hosting dịch vụ Telnet của Server1 lên Internet thông qua port 2321 của địa chỉ IP public 200.0.0.99:

```
R3(config)#ip nat inside source static tcp 10.1.1.2 23 200.0.0.99 2321
```

Kiểm tra:

Ta kiểm tra router R3 để xác nhận rằng các entry NAT tĩnh ở trên đã được cập nhật vào bảng NAT của nó:

```
R3#show ip nat translations
Pro Inside global      Inside local        Outside local       Outside global
tcp 200.0.0.99:2321    10.1.1.2:23          ---                ---
tcp 200.0.0.97:80      10.1.1.2:80          ---                ---
--- 200.0.0.96          10.2.1.2            ---                ---
tcp 200.0.0.99:2323    10.3.1.2:23          ---                ---
tcp 200.0.0.99:8080    10.3.1.2:80          ---                ---
```

Ta thực hiện truy nhập các dịch vụ trên từ Internet_Host để kiểm tra rằng các entry này đều hoạt động.

Từ Internet_Host telnet đến 200.0.0.99, port 2321:

```
Internet_Host>telnet 200.0.0.99 2321
Trying 200.0.0.99, 2321 ... Open
```

User Access Verification

Password:
Server1> <- Telnet đến Server1

Từ Internet_Host telnet đến 200.0.0.99, port 2323:

```
Internet_Host>telnet 200.0.0.99 2323
Trying 200.0.0.99, 2323 ... Open
```

User Access Verification

Password:
Server3> <- Telnet đến Server3

Cuối cùng, ta kiểm tra rằng, có thể truy nhập web đến Server3 thông qua port 8080 của địa chỉ 200.0.0.99:

```
Internet_Host>telnet 200.0.0.99 8080
Trying 200.0.0.99, 8080 ... Open
exit
HTTP/1.1 400 Bad Request
Date: Mon, 10 Aug 2020 04:04:12 GMT
Server: cisco-IOS
Accept-Ranges: none
400 Bad Request
[Connection to 200.0.0.99 closed by foreign host]
```

} HTTP Response từ Server3, code: 400

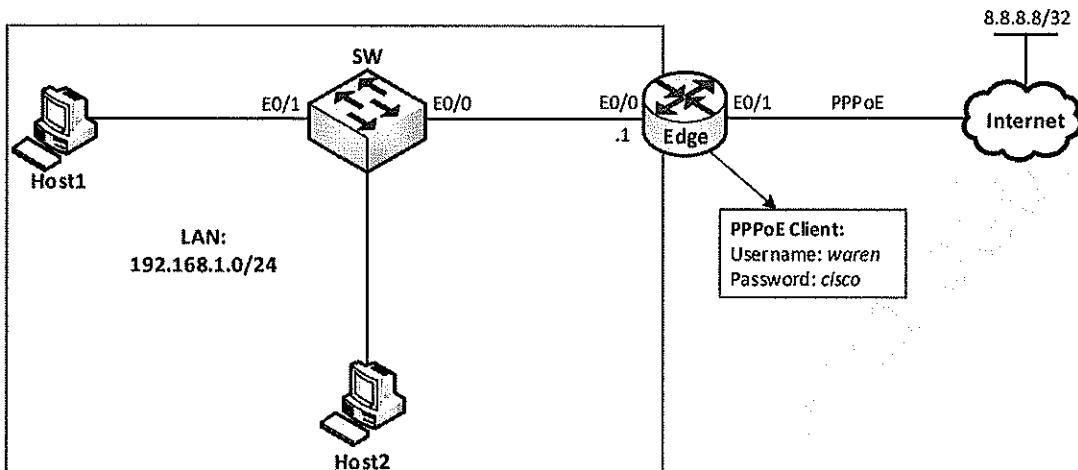
Bảng NAT của router R3 thể hiện rằng các hoạt động NAT đã diễn ra cho các thao tác truy nhập ở trên:

```
R3#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 200.0.0.99:2321    10.1.1.2:23       101.0.0.2:64913    101.0.0.2:64913
tcp 200.0.0.99:2321    10.1.1.2:23       ---             ---
tcp 200.0.0.97:80      10.1.1.2:80       ---             ---
--- 200.0.0.96          10.2.1.2         ---             ---
tcp 200.0.0.99:2323    10.3.1.2:23       101.0.0.2:30660    101.0.0.2:30660
tcp 200.0.0.99:2323    10.3.1.2:23       ---             ---
tcp 200.0.0.99:8080    10.3.1.2:80       101.0.0.2:56713    101.0.0.2:56713
tcp 200.0.0.99:8080    10.3.1.2:80       ---             ---
```

Đến đây, chúng ta đã hoàn thành yêu cầu cuối cùng của bài lab về kỹ thuật NAT.

Lab 19 – PPPoE

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Bài lab gồm các thiết bị được kết nối với nhau như trên sơ đồ hình 1. Trong đó: các router và switch sử dụng hệ điều hành IOL, các host là các VPC được tích hợp sẵn trên EVE.
- Trong bài lab này, chúng ta sẽ thực hiện cấu hình router Cisco đảm nhận chức năng PPPoE client thường gặp trong các FTTH router truy nhập Internet hiện nay.
- Các thiết bị trên bài lab đều đã được cấu hình hostname, các bạn học viên không cần phải thiết lập lại thông số này. Ngoài ra, switch SW và thiết bị giả lập Internet đã được cấu hình đầy đủ, các bạn không can thiệp vào các thiết bị này trong suốt quá trình thực hiện bài lab.

Yêu cầu:

1. Cấu hình trên LAN:

- Cấu hình router Edge đảm nhận vai trò DHCP server cấp phát IP cho các host thuộc mạng LAN 192.168.1.0/24.
- Việc cấp phát IP cần loại ra địa chỉ IP tĩnh 192.168.1.1 đã sử dụng trên cổng E0/0 của router Edge.

2. PPPoE client:

- Cấu hình router Edge đảm nhận vai trò PPPoE client mở đường link đi Internet. Tài khoản Internet của router Edge có username là "waren" và password là "cisco".
- Sau khi thông suốt link PPPoE, thực hiện cấu hình trên router Edge đảm bảo các host trong mạng LAN truy nhập được Internet.
- Việc truy nhập Internet được kiểm tra bằng cách ping đi 8.8.8.8 từ các host trong mạng LAN.

Thực hiện:**1. Cấu hình trên LAN:****Cấu hình:**

Ta thực hiện đặt địa chỉ IP và cấu hình DHCP server trên router Edge:

```
Edge(config)#interface e0/0
Edge(config-if)#no shutdown
Edge(config-if)#ip address 192.168.1.1 255.255.255.0
Edge(config-if)#exit
Edge(config)#ip dhcp excluded-address 192.168.1.1
Edge(config)#ip dhcp pool LAN
Edge(dhcp-config)#network 192.168.1.0 /24
Edge(dhcp-config)#default-router 192.168.1.1
Edge(dhcp-config)#exit
```

Kiểm tra:

Ta kiểm tra rằng các host đều đã có thể nhận được cấu hình IP từ DHCP:

```
Host1> dhcp -r
DDORA IP 192.168.1.2/24 GW 192.168.1.1

Host2> dhcp -r
DDORA IP 192.168.1.3/24 GW 192.168.1.1
```

Bảng DHCP binding của router Edge:

Edge#show ip dhcp binding			
Bindings from all pools not associated with VRF:			
IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
192.168.1.2	0100.5079.6668.03	Jul 27 2021 06:18 PM	Automatic
192.168.1.3	0100.5079.6668.05	Jul 27 2021 06:18 PM	Automatic

2. PPPoE client:**Cấu hình:**

Trước hết, chúng ta cấu hình router Edge đảm nhận vai trò PPPoE Client kết nối đến ISP để thông suốt đường link PPPoE đi Internet:

```
Edge(config)#interface e0/1
Edge(config-if)#no shutdown
Edge(config-if)#pppoe enable
Edge(config-if)#pppoe-client dial-pool-number 1
Edge(config-if)#exit
Edge(config)#interface dialer 0
Edge(config-if)#dialer pool 1
Edge(config-if)#encapsulation ppp
Edge(config-if)#ppp pap sent-username waren password cisco
Edge(config-if)#ip address negotiated
```

```
Edge(config-if)#ip mtu 1492
Edge(config-if)#ip tcp adjust-mss 1452
Edge(config-if)#exit
```

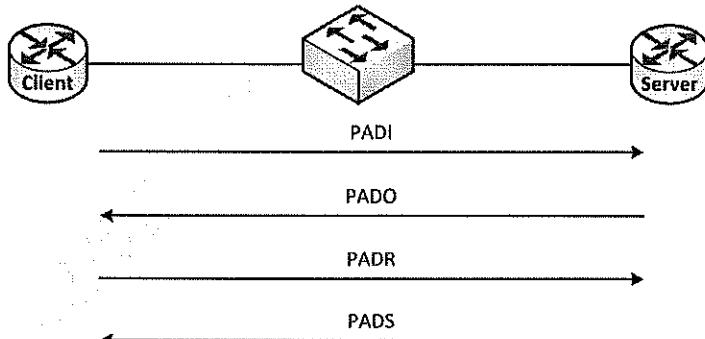
Tiếp theo, sau khi thông suốt link PPPoE, chúng ta cấu hình default – routing và NAT trên router Edge để các host bên trong LAN có thể truy nhập được Internet:

```
Edge(config)#ip route 0.0.0.0 0.0.0.0 dialer 0
Edge(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Edge(config)#ip nat inside source list 1 interface dialer 0 overload
Edge(config)#interface e0/0
Edge(config-if)#ip nat inside
Edge(config-if)#exit
Edge(config)#interface dialer 0
Edge(config-if)#ip nat outside
Edge(config-if)#exit
```

Ghi chú:

PPPoE – PPP over Ethernet là kỹ thuật cho phép truyền frame PPP qua môi trường Ethernet. Điều này cho phép triển khai các đường link point – to – point qua một môi trường multi access, từ đó có thể áp dụng trên data link các phương pháp xác thực mà các kỹ thuật multi access không hỗ trợ, cũng như tận dụng được những đặc điểm của data link point – to – point dù đang sử dụng môi trường truyền tải multi access. PPPoE được sử dụng rộng rãi trong các kỹ thuật truy nhập Internet băng rộng như ADSL hay FTTH,...

PPPoE sử dụng mô hình client – server. Hoạt động thiết lập một session PPPoE được mô tả trong hình 2:



Hình 2 – Trao đổi thiết lập PPPoE session.

Tóm lược các bước như sau:

- Khi một PPPoE client muốn thiết lập kết nối PPPoE, nó gửi broadcast gói tin *PADI* (*PPPoE Active Discovery Initiation*) vào môi trường multi – access.
- Nếu trên môi trường multi access này tồn tại một PPPoE server, server sẽ hồi đáp một gói tin *PADO* (*PPPoE Active Discovery Offer*) đến địa chỉ MAC của client đã khởi tạo session.
- Nếu client chấp nhận gói tin offer trả về này, nó sẽ gửi đi gói tin *PADR* (*PPPoE Active Discovery Request*) đến server để yêu cầu dịch vụ PPP.
- Nếu server đồng ý với request nhận được, nó sẽ hồi đáp lại cho client gói tin *PADS* (*PPPoE Active Discovery Session confirmation*), client và server có thể bắt đầu trao đổi các gói PPP bên trong các Ethernet frame để thực hiện thương lượng các thông số và thiết lập kết nối PPP.

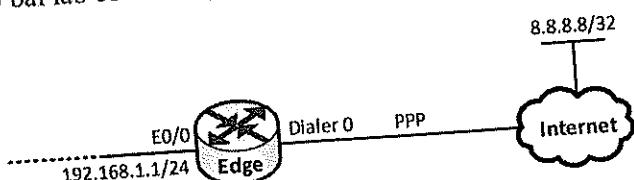
Việc cấu hình PPPoE client trên router khá rõ ràng; chúng ta tạo ra một interface luân lý dialer, cấu hình các thông số PPP trên interface này rồi áp nó vào một cổng Ethernet bằng cách sử dụng một thông số có tên là “dialer pool”; cổng Ethernet này, lúc đó, sẽ được sử dụng để truyền tải các PPP frame do interface dialer tạo ra. Trong bài lab của chúng ta, cổng dialer được đặt số hiệu là 0, và cổng Ethernet dùng để truyền tải PPP là cổng E0/1:

```
Edge(config)#interface e0/1
Edge(config-if)#no shutdown
Edge(config-if)#pppoe enable
Edge(config-if)#pppoe-client dial-pool-number 1
Edge(config-if)#exit
Edge(config)#interface dialer 0
Edge(config-if)#dialer pool 1
Edge(config-if)#encapsulation ppp
Edge(config-if)#ppp pap sent-username waren password cisco
```

Hai giá trị dial pool phải match nhau

Thông thường, PPPoE server trên các ISP thực hiện xác thực người dùng bằng phương pháp xác thực PAP của PPP, do đó trên các PPPoE client router, chúng ta cấu hình router gửi username và password xác thực đến ISP để có thể active được đường link PPP (trên Ethernet). Đây chính là username và password của tài khoản Internet mà người dùng nhận được khi đăng ký thuê bao. Trong bài lab của chúng ta, tài khoản giả lập có username là “waren” và password là “cisco”.

Nếu các thao tác thiết lập link PPPoE ở trên được tiến hành đúng, một đường link PPPoE sẽ được mở đến ISP. Về mặt luân lý, router Edge của khách hàng đang sử dụng một cổng PPP (dialer 0) để nối đến ISP, cổng outside thực sự là cổng Dialer 0, cổng Ethernet chỉ đóng vai trò một phương tiện truyền tải lớp dưới mà thôi. Đường Internet trong sơ đồ bài lab có thể được thể hiện lại như sau:



Hình 3 – Đường đi Internet với interface dialer 0.

Trên cổng PPP Dialer 0, để có được địa chỉ IP, router Edge có thể xin cấp phát IP động từ ISP, tuy nhiên, hoạt động cấp phát IP động trên link PPP không dựa vào giao thức DHCP như trong Ethernet LAN mà sử dụng giao thức IPCP chuyên dụng của PPP. Để xin cấp phát IP bằng IPCP từ ISP, chúng ta cấu hình lệnh “ip address negotiated” trên cổng Dialer 0 của router:

```
Edge(config-if)#ip address negotiated
```

Một điểm cần lưu ý là vì PPP chạy trên Ethernet nên dẫn đến này sinh vấn đề về MTU. Giá trị MTU mặc định của giao thức Ethernet là 1500 byte và chúng ta có thêm 8 byte header PPP được đóng gói vào bên trong Ethernet frame, do đó giá trị IP MTU của PPPoE chỉ còn lại $1500 - 8 = 1492$ byte. Do đó, chúng ta cần cấu hình lại giá trị IP MTU trên cổng Dialer 0 thành 1492:

```
Edge(config-if)#ip mtu 1492
```

Với giá trị IP MTU là 1492 byte, giá trị TCP MSS của các TCP session đi ngang qua cổng Dialer 0 cần phải được hiệu chỉnh về 1452 (= 1492 – 20 byte IP header – 20 byte TCP header). Để điều này được thực hiện, chúng ta cấu hình câu lệnh sau trên cổng Dialer:

```
Edge(config-if)#ip tcp adjust-mss 1452
```

Khi lệnh này được thực thi, router sẽ hiệu chỉnh tất cả giá trị MSS của các gói TCP đi ngang qua cổng Dialer (cả đi vào và đi ra khỏi cổng) thành 1452 khi giá trị này lớn hơn 1452.

Với các hiệu chỉnh về MTU và MSS đã thực hiện ở trên, các session TCP đi ngang qua router Edge sẽ tránh được hiện tượng phân mảnh gói tin IP từ đó đảm bảo việc truy nhập đến các tài nguyên mạng trên Internet không xảy ra lỗi.

Cuối cùng, các thao tác về default – routing và NAT được tiến hành trên router biên giống như trong các bài lab trước mà chúng ta đã thực hiện. Chỉ có một điểm khác biệt cần lưu ý là cổng outside nối đi Internet của router biên lúc này là cổng Dialer 0 chứ không phải cổng E0/1 – cổng E0/1 lúc này chỉ còn đóng vai trò một phương tiện truyền tải mà thôi.

Kiểm tra:

Trước hết, chúng ta kiểm tra rằng session PPPoE đã được thiết lập thành công giữa router Edge và gateway Internet của ISP:

```
Edge#show pppoe session
 1 client session

Uniq ID  PPPoE  RemMAC          Port          VT  VA      State
          SID   LocMAC
          N/A    1   aabb.cc00.2000  Et0/1        VA-st  Type
                                         aabb.cc00.1010          Di0  Vi2      UP
```

Router Edge đã nhận được địa chỉ IP cấp phát từ ISP:

```
Edge#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
Ethernet0/0        192.168.1.1    YES  NVRAM  up           up
Ethernet0/1        unassigned     YES  NVRAM  up           up
Ethernet0/2        unassigned     YES  NVRAM  administratively down  down
Ethernet0/3        unassigned     YES  NVRAM  administratively down  down
Dialer0            100.0.0.2       YES  IPCP   up           up
NVI0               192.168.1.1    YES  unset   up           up
Virtual-Access1    unassigned     YES  unset   up           up
Virtual-Access2    unassigned     YES  unset   up           up
```

Default – route trên router Edge:

```
Edge#show ip route static
(...)
S* 0.0.0.0/0 is directly connected, Dialer0
```

NAT overload đã được cấu hình đầy đủ trên router Edge:

```
Edge#show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 4, occurred 00:03:06 ago
Outside interfaces:
  Dialer0, Virtual-Access2
Inside interfaces:
  Ethernet0/0
Hits: 8 Misses: 0
CEF Translated packets: 8, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface Dialer0 refcount 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0

Edge#show access-list 1
Standard IP access list 1
  10 permit 192.168.1.0, wildcard bits 0.0.0.255
```

Các host đã có thể truy nhập được Internet:

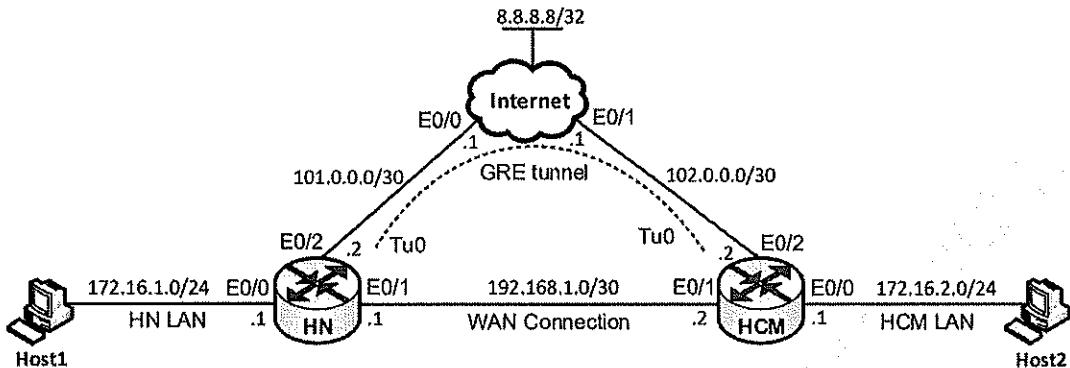
```
Host1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=1.269 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=1.989 ms

Host2> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=3.907 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=3.442 ms
```

Đến đây, chúng ta đã hoàn thành các yêu cầu đặt ra của bài lab.

Lab 20 – GRE VPN

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Bài lab gồm các thiết bị được kết nối với nhau theo sơ đồ hình 1. Trong đó: các router chạy hệ điều hành IOL và các host là các VPC được tích hợp sẵn trên EVE.
- Bài lab giả lập một mạng doanh nghiệp có hai chi nhánh tại Hà Nội (router HN) và TPHCM (router HCM). Hai chi nhánh này được đấu nối với nhau bởi một đường truyền WAN (kết nối hai cổng E0/1 của hai router) và cả hai chi nhánh đều có đường truyền Internet với IP mặt ngoài cố định (tại HN là 101.0.0.2 và tại HCM là 102.0.0.2). Để dự phòng cho đường truyền WAN, người quản trị thực hiện thiết lập thêm một đường GRE VPN giữa hai chi nhánh này thông qua Internet.
- Trong bài lab này, các bạn học viên được yêu cầu cấu hình thiết lập đường VPN theo như mô tả ở trên, thực hiện cấu hình định tuyến OSPF Area 0 để đường VPN này đóng vai trò dự phòng cho đường truyền WAN giữa hai chi nhánh.
- Bên cạnh đó, các bạn học viên cũng phải cấu hình cung cấp các dịch vụ DHCP và Internet cho các user trong mạng doanh nghiệp ở trên.
- Các thiết bị trên sơ đồ đều đã được cấu hình hostname, các bạn học viên không cần phải thiết lập lại thông số này. Ngoài ra, các bạn cũng không can thiệp vào thiết bị giả lập Internet trong suốt quá trình thực hiện bài lab.

Yêu cầu:

1. Cấu hình cơ bản:

- Các bạn học viên thực hiện cấu hình địa chỉ IP trên các cổng của các router như được chỉ ra trên sơ đồ hình 1.
- Sau khi cấu hình xong, các bạn thực hiện ping kiểm tra để xác nhận rằng đường truyền WAN đã thông suốt giữa hai router.

2. Cấu hình định tuyến:

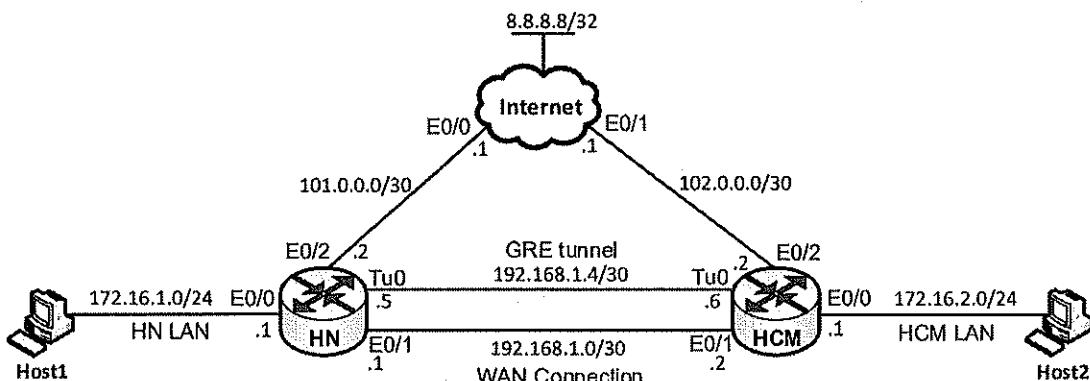
Thực hiện cấu hình OSPF Area 0 đảm bảo hai mạng LAN của hai chi nhánh HN và HCM có thể đi đến nhau được.

3. Các dịch vụ DHCP và Internet:

- Cấu hình để các router HN và HCM cấp phát IP cho các host thuộc mạng LAN của mình.
- Cấu hình để các router HN và HCM cung cấp dịch vụ truy nhập Internet cho các host trên các mạng LAN của mình đồng thời phải đóng vai trò dự phòng Internet cho chi nhánh còn lại.

4. GRE VPN:

- Trên hai router, thực hiện cấu hình một đường GRE VPN xuyên qua Internet, sử dụng IP thiết lập tunnel là các địa chỉ IP mặt ngoài của hai router.
- Sau khi cấu hình xong VPN, thực hiện đặt địa chỉ IP nội bộ cho đường tunnel như được chỉ ra trên sơ đồ hình 2:



Hình 2 – Sơ đồ mạng với dự phòng VPN.

- Cấu hình để đường VPN mới tạo tham gia OSPF Area 0. Kiểm tra xác nhận rằng hai chi nhánh đi đến nhau qua đường WAN là chính, đường VPN chỉ để dự phòng.

Thực hiện:

1. Cấu hình cơ bản:

Cấu hình:

```

HN(config)#interface e0/0
HN(config-if)#no shutdown
HN(config-if)#ip address 172.16.1.1 255.255.255.0
HN(config-if)#exit
HN(config)#interface e0/1
HN(config-if)#no shutdown
HN(config-if)#ip address 192.168.1.1 255.255.255.252
HN(config-if)#exit

```

```
HCM(config)#interface e0/0
HCM(config-if)#no shutdown
HCM(config-if)#ip address 172.16.2.1 255.255.255.0
HCM(config-if)#exit
HCM(config)#interface e0/1
HCM(config-if)#no shutdown
HCM(config-if)#ip address 192.168.1.2 255.255.255.252
HCM(config-if)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng hai chi nhánh HN và HCM đã thông suốt đường truyền WAN:

```
HN#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 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

2. Cấu hình định tuyến:**Cấu hình:**

```
HN(config)#router ospf 1
HN(config-router)#network 172.16.1.1 0.0.0.0 area 0
HN(config-router)#network 192.168.1.1 0.0.0.0 area 0
HN(config-router)#exit

HCM(config)#router ospf 1
HCM(config-router)#network 172.16.2.1 0.0.0.0 area 0
HCM(config-router)#network 192.168.1.2 0.0.0.0 area 0
HCM(config-router)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng hai router HN và HCM đã chạy định tuyến được với nhau thông qua WAN link.

Trên HN:

```
HN#show ip ospf neighbor
Neighbor ID      Pri   State          Dead Time    Address          Interface
192.168.1.2      1     FULL/DR       00:00:34     192.168.1.2    Ethernet0/1

HN#show ip route ospf
(...)
  172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O      172.16.2.0/24 [110/20] via 192.168.1.2, 00:01:19, Ethernet0/1
```

Trên HCM:

```
HCM#show ip ospf neighbor
Neighbor ID      Pri   State          Dead Time    Address          Interface
192.168.1.1      1     FULL/BDR      00:00:31     192.168.1.1    Ethernet0/1
```

```
HCM#show ip route ospf
(...)
    172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O        172.16.1.0/24 [110/20] via 192.168.1.1, 00:01:25, Ethernet0/1
```

Hai mạng LAN của hai chi nhánh đã có thể đi đến nhau được:

```
HN#ping 172.16.2.1 source 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

3. Các dịch vụ DHCP và Internet:

Cấu hình:

Ta cấu hình các router HN và HCM cấp phát IP bằng DHCP cho các host thuộc các mạng LAN của mình:

```
HN(config)#ip dhcp excluded-address 172.16.1.1
HN(config)#ip dhcp pool HN_LAN
HN(dhcp-config)#network 172.16.1.0 /24
HN(dhcp-config)#default-router 172.16.1.1
HN(dhcp-config)#exit

HCM(config)#ip dhcp excluded-address 172.16.2.1
HCM(config)#ip dhcp pool HCM_LAN
HCM(dhcp-config)#network 172.16.2.0 /24
HCM(dhcp-config)#default-router 172.16.2.1
HCM(dhcp-config)#exit
```

Cấu hình dịch vụ Internet trên router HN:

```
HN(config)#ip sla 1
HN(config-ip-sla)#icmp-echo 101.0.0.1 source-ip 101.0.0.2
HN(config-ip-sla-echo)#frequency 5
HN(config-ip-sla-echo)#exit
HN(config)#ip sla schedule 1 start-time now life forever

HN(config)#track 1 ip sla 1
HN(config-track)#exit

HN(config)#ip route 0.0.0.0 0.0.0.0 101.0.0.1 track 1
HN(config)#router ospf 1
HN(config-router)#default-information originate
HN(config-router)#exit

HN(config)#access-list 1 permit 172.16.1.0 0.0.0.255
HN(config)#access-list 1 permit 172.16.2.0 0.0.0.255
HN(config)#ip nat inside source list 1 interface e0/2 overload
```

```
HN(config)#interface range e0/0 - 1
HN(config-if-range)#ip nat inside
HN(config-if-range)#exit
HN(config)#interface e0/2
HN(config-if)#ip nat outside
HN(config-if)#exit
```

Cấu hình dịch vụ Internet trên router HCM:

```
HCM(config)#interface e0/2
HCM(config-if)#no shutdown
HCM(config-if)#ip address 102.0.0.2 255.255.255.0
HCM(config-if)#exit

HN(config)#ip sla 1
HN(config-ip-sla)#icmp-echo 102.0.0.1 source-ip 102.0.0.2
HN(config-ip-sla-echo)#frequency 5
HN(config-ip-sla-echo)#exit
HN(config)#ip sla schedule 1 start-time now life forever

HCM(config)#track 1 ip sla 1
HCM(config-track)#exit

HCM(config)#ip route 0.0.0.0 0.0.0.0 102.0.0.1 track 1
HCM(config)#router ospf 1
HCM(config-router)#default-information originate
HCM(config-router)#exit

HCM(config)#access-list 1 permit 172.16.1.0 0.0.0.255
HCM(config)#access-list 1 permit 172.16.2.0 0.0.0.255
HCM(config)#ip nat inside source list 1 interface e0/2 overload
HCM(config)#interface range e0/0 - 1
HCM(config-if-range)#ip nat inside
HCM(config-if-range)#exit
HCM(config)#interface e0/2
HCM(config-if)#ip nat outside
HCM(config-if)#exit
```

Ghi chú:

Với dịch vụ Internet, tại mỗi router, chúng ta thực hiện cấu hình static default – route cho hoạt động truy nhập Internet đồng thời lan truyền default – route này đến router kia bằng OSPF. Tại mỗi router, default – route cấu hình trên chính bản thân router sẽ được ưu tiên hơn default – route nhận được từ router kia vì AD của static route bằng 1, trong khi AD của OSPF route bằng 110, và vì thế default – route học bởi OSPF chỉ được sử dụng để dự phòng khi default – route của chính router này bị down.

Bên cạnh đó, với static default – route trên mỗi router, chúng ta cần cấu hình thêm hoạt động track với IP SLA để khi xảy ra sự cố với đường truyền Internet, static default – route sẽ được gỡ bỏ và default – route OSPF sẽ được đưa vào sử dụng thay thế.

Ngoài ra, access – list trong hoạt động NAT của mỗi router cần phải permit địa chỉ IP trên cả hai mạng LAN vì mỗi router không chỉ đảm nhận nhiệm vụ hỗ trợ mạng LAN của mình truy nhập Internet mà còn phải hỗ trợ mạng LAN của router còn lại truy nhập Internet khi bến đó xảy ra sự cố gián đoạn Internet.

Kiểm tra:

Các host thuộc các mạng LAN đều đã nhận được IP từ DHCP:

```
Host1> dhcp -r
DDORA IP 172.16.1.2/24 GW 172.16.1.1

Host2> dhcp -r
DDORA IP 172.16.2.2/24 GW 172.16.2.1
```

Các host thuộc các mạng LAN khác nhau đã có thể đi đến nhau được:

```
Host1> ping 172.16.2.2
84 bytes from 172.16.2.2 icmp_seq=1 ttl=62 time=3.539 ms
84 bytes from 172.16.2.2 icmp_seq=2 ttl=62 time=2.136 ms
```

Ta kiểm tra rằng các host đã có thể truy nhập được Internet:

```
Host1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=0.957 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=1.346 ms

Host2> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=2.141 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=1.985 ms
```

Các host trên các mạng LAN đang truy nhập Internet theo gateway của chi nhánh mình:

```
Host1> trace 8.8.8.8 <- Host1 đi Internet theo gateway HN
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
 1  172.16.1.1    1.435 ms  5.469 ms  1.055 ms
 2  *101.0.0.1    2.576 ms (ICMP type:3, code:3, Destination port unreachable)  *

Host2> trace 8.8.8.8 <- Host2 đi Internet theo gateway HCM
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
 1  172.16.2.1    1.513 ms  0.470 ms  0.460 ms
 2  *102.0.0.1    2.138 ms (ICMP type:3, code:3, Destination port unreachable)  *
```

Ta kiểm tra rằng khi một chi nhánh bị lỗi kết nối Internet, lưu lượng Internet của chi nhánh ấy sẽ được chuyển hướng qua router Internet của chi nhánh còn lại. Ta thử với phía HN trước.

Thực hiện shutdown cổng E0/0 của router giả lập Internet để giả lập sự kiện đường Internet phía HN down:

```
Internet(config)#interface e0/0
Internet(config-if)#shutdown
```

Lúc này, IP SLA tại HN ping đến địa chỉ gateway 100.0.0.1 sẽ trả kết quả timeout, track object tương ứng sẽ chuyển qua trạng thái down, static default – route được gỡ khỏi bảng định tuyến, default – route học bởi OSPF sẽ được cập nhật thay thế, router HN lái dữ liệu đi Internet qua hướng dự phòng là thông qua HCM:

```
*Aug 2 08:14:39.760: %TRACK-6-STATE: 1 ip sla 1 state Up -> Down
HN#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
 Known via "ospf 1", distance 110, metric 1, candidate default path
 Tag 1, type extern 2, forward metric 10
 Last update from 192.168.1.2 on Ethernet0/1, 00:03:03 ago
```

Routing Descriptor Blocks:

```
* 192.168.1.2, from 192.168.1.2, 00:03:03 ago, via Ethernet0/1
  Route metric is 1, traffic share count is 1
  Route tag 1
```

Ta kiểm tra điều này bằng cách ping và trace 8.8.8.8 từ Host1:

```
Host1> ping 8.8.8.8 <- HN LAN vẫn truy nhập được Internet
84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=4.052 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=3.686 ms

Host1> trace 8.8.8.8 <- Lưu lượng đi Internet được trung chuyển qua site HCM
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
 1  172.16.1.1    1.258 ms  0.798 ms  0.894 ms
 2  192.168.1.2   2.318 ms  2.882 ms  2.022 ms
 3  *102.0.0.1    4.321 ms (ICMP type:3, code:3, Destination port unreachable)
```

Chúng ta thực hiện khôi phục lại kết nối Internet tại phía HN để xác nhận rằng khi đường Internet chính up trở lại, HN LAN sẽ tiếp tục đi Internet theo đường chính này:

```
Internet(config)#interface e0/0
Internet(config-if)#no shutdown

*Aug 2 08:25:05.213: %TRACK-6-STATE: 1 ip sla 1 state Down -> Up
HN#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
  Known via "static", distance 1, metric 0, candidate default path
  Routing Descriptor Blocks:
    *101.0.0.1
      Route metric is 0, traffic share count is 1

Host1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=2.492 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=2.826 ms
Host1> trace 8.8.8.8 <- HN LAN truy nhập Internet theo link Internet tại HN
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
  1  172.16.1.1    1.020 ms  0.972 ms  0.789 ms
  2  *101.0.0.1    2.044 ms (ICMP type:3, code:3, Destination port unreachable) *
```

Ta có thể kiểm tra tương tự với hoạt động dự phòng Internet tại đầu HCM.

4. GRE VPN:

Cấu hình:

Ta thực hiện cấu hình một GRE tunnel nối giữa HN và HCM thông qua Internet, sử dụng IP thiết lập tunnel là các địa chỉ IP public mặt ngoài của hai router. Sau khi tunnel up/up, như thế có một đường data link được thêm vào để kết nối giữa hai router, và chúng ta cấu hình địa chỉ IP của hai cổng tunnel ở hai đầu đường link này là các IP cùng mạng (192.168.1.5/30 và 192.168.1.6/30) (các bạn học viên tham khảo hình 2):

```
HN(config)#interface tunnel 0
HN(config-if)#tunnel source 101.0.0.2
HN(config-if)#tunnel destination 102.0.0.2
HN(config-if)#ip address 192.168.1.5 255.255.255.252
```

```
HN(config-if)#exit
HCM(config)#interface tunnel 0
HCM(config-if)#tunnel source 102.0.0.2
HCM(config-if)#tunnel destination 101.0.0.2
HCM(config-if)#ip address 192.168.1.6 255.255.255.252
HCM(config-if)#exit
```

Sau khi cấu hình xong các tunnel, chúng ta cho các interface tunnel này tham gia định tuyến OSPF Area 0:

```
HN(config)#router ospf 1
HN(config-router)#network 192.168.1.5 0.0.0.0 area 0
HN(config-router)#exit
HCM(config)#router ospf 1
HCM(config-router)#network 192.168.1.6 0.0.0.0 area 0
HCM(config-router)#exit
```

Kiểm tra:

Các cổng tunnel trên hai router đều đã up/up và thông suốt IP:

```
HN#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
Ethernet0/0        172.16.1.1    YES NVRAM  up           up
Ethernet0/1        192.168.1.1   YES NVRAM  up           up
Ethernet0/2        101.0.0.2     YES NVRAM  up           up
Ethernet0/3        unassigned    YES NVRAM  administratively down down
NVI0              172.16.1.1    YES unset   up           up
Tunnel0            192.168.1.5   YES manual  up           up

HCM#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
Ethernet0/0        172.16.2.1    YES NVRAM  up           up
Ethernet0/1        192.168.1.2   YES NVRAM  up           up
Ethernet0/2        102.0.0.2     YES NVRAM  up           up
Ethernet0/3        unassigned    YES NVRAM  administratively down down
NVI0              172.16.2.1    YES unset   up           up
Tunnel0            192.168.1.6   YES manual  up           up

HN#ping 192.168.1.6 <- Tunnel đã thông suốt IP
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Ta kiểm tra rằng OSPF đã hội tụ khi sơ đồ có thêm một link tunnel mới:

```
HN#show ip ospf neighbor
Neighbor ID      Pri  State        Dead Time    Address          Interface
192.168.1.2       0    FULL/DR      00:00:39    192.168.1.6    Tunnel0
192.168.1.2       1    FULL/DR      00:00:33    192.168.1.2    Ethernet0/1

HCM#show ip ospf neighbor
Neighbor ID      Pri  State        Dead Time    Address          Interface
192.168.1.1       0    FULL/DR      00:00:39    192.168.1.5    Tunnel0
192.168.1.1       1    FULL/BDR     00:00:37    192.168.1.1    Ethernet0/1
```

Vì cost của cổng tunnel cao hơn rất nhiều so với cost của cổng Ethernet nên hiện nay các router đã chọn đường đi đến các mạng LAN của nhau thông qua link WAN chứ không thông qua link tunnel:

```
HN#show ip ospf interface tunnel 0
Tunnel0 is up, line protocol is up
  Internet Address 192.168.1.5/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 192.168.1.1, Network Type POINT_TO_POINT, Cost: 1000
(...)

HN#show ip ospf interface e0/1
Ethernet0/1 is up, line protocol is up
  Internet Address 192.168.1.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 10
(...)

HN#show ip route ospf
(...)
  172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O  172.16.2.0/24 [110/20] via 192.168.1.2, 00:52:55, Ethernet0/1

HCM#show ip route ospf
(...)
  172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O  172.16.1.0/24 [110/20] via 192.168.1.1, 00:53:04, Ethernet0/1
```

Trong trường hợp bình thường, HN LAN và HCM LAN đi đến nhau thông qua link WAN:

```
Host1> trace 172.16.2.2
trace to 172.16.2.2, 8 hops max, press Ctrl+C to stop
 1  172.16.1.1    1.053 ms  0.636 ms  0.688 ms
 2  192.168.1.2   1.803 ms  1.779 ms  2.470 ms
 3  *172.16.2.2   4.693 ms (ICMP type:3, code:3, Destination port unreachable)

Host2> trace 172.16.1.2
trace to 172.16.1.2, 8 hops max, press Ctrl+C to stop
 1  172.16.2.1   1.125 ms  0.987 ms  0.753 ms
 2  192.168.1.1   2.695 ms  2.456 ms  2.581 ms
 3  *172.16.1.2   2.889 ms (ICMP type:3, code:3, Destination port unreachable)
```

Ta shutdown một trong hai cổng WAN của hai router để già lập tình huống đường truyền WAN gấp sự cố:

```
HN(config)#interface e0/1
HN(config-if)#shutdown
```

Lúc này, bảng định tuyến của mỗi router sẽ cập nhật route để đi đến mạng LAN của router còn lại là theo link tunnel:

```
HN#show ip route ospf
(...)
 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O 172.16.2.0/24 [110/1010] via 192.168.1.6, 00:01:16, Tunnel0
 192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
O 192.168.1.0/30 [110/1010] via 192.168.1.6, 00:01:16, Tunnel0
HCM#show ip route ospf
(...)
 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O 172.16.1.0/24 [110/1010] via 192.168.1.5, 00:01:38, Tunnel0
```

Hai mạng LAN vẫn đi đến nhau được, nhưng thông qua link tunnel:

```
Host1> trace 172.16.2.2
trace to 172.16.2.2, 8 hops max, press Ctrl+C to stop
 1 172.16.1.1    1.177 ms  0.921 ms  1.106 ms
 2 192.168.1.6   2.514 ms  3.986 ms  2.227 ms
 3 *172.16.2.2   5.337 ms (ICMP type:3, code:3, Destination port unreachable)

Host2> trace 172.16.1.2
trace to 172.16.1.2, 8 hops max, press Ctrl+C to stop
 1 172.16.2.1   0.972 ms  0.629 ms  0.667 ms
 2 192.168.1.5   2.182 ms  2.608 ms  1.950 ms
 3 *172.16.1.2   3.684 ms (ICMP type:3, code:3, Destination port unreachable)
```

Ta mở lại cổng E0/1 của HN trở lại như cũ:

```
HN(config)#interface e0/1
HN(config-if)#no shutdown
```

Đường WAN kết nối giữa HN và HCM đã thông suốt, lúc này, các router lại chọn đường đi đến các mạng LAN của nhau thông qua đường WAN này:

```
HN#show ip route ospf
(...)
 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O 172.16.2.0/24 [110/20] via 192.168.1.2, 00:06:29, Ethernet0/1
HCM#show ip route ospf
(...)

 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O 172.16.1.0/24 [110/20] via 192.168.1.1, 00:06:34, Ethernet0/1
```

Hai mạng LAN đi đến nhau thông qua đường truyền WAN:

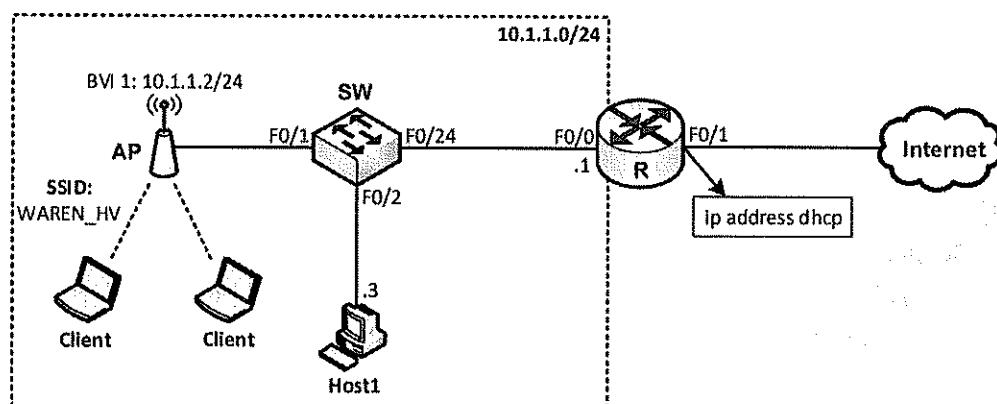
```
Host1> trace 172.16.2.2
trace to 172.16.2.2, 8 hops max, press Ctrl+C to stop
1 172.16.1.1  0.408 ms  0.274 ms  0.462 ms
2  192.168.1.2  0.774 ms  0.572 ms  2.092 ms
3  *172.16.2.2  3.088 ms (ICMP type:3, code:3, Destination port unreachable)

Host2> trace 172.16.1.2
trace to 172.16.1.2, 8 hops max, press Ctrl+C to stop
1  172.16.2.1  0.552 ms  0.421 ms  0.453 ms
2  192.168.1.1  0.855 ms  0.721 ms  0.895 ms
3  *172.16.1.2  1.331 ms (ICMP type:3, code:3, Destination port unreachable)
```

Hoạt động dự phòng kết nối WAN với đường VPN đã diễn ra đúng như yêu cầu. Chúng ta đã hoàn thành tất cả các yêu cầu đặt ra của bài lab.

Lab 21 – Cấu hình Access – Point một SSID

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Sơ đồ bài lab giả lập một tình huống sử dụng access – point để cung cấp truy nhập không dây cho các thiết bị di động. Trong tình huống này, router R đóng vai trò như một router biên cung cấp đường đi Internet; cổng LAN F0/0 của router R kết nối đến một switch Ethernet để cung cấp các kết nối LAN có dây; đến lượt nó, switch lại kết nối đến một access – point để mở rộng mạng LAN ra thành các kết nối không dây. Switch trong bài lab này không thực hiện chia VLAN.
- Hệ thống mạng LAN trong sơ đồ trên không thực hiện chia VLAN, chỉ sử dụng một broadcast – domain duy nhất và được quy hoạch dải IP là 10.1.1.0/24. Cổng F0/0 của router nhận IP là 10.1.1.1/24 và là địa chỉ default – gateway cho các host thuộc mạng LAN; access – point sẽ được cấu hình IP trên interface BVI 1 là 10.1.1.2/24 để làm IP quản lý; Host 1 được cấu hình IP là 10.1.1.3/24 để làm thiết bị truy nhập web vào access – point từ đó thiết lập các thông số cần thiết cho access – point này.
- Trong bài lab này, các bạn học viên cần phải thực hiện thiết lập hệ thống mạng có dây và mở rộng không dây để cung cấp các kết nối wifi cho các thiết bị di động.

Yêu cầu:

1. Thiết lập hệ thống có dây:

- Các bạn học viên thực hiện kết nối các thiết bị như trên sơ đồ hình 1.
- Thực hiện cấu hình router R làm DHCP server cấp phát IP cho các user thuộc mạng LAN 10.1.1.0/24. Khi cấu hình DHCP server, các bạn học viên cần loại trừ không cấp phát xuống các địa chỉ IP đã được sử dụng gồm 10.1.1.1, 10.1.1.2 và 10.1.1.3.
- Cấu hình router R để cung cấp kết nối Internet cho các user thuộc mạng LAN vừa nêu.

2. Cấu hình Access – point:

- Thực hiện đặt địa chỉ quản lý trên interface BVI 1 của access – point như được chỉ ra trên hình 1.
- Cấu hình để access – point cung cấp kết nối không dây với các thông số như sau:
 - SSID: WAREN_HV
 - Sử dụng chuẩn bảo mật WPA2 với PSK (Pre – shared key) là “cisco123456”.

Thực hiện:

1. Thiết lập hệ thống có dây:

Cấu hình:

Thực hiện cấu hình IP trên các cổng của router R:

```
R(config)#interface f0/0
R(config-if)#no shutdown
R(config-if)#ip address 10.1.1.1 255.255.255.0
R(config-if)#exit

R(config)#interface f0/1
R(config-if)#no shutdown
R(config-if)#ip address dhcp
R(config-if)#exit
```

Cấu hình DHCP server:

```
R(config)#ip dhcp excluded-address 10.1.1.1 10.1.1.3
R(config)#ip dhcp pool LAN
R(dhcp-config)#network 10.1.1.0 /24
R(dhcp-config)#default-router 10.1.1.1
R(dhcp-config)#dns-server 8.8.8.8
R(dhcp-config)#exit
```

Cấu hình NAT để cho phép các user thuộc mạng LAN 10.1.1.0/24 truy nhập Internet:

```
R(config)#access-list 1 permit 10.1.1.0 0.0.0.255
R(config)#ip nat inside source list 1 interface f0/1 overload
R(config)#interface f0/0
R(config-if)#ip nat inside
R(config-if)#exit
R(config)#interface f0/1
R(config-if)#ip nat outside
R(config-if)#exit
```

Kiểm tra:

Ta kiểm tra rằng router R đã có đầy đủ IP trên các cổng:

R#show ip interface brief					
Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	10.1.1.1	YES	NVRAM	up	up
FastEthernet0/1	192.168.2.53	YES	DHCP	up	up
Serial0/0/0	unassigned	YES	NVRAM	administratively down	down
NVI0	unassigned	NO	unset	up	up

Router R đã có default – route đi Internet:

```
R#show ip route static
S* 0.0.0.0/0 [254/0] via 192.168.2.1
```

Cấu hình DHCP server đã được thiết lập đầy đủ:

```
R#show run | section dhcp
no ip dhcp use vrf connected
ip dhcp excluded-address 10.1.1.1 10.1.1.3
ip dhcp pool LAN
  network 10.1.1.0 255.255.255.0
  default-router 10.1.1.1
  dns-server 8.8.8.8
  ip address dhcp
```

Từ router R đã có thể truy nhập được Internet:

```
R#ping 8.8.8.8 source 10.1.1.1 <- NAT thành công
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 10.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/33/36 ms
```

2. Cấu hình Access – point:

Cấu hình:

Trước hết, các bạn học viên thực hiện kết nối console đến access – point, tiến hành thao tác xóa hết cấu hình cũ trên thiết bị này:

```
ap#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
ap#reload
Proceed with reload? [confirm]
```

Access – point của Cisco sau khi được xóa hết cấu hình cũ và khởi động lại sẽ load vào cấu hình mặc định ban đầu. Trong cấu hình này, các username và password đều được cài đặt sẵn là “Cisco”, do đó để đăng nhập vào mode Privilege của thiết bị, chúng ta nhập enable password như vừa nêu:

```
ap>enable
Password: <- Nhập password là "Cisco"
ap#
```

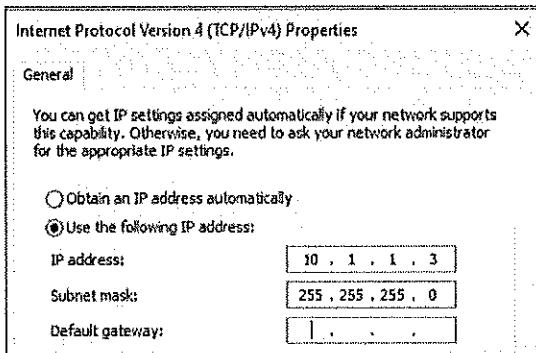
Tiếp theo, chúng ta thực hiện đặt địa chỉ IP quản lý cho access – point là 10.1.1.2/24 theo yêu cầu đặt ra. IP quản lý này được gán trên interface BVI 1 của thiết bị. Để so sánh, ta có thể coi interface này giống như interface vlan 1 của Catalyst switch – cũng được sử dụng để cấu hình IP quản lý cho switch.

```
ap#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)#interface bvi 1
ap(config-if)#no shutdown
ap(config-if)#ip address 10.1.1.2 255.255.255.0
ap(config-if)#end
```

Ta thực hiện kiểm tra rằng địa chỉ đã được đặt trên cổng BVI 1:

Interface	IP-Address	OK?	Method	Status	Protocol
BVI1	10.1.1.2	YES	TFTP	up	up
Dot11Radio0	unassigned	YES	unset	administratively down	down
Dot11Radiol	unassigned	YES	unset	administratively down	down
GigabitEthernet0	unassigned	YES	TFTP	up	up

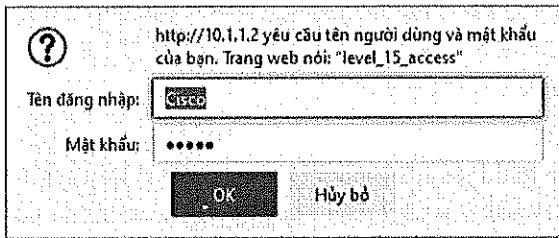
Tiếp theo, ta thực hiện cấu hình IP tĩnh 10.1.1.3/14 cho Host1 – là host sẽ được sử dụng để truy nhập vào giao diện web của access – point để cấu hình (hình 2):



Hình 2 – Địa chỉ IP của Host1.

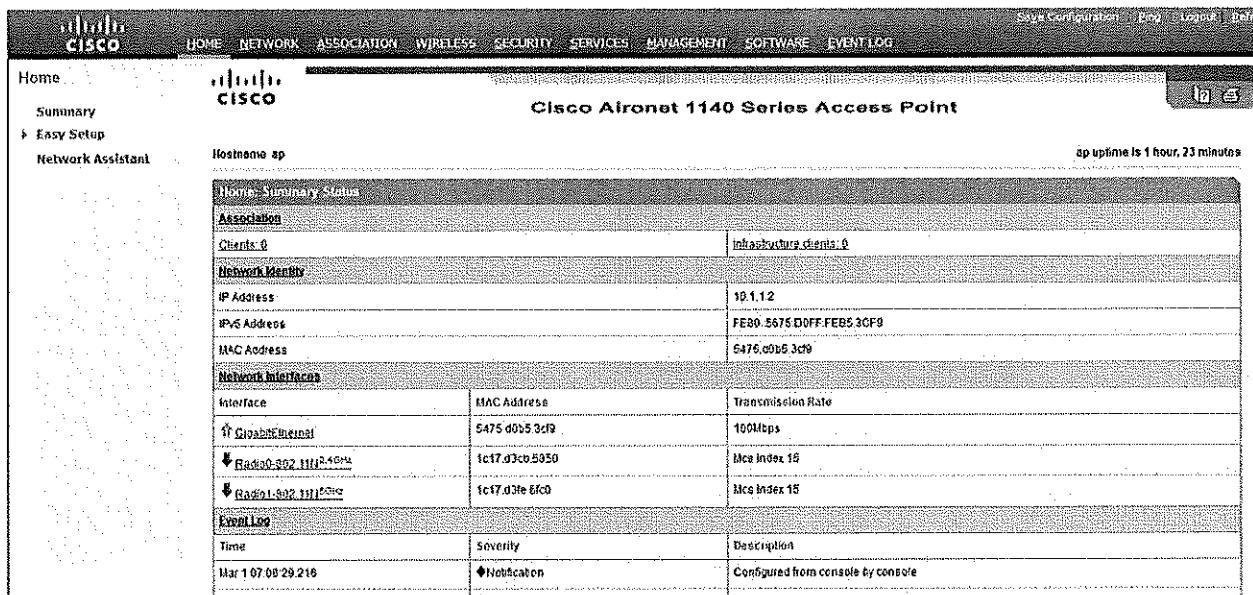
Vì Host1 chỉ sử dụng để truy nhập trực tiếp đến access – point cùng mạng nên ta không cần cấu hình default – gateway cho host này.

Để cấu hình các thông số WiFi theo yêu cầu đặt ra, chúng ta thực hiện truy nhập web đến access – point từ Host1. Các bạn học viên có thể sử dụng một trình duyệt web bất kỳ để thực hiện thao tác truy nhập này. Chúng ta nhập địa chỉ của access – point 10.1.1.2 vào thanh địa chỉ của trình duyệt để truy nhập; một cửa sổ hiện ra yêu cầu chúng ta nhập username và password. Như đã đề cập ở trên, username và password mặc định đều được thiết lập là “Cisco/Cisco”, chúng ta nhập các giá trị này (hình 3):



Hình 3 – Username và password là “Cisco/Cisco”.

Sau khi ta đăng nhập, giao diện web của access – point hiện ra (hình 4):



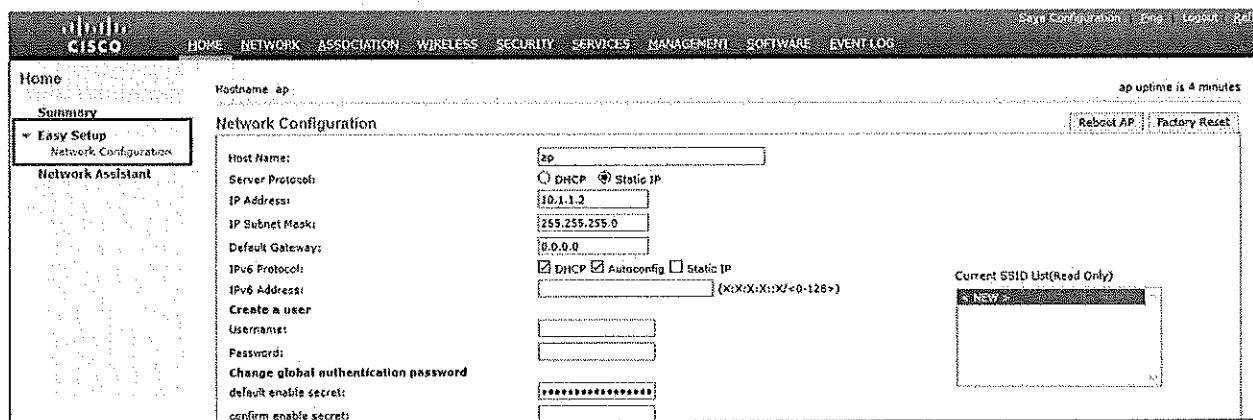
Hình 4 – Giao diện web của access – point.

Tiếp theo, ta thực hiện các bước sau để hoàn thành yêu cầu đặt ra:

- Khai báo SSID cùng với cấu hình bảo mật đi kèm.
- Tinh chỉnh cấu hình SSID.
- Bật thu/phát không dây.

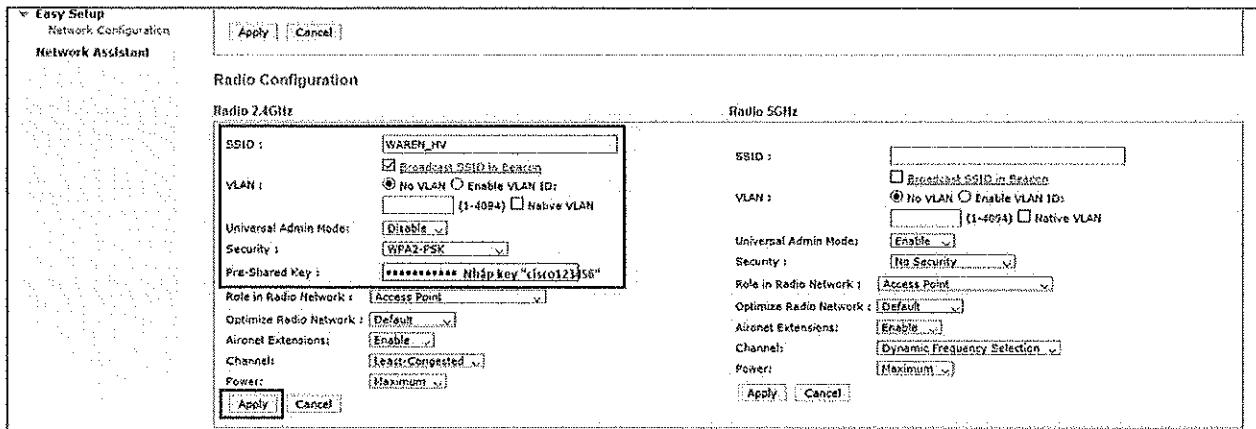
Khai báo SSID và cấu hình bảo mật:

Trên cửa sổ giao diện web của access – point, chúng ta click chọn “Easy Setup”, kế tiếp trong mục này, ta click chọn tiếp “Network Configuration”, phần cửa sổ “Network Configuration” hiện ra ở bên phải của giao diện (hình 5):



Hình 5 – Easy Setup và Network Configuration.

Các bạn học viên kéo thanh cuộn cửa sổ xuống phía dưới, đi tới phần “Radio Configuration”. Tại đây, chúng ta thực hiện khai báo SSID và pre – shared key cho phương thức bảo mật WPA2 của mạng Wifi trong khu vực “Radio 2.4 GHz” (hình 6):



Hình 6 – Khai báo SSID và Key cho phương thức bảo mật WPA2.

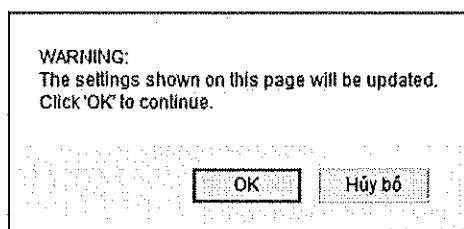
Trong đó:

- SSID: WAREN_HV
- Ta nhớ check vào ô “Broadcast SSID in Beacon”.
- Trong mục khai báo về VLAN, ta chọn “No VLAN”.
- Chọn “Disable” cho mục “Universal Admin Mode”.
- Trong mục “Security”, các bạn xổ thanh cuộn xuống và chọn “WPA2-PSK”. Lúc này ô khai báo “Pre-Shared Key” hiện ra, chúng ta nhập key là “cisco123” – chính là password Wifi định sử dụng.
- Các ô khác các bạn để như mặc định, không thay đổi.

Sau khi khai báo xong như vừa nêu, chúng ta nhấn “Apply” để cập nhật cấu hình.

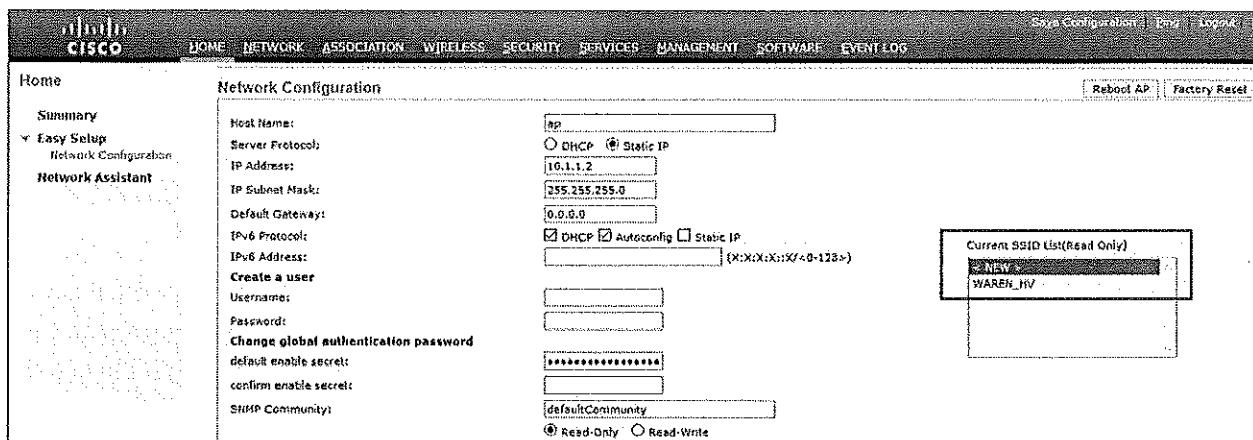
Với thiết lập như trên, access – point được cấu hình để phát ra một SSID trong băng tần 2,4 GHz. Nếu muốn phát ra băng tần 5 GHz, các bạn học viên có thể thực hiện thao tác vừa rồi nhưng trong khu vực “Radio 5GHz” (xem hình 6).

Sau khi nhấn “Apply”, một hộp thoại hỏi ý kiến hiện ra, chúng ta chọn “OK” để xác nhận cấu hình (hình 7):



Hình 7 – Nhấn “OK” để xác nhận cấu hình.

Các bạn có thể kiểm tra trong mục “Current SSID List (Read Only)” của ô “Network Configuration” ở phía trên để xác nhận rằng SSID của chúng ta đã được khai báo thành công (hình 8):



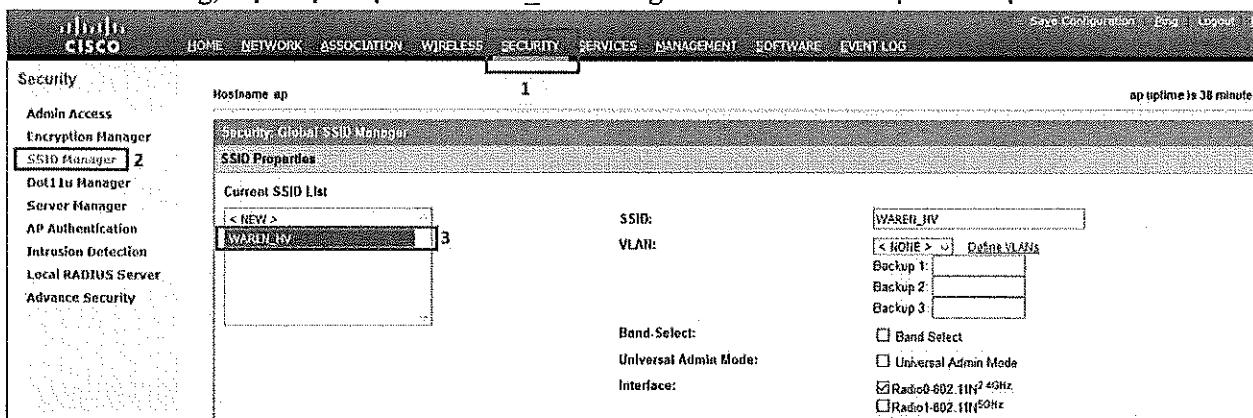
Hình 8 – SSID “WAREN_HV” đã được khai báo thành công.

Tinh chỉnh cấu hình SSID:

SSID đã được khai báo, tuy nhiên hiện nó chưa được access – point phát ra ngoài. Chúng ta còn cần phải tinh chỉnh thêm một vài thông số của SSID này.

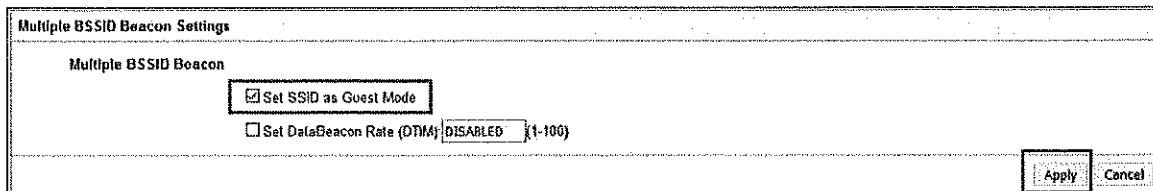
Để tiếp tục tinh chỉnh cho SSID “WAREN_HV”, chúng ta click chọn SSID này trong danh sách SSID của cửa sổ “SSID Manager”. Các bước chọn được thể hiện trong hình 9:

1. Đầu tiên, ta chọn “SECURITY” trên thanh menu của giao diện.
2. Ké tiếp, ta chọn “SSID Manager”.
3. Cuối cùng, thực hiện chọn “WAREN_HV” trong danh sách SSID được hiển thị.



Hình 9 – SSID “WAREN_HV” trong danh sách SSID.

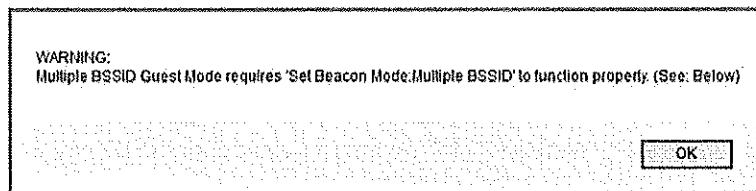
Trong cửa sổ “SSID Manager” ở trên, các bạn học viên kéo thanh cuộn xuống phía dưới đến mục “Multiple BSSID Beacon Settings”; tại đây, các bạn check chọn “Set SSID as Guest Mode” và nhấn “Apply” để cập nhật cấu hình (hình 10):



Hình 10 – Chọn “Set SSID as Guest Mode”.

Một hộp thoại như trên hình 7 sẽ hiện ra để các bạn xác nhận cấu hình, chúng ta chọn “OK”. Điều này diễn ra thường xuyên mỗi khi chúng ta thiết lập một tùy chọn nào đó cho access – point; do đó, trong phần còn lại của bài lab sẽ không mô tả lại vấn đề này; các bạn học viên chỉ cần nhấn “OK” xác nhận mỗi khi hộp thoại này hiện ra.

Lưu ý: Khi các bạn chọn “Set SSID as Guest Mode”, một cửa sổ cảnh báo hiện ra, các bạn chỉ cần nhấn “OK” bỏ qua thông báo này (hình 11).



Hình 11 – Cửa sổ thông báo.

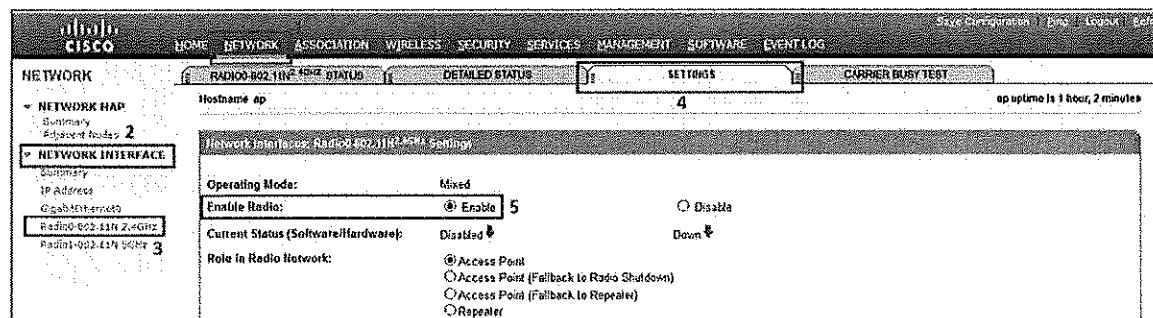
Đến đây, chúng ta đã hoàn thành tác vụ khai báo SSID và thiết lập bảo mật WPA2 đi kèm. Kế tiếp, chúng ta chuyển qua bước bật thu/phát Wifi cho SSID này.

Bật thu/phát không dây:

Để bật thu phát không dây, chúng ta thực hiện tuần tự như sau:

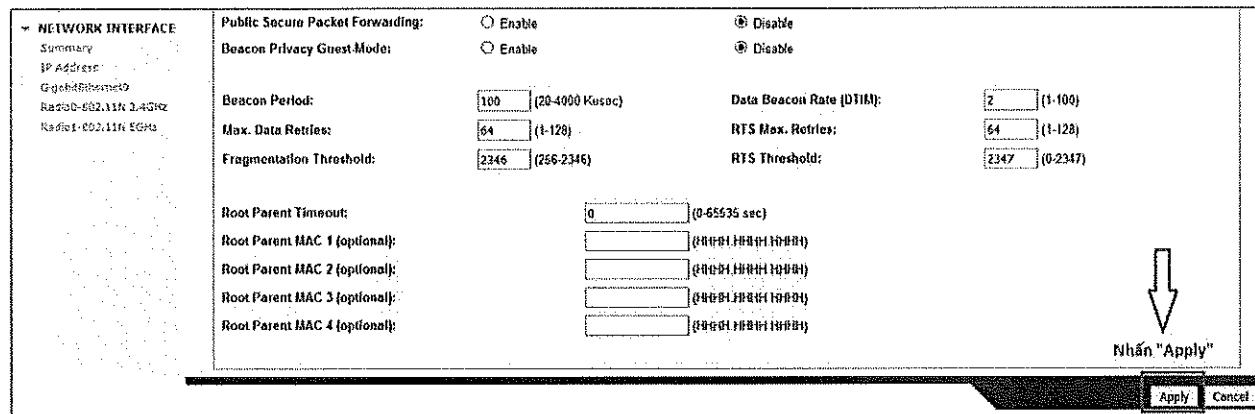
- Chọn “NETWORK” trên thanh menu của giao diện.
- Trong tab bên trái cửa sổ, chọn tiếp “NETWORK INTERFACE”.
- Trong mục này, chọn tiếp “Radio0-802.11N 2.4GHz”.
- Trong cửa sổ bên phải, ta chọn tiếp thẻ “SETTINGS”.
- Cuối cùng, trong mục “Enable Radio”, ta click chọn “Enable”.

Quá trình này được thể hiện trong hình 12:



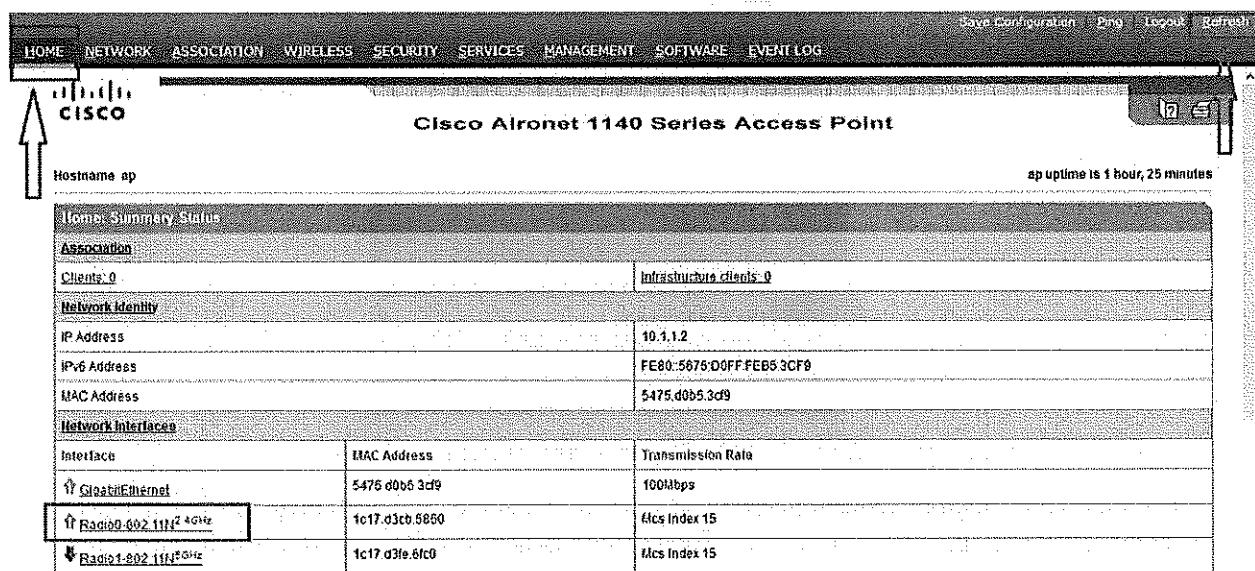
Hình 12 – Enable thu/phát băng tần 2,4GHz.

Tiếp theo, chúng ta kéo thanh cuộn cửa sổ xuống dưới cùng. Tại đây, các bạn nhấn “Apply” để cập nhật thông số vừa thiết lập (hình 13).



Hình 13 – Nhấn “Apply” cập nhật cấu hình.

Lúc này, access – point đã thực hiện phát ra một kênh không dây thuộc dải tần 2,4GHz với SSID “WAREN_HV”. Chúng ta có thể xác nhận rằng kênh không dây vừa nêu đã được enable thành công bằng cách trở lại trang chủ của giao diện bằng cách chọn “HOME” trong thanh menu (hình 14):



Hình 14 – Kiểm tra xác nhận kênh radio đã được enable thành công.

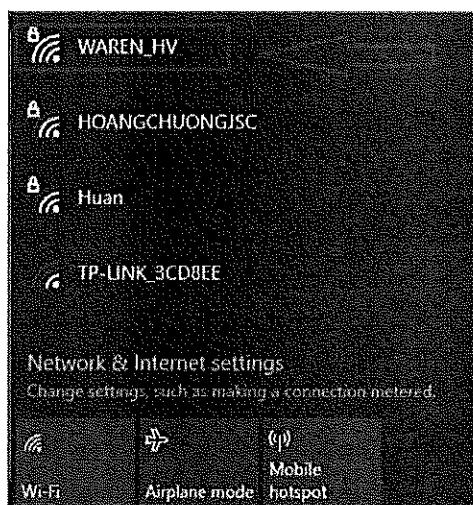
Trong cửa sổ giao diện, ta quan sát thông tin khái quát về kênh radio 2,4GHz tại mục “Radio0-802.11N^{2.4GHz}” (hình 14). Dấu mũi tên hướng lên màu xanh cho thấy kênh đã hoạt động.

Đôi khi giao diện web của access – point cập nhật bị chậm, ta sẽ thấy kênh vẫn chưa được chỉ thị là đã được bật lên mà vẫn báo chưa enable (mũi tên màu đỏ hướng xuống). Khi đó, chúng ta thực hiện nhấn vào mục “Refresh” tại góc trên cùng bên phải của giao diện (các bạn xem hình 14 ở trên) để giao diện được cập nhật đúng tình trạng của interface radio 0.

Kiểm tra:

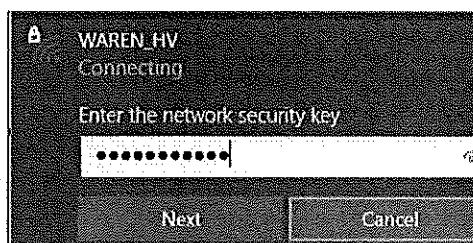
Đến đây, chúng ta đã hoàn thành việc cấu hình access – point phát ra kênh Wifi như yêu cầu. Tiếp theo, chúng ta thực hiện kiểm tra kết quả cấu hình đã thực hiện.

Sử dụng một thiết bị đầu cuối không dây bất kỳ để xác nhận rằng lúc này đã có một kênh Wifi có SSID “WAREN_HV” đã được broadcast (hình 15):



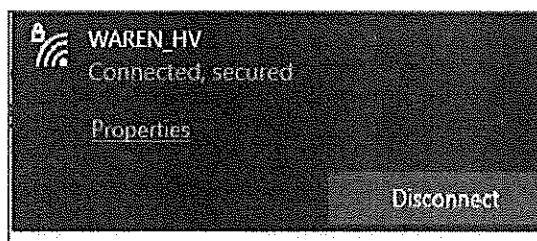
Hình 15 – Kênh Wifi “WAREN_HV” đã được broadcast.

Tiếp theo, ta thực hiện kết nối Wifi vào SSID này (hình 16):



Hình 16 – Kết nối vào SSID “WAREN_HV”.

Lúc này, một cửa sổ hiện ra yêu cầu nhập password Wifi. Chúng ta thực hiện nhập key “cisco123456” như đã cấu hình ở trên và nhấn “Next” để tiếp tục đăng nhập. Thông tin chỉ thị trên thiết bị đầu cuối cho thấy thiết bị này đã truy nhập Wifi thành công (hình 17):



Hình 17 – Truy nhập Wifi thành công.

Ta có thể kiểm tra các thông số mạng mà thiết bị đầu cuối nhận được qua kết nối Wifi (chúng ta nhấn vào link “Properties” trong giao diện thông tin trên hình 17 ở trên):

```
SSID: WAREN_HV
Protocol: Wi-Fi 4 (802.11n)
Security type: WPA2-Personal
Network band: 2.4 GHz
Network channel: 7
Link speed (Receive/Transmit): 144/72 (Mbps)
Link-local IPv6 address: fe80::d46c:8d1:9c51:d34a%16
IPv4 address: 10.1.1.5
IPv4 DNS servers: 8.8.8.8
Manufacturer: Qualcomm Atheros Communications Inc.
Description: Qualcomm Atheros AR9485WB-EG Wireless Network Adapter
Driver version: 3.0.2.201
Physical address (MAC): 08-ED-B9-B4-A4-A1
```

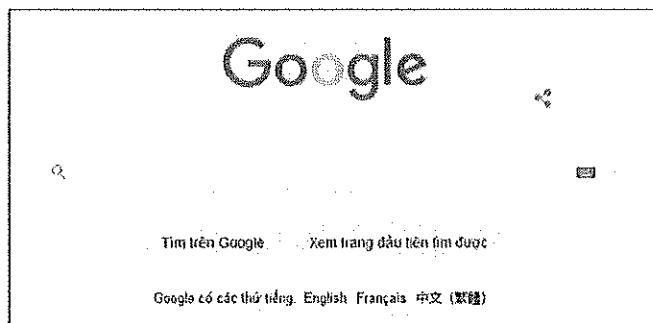
Ta kiểm tra rằng thiết bị đã có thể đi được Internet:

```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=37ms TTL=115
Reply from 8.8.8.8: bytes=32 time=40ms TTL=115
Reply from 8.8.8.8: bytes=32 time=34ms TTL=115
Reply from 8.8.8.8: bytes=32 time=36ms TTL=115

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 34ms, Maximum = 40ms, Average = 36ms
```

Từ thiết bị đầu cuối, chúng ta cũng có thể truy nhập web trên Internet (hình 18):

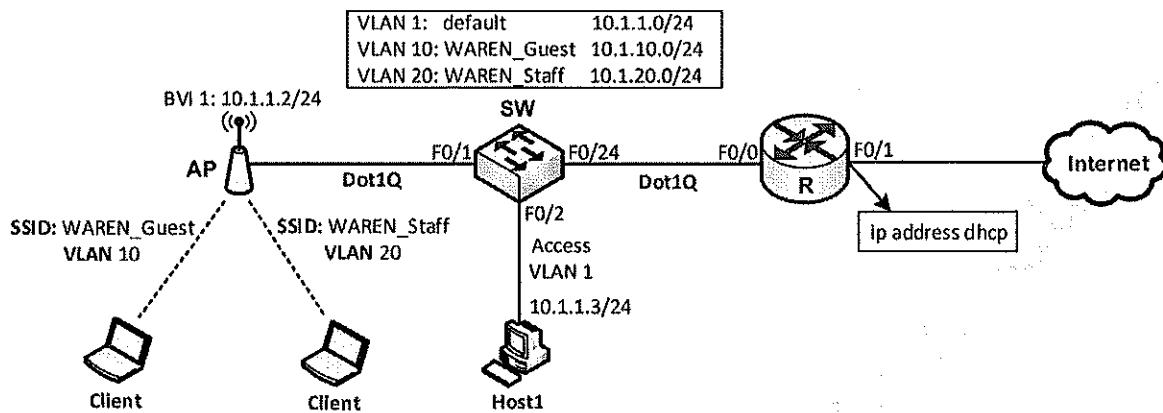


Hình 18 – Truy nhập web thành công.

Đến đây, chúng ta đã hoàn thành bài lab được yêu cầu.

Lab 22 – Cấu hình Access – point nhiều SSID

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Trong bài lab này, các bạn học viên sẽ thực tập cấu hình access – point phát ra hai SSID:
 - SSID: “WAREN_Guest”, cung cấp truy nhập Wifi vào VLAN 10 của hệ thống.
 - SSID: “WAREN_Staff”, cung cấp truy nhập Wifi vào VLAN 20 của hệ thống.
- Với hệ thống mạng có dây:
 - Trên switch, thực hiện tạo hai VLAN 10 và 20 cho hai SSID đã nêu ở trên.
 - Các đường link kết nối switch với router và access – point được thiết lập trunking Dot1Q.
 - Router R sẽ được cấu hình để định tuyến giữa các VLAN và cung cấp đường truyền Internet cho các user trên các VLAN này.
 - Quy hoạch IP cho các VLAN được chỉ ra như trên sơ đồ hình 1.

Yêu cầu:

1. Cấu hình mạng có dây:

- Cấu hình tạo các VLAN 10 và 20 trên switch. Các bạn học viên nên đặt tên gọi nhớ cho các VLAN này trùng với các SSID tương ứng do access – point phát ra.
- Thiết lập trunking Dot1Q trên các cổng của switch kết nối đến access – point và router.
- Cấu hình router R định tuyến VLAN cho các VLAN trên switch theo quy hoạch IP đã chỉ ra trên sơ đồ hình 1.
- Bên cạnh đó, cấu hình router làm DHCP server cấp phát IP cho các user thuộc các VLAN của hệ thống mạng.
- Cấu hình router R cung cấp truy nhập Internet cho các user thuộc các VLAN của hệ thống.

2. Cấu hình access – point:

- Cấu hình access – point phát ra hai SSID như sau:
 - “WAREN_Guest”: cung cấp truy nhập vào VLAN 10.
 - “WAREN_Staff”: cung cấp truy nhập vào VLAN 20.
- Thực hiện bảo mật cho hai SSID bằng WPA2 với key bảo mật như sau:
 - “WAREN_Guest”: key là “cisco123456”.
 - “WAREN_Staff”: key là “waren123456”.

Thực hiện:

1. Cấu hình mạng có dây:

Cấu hình:

Trên switch:

```
SW(config)#vlan 10
SW(config-vlan)#name WAREN_Guest
SW(config-vlan)#exit
SW(config)#vlan 20
SW(config-vlan)#name WAREN_Staff
SW(config-vlan)#exit

SW(config)#interface range f0/1,f0/24
SW(config-if-range)#switchport trunk encapsulation dot1q
SW(config-if-range)#switchport mode trunk
SW(config-if-range)#exit
```

Trên router:

```
R(config)#interface f0/0
R(config-if)#no shutdown
R(config-if)#ip address 10.1.1.1 255.255.255.0
R(config-if)#exit
R(config)#interface f0/0.10
R(config-subif)#encapsulation dot1Q 10
R(config-subif)#ip address 10.1.10.1 255.255.255.0
R(config-subif)#exit
R(config)#interface f0/0.20
R(config-subif)#encapsulation dot1Q 20
R(config-subif)#ip address 10.1.20.1 255.255.255.0
R(config-subif)#exit

R(config)#ip dhcp excluded-address 10.1.1.1 10.1.1.3
R(config)#ip dhcp excluded-address 10.1.10.1
R(config)#ip dhcp excluded-address 10.1.20.1
R(config)#ip dhcp pool WAREN_Guest
R(dhcp-config)#network 10.1.10.0 /24
R(dhcp-config)#default-router 10.1.10.1
R(dhcp-config)#dns-server 8.8.8.8
R(dhcp-config)#exit
```

```
R(config)#ip dhcp pool WAREN_staff
R(dhcp-config)#network 10.1.20.0 /24
R(dhcp-config)#default-router 10.1.20.1
R(dhcp-config)#dns-server 8.8.8.8
R(dhcp-config)#exit

R(config)#interface f0/1
R(config-if)#no shutdown
R(config-if)#ip address dhcp
R(config-if)#exit

R(config)#access-list 1 permit 10.1.1.0 0.0.0.255
R(config)#access-list 1 permit 10.1.10.0 0.0.0.255
R(config)#access-list 1 permit 10.1.20.0 0.0.0.255
R(config)#ip nat inside source list 1 interface f0/1 overload
R(config)#interface f0/0
R(config-if)#ip nat inside
R(config-if)#exit
R(config)#interface f0/0.10
R(config-subif)#ip nat inside
R(config-subif)#exit
R(config)#interface f0/0.20
R(config-subif)#ip nat inside
R(config-subif)#exit
R(config)#interface f0/1
R(config-if)#ip nat outside
R(config-if)#exit
```

Kiểm tra:

Các VLAN đã được tạo ra đầy đủ trên switch:

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, Fa0/25, Fa0/26 Fa0/27, Fa0/28, Fa0/29, Fa0/30 Fa0/31, Fa0/32, Fa0/33, Fa0/34 Fa0/35, Fa0/36, Fa0/37, Fa0/38 Fa0/39, Fa0/40, Fa0/41, Fa0/42 Fa0/43, Fa0/44, Fa0/45, Fa0/46 Fa0/47, Fa0/48, Gi0/1, Gi0/2 Gi0/3, Gi0/4
10	WAREN_Guest	active	
20	WAREN_Staff	active	
(...)			

Các cổng trunk đã được thiết lập:

```
SW#show interfaces trunk

Port      Mode          Encapsulation  Status      Native vlan
Fa0/1    on           802.1q        trunking    1
Fa0/24   on           802.1q        trunking    1

Port      Vlans allowed on trunk
Fa0/1    1-4094
Fa0/24   1-4094

Port      Vlans allowed and active in management domain
Fa0/1    1,10,20
Fa0/24   1,10,20

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    1,10,20
Fa0/24   1,10,20
```

Trên router, các interface và sub – interface đã được cấu hình đầy đủ:

```
R#show ip interface brief

Interface            IP-Address      OK? Method Status      Protocol
FastEthernet0/0      10.1.1.1       YES manual up          up
FastEthernet0/0.10    10.1.10.1     YES manual up         up
FastEthernet0/0.20    10.1.20.1     YES manual up         up
FastEthernet0/1       192.168.2.60   YES DHCP up          up
Serial0/0/0          unassigned     YES unset administratively down down
Serial0/0/1          unassigned     YES unset administratively down down
NVI0                 unassigned     NO  unset up          up
```

Các pool DHCP đã được thiết lập cho các VLAN:

```
R#show running-config | section dhcp
no ip dhcp use vrf connected
ip dhcp excluded-address 10.1.1.1 10.1.1.3
ip dhcp excluded-address 10.1.10.1
ip dhcp excluded-address 10.1.20.1
ip dhcp pool WAREN_Guest
  network 10.1.10.0 255.255.255.0
  default-router 10.1.10.1
  dns-server 8.8.8.8
ip dhcp pool WAREN_staff
  network 10.1.20.0 255.255.255.0
  default-router 10.1.20.1
  dns-server 8.8.8.8
ip address dhcp
```

Từ router R, đã có thể truy nhập được Internet bằng địa chỉ IP quy hoạch cho các VLAN:

```
R#ping 8.8.8.8 source 10.1.1.1
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 10.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/32/36 ms

R#ping 8.8.8.8 source 10.1.10.1
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 10.1.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/36/44 ms

R#ping 8.8.8.8 source 10.1.20.1
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 10.1.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/32/36 ms
```

2. Cấu hình access – point:

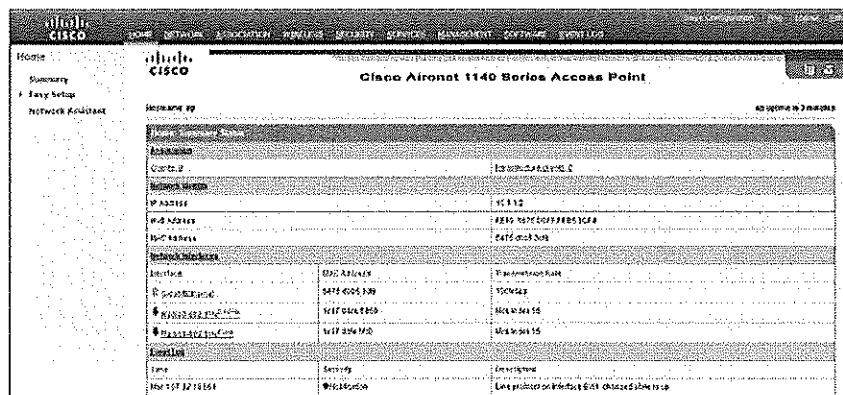
Cấu hình:

Tương tự như bài lab trước, các bạn học viên cũng thực hiện xóa hết cấu hình cũ của access – point, sau đó đặt IP quản lý trên interface bvi 1 như được chỉ ra trên sơ đồ lab:

```
ap(config)#interface bvi 1
ap(config-if)#no shutdown
ap(config-if)#ip address 10.1.1.2 255.255.255.0
ap(config-if)#exit
```

Nhắc lại rằng, sau khi reset access – point về cấu hình mặc định, password đăng nhập vào thiết bị sẽ được thiết lập sẵn là “Cisco” (chữ “C” đầu tiên viết hoa).

Tiếp theo, chúng ta cũng thực hiện truy nhập web từ Host1 đến access – point bằng địa chỉ 10.1.1.2 đã thiết lập ở trên. Giống như bài lab trước, giao diện web của access – point được mở để thực hiện thiết lập cấu hình (hình 2):



Hình 2 – Giao diện web của access – point.

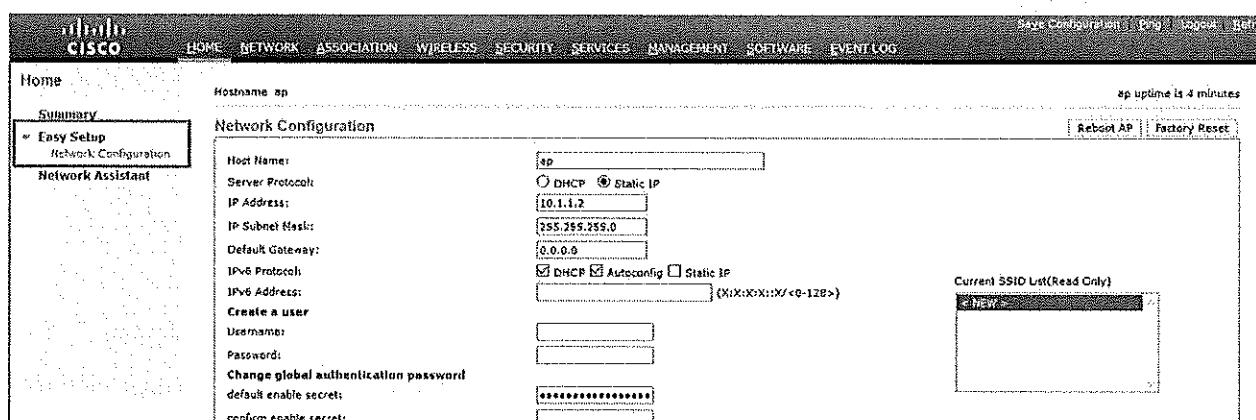
Nhắc lại rằng, tương tự như bài lab trước, một cửa sổ sẽ hiện ra yêu cầu nhập username và password, chúng ta nhập hai thông số này là “Cisco/Cisco” để truy nhập được vào giao diện web.

Để thiết lập các SSID của mạng không dây như yêu cầu, chúng ta tiến hành theo các bước như sau:

1. Khai báo các SSID cùng các thông số VLAN và key bảo mật WPA2 tương ứng.
2. Tinh chỉnh các SSID đã khai báo.
3. Bật thu/phát không dây.

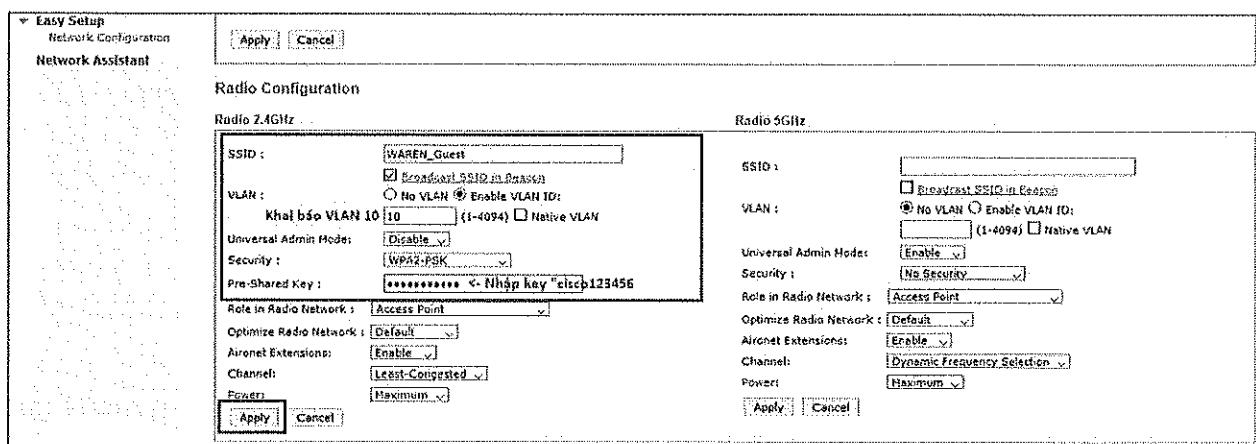
Khai báo SSID và các thông số liên quan:

Trong cửa sổ giao diện, chúng ta chọn “Easy Setup” ở tab bên trái, tiếp đó, chúng ta click chọn “Network Configuration” (hình 3):



Hình 3 – Cửa sổ “Easy Setup” và mục “Network Configuration”.

Tiếp theo, chúng ta kéo thanh cuộn cửa sổ xuống phía dưới. Trong ô “Radio Configuration”, chúng ta thực hiện khai báo SSID “WAREN_Guest” và các thông số liên quan trong khu vực “Radio 2.4GHz” (hình 4):



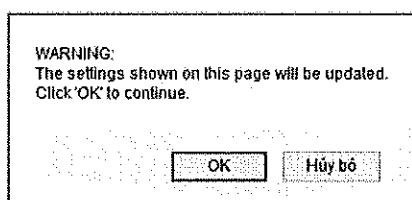
Hình 4 – Khai báo SSID “WAREN_Guest”.

Các thông số được khai báo cho SSID “WAREN_Guest”:

- SSID: WAREN_Guest.
- Click chọn “Enable VLAN ID:”, tiếp đó, trong ô khai báo VLAN ID, chúng ta nhập giá trị là “10” – chính là VLAN ID của VLAN kết nối với SSID này.
- Trong mục “Universal Admin Mode:”, chúng ta chọn “Disable”.
- Trong ô “Security:”, ta chọn “WPA2-PSK”. Khi đó, ô “Pre-shared Key:” hiện ra, chúng ta nhập key chính là password WiFi dùng cho SSID “WAREN_Guest”: cisco123456.
- Các ô còn lại chúng ta giữ nguyên không thay đổi.

Sau khi khai báo xong, các bạn nhấn “Apply” để cập nhật cấu hình.

Khi cửa sổ yêu cầu xác nhận trong hình 5 hiện ra, các bạn nhấn “OK” để tiếp tục:



Hình 5 – Nhấn “OK” để đồng ý cập nhật cấu hình.

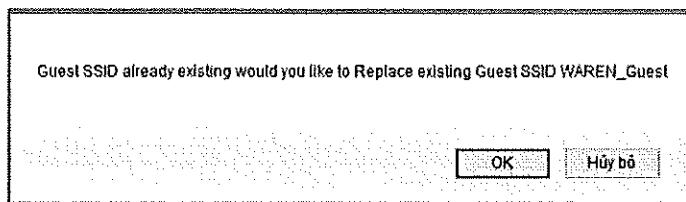
Tương tự như bài lab trước, mỗi khi có cửa sổ này hiện ra, các bạn chỉ cần nhấn “OK” để tiếp tục.

Kế tiếp, chúng ta khai báo SSID “WAREN_Staff” và các thông số đi kèm giống như đã thực hiện ở trên (hình 6):

Field	Value
SSID :	WAREN_Staff
VLAN :	Enable VLAN ID: 10
Security :	WPA2-PSK
Pre-Shared Key :	cisco123456

Hình 6 – Khai báo SSID “WAREN_Staff”.

Khi chúng ta nhấn “Apply”, một cửa sổ khác hiện ra hỏi ý kiến về việc có thay thế SSID “WAREN_Staff” cho “WAREN_Guest” trên băng tần 2,4GHz hay không (hình 7). Chúng ta vẫn nhấn “OK” để tiếp tục. Lúc này, chỉ có một SSID được hoạt động, tuy nhiên, chúng ta sẽ thực hiện tinh chỉnh lại để có thể sử dụng được đồng thời cả hai SSID vừa khai báo.



Hình 7 – Nhấn “OK” để tiếp tục.

Sau khi khai báo xong hai SSID và các thông số đi kèm, hai SSID này đã được hiển thị trên danh sách SSID (Current SSID (Read Only)) của cửa sổ ‘Network Configuration’ trong mục “Easy Setup”(hình 8):



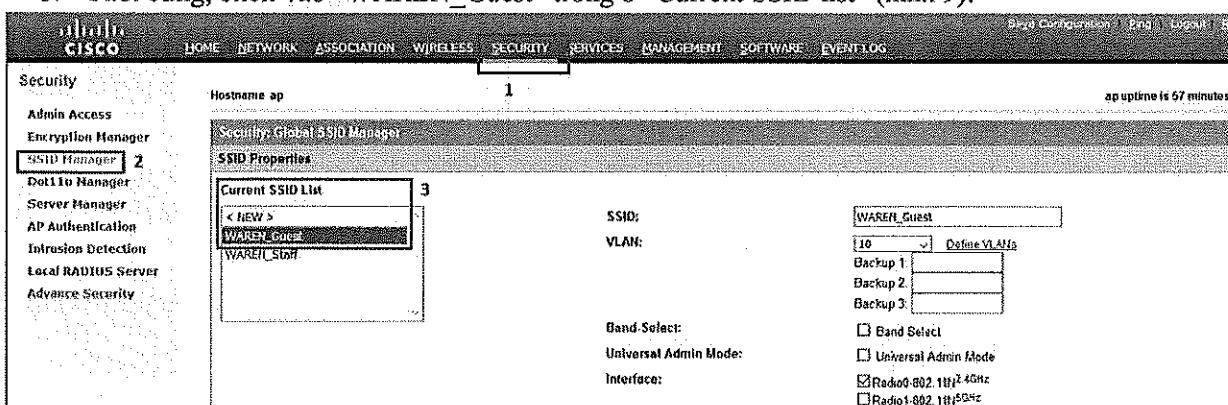
Hình 8 – Các SSID đã khai báo.

Tiếp theo, chúng ta qua bước tinh chỉnh cho hai SSID vừa tạo để active hai SSID này.

Tinh chỉnh SSID:

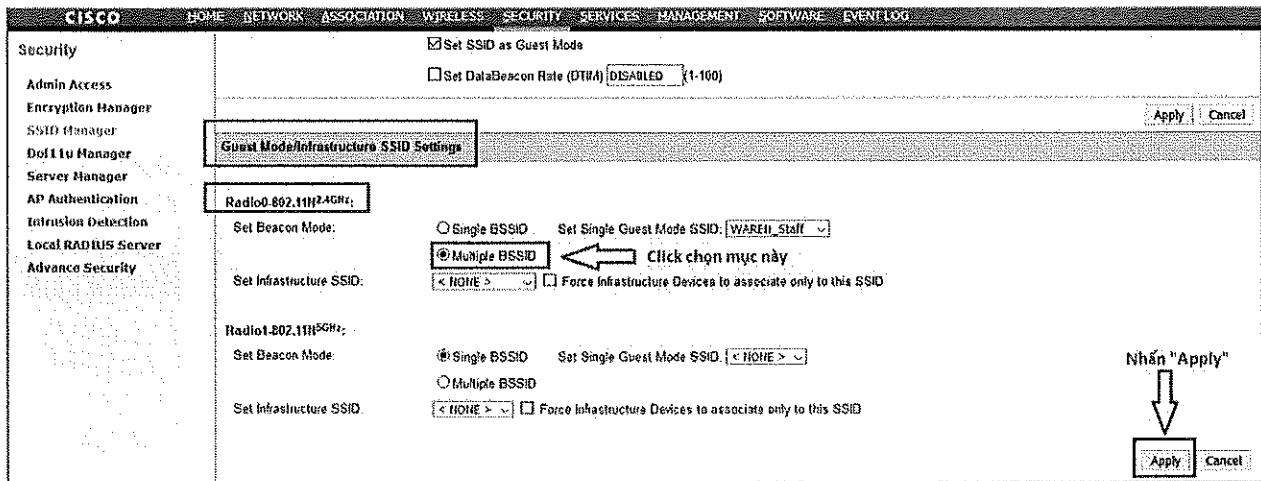
Trước hết, ta tinh chỉnh cho SSID “WAREN_Guest”:

- Các bạn học viên chọn “SECURITY” trong thanh menu của giao diện.
- Kế tiếp, chọn “SSID Manager”
- Cuối cùng, click vào “WAREN_Guest” trong ô “Current SSID list” (hình 9):



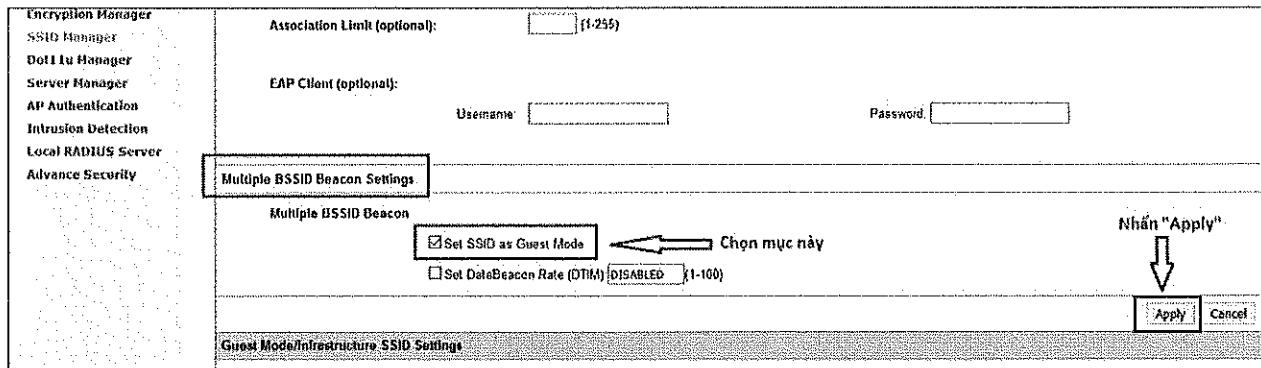
Hình 9 – Chọn SSID “WAREN_Guest”.

Tiếp theo, các bạn kéo thanh cuộn cửa sổ xuống dưới cùng. Trong ô “Guest Mode/Infrastructure SSID Settings”, chúng ta click chọn “Multiple BSSID” của mục “Radio-802.11N^{2.4GHz}”, sau đó nhấn “Apply” để cập nhật cấu hình (hình 10):



Hình 10 – Chọn “Multiple BSSID” cho SSID “WAREN_Guest”.

Tiếp theo, chúng ta lại kéo thanh cuộn cửa sổ xuống phía dưới đến mục “Multiple BSSID Beacon Settings”, click chọn “Set SSID as Guest Mode” và nhấn “Apply” cho mục này (hình 11):



Hình 11 – Chọn “Set SSID as Guest Mode” cho SSID “WAREN_Guest”.

Đến đây, chúng ta hoàn thành việc tinh chỉnh cho SSID “WAREN_Guest”.

Tiếp theo, chúng ta thực hiện tinh chỉnh cho SSID “WAREN_Staff”. Các bạn học viên thực hiện chọn SSID này trong danh sách SSID và click chọn hai thông số “Multiple SSID” và “Set SSID as Guest Mode” giống như với SSID “WAREN_Guest” đã thực hiện ở trên.

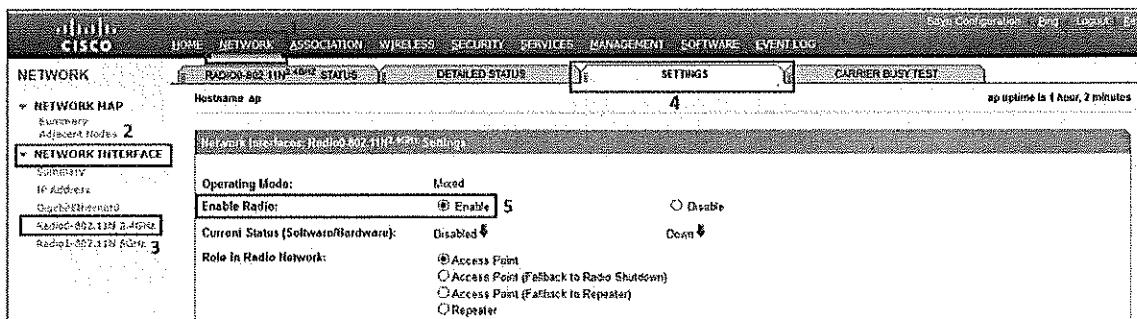
Sau khi tinh chỉnh xong cho hai SSID đã khai báo, chúng ta đi qua bước kế tiếp là bật thu/phát không dây trên băng tần 2,4GHz cho hai SSID này.

Bật thu/phát không dây:

Chúng ta thực hiện bật thu/phát không dây giống như trong bài lab trước. Các bước thực hiện:

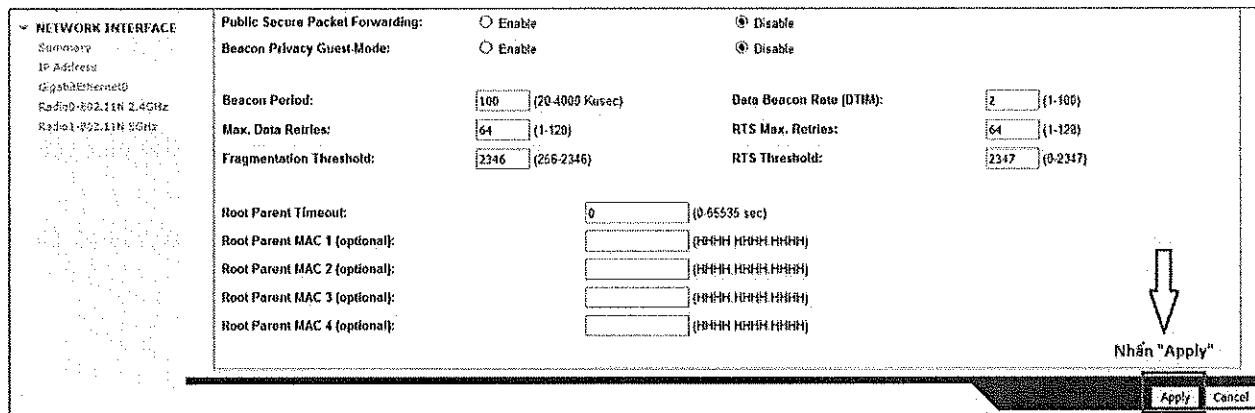
6. Chọn “NETWORK” trên thanh menu của giao diện.
7. Trong tab bên trái cửa sổ, chọn tiếp “NETWORK INTERFACE”.
8. Trong mục này, chọn tiếp “Radio0-802.11N 2.4GHz”.
9. Trong cửa sổ bên phải, ta chọn tiếp thẻ “SETTINGS”.
10. Cuối cùng, trong mục “Enable Radio”, ta click chọn “Enable”.

Quá trình này được thể hiện trong hình 12:



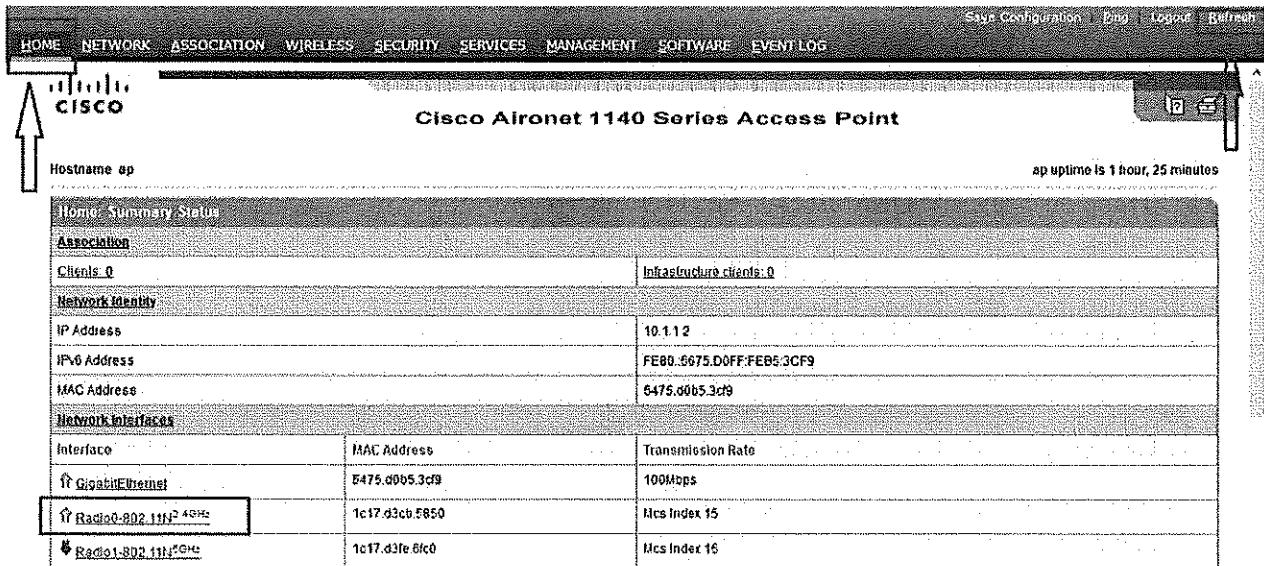
Hình 12 – Enable thu/phát băng tần 2,4GHz.

Tiếp theo, chúng ta kéo thanh cuộn cửa sổ xuống dưới cùng. Tại đây, các bạn nhấn “Apply” để cập nhật thông số vừa thiết lập (hình 13).



Hình 13 – Nhấn “Apply” cập nhật cấu hình.

Lúc này, access – point đã thực hiện phát ra một kênh không dây thuộc dải tần 2,4GHz với SSID “WAREN_HV”. Chúng ta có thể xác nhận rằng kênh không dây vừa nêu đã được enable thành công bằng cách trở lại trang chủ của giao diện bằng cách chọn “HOME” trong thanh menu (hình 14):



Hình 14 – Kiểm tra xác nhận kênh radio đã được enable thành công.

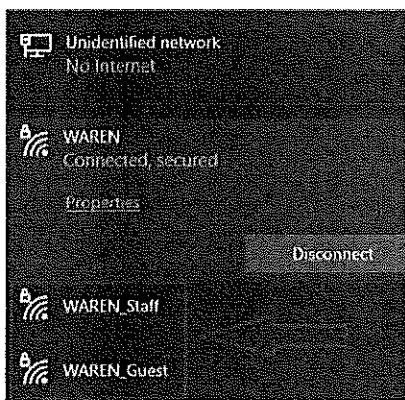
Trong cửa sổ giao diện, ta quan sát thông tin khái quát về kênh radio 2,4GHz tại mục “Radio0-802.11N^{2.4GHz}” (hình 14). Đầu mũi tên hướng lên màu xanh cho thấy kênh đã hoạt động.

Đôi khi giao diện web của access – point cập nhật bị chậm, ta sẽ thấy kênh vẫn chưa được chỉ thị là đã được bật lên mà vẫn báo chưa enable (mũi tên màu đỏ hướng xuống). Khi đó, chúng ta thực hiện nhấn vào mục “Refresh” tại góc trên cùng bên phải của giao diện (các bạn xem hình 14 ở trên) để giao diện được cập nhật đúng tình trạng của interface radio 0.

Kiểm tra:

Đến đây, chúng ta đã hoàn thành việc cấu hình access – point phát ra kênh Wifi với hai SSID như yêu cầu. Tiếp theo, chúng ta thực hiện kiểm tra kết quả cấu hình đã thực hiện.

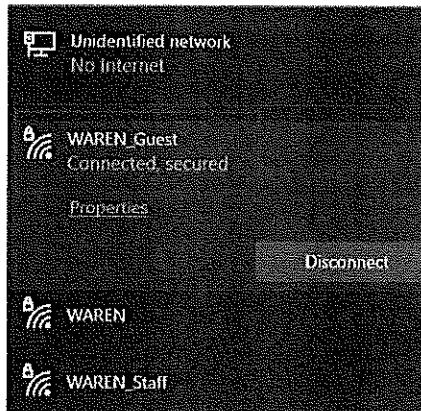
Sử dụng một thiết bị đầu cuối không dây bất kỳ để xác nhận rằng lúc này đã có hai SSID là “WAREN_Guest” và “WAREN_Staff” đã được broadcast (hình 15):



Hình 15 – Các SSID đã được broadcast.

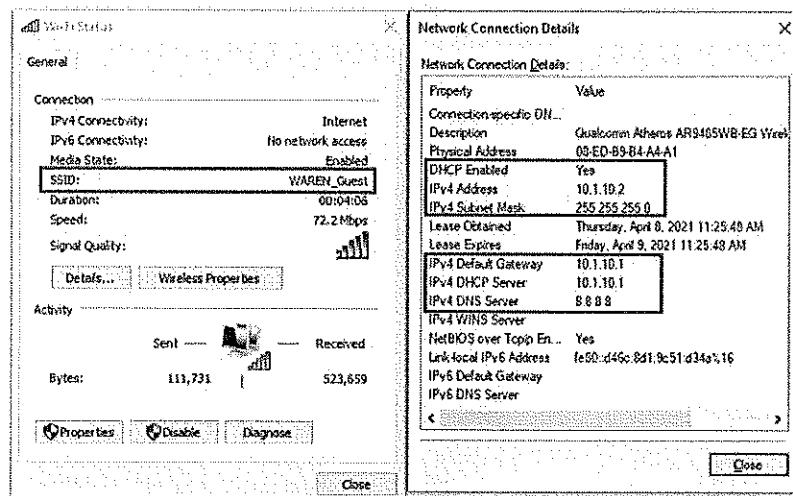
Chúng ta thực hiện kết nối lần lượt vào từng mạng Wifi này và truy nhập thử Internet để xác nhận rằng các SSID này đều hoạt động tốt.

Với SSID “WAREN_Guest”, sau khi click chọn và nhập password wifi “cisco123456”, thiết bị kết nối thành công (hình 16):



Hình 16 – Kết nối thành công đến “WAREN_Guest”.

Sau khi kết nối thành công, card mạng wifi của thiết bị đầu cuối đã nhận được đầy đủ cấu hình IP cho hoạt động truy nhập mạng (hình 17):



Hình 17 – Thông số IP trên card mạng Wifi của thiết bị đầu cuối.

Ta thấy, thiết bị đã được cấp phát đầy đủ cấu hình IP của VLAN 10 trên hệ thống. Với cấu hình IP này, thiết bị có thể thông qua VLAN 10 truy nhập Internet thành công:

```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=41ms TTL=115
Reply from 8.8.8.8: bytes=32 time=61ms TTL=115
```

```
Reply from 8.8.8.8: bytes=32 time=35ms TTL=115
Reply from 8.8.8.8: bytes=32 time=34ms TTL=115
```

Ping statistics for 8.8.8.8:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 34ms, Maximum = 61ms, Average = 42ms
```

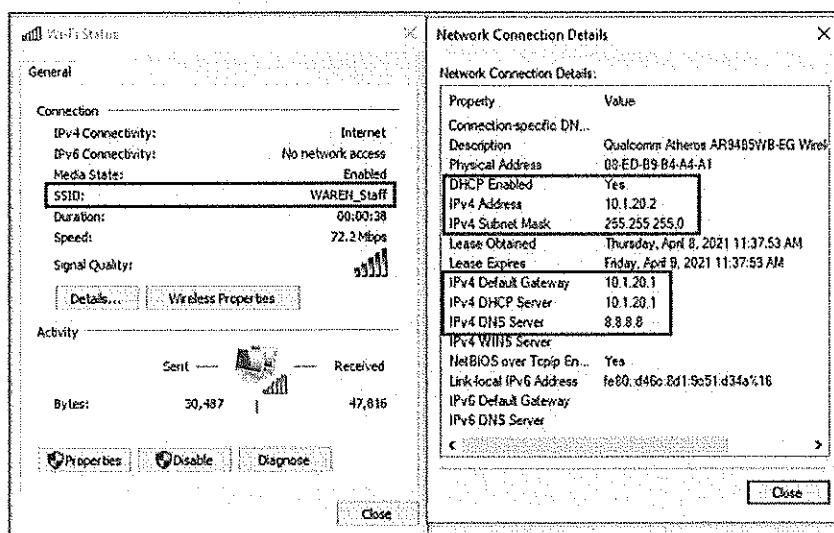
Truy nhập web trên Internet với SSID “WAREN_Guest” (hình 18):



Hình 18 – Truy nhập web thành công với SSID “WAREN_Guest”.

Đến đây, ta đã hoàn tất kiểm tra hoạt động của SSID “WAREN_Guest”.

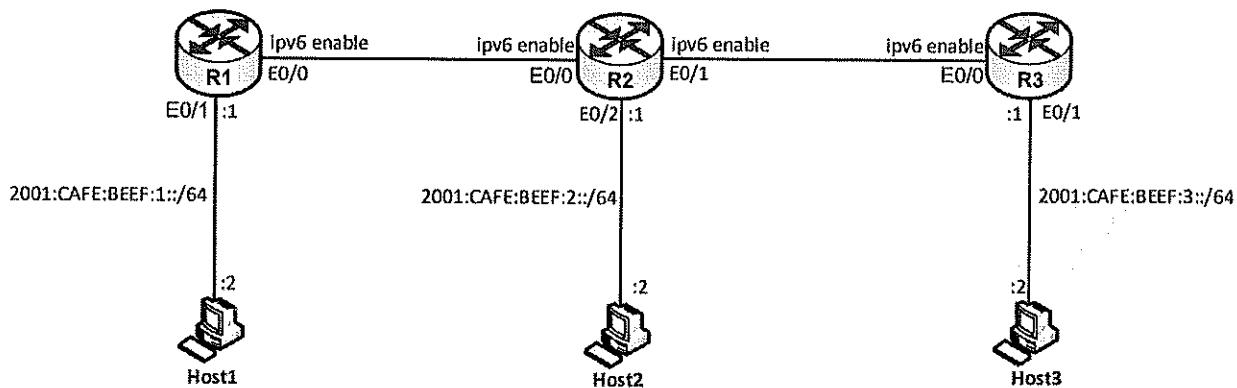
Các bạn học viên có thể thực hiện kiểm tra tương tự với SSID “WAREN_Staff” gồm truy nhập với key bảo mật đúng, card mạng tiếp nhận được cấu hình IP của VLAN 20 và truy nhập mạng thành công. Nếu kiểm tra đạt được giống như trên, chúng ta đã cấu hình thành công cho SSID này. Hình 19 ở dưới cho thấy thiết bị đầu cuối đã kết nối thành công đến mạng WAREN_Staff và nhận được cấu hình IP của VLAN 20:



Hình 19 – Cấu hình IP trên card mạng Wifi khi tham gia SSID “WAREN_Staff”.

Lab 23 – IPv6 – Bài số 1

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Sơ đồ bài lab gồm các thiết bị được kết nối với nhau như trên sơ đồ hình 1. Trong đó, các router chạy hệ điều hành IOL, các host là các VPC tích hợp sẵn trên EVE.
- Trên bài lab này, các bạn học viên sẽ thực tập cấu hình địa chỉ IPv6 trên các thiết bị và thiết lập static routing để các IPv6 LAN đi đến nhau được.
- Các thiết bị đều đã được cấu hình sẵn hostname, các bạn không cần thiết lập lại thông số này.

Yêu cầu:

1. Cấu hình đặt địa chỉ IPv6:

- Trên các cổng đầu nối lẫn nhau giữa các router thực hiện bật IPv6 như được chỉ ra trên hình 1.
- Bên cạnh đó, thực hiện cấu hình các địa chỉ IPv6 Global trên các cổng router và các host như được chỉ ra trên sơ đồ bài lab. Các host đóng vai trò như các user của các mạng LAN trên từng router.

2. Cấu hình Static routing:

- Thực hiện cấu hình static routing trên các router đảm bảo các mạng LAN của các router có thể thấy được nhau.
- Việc kiểm tra được thực hiện bằng cách ping lẫn nhau giữa các host trên sơ đồ.

Thực hiện:

1. Cấu hình đặt địa chỉ IPv6:

Cấu hình:

Trên R1:

```
R1(config)#ipv6 unicast-routing
R1(config)#interface e0/0
R1(config-if)#no shutdown
R1(config-if)#ipv6 enable
R1(config-if)#exit
R1(config)#interface e0/1
R1(config-if)#no shutdown
R1(config-if)#ipv6 address 2001:cafe:beef:1::1/64
R1(config-if)#exit
```

Trên R2:

```
R2(config)#ipv6 unicast-routing
R2(config)#interface range e0/0 - 1
R2(config-if-range)#no shutdown
R2(config-if-range)#ipv6 enable
R2(config-if-range)#exit
R2(config)#interface e0/2
R2(config-if)#no shutdown
R2(config-if)#ipv6 address 2001:cafe:beef:2::1/64
R2(config-if)#exit
```

Trên R3:

```
R3(config)#ipv6 unicast-routing
R3(config)#interface e0/0
R3(config-if)#no shutdown
R3(config-if)#ipv6 enable
R3(config-if)#exit
R3(config)#interface e0/1
R3(config-if)#no shutdown
R3(config-if)#ipv6 address 2001:cafe:beef:3::1/64
R3(config-if)#exit
```

Trên Host1:

```
Host1> ip 2001:cafe:beef:1::2/64
PC1 : 2001:cafe:beef:1::2/64
```

Trên Host2:

```
Host2> ip 2001:cafe:beef:2::2/64
PC1 : 2001:cafe:beef:2::2/64
```

Trên Host3:

```
Host3> ip 2001:cafe:beef:3::2/64
PC1 : 2001:cafe:beef:3::2/64
```

Kiểm tra:

Ta kiểm tra rằng các địa chỉ IPv6 đã được thiết lập đầy đủ trên các router.

Trên R1:

```
R1#show ipv6 interface brief
Ethernet0/0          [up/up]
    FE80::A8BB:CCFF:FE00:1000
Ethernet0/1          [up/up]
    FE80::A8BB:CCFF:FE00:1010
    2001:CAFE:BEEF:1::1
Ethernet0/2          [administratively down/down]
    unassigned
Ethernet0/3          [administratively down/down]
    unassigned
```

Trên R2:

```
R2#show ipv6 interface brief
Ethernet0/0          [up/up]
    FE80::A8BB:CCFF:FE00:2000
Ethernet0/1          [up/up]
    FE80::A8BB:CCFF:FE00:2010
Ethernet0/2          [up/up]
    FE80::A8BB:CCFF:FE00:2020
    2001:CAFE:BEEF:2::1
Ethernet0/3          [administratively down/down]
    unassigned
```

Trên R3:

```
R3#show ipv6 interface brief
Ethernet0/0          [up/up]
    FE80::A8BB:CCFF:FE00:3000
Ethernet0/1          [up/up]
    FE80::A8BB:CCFF:FE00:3010
    2001:CAFE:BEEF:3::1
Ethernet0/2          [administratively down/down]
    unassigned
Ethernet0/3          [administratively down/down]
    unassigned
```

Trên các link đầu nối giữa các router, chúng ta không đặt địa chỉ IP cụ thể mà chỉ sử dụng lệnh “`ipv6 enable`”. Lệnh này sẽ bật IPv6 và phát sinh một địa chỉ Link – local trên cổng theo luật EUI – 64. Ta có thể kiểm tra điều này trên một cổng, ví dụ, E0/0 của R1:

```
R1#show interfaces e0/0 | inc bia
  Hardware is AmdP2, address is aabb.cc00.1000 (bia aabb.cc00.1000)
R1#show ipv6 interface brief e0/0
Ethernet0/0      [up/up]
  FE80::A8BB:CCFF:FE00:1000
```

Từ kết quả show, chúng ta có thể thấy rằng địa chỉ Link local trên cổng E0/0 được tạo thành từ địa chỉ MAC trên cổng này:

- Địa chỉ MAC “aabb.cc00.1000” được đảo bit thứ 7 trở thành “a8bb.cc00.1000”.
- Dãy “ffffe” được chèn vào giữa: “a8bb.cc~~ffff~~e00.1000”.
- Kết hợp với prefix “fe80”, chúng ta thu được địa chỉ IPv6 như trên kết quả show: “fe80::a8bb:ccff:fe00:1000”.

Trên các host:

```
Host1> show ipv6
NAME          : Host1[1]
LINK-LOCAL SCOPE : fe80::250:79ff:fe66:6804/64
GLOBAL SCOPE    : 2001:cafe:beef:1::2/64
DNS           :
ROUTER LINK-LAYER : aa:bb:cc:00:10:10
MAC            : 00:50:79:66:68:04
LPORT          : 20000
RHOST:PORT     : 127.0.0.1:30000
MTU:           : 1500

Host2> show ipv6
NAME          : Host2[1]
LINK-LOCAL SCOPE : fe80::250:79ff:fe66:6805/64
GLOBAL SCOPE    : 2001:cafe:beef:2::2/64
DNS           :
ROUTER LINK-LAYER : aa:bb:cc:00:20:20
MAC            : 00:50:79:66:68:05
LPORT          : 20000
RHOST:PORT     : 127.0.0.1:30000
MTU:           : 1500

Host3> show ipv6
NAME          : Host3[1]
LINK-LOCAL SCOPE : fe80::250:79ff:fe66:6806/64
GLOBAL SCOPE    : 2001:cafe:beef:3::3/64
DNS           :
ROUTER LINK-LAYER : aa:bb:cc:00:30:10
MAC            : 00:50:79:66:68:06
LPORT          : 20000
RHOST:PORT     : 127.0.0.1:30000
MTU:           : 1500
```

Trên mỗi host, chúng ta thấy rằng bên cạnh địa chỉ Global unicast đã được cấu hình tĩnh, một địa chỉ link-local cũng đã được phát sinh trên card mạng của host theo luật EUI – 64.

Ngoài ra, các host đều cập nhật được địa chỉ MAC của router default – gateway của mình; điều này xảy ra là do các host nhận được bản tin *RA (Router Advertisement)* từ các router, bản tin này mang theo thông tin địa chỉ MAC trên cổng mạng của router và IPv6 prefix đang được sử dụng trên cổng ấy.

Chúng ta tiếp tục kiểm tra rằng các đường link đã được thông suốt IP.

R1 và R2:

```
R1#ping FE80::A8BB:CCFF:FE00:2000 <- Địa chỉ link-local của cổng E0/0 trên R2
Output Interface: Ethernet0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::A8BB:CCFF:FE00:2000, timeout is 2 seconds:
Packet sent with a source address of FE80::A8BB:CCFF:FE00:1000%Ethernet0/0
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/15 ms
```

Lưu ý rằng, khi thực hiện ping kiểm tra với địa chỉ link – local, ta cần chỉ ra Output interface của các gói tin ping vì một địa chỉ link – local chỉ giới hạn phạm vi trên một đường link và có thể được sử dụng đồng thời trên nhiều link khác nhau. Khi chỉ ra Output Interface, chúng ta phải ghi tường minh tên cổng, không được viết tắt (ví dụ ở trên là “Ethernet0/0”, không được viết là “E0/0”).

R2 và R3:

```
R2#ping FE80::A8BB:CCFF:FE00:3000 <- Địa chỉ link-local của cổng E0/0 trên R3
Output Interface: Ethernet0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::A8BB:CCFF:FE00:3000, timeout is 2 seconds:
Packet sent with a source address of FE80::A8BB:CCFF:FE00:2010%Ethernet0/1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Từ các host có thể ping lên được các router gateway:

```
Host1> ping 2001:cafe:beef:1::1
2001:cafe:beef:1::1 icmp6_seq=1 ttl=64 time=0.877 ms
2001:cafe:beef:1::1 icmp6_seq=2 ttl=64 time=0.943 ms

Host2> ping 2001:cafe:beef:2::1
2001:cafe:beef:2::1 icmp6_seq=1 ttl=64 time=1.035 ms
2001:cafe:beef:2::1 icmp6_seq=2 ttl=64 time=0.857 ms

Host3> ping 2001:cafe:beef:3::1
2001:cafe:beef:3::1 icmp6_seq=1 ttl=64 time=1.545 ms
2001:cafe:beef:3::1 icmp6_seq=2 ttl=64 time=1.093 ms
```

Ta cũng có thể kiểm tra rằng từ các host có thể ping bằng địa chỉ link – local đến được các router:

```
Host1> ping FE80::A8BB:CCFF:FE00:1010 <- Địa chỉ link-local của cổng E0/1 trên R1
FE80::A8BB:CCFF:FE00:1010 icmp6_seq=1 ttl=64 time=12.603 ms
FE80::A8BB:CCFF:FE00:1010 icmp6_seq=2 ttl=64 time=0.509 ms

Host2> ping FE80::A8BB:CCFF:FE00:2020 <- Địa chỉ link-local của cổng E0/2 trên R2
FE80::A8BB:CCFF:FE00:2020 icmp6_seq=1 ttl=64 time=8.297 ms
FE80::A8BB:CCFF:FE00:2020 icmp6_seq=2 ttl=64 time=1.087 ms
```

```
Host3> ping FE80::A8BB:CCFF:FE00:3010 <- Địa chỉ link-local của cổng E0/1 trên R3
FE80::A8BB:CCFF:FE00:3010 icmp6_seq=1 ttl=64 time=10.578 ms
FE80::A8BB:CCFF:FE00:3010 icmp6_seq=2 ttl=64 time=0.549 ms
```

Đến đây, chúng ta đã hoàn thành yêu cầu về cấu hình địa chỉ IPv6 trên các cổng và kiểm tra tính thông suốt của các kết nối IP, kể cả sử dụng địa chỉ link – local hay global.

2. Cấu hình static routing:

Cấu hình:

Trên R1:

```
R1(config)#ipv6 route 2001:cafe:beef:2::/64 e0/0 FE80::A8BB:CCFF:FE00:2000
R1(config)#ipv6 route 2001:cafe:beef:3::/64 e0/0 FE80::A8BB:CCFF:FE00:2000
```

Trên R2:

```
R2(config)#ipv6 route 2001:cafe:beef:1::/64 e0/0 FE80::A8BB:CCFF:FE00:1000
R2(config)#ipv6 route 2001:cafe:beef:3::/64 e0/1 FE80::A8BB:CCFF:FE00:3000
```

Trên R3:

```
R3(config)#ipv6 route 2001:cafe:beef:1::/64 e0/0 FE80::A8BB:CCFF:FE00:2010
R3(config)#ipv6 route 2001:cafe:beef:2::/64 e0/0 FE80::A8BB:CCFF:FE00:2010
```

Ghi chú:

Giống như với IPv4 static routing, để đưa một route tĩnh vào bảng định tuyến IPv6, chúng ta cũng sử dụng câu lệnh: “`ipv6 route...`” (điểm khác biệt là sử dụng từ khóa “`ipv6`” thay cho “`ip`” và destination network được chỉ ra là một địa chỉ mạng IPv6). Trong trường hợp bài lab của chúng ta, vì các link đầu nối giữa các router chỉ sử dụng các địa chỉ link – local nên next – hop IP là địa chỉ link – local của router láng giềng; tuy nhiên, do một địa chỉ link – local có thể được sử dụng trên nhiều interface (vì phạm vi hoạt động của nó chỉ là trên một đường link) nên ta cần phải chỉ thêm output interface trong các lệnh static route để xác định rõ next – hop IP đó nằm ở phía interface nào. Các lệnh cấu hình static route đã thực hiện đều sử dụng cả hai tham số output – interface và next – hop – IP trong câu lệnh.

Kiểm tra:

Ta kiểm tra bảng định tuyến của các router:

```
R1#show ipv6 route static
(...)
S 2001:CAFE:BEEF:2::/64 [1/0]
    via FE80::A8BB:CCFF:FE00:2000, Ethernet0/0
S 2001:CAFE:BEEF:3::/64 [1/0]
    via FE80::A8BB:CCFF:FE00:2000, Ethernet0/0

R2#show ipv6 route static
(...)
S 2001:CAFE:BEEF:1::/64 [1/0]
    via FE80::A8BB:CCFF:FE00:1000, Ethernet0/0
S 2001:CAFE:BEEF:3::/64 [1/0]
    via FE80::A8BB:CCFF:FE00:3000, Ethernet0/1
```

```
R3#show ipv6 route static
(...)
S 2001:CAFE:BEEF:1::/64 [1/0]
    via FE80::A8BB:CCFF:FE00:2010, Ethernet0/0
S 2001:CAFE:BEEF:2::/64 [1/0]
    via FE80::A8BB:CCFF:FE00:2010, Ethernet0/0
```

Các host trên các mạng LAN lúc này đã có thể đi đến nhau được:

```
Host1> ping 2001:cafe:beef:2::2
2001:cafe:beef:2::2 icmp6_seq=1 ttl=60 time=20.885 ms
2001:cafe:beef:2::2 icmp6_seq=2 ttl=60 time=2.622 ms

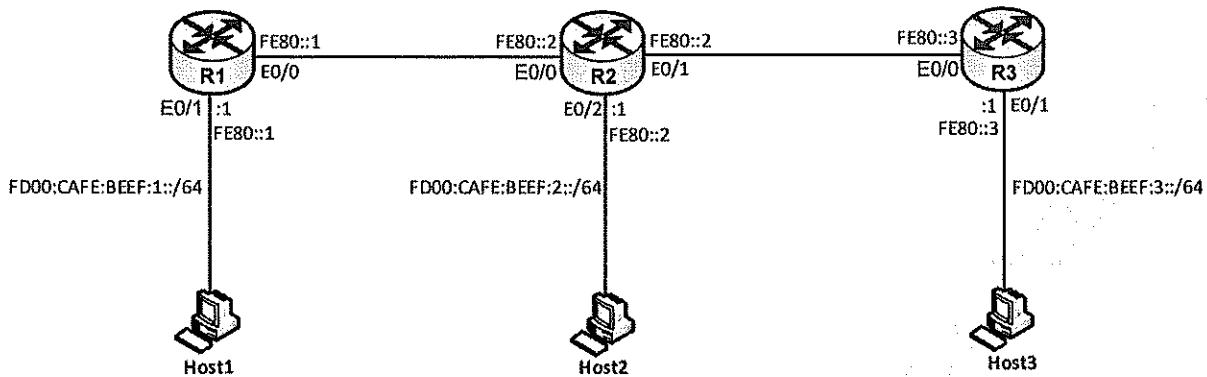
Host1> ping 2001:cafe:beef:3::2
2001:cafe:beef:3::2 icmp6_seq=1 ttl=58 time=13.695 ms
2001:cafe:beef:3::2 icmp6_seq=2 ttl=58 time=2.581 ms

Host2> ping 2001:cafe:beef:3::2
2001:cafe:beef:3::2 icmp6_seq=1 ttl=60 time=1.230 ms
2001:cafe:beef:3::2 icmp6_seq=2 ttl=60 time=2.781 ms
```

Đến đây, chúng ta đã hoàn thành các yêu cầu đặt ra của bài lab.

Lab 24 – IPv6 – Bài số 2

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Sơ đồ bài lab gồm các thiết bị được kết nối với nhau như trên sơ đồ hình 1. Trong đó, các router chạy hệ điều hành IOL, các host là các VPC tích hợp sẵn trên EVE.
- Trên bài lab này, các bạn học viên sẽ thực tập cấu hình địa chỉ IPv6 trên các thiết bị và cấu hình định tuyến với các giao thức RIPng, OSPFv3 để các IPv6 LAN có thể đi đến nhau được.
- Các thiết bị đều đã được cấu hình sẵn hostname, các bạn không cần thiết lập lại thông số này.

Yêu cầu:

1. Cấu hình đặt địa chỉ IPv6:

- Trên các router, thực hiện cấu hình đặt địa chỉ IPv6 trên các cổng như được chỉ ra trên sơ đồ hình 1. Lưu ý rằng, các router chuyển đổi các địa chỉ link – local trên các cổng thành định dạng FE80::x, trong đó, x là số hiệu của router.
- Trên các host, thực hiện cấu hình để chúng có thể nhận được IP theo quy hoạch IP trên sơ đồ bằng phương thức SLAAC.

2. RIPng:

Cấu hình định tuyến RIPng trên các router đảm bảo các mạng LAN của các router có thể đi đến nhau được.

3. OSPFv3:

- Gỡ bỏ cấu hình RIPng đã thực hiện ở bước 2.
- Cấu hình định tuyến OSPFv3 đảm bảo các mạng LAN trên các router có thể đi đến nhau được.

Thực hiện:**1. Cấu hình đặt địa chỉ IPv6:****Cấu hình:**

Trên R1:

```
R1(config)#ipv6 unicast-routing
R1(config)#interface range e0/0 - 1
R1(config-if-range)#no shutdown
R1(config-if-range)#ipv6 address fe80::1 link-local
R1(config-if-range)#exit
R1(config)#interface e0/1
R1(config-if)#ipv6 address fd00:cafe:beef:1::1/64
R1(config-if)#exit
```

Trên R2:

```
R2(config)#ipv6 unicast-routing
R2(config)#interface range e0/0 - 2
R2(config-if-range)#no shutdown
R2(config-if-range)#ipv6 address fe80::2 link-local
R2(config-if-range)#exit
R2(config)#interface e0/2
R2(config-if)#ipv6 address fd00:cafe:beef:2::1/64
R2(config-if)#exit
```

Trên R3:

```
R3(config)#ipv6 unicast-routing
R3(config)#interface range e0/0 - 1
R3(config-if-range)#no shutdown
R3(config-if-range)#ipv6 address fe80::3 link-local
R3(config-if-range)#exit
R3(config)#interface e0/1
R3(config-if)#ipv6 address fd00:cafe:beef:3::1/64
R3(config-if)#exit
```

Trên Host1:

```
Host1> ip auto
GLOBAL SCOPE      : fd00:cafe:beef:1:2050:79ff:fe66:6804/64
ROUTER LINK-LAYER : aa:bb:cc:00:10:10
```

Trên Host2:

```
Host2> ip auto
GLOBAL SCOPE      : fd00:cafe:beef:2:2050:79ff:fe66:6805/64
ROUTER LINK-LAYER : aa:bb:cc:00:20:20
```

Trên Host3:

```
Host3> ip auto
GLOBAL SCOPE      : fd00:cafe:beef:3:2050:79ff:fe66:6806/64
ROUTER LINK-LAYER : aa:bb:cc:00:30:10
```

Ghi chú:

Ta có thể thay đổi địa chỉ link – local mặc định trên các cổng router thành định dạng dễ dàng hơn cho việc quản lý của chúng ta bằng cách lên cổng router sử dụng lệnh:

```
R(config-if)#ipv6 address Địa chỉ_link_local_mới link-local
```

Lưu ý rằng, địa chỉ mới chúng ta đặt trên cổng vẫn phải nằm trong dải IP quy ước dành cho địa chỉ link local “FE80::/10”. Ngoài ra, trong câu lệnh, chúng ta không được quên tùy chọn “link-local” ở cuối câu lệnh.

Mặt khác, vì địa chỉ link – local chỉ có tác dụng trên phạm vi một đường link nên cùng một địa chỉ link – local chúng ta có thể đặt trên đồng thời nhiều cổng của router.

Trên VPC host của EVE, để cấu hình host nhận IP tự động từ cơ chế *SLAAC (StateLess Address Auto Configuration)*, chúng ta sử dụng lệnh “VPC>ip auto”. Lúc này, host sẽ dựa vào IPv6 prefix được cung cấp từ bản tin RA của router để tự phát sinh ra địa chỉ IPv6 trên cổng theo luật EUI – 64. Bên cạnh đó, host cũng cập nhật được địa chỉ MAC của router để phục vụ cho hoạt động gửi dữ liệu đến các subnet khác.

Kiểm tra:

Chúng ta kiểm tra rằng các router đã được đặt địa chỉ IPv6 như yêu cầu đặt ra:

```
R1#show ipv6 interface brief
Ethernet0/0          [up/up]
  FE80::1
Ethernet0/1          [up/up]
  FE80::1
  FD00:CAFE:BEEF:1::1
Ethernet0/2          [administratively down/down]
  unassigned
Ethernet0/3          [administratively down/down]
  unassigned

R2#show ipv6 interface brief
Ethernet0/0          [up/up]
  FE80::2
Ethernet0/1          [up/up]
  FE80::2
Ethernet0/2          [up/up]
  FE80::2
  FD00:CAFE:BEEF:2::1
Ethernet0/3          [administratively down/down]
  unassigned

R3#show ipv6 interface brief
Ethernet0/0          [up/up]
  FE80::3
```

Ethernet0/1	[up/up]
FE80::3	
FD00:CAFE:BEEF:3::1	
Ethernet0/2	[administratively down/down]
unassigned	
Ethernet0/3	[administratively down/down]
unassigned	

Trên các host:

Host1> show ipv6	
NAME	: Host1[1]
LINK-LOCAL SCOPE	: fe80::250:79ff:fe66:6804/64
GLOBAL SCOPE	: fd00:cafe:beef:1:2050:79ff:fe66:6804/64
DNS	:
ROUTER LINK-LAYER	: aa:bb:cc:00:10:10
MAC	: 00:50:79:66:68:04
LPORT	: 20000
RHOST:PORT	: 127.0.0.1:30000
MTU:	: 1500
Host2> show ipv6	
NAME	: Host2[1]
LINK-LOCAL SCOPE	: fe80::250:79ff:fe66:6805/64
GLOBAL SCOPE	: fd00:cafe:beef:2:2050:79ff:fe66:6805/64
DNS	:
ROUTER LINK-LAYER	: aa:bb:cc:00:20:20
MAC	: 00:50:79:66:68:05
LPORT	: 20000
RHOST:PORT	: 127.0.0.1:30000
MTU:	: 1500
Host3> show ipv6	
NAME	: Host3[1]
LINK-LOCAL SCOPE	: fe80::250:79ff:fe66:6806/64
GLOBAL SCOPE	: fd00:cafe:beef:3:2050:79ff:fe66:6806/64
DNS	:
ROUTER LINK-LAYER	: aa:bb:cc:00:30:10
MAC	: 00:50:79:66:68:06
LPORT	: 20000
RHOST:PORT	: 127.0.0.1:30000
MTU:	: 1500

Ta kiểm tra rằng các link đầu nối giữa các router đã thông suốt IPv6:

```
R1#ping fe80::2 <- Kiểm tra link giữa R1 và R2
Output Interface: Ethernet0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::2, timeout is 2 seconds:
Packet sent with a source address of FE80::1%Ethernet0/0
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/20 ms
```

```
R2#ping fe80::3 <- Kiểm tra link giữa R2 và R3
Output Interface: Ethernet0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::3, timeout is 2 seconds:
Packet sent with a source address of FE80::2%Ethernet0/1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/21 ms
```

Ping kiểm tra giữa các host và gateway của chúng:

```
Host1> ping fd00:cafe:beef:1::1
fd00:cafe:beef:1::1 icmp6_seq=1 ttl=64 time=0.830 ms
fd00:cafe:beef:1::1 icmp6_seq=2 ttl=64 time=0.974 ms

Host2> ping fd00:cafe:beef:2::1
fd00:cafe:beef:2::1 icmp6_seq=1 ttl=64 time=0.336 ms
fd00:cafe:beef:2::1 icmp6_seq=2 ttl=64 time=1.093 ms

Host3> ping fd00:cafe:beef:3::1
fd00:cafe:beef:3::1 icmp6_seq=1 ttl=64 time=0.418 ms
fd00:cafe:beef:3::1 icmp6_seq=2 ttl=64 time=0.549 ms
```

2. Cấu hình định tuyến RIPng:

Cấu hình:

Ta thực hiện bật định tuyến RIPng trên các router:

```
R1(config)#interface range e0/0 - 1
R1(config-if-range)#ipv6 rip RIPNG enable
R1(config-if-range)#exit

R2(config)#interface range e0/0 - 2
R2(config-if-range)#ipv6 rip RIPNG enable
R2(config-if-range)#exit

R3(config)#interface range e0/0 - 1
R3(config-if-range)#ipv6 rip RIPNG enable
R3(config-if-range)#exit
```

Ghi chú:

Khác với cấu hình định tuyến RIPv2 đã thực hành trong các bài lab định tuyến cho địa chỉ IPv4, khi cấu hình RIPng, chúng ta thực hiện bật tường minh giao thức trên từng cổng của router mà không phải sử dụng lệnh “network”. Câu lệnh để enable định tuyến RIPng trên một cổng của router:

```
R(config-if)#ipv6 rip Tên_của_tiến_trình_RIPng enable
```

Một điểm khác biệt của cấu hình RIPng so với RIPv2 là tiến trình RIPng trên router cần phải có một tên gọi định danh; tên định danh này chỉ có ý nghĩa nội bộ trong một router và có thể khác nhau từ router này qua router khác. Trong bài lab này, để tiện cho việc theo dõi, chúng ta sử dụng chung một tên gọi cho các tiến trình RIPng trên các router là “RIPNG”.

RIPng hoàn toàn giống với RIPv2 trên mọi phương diện (cũng vẫn là giao thức Distance – vector, vẫn sử dụng các timer, các quy tắc chống loop giống hệt,...), ngoại trừ là sử dụng để định tuyến cho địa chỉ IPv6.

Kiểm tra:

Chúng ta kiểm tra rằng định tuyến đã hội tụ đầy đủ trên các router:

```
R1#show ipv6 route rip
(...)
R    FD00:CAFE:BEEF:2::/64 [120/2]
      via FE80::2, Ethernet0/0
R    FD00:CAFE:BEEF:3::/64 [120/3]
      via FE80::2, Ethernet0/0

R2#show ipv6 route rip
(...)
R    FD00:CAFE:BEEF:1::/64 [120/2]
      via FE80::1, Ethernet0/0
R    FD00:CAFE:BEEF:3::/64 [120/2]
      via FE80::3, Ethernet0/1

R3#show ipv6 route rip
(...)
R    FD00:CAFE:BEEF:1::/64 [120/3]
      via FE80::2, Ethernet0/0
R    FD00:CAFE:BEEF:2::/64 [120/2]
      via FE80::2, Ethernet0/0
```

Kết quả show cho thấy mỗi router đều đã học được thông tin đầy đủ về các mạng LAN của các router khác. Một điểm cần lưu ý là mỗi route trong bảng định tuyến đều sử dụng *Next – hop – IP là địa chỉ link – local của router láng giềng* mà không sử dụng loại địa chỉ khác (unique – local, global). Trong bài lab này, chúng ta không sử dụng các địa chỉ unique – local và global trên các link đầu nối giữa các router, nhưng nếu sử dụng thì các địa chỉ loại này cũng sẽ không được dùng làm next – hop – IP trong các route được xây dựng bởi các giao thức định tuyến.

Các host thuộc các mạng LAN khác nhau đã có thể đi đến nhau được:

```
Host1> ping fd00:cafe:bef:2:2050:79ff:fe66:6805 <- Host1 ping Host2
fd00:cafe:bef:2:2050:79ff:fe66:6805 icmp6_seq=1 ttl=60 time=20.814 ms
fd00:cafe:bef:2:2050:79ff:fe66:6805 icmp6_seq=2 ttl=60 time=2.741 ms
Host1> ping fd00:cafe:bef:3:2050:79ff:fe66:6806 <- Host1 ping Host3
fd00:cafe:bef:3:2050:79ff:fe66:6806 icmp6_seq=1 ttl=58 time=10.467 ms
fd00:cafe:bef:3:2050:79ff:fe66:6806 icmp6_seq=2 ttl=58 time=3.337 ms
Host2> ping fd00:cafe:bef:3:2050:79ff:fe66:6806 <- Host2 ping Host3
fd00:cafe:bef:3:2050:79ff:fe66:6806 icmp6_seq=1 ttl=60 time=3.606 ms
fd00:cafe:bef:3:2050:79ff:fe66:6806 icmp6_seq=2 ttl=60 time=2.607 ms
```

Đến đây, chúng ta đã hoàn thành cấu hình giao thức định tuyến RIPng cho các router.

3. Cấu hình định tuyến OSPFv3:**Cấu hình:**

Trước hết, chúng ta gỡ bỏ cấu hình RIPng đã cấu hình ở bước trên:

```
R1-2-3(config)#no ipv6 router rip RIPNG
```

Tiếp theo, chúng ta thực hiện cấu hình OSPFv3 trên các router.

Trên R1:

```
R1(config)#router ospfv3 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#exit
R1(config)#interface range e0/0 - 1
R1(config-if-range)#ospfv3 1 ipv6 area 0
R1(config-if-range)#exit
```

Trên R2:

```
R2(config)#router ospfv3 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#exit
R2(config)#interface range e0/0 - 2
R2(config-if-range)#ospfv3 1 ipv6 area 0
R2(config-if-range)#exit
```

Trên R3:

```
R3(config)#router ospfv3 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#exit
R3(config)#interface range e0/0 - 1
R3(config-if-range)#ospfv3 1 ipv6 area 0
R3(config-if-range)#exit
```

Ghi chú:

OSPFv3 là version tiếp theo của OSPF. Tuy là version kế tiếp nhưng OSPFv3 không tương thích với OSPFv2 được dùng phổ biến từ trước đến giờ. OSPFv2 chỉ có thể định tuyến cho địa chỉ IPv4 nhưng OSPFv3 có thể định tuyến được cho cả địa chỉ IPv4 và địa chỉ IPv6. OSPFv2 sử dụng nền tảng truyền tải cho các gói tin OSPF trao đổi giữa các router là IPv4, OSPFv3 sử dụng nền tảng truyền tải cho các gói tin OSPF là IPv6; do đó, để chạy định tuyến OSPFv3, trước hết chúng ta phải có một hệ thống mạng chạy IPv6.

Giống như OSPFv2, các router chạy OSPFv3 cũng cần phải thiết lập một giá trị dùng để định danh duy nhất cho router trong cộng đồng các router chạy OSPF, đó là giá trị *Router – ID*. Router – ID của router chạy OSPFv3 cũng vẫn sử dụng định dạng của một địa chỉ IPv4 và mặc định sẽ được router thiết lập là địa chỉ IPv4 cao nhất trong các interface đang active, ưu tiên cổng loopback. Do đó, nếu sơ đồ mạng chạy Dual – stack, có cả địa chỉ IPv4 và IPv6 thì router sẽ xây dựng được router – id dựa trên địa chỉ IPv4 có sẵn, nhưng nếu sơ đồ mạng thuần túy IPv6 (như sơ đồ lab đang thực hiện) thì router sẽ không thể có được router – id và OSPFv3 sẽ không chạy. Vì vậy, trong trường hợp này, chúng ta cần cấu hình tĩnh giá trị router – id cho các router:

```
R(config)#router ospfv3 Process-ID
R(config-router)#router-id A.B.C.D
```

Trong bài lab này, ta quy ước R1, R2, R3 có router – id lần lượt là 1.1.1.1, 2.2.2.2, 3.3.3.3.

Việc enable OSPFv3 cũng không còn sử dụng lệnh “network” như với OSPFv2 mà thao tác này được thực hiện một cách tương tự trên từng cổng của router bằng lệnh:

```
R(config-if)#ospfv3 process-id ipv6 enable
```

Nếu trên mạng có sử dụng cả địa chỉ IPv4 nữa thì chúng ta cũng có thể bật cả định tuyến OSPFv3 cho IPv4:

```
R(config-if)#ospfv3 process-id ipv4 enable
```

Lưu ý rằng, dù chạy định tuyến cho loại địa chỉ nào thì trên mạng vẫn cần phải được cấu hình IPv6 để truyền tải cho OSPFv3.

Về tổng thể, nhìn chung OSPFv3 sử dụng thuật toán và các khái niệm trong hoạt động rất giống với OSPFv2 (tất nhiên, về chi tiết, có nhiều điểm khác biệt), nên nếu đã quen với OSPFv2, các bạn học viên hoàn toàn có thể thao tác cơ bản được với OSPFv3.

Kiểm tra:

Các router đã thiết lập quan hệ láng giềng OSPFv3 với nhau:

```
R1#show ipv6 ospf neighbor
```

OSPFv3 Router with ID (1.1.1.1) (Process ID 1)

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
2.2.2.2	1	FULL/DR	00:00:35	3	Ethernet0/0

```
R2#show ipv6 ospf neighbor
```

OSPFv3 Router with ID (2.2.2.2) (Process ID 1)

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
3.3.3.3	1	FULL/BDR	00:00:33	3	Ethernet0/1
1.1.1.1	1	FULL/BDR	00:00:31	3	Ethernet0/0

```
R3#show ipv6 ospf neighbor
```

OSPFv3 Router with ID (3.3.3.3) (Process ID 1)

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
2.2.2.2	1	FULL/DR	00:00:36	4	Ethernet0/0

Chúng ta kiểm tra rằng các router đã cập nhật được đầy đủ thông tin định tuyến thông qua OSPFv3:

```
R1#show ipv6 route ospf
```

(...)

O	FD00:CAFE:BEEF:2::/64 [110/20]	via FE80::2, Ethernet0/0
O	FD00:CAFE:BEEF:3::/64 [110/30]	via FE80::2, Ethernet0/0

```
R2#show ipv6 route ospf
(...)
O  FD00:CAFE:BEEF:1::/64 [110/20]
    via FE80::1, Ethernet0/0
O  FD00:CAFE:BEEF:3::/64 [110/20]
    via FE80::3, Ethernet0/1

R3#show ipv6 route ospf
(...)
O  FD00:CAFE:BEEF:1::/64 [110/30]
    via FE80::2, Ethernet0/0
O  FD00:CAFE:BEEF:2::/64 [110/20]
    via FE80::2, Ethernet0/0
```

Các host thuộc các mạng LAN đã có thể đi đến nhau:

```
Host1> ping fd00:cafe:beef:2:2050:79ff:fe66:6805 <- Host1 ping Host2
fd00:cafe:beef:2:2050:79ff:fe66:6805 icmp6_seq=1 ttl=60 time=2.512 ms
fd00:cafe:beef:2:2050:79ff:fe66:6805 icmp6_seq=2 ttl=60 time=1.917 ms

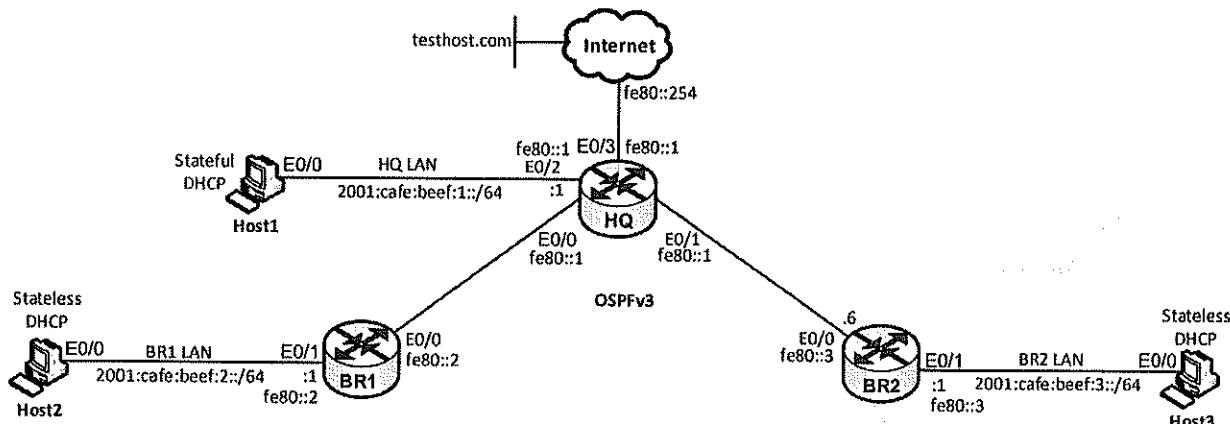
Host1> ping fd00:cafe:beef:3:2050:79ff:fe66:6806 <- Host1 ping Host3
fd00:cafe:beef:3:2050:79ff:fe66:6806 icmp6_seq=1 ttl=58 time=1.248 ms
fd00:cafe:beef:3:2050:79ff:fe66:6806 icmp6_seq=2 ttl=58 time=2.209 ms

Host2> ping fd00:cafe:beef:3:2050:79ff:fe66:6806 <- Host2 ping Host3
fd00:cafe:beef:3:2050:79ff:fe66:6806 icmp6_seq=1 ttl=60 time=0.933 ms
fd00:cafe:beef:3:2050:79ff:fe66:6806 icmp6_seq=2 ttl=60 time=12.774 ms
```

Đến đây, chúng ta đã hoàn thành cấu hình OSPFv3 và hoàn tất các yêu cầu đặt ra của bài lab.

Lab 25 – IPv6 – Bài số 3

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Sơ đồ bài lab gồm các thiết bị được kết nối với nhau như trên sơ đồ hình 1. Trong đó: tất cả các thiết bị đều là các router chạy hệ điều hành IOL (các host được giả lập bởi các router).
- Trên sơ đồ này, các bạn học viên sẽ thực hành cấu hình thiết lập địa chỉ IPv6 trên các router, chạy định tuyến OSPFv3 và cấu hình để các host nhận IPv6 bằng các phương thức Stateful DHCP và Stateless DHCP.
- Các thiết bị đều đã được đặt sẵn hostname, các bạn không cần phải thiết lập lại thông số này. Ngoài ra, các bạn học viên không can thiệp vào cấu hình của thiết bị giả lập Internet trong suốt quá trình thực hiện bài lab.

Yêu cầu:

1. Cấu hình địa chỉ IPv6:

- Trên các router, thực hiện cấu hình địa chỉ IPv6 global như được chỉ ra trên hình 1.
- Bên cạnh đó, thực hiện cấu hình địa chỉ link – local trên các cổng của các router này theo định dạng FE80::x (trong đó, với HQ, x = 1; với BR1, x = 2 và với BR2, x = 3).

2. Cấu hình định tuyến:

- Thực hiện cấu hình giao thức định tuyến OSPFv3 trên các router đảm bảo mọi địa chỉ global trên sơ đồ có thể đi đến nhau được.
- Bên cạnh đó, thực hiện cấu hình một static default – route trên router HQ trỏ về hướng Gateway Internet và cấu hình để OSPFv3 lan truyền default – route này đến các router BR1 và BR2.

3. Cấu hình DHCPv6:

- Cấu hình router HQ đảm nhận vai trò DHCPv6 để cấp phát cấu hình IPv6 một cách thích hợp cho các host thuộc các mạng LAN của mạng doanh nghiệp ở trên. Địa chỉ của DNS server được cấp bởi DHCPv6 là: “2001:1234:5678:CDEF::1”.
- Các host thuộc HQ LAN sẽ nhận IPv6 theo phương thức Stateful DHCP và các host thuộc các mạng LAN của các chi nhánh (BR1 LAN và BR2 LAN) sẽ nhận IPv6 theo phương thức Stateless DHCPv6.
- Sau khi nhận được cấu hình IP, các host đều phải có thể truy nhập được Internet. Việc truy nhập Internet được thực hiện bằng cách ping kiểm tra đến địa chỉ “testhost.com” từ các host.

Thực hiện:

1. Cấu hình địa chỉ IPv6:

Cấu hình:

Trên HQ:

```
HQ(config)#interface range e0/0 - 3
HQ(config-if-range)#no shutdown
HQ(config-if-range)#ipv6 address fe80::1 link-local
HQ(config-if-range)#exit

HQ(config)#interface e0/2
HQ(config-if)#no shutdown
HQ(config-if)#ipv6 address 2001:cafe:beef:1::1/64
HQ(config-if)#exit
```

Trên BR1:

```
BR1(config)#interface range e0/0 - 1
BR1(config-if-range)#no shutdown
BR1(config-if-range)#ipv6 address fe80::2 link-local
BR1(config-if-range)#exit

BR1(config)#interface e0/1
BR1(config-if)#ipv6 address 2001:cafe:beef:2::1/64
BR1(config-if)#exit
```

Trên BR2:

```
BR2(config)#interface range e0/0 - 1
BR2(config-if-range)#no shutdown
BR2(config-if-range)#ipv6 address fe80::3 link-local
BR2(config-if-range)#exit

BR2(config)#interface e0/1
BR2(config-if)#ipv6 address 2001:cafe:beef:3::1/64
BR2(config-if)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng các địa chỉ đều đã được cấu hình đầy đủ trên các router:

```
HQ#show ipv6 interface brief
Ethernet0/0          [up/up]
  FE80::1
Ethernet0/1          [up/up]
  FE80::1
Ethernet0/2          [up/up]
  FE80::1
  2001:CAFE:BEEF:1::1
Ethernet0/3          [up/up]
  FE80::1

BR1#show ipv6 interface brief
Ethernet0/0          [up/up]
  FE80::2
Ethernet0/1          [up/up]
  FE80::2
  2001:CAFE:BEEF:2::1
Ethernet0/2          [administratively down/down]
  unassigned
Ethernet0/3          [administratively down/down]
  unassigned

BR2#show ipv6 interface brief
Ethernet0/0          [up/up]
  FE80::3
Ethernet0/1          [up/up]
  FE80::3
  2001:CAFE:BEEF:3::1
Ethernet0/2          [administratively down/down]
  unassigned
Ethernet0/3          [administratively down/down]
  unassigned
```

Các đường link nối giữa các router đều đã thông suốt:

```
HQ#ping fe80::2 <- Link nối đến BR1 thông suốt
Output Interface: Ethernet0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::2, timeout is 2 seconds:
Packet sent with a source address of FE80::1%Ethernet0/0
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/19 ms
HQ#ping fe80::3 <- Link nối đến BR2 thông suốt
Output Interface: Ethernet0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::3, timeout is 2 seconds:
Packet sent with a source address of FE80::1%Ethernet0/1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms
```

```
HQ#ping fe80::254 <- Link nối đến Gateway Internet thông suốt
Output Interface: Ethernet0/3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::254, timeout is 2 seconds:
Packet sent with a source address of FE80::1%Ethernet0/3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

2. Cấu hình định tuyến:

Cấu hình:

Trước hết, ta thực hiện cấu hình định tuyến OSPFv3 trên các router.

Trên HQ:

```
HQ(config)#ipv6 unicast-routing
HQ(config)#router ospfv3 1
HQ(config-router)#router-id 10.0.0.1
HQ(config-router)#exit
HQ(config)#interface range e0/0 - 2
HQ(config-if-range)#ospfv3 1 ipv6 area 0
HQ(config-if-range)#exit
```

Trên BR1:

```
BR1(config)#ipv6 unicast-routing
BR1(config)#router ospfv3 1
BR1(config-router)#router-id 10.0.0.2
BR1(config-router)#exit
BR1(config)#interface range e0/0 - 1
BR1(config-if-range)#ospfv3 1 ipv6 area 0
BR1(config-if-range)#exit
```

Trên BR2:

```
BR2(config)#ipv6 unicast-routing
BR2(config)#router ospfv3 1
BR2(config-router)#router-id 10.0.0.3
BR2(config-router)#exit
BR2(config)#interface range e0/0 - 1
BR2(config-if-range)#ospfv3 1 ipv6 area 0
BR2(config-if-range)#exit
```

Tiếp theo, ta thực hiện cấu hình một static default – route phục vụ hoạt động truy nhập Internet trên router HQ và cấu hình để OSPFv3 lan truyền default – route này vào các router còn lại:

```
HQ(config)#ipv6 route ::/0 e0/3 fe80::254
```

```
HQ(config)#router ospfv3 1
HQ(config-router)#address-family ipv6
HQ(config-router-af)#default-information originate
HQ(config-router-af)#end
```

Kiểm tra:

Chúng ta kiểm tra rằng các router đã hội tụ định tuyến và đã học được đầy đủ các địa chỉ:

```
HQ#show ipv6 route ospf
(...)
O 2001:CAFE:BEEF:2::/64 [110/20]
    via FE80::2, Ethernet0/0
O 2001:CAFE:BEEF:3::/64 [110/20]
    via FE80::3, Ethernet0/1

BR1#show ipv6 route ospf
(...)
OE2 ::/0 [110/1], tag 1
    via FE80::1, Ethernet0/0
O 2001:CAFE:BEEF:1::/64 [110/20]
    via FE80::1, Ethernet0/0
O 2001:CAFE:BEEF:3::/64 [110/30]
    via FE80::1, Ethernet0/0

BR2#show ipv6 route ospf
(...)
OE2 ::/0 [110/1], tag 1
    via FE80::1, Ethernet0/0
O 2001:CAFE:BEEF:1::/64 [110/20]
    via FE80::1, Ethernet0/0
O 2001:CAFE:BEEF:2::/64 [110/30]
    via FE80::1, Ethernet0/0
```

Các mạng LAN đã có thể đi đến nhau được một cách đầy đủ:

```
HQ#ping 2001:cafe:beef:2::1 source 2001:cafe:beef:1::1 <- HQ LAN đi đến qua BR1 LAN
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:CAFE:BEEF:2::1, timeout is 2 seconds:
Packet sent with a source address of 2001:CAFE:BEEF:1::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

HQ#ping 2001:cafe:beef:3::1 source 2001:cafe:beef:1::1 <- HQ LAN đi đến qua BR2 LAN
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:CAFE:BEEF:3::1, timeout is 2 seconds:
Packet sent with a source address of 2001:CAFE:BEEF:1::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
BR1#ping 2001:cafe:beef:3::1 source 2001:cafe:beef:2::1 <- BR1 LAN di đến được BR2 LAN
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:CAFE:BEEF:3::1, timeout is 2 seconds:
Packet sent with a source address of 2001:CAFE:BEEF:2::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

3. Cấu hình DHCPv6:

Cấu hình:

Trước hết, ta cấu hình để router HQ đảm nhận vai trò của một DHCP server:

```
HQ(config)#ipv6 dhcp pool HQ
HQ(config-dhcpv6)#address prefix 2001:cafe:beef:1::/64
HQ(config-dhcpv6)#dns-server 2001:1234:5678:cdef::1
HQ(config-dhcpv6)#domain-name waren.vn
HQ(config-dhcpv6)#exit

HQ(config)#interface range e0/0 - 2
HQ(config-if-range)#ipv6 dhcp server HQ
HQ(config-if-range)#exit
```

Tiếp theo, ta cấu hình để các router chi nhánh đảm nhận vai trò DHCP Relay Agent:

```
BR1-2(config)#interface e0/1
BR1-2(config-if)#ipv6 dhcp relay destination 2001:cafe:beef:1::1
BR1-2(config-if)#exit
```

Cuối cùng, ta cấu hình các router Gateway của các mạng LAN để hướng dẫn các host trên các mạng LAN ấy nhận IP theo phương thức thích hợp (HQ LAN nhận IP theo phương thức Stateful DHCP, các LAN BR1 và BR2 nhận IP theo phương thức Stateless DHCP):

```
HQ(config)#interface e0/2
HQ(config-if)#ipv6 nd managed-config-flag <- Stateful DHCP
HQ(config-if)#exit

BR1-2(config)#interface e0/1
BR1-2(config-if)#ipv6 nd other-config-flag <- Stateless DHCP
BR1-2(config-if)#exit
```

Ghi chú:

Để cấu hình một router trở thành DHCP server, tương tự như với IPv4, chúng ta cũng thực hiện tạo một pool ghi chú các thành phần về IP mà server này sẽ cấp phát xuống cho các host. Trong bài lab này, ta tạo pool có tên là "HQ" trên router HQ:

```
HQ(config)#ipv6 dhcp pool HQ
HQ(config-dhcpv6)#address prefix 2001:cafe:beef:1::/64 <- Dài IP sẽ cấp xuống cho host
HQ(config-dhcpv6)#dns-server 2001:1234:5678:cdef::1 <- Địa chỉ của DNS server
HQ(config-dhcpv6)#domain-name waren.vn <- Domain name cấp xuống các host
HQ(config-dhcpv6)#exit
```

Điểm khác biệt với cấu hình DHCPv4 là chúng ta phải lên các cổng của router có khả năng phải tiếp nhận các gói tin DHCP Request từ phía client để enable chức năng DHCP server và trả đến pool đã thiết lập:

```
HQ(config)#interface range e0/0 - 2
HQ(config-if-range)#ipv6 dhcp server HQ <- pool HQ đã cấu hình ở trên
HQ(config-if-range)#exit
```

Trong sơ đồ bài lab của chúng ta, cổng E0/2 của router HQ là cổng kết nối đến HQ LAN, là cổng sẽ tiếp nhận các yêu cầu về DHCP đến từ mạng LAN này. Các cổng E0/0, E0/1 nối đến các router chi nhánh sẽ tiếp nhận các yêu cầu DHCP đến từ các mạng LAN của các chi nhánh BR1 và BR2.

Router Gateway của các host có thể định hướng cho các host cách thức chúng nhận cấu hình IP tự động bằng cách bật/tắt các bit điều khiển “M” (*Managed address configuration*) và “O” (*Other configuration*) trong bản tin RA (Router Advertisement) mà chúng phát vào mạng LAN. Trong đó:

- $M = 0, O = 0$ (*default*): Các host sẽ nhận cấu hình IP của mình chỉ từ bản tin RA. Đây chính là phương thức SLAAC.
- $M = 1, O = 0$: Các host sẽ nhận cấu hình IP hoàn toàn thông qua DHCP. Đây chính là phương thức *Stateful DHCP*.
- $M = 0, O = 1$: Các host sẽ nhận thông tin về prefix của network mà nó đứng trong đó bằng phương thức SLAAC (từ các gói tin RA của router), những thông tin khác (DNS – server, domain – name,...) sẽ được nhận từ DHCP. Đây chính là phương thức *Stateless DHCP*.
- $M = 1, O = 1$: Các host sẽ đồng thời nhận thông tin IP từ phương thức SLAAC và DHCP. Host sẽ có thể có đồng thời hai địa chỉ IP được thiết lập tự động trên card mạng đến từ hai phương thức vừa nêu. Cách thiết lập này ít được sử dụng.

Từ những điểm vừa trình bày, chúng ta sẽ cấu hình router HQ bật bit M trên bản tin RA gửi đến Host1 để host này chỉ nhận IP từ DHCP và cấu hình các router BR1, BR2 bật bit O trên các bản tin RA gửi đến các host Host2, Host3 để các host này nhận thông tin prefix từ SLAAC và các thông tin DNS, domain – name từ DHCPv6:

```
HQ(config)#interface e0/2
HQ(config-if)#ipv6 nd managed-config-flag <- Stateful DHCP (bật bit M, không bật bit O)
HQ(config-if)#exit

BR1-2(config)#interface e0/1
BR1-2(config-if)#ipv6 nd other-config-flag<- Stateless DHCP(không bật bit M, bật bit O)
BR1-2(config-if)#exit
```

Cuối cùng, chúng ta dừng quên cấu hình để các router BR1 và BR2 đảm nhận vai trò DHCP Relay Agent:

```
BR1-2(config)#interface e0/1
BR1-2(config-if)#ipv6 dhcp relay destination 2001:cafe:beef:1::1
BR1-2(config-if)#exit
```

Câu lệnh để cấu hình DHCP Relay Agent với IPv6, giống như với IPv4, vẫn được đặt trên cổng của router gateway mà nối đến các DHCP client:

```
R(config-if)#ipv6 dhcp relay destination Địa chỉ IPv6 _của_DHCP_server
```

Tương tự như với IPv4, địa chỉ của DHCP server và địa chỉ trên cổng cấu hình lệnh này phải đi đến nhau được. Do đó, để triển khai DHCP Relay Agent, trước đó ta cần cấu hình định tuyến một cách đầy đủ.

Kiểm tra:

Ta cấu hình các host nhận IP tự động theo các phương thức đã được yêu cầu.

Trên Host1:

```
Host1(config)#interface e0/0
Host1(config-if)#no shutdown
Host1(config-if)#ipv6 enable
Host1(config-if)#ipv6 address dhcp
Host1(config-if)#exit
```

Trên Host2, Host3:

```
Host2-3(config)#interface e0/0
Host2-3(config-if)#no shutdown
Host2-3(config-if)#ipv6 address autoconfig
Host2-3(config-if)#exit
```

Với Cisco IOS, để xin cấp phát IP từ DHCPv6, chúng ta sử dụng câu lệnh “`ipv6 address dhcp`” trên cổng. Tuy nhiên, vì các gói tin DHCP sẽ sử dụng source IP là địa chỉ link – local, đòi hỏi cổng phải có địa chỉ link – local nên trước đó ta cần gõ lệnh “`ipv6 enable`” trên cổng để phát sinh địa chỉ link – local cho cổng này.

Để nhận IP theo cơ chế SLAAC, chúng ta sử dụng lệnh “`ipv6 address autoconfig`” trên cổng của router. Với các host Host2 và Host3, sau khi gõ lệnh này chúng sẽ nhận được IP prefix của mạng LAN và tự động phát sinh địa chỉ theo luật EUI – 64, ngoài ra chúng sẽ lấy thông tin DNS, Domain – name từ DHCPv6.

Địa chỉ IPv6 trên các host:

```
Host1#show ipv6 interface brief e0/0
Ethernet0/0          [up/up]
  FE80::A8BB:CCFF:FE00:5000
  2001:CAFE:BEEF:1:7CB0:89F:3257:AC45

Host2#show ipv6 interface brief e0/0
Ethernet0/0          [up/up]
  FE80::A8BB:CCFF:FE00:6000
  2001:CAFE:BEEF:2:A8BB:CCFF:FE00:6000

Host3#show ipv6 interface brief e0/0
Ethernet0/0          [up/up]
  FE80::A8BB:CCFF:FE00:7000
  2001:CAFE:BEEF:3:A8BB:CCFF:FE00:7000
```

Các host đều đã nhận được thông tin cần thiết từ DHCPv6:

```
Host1#show ipv6 dhcp interface
Ethernet0/0 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:38:26
  List of known servers:
    Reachable via address: FE80::1
    DUID: 00030001AABBCC001000
```

```
Preference: 0
Configuration parameters:
  IA NA: IA ID 0x00030001, T1 43200, T2 69120
    Address: 2001:CAFE:BEEF:1:7CB0:89F:3257:AC45/128
      preferred lifetime 86400, valid lifetime 172800
      expires at Aug 28 2021 05:19 AM (171507 seconds)
  DNS server: 2001:1234:5678:CDEF::1
  Domain name: waren.vn
  Information refresh time: 0
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled

Host2#show ipv6 dhcp interface
Ethernet0/0 is in client mode
  Prefix State is IDLE (1)
  Information refresh timer expires in 23:38:27
  Address State is IDLE
  List of known servers:
    Reachable via address: FE80::2
    DUID: 00030001AABBCC001000
    Preference: 0
  Configuration parameters:
    DNS server: 2001:1234:5678:CDEF::1
    Domain name: waren.vn
    Information refresh time: 0
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled

Host3#show ipv6 dhcp interface
Ethernet0/0 is in client mode
  Prefix State is IDLE (0)
  Information refresh timer expires in 23:38:21
  Address State is IDLE
  List of known servers:
    Reachable via address: FE80::3
    DUID: 00030001AABBCC001000
    Preference: 0
  Configuration parameters:
    DNS server: 2001:1234:5678:CDEF::1
    Domain name: waren.vn
    Information refresh time: 0
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled
```

Kết quả show cho thấy, Host1 nhận full cấu hình IP từ DHCP (địa chỉ IP, địa chỉ DNS – server, domain – name), trong khi các host Host2 và Host3 chỉ nhận địa chỉ DNS – server và domain – name từ DHCP.

Kiểm tra trên DHCP server ta thấy rằng server này đã cấp xuống một địa chỉ cho Host1:

```
HQ#show ipv6 dhcp binding
Client: FE80::A8BB:CCFF:FE00:5000 <- Địa chỉ Link-local của Host1
  DUID: 00030001AABBCC005000
```

```
Username : unassigned
VRF : default
IA NA: IA ID 0x00030001, T1 43200, T2 69120
Address: 2001:CAFE:BEEF:1:7CB0:89F:3257:AC45 <- Địa chỉ cấp cho Host1
    preferred lifetime 86400, valid lifetime 172800
    expires at Aug 28 2021 05:19 AM (171199 seconds)
```

Các host đều đã có được default – gateway rút ra được từ bản tin RA gửi xuống của router:

```
Host1#show ipv6 route
(...)
ND ::/0 [2/0]
    via FE80::1, Ethernet0/0
LC 2001:CAFE:BEEF:1:7CB0:89F:3257:AC45/128 [0/0]
    via Ethernet0/0, receive
L  FF00::/8 [0/0]
    via Null0, receive

Host2#show ipv6 route
(...)
ND ::/0 [2/0]
    via FE80::2, Ethernet0/0
NDp 2001:CAFE:BEEF:2::/64 [2/0]
    via Ethernet0/0, directly connected
L  2001:CAFE:BEEF:2:A8BB:CCFF:FE00:6000/128 [0/0]
    via Ethernet0/0, receive
L  FF00::/8 [0/0]
    via Null0, receive

Host3#show ipv6 route
(...)
ND ::/0 [2/0]
    via FE80::3, Ethernet0/0
NDp 2001:CAFE:BEEF:3::/64 [2/0]
    via Ethernet0/0, directly connected
L  2001:CAFE:BEEF:3:A8BB:CCFF:FE00:7000/128 [0/0]
    via Ethernet0/0, receive
L  FF00::/8 [0/0]
    via Null0, receive
```

Ta nhắc lại rằng, DHCPv6 không còn cấp phát địa chỉ của default – gateway xuống cho các host nữa, thông tin về default – gateway (địa chỉ MAC) sẽ được đưa xuống cho các host bằng bản tin RA của router.

Với cấu hình IP nhận được đầy đủ như trên, các host đã có thể truy nhập Internet bằng tên miền:

```
Host1#ping testhost.com
Translating "testhost.com"...domain server (2001:1234:5678:CDEF::1) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1234:5678:ABCD::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

```
Host2#ping testhost.com
Translating "testhost.com"...domain server (2001:1234:5678:CDEF::1) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1234:5678:ABCD::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

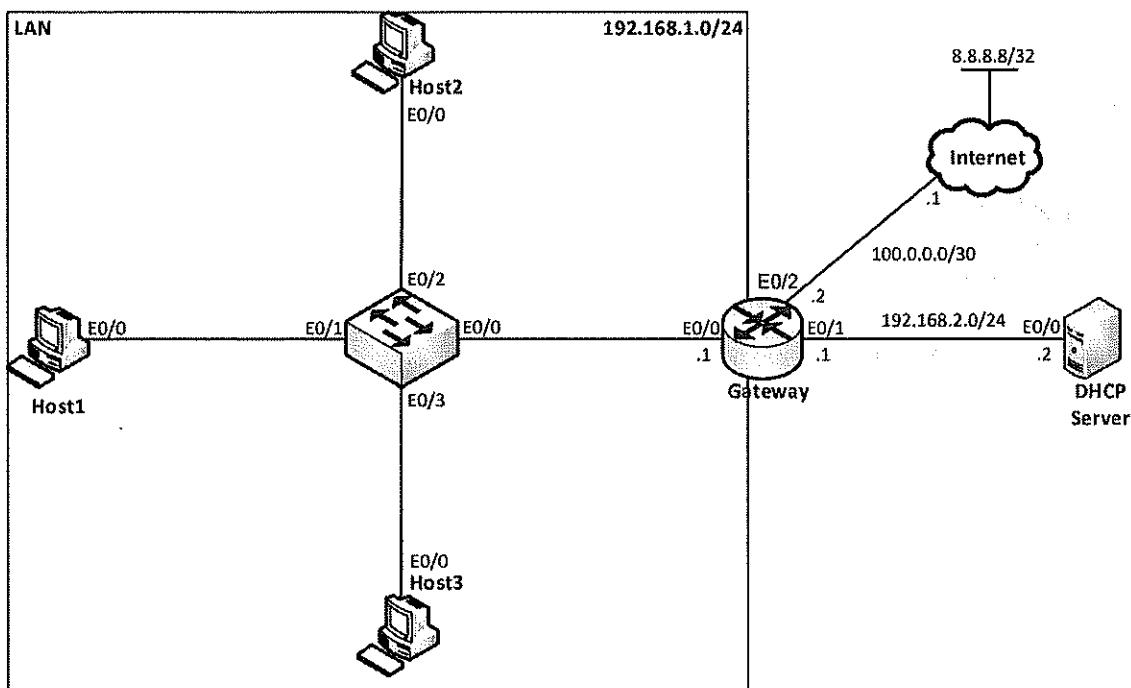
Host3#ping testhost.com
Translating "testhost.com"...domain server (2001:1234:5678:CDEF::1) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1234:5678:ABCD::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Đến đây, chúng ta đã hoàn thành các yêu cầu đặt ra của bài lab.

Lab 26 – Một số tính năng bảo mật trên switch

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Bài lab gồm các thiết bị được kết nối với nhau theo sơ đồ được chỉ ra trên hình 1. Tất cả các thiết bị đều là router hoặc switch, chạy hệ điều hành IOL.
 - Trong bài lab này, các bạn học viên sẽ thực hành cấu hình một số tính năng bảo mật trên switch Cisco gồm: DHCP Snooping, Dynamic ARP Inspection (DAI) và Port – security.
 - Các thiết bị đã được thiết lập sẵn cấu hình ban đầu bao gồm:
 - Cấu hình hostname trên các thiết bị.
 - Cấu hình DHCP Relay Agent trên router Gateway.
 - Cấu hình cung cấp dịch vụ Internet cho mạng LAN trên router Gateway.
 - Cấu hình DHCP Server cấp phát IP cho các host thuộc mạng 192.168.1.0/24.
 - Cấu hình xin cấp phát IP tự động từ DHCP trên Host1 và DHCP server giả mạo trên Host2.
- Các bạn học viên không thay đổi các cấu hình vừa nêu trong suốt quá trình thực hiện bài lab.

Yêu cầu:**1. DHCP Snooping:**

- Hiện tại Host1 không thể truy nhập được Internet vì nhận được cấu hình IP sai lệch từ DHCP.
- Hãy khắc phục vấn đề vừa nêu bằng cách cấu hình tính năng chống tấn công giả mạo DHCP (DHCP snooping) trên switch SW.
- Sau khi khắc phục xong, thực hiện xin lại DHCP trên các host Host1 và Host3, xác nhận rằng các host này đã nhận được IP một cách đúng đắn và có thể truy nhập được Internet.

2. Dynamic ARP Inspection (DAI):

Thực hiện cấu hình tính năng DAI trên switch SW để chống tấn công giả mạo ARP trên mạng LAN của sơ đồ.

3. Port – security:

- Cấu hình tính năng Port – security trên cổng nối đến Host1 của SW đảm bảo rằng chỉ Host1 được phép truy nhập vào cổng này.
- Việc kiểm soát truy nhập dựa vào địa chỉ MAC của Host1. Nếu địa chỉ MAC thay đổi, cổng sẽ bị đưa vào trạng thái err – disabled.

Thực hiện:**1. DHCP Snooping:****Cấu hình:**

Các thiết bị mạng đều đã được cấu hình đầy đủ, tuy nhiên Host1 vẫn không thể truy nhập được Internet:

```
Host1>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:
U.U.U
Success rate is 0 percent (0/5)
```

Nguyên nhân của điều này là do Host1 đã nhận được một cấu hình IP sai lệch từ DHCP server giả mạo được thiết lập trên Host2:

```
Host1#show ip interface brief e0/0
Interface          IP-Address      OK? Method Status      Protocol
Ethernet0/0        192.168.1.2    YES  DHCP     up           up

Host1#show ip route static
(...)
S*   0.0.0.0/0 [254/0] via 192.168.1.101

Host2#show ip interface brief e0/0
Interface          IP-Address      OK? Method Status      Protocol
Ethernet0/0        192.168.1.101  YES  TFTP    up           up
```

```
Host2#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/           Lease expiration      Type
                  Hardware address/
                  User name
192.168.1.2        01aa.bbcc.0010.00    Aug 31 2021 05:33 PM  Automatic
DHCP_Server#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/           Lease expiration      Type
                  Hardware address/
                  User name
```

Trong kết quả show ở trên, Host1 có được IP là 192.168.1.2 thuộc dải IP 192.168.1.0/24 của mạng LAN nhưng lại nhận được địa chỉ default – gateway sai lệch là 192.168.1.101 chính là địa chỉ của Host2. Như vậy, mọi lưu lượng đi Internet của Host1 sẽ đều được chuyển đến cho Host2 chứ không phải đến gateway thật sự của mạng LAN.

Bên cạnh đó, chúng ta cũng thấy bảng DHCP binding chỉ rõ là Host2 đã cấp phát IP được xuống cho Host1 trong khi DHCP Server thì lại chưa cấp phát được địa chỉ IP nào cả. Host1 đã bị tấn công giả mạo DHCP.

Để ngăn chặn điều này, chúng ta cấu hình tính năng DHCP snooping trên switch SW:

```
SW(config)#ip dhcp snooping
SW(config)#ip dhcp snooping vlan 1
SW(config)#interface e0/0
SW(config-if)#ip dhcp snooping trust
SW(config-if)#exit
SW(config)#no ip dhcp snooping information option
```

Ghi chú:

Tính năng DHCP Snooping được sử dụng để ngăn chặn phương thức tấn công giả mạo DHCP (DHCP Spoofing) trên nội bộ mạng LAN. Với phương thức tấn công này, kẻ tấn công thực hiện dựng lên một DHCP server giả để rót thông tin IP sai lệch xuống cho người dùng trên cùng VLAN từ đó gây ảnh hưởng đến việc truy nhập mạng hoặc đánh cắp thông tin từ người dùng. Hoạt động của DHCP snooping có thể được trình bày khái quát như sau:

- Các cổng thuộc VLAN áp dụng DHCP snooping sẽ được chia thành hai loại: *trusted port* và *untrusted port*. Mặc định, tất cả các cổng của VLAN áp dụng DHCP Snooping sẽ là untrusted port, ta phải cấu hình tinh tế để chỉ định cổng nào là trusted port.
- Để xin cấp cấu hình IP, các DHCP client sẽ gửi các gói tin DHCP lên cho DHCP server và DHCP server sẽ hồi đáp về các gói tin DHCP khác xuống cho client. Các gói tin theo chiều từ client lên server gồm: DHCP Discover, DHCP Request,..v.v... và các gói tin theo chiều từ server xuống client gồm: DHCP Offer, DHCP ACK,..v.v...

Tính năng DHCP snooping sẽ drop mọi gói tin DHCP thuộc nhóm server trả lời client khi chúng đi vào các untrusted port và cho qua mọi gói tin DHCP đi vào trusted port. Với cách hoạt động như vậy, nếu ta bố trí để các untrusted port là các port đầu nối đến người dùng và trusted port là các port đầu nối uplink hoặc kết nối đến DHCP server, ta có thể ngăn chặn được việc một thành viên nào đó trong

số những người dùng giả mạo DHCP server để cấp thông tin IP sai lệch xuống cho các thành viên khác.

- Ngoài ra, tính năng DHCP snooping còn theo dõi mọi gói tin DHCP đi ngang qua VLAN và thiết lập bảng thông tin *DHCP snooping binding* gồm các dòng cho biết host được cấp IP có MAC là gì, đấu nối vào interface nào và đang sử dụng IP nào.

Bảng này không sử dụng cho tính năng DHCP snooping để chống giả mạo DHCP mà sẽ được sử dụng cho tính năng *DAI (Dynamic ARP Inspection)* để chống tấn công giả mạo ARP.

Để cấu hình DHCP snooping trên một VLAN, chúng ta thực hiện các bước như sau:

1. Bật tính năng DHCP snooping trên switch:

```
SW(config)#ip dhcp snooping
```

2. Chỉ định VLAN sẽ áp tính năng này:

```
SW(config)#ip dhcp snooping vlan vlan-list
```

Trong đó: “*vlan-list*” là danh sách các VLAN sẽ được áp tính năng DHCP snooping. Trong bài lab này của chúng ta, chỉ có một VLAN được áp tính năng này là VLAN 1.

3. Chỉ định trusted port:

```
SW(config-if)#ip dhcp snooping trust
```

Như đã trình bày ở trên, ta chỉ định các cổng đấu nối về phía DHCP server là các trusted port để có thể tiếp nhận các gói DHCP mà server trả về cho client từ các cổng này. Trong bài lab đang thực hiện, cổng E0/0 của switch SW là cổng đi về phía DHCP server nên ta thực hiện khai báo cổng này là trusted port.

4. Khi bật tính năng DHCP snooping trên switch, switch sẽ tự động chèn thêm *option 82* vào các gói tin DHCP đi từ client lên server. Option 82 thường được sử dụng để cung cấp thêm thông tin về thiết bị hoặc port mà client kết nối vào. Thông tin này cho phép DHCP server thực hiện cấp phát IP theo một chính sách thêm vào nào đó; ví dụ: range IP được cấp có thể được chia thành nhiều dải và mỗi dải sẽ cấp cho các client thuộc về các switch khác nhau hoặc client kết nối vào port này sẽ chỉ nhận IP thuộc dải này, còn client kết nối vào port kia sẽ chỉ nhận được IP thuộc dải kia,.v.v...

Thông thường option 82 được sử dụng trên DHCP relay agent nên khi gói tin DHCP của client có chèn thêm option 82 thì trường “*giaddr*” trong gói DHCP sẽ ghi vào địa chỉ của agent sử dụng option 82. Tuy nhiên, trong tình huống sử dụng DHCP snooping, switch chèn option 82 nhưng nó không phải là DHCP relay agent nên switch sẽ để trường này nhận giá trị là 0. Điều này dẫn đến gói DHCP đến từ client sẽ được xem là bị lỗi và bị drop bỏ khiến cho client sẽ không nhận được cấu hình IP.

Để khắc phục vấn đề nêu trên, khi cấu hình DHCP snooping trên switch, ta cần phải tắt thao tác chèn option 82 trên switch bằng câu lệnh:

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

Kiểm tra:

Chúng ta thực hiện kiểm tra thông số của DHCP Snooping đã cấu hình trên switch:

```
SW#show ip dhcp snooping
Switch DHCP snooping is enabled <- Tính năng DHCP Snooping đã được bật
Switch DHCP learning is disabled
```

```
DHCP snooping is configured on following VLANs:  
1  
DHCP snooping is operational on following VLANs:  
1  
DHCP snooping is configured on the following L3 Interfaces:  
  
Insertion of option 82 is disabled <- Option 82 đã được tắt  
circuit-id default format: vlan-mod-port  
remote-id: aabb.cc00.6000 (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)  
-----  
Ethernet0/0 yes yes unlimited <- E0/0 là trusted port  
Custom circuit-ids:
```

Chúng ta thực hiện xin cấp phát lại IP cho Host1 bằng DHCP:

```
Host1(config)#interface e0/0  
Host1(config-if)#shutdown  
Host1(config-if)#  
*Aug 30 15:57:31.425: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down  
Host1(config-if)#  
*Aug 30 15:57:32.432: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down  
Host1(config-if)#no shutdown  
Host1(config-if)#exit  
Host1(config)#  
*Aug 30 15:57:41.644: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up  
*Aug 30 15:57:42.650: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
```

Lúc này, Host1 đã nhận được cấu hình IP đúng đắn:

```
Host1#show ip interface brief e0/0  
Interface IP-Address OK? Method Status Protocol  
Ethernet0/0 192.168.1.2 YES DHCP up up  
  
Host1#show ip route static  
(...)  
S* 0.0.0.0/0 [254/0] via 192.168.1.1  
192.168.2.0/32 is subnetted, 1 subnets  
S 192.168.2.2 [254/0] via 192.168.1.1, Ethernet0/0
```

Kết quả show cho thấy Host1 đã nhận được địa chỉ IP 192.168.1.2 với default – gateway đúng 192.168.1.1. Bảng định tuyến của Host1 cũng phát sinh là một host route cho địa chỉ của DHCP server, chính là địa chỉ 192.168.2.2 của server hợp lệ trong bài lab.

Lúc này, Host1 đã có thể truy nhập được Internet:

```
Host1#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 = 1/1/2 ms
```

Như vậy, chúng ta đã chống lại được tấn công giả mạo DHCP trong mạng LAN từ Host2.

Chúng ta cho Host3 xin IP từ DHCP:

```
Host3(config)#interface e0/0
Host3(config-if)#no shutdown
Host3(config-if)#ip address dhcp client-id e0/0
Host3(config-if)#exit
```

Host3 cũng nhận được cấu hình IP đúng đắn từ DHCP server:

```
Host3#show ip interface brief e0/0
Interface          IP-Address      OK? Method Status      Protocol
Ethernet0/0        192.168.1.3    YES DHCP     up           up

Host3#show ip route static
(...)
S* 0.0.0.0/0 [254/0] via 192.168.1.1
    192.168.2.0/32 is subnetted, 1 subnets
S    192.168.2.2 [254/0] via 192.168.1.1, Ethernet0/0
```

Host3 truy nhập được Internet:

```
Host3#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 = 1/1/2 ms
```

Tính năng DHCP snooping theo dõi tất cả các gói DHCP đi qua switch và xây dựng bảng DHCP Snooping binding dựa trên thông tin đọc được từ các gói này:

SW#show ip dhcp snooping binding						
MacAddress	IpAddress	Lease (sec)	Type	VLAN	Interface	
AA:BB:CC:00:30:00	192.168.1.3	86100	dhcp-snooping	1	Ethernet0/3	
AA:BB:CC:00:10:00	192.168.1.2	84912	dhcp-snooping	1	Ethernet0/1	
Total number of bindings: 2						

Như đã đề cập trong phần “Ghi chú”, bảng này cho thấy rõ địa chỉ IP nào đã được cấp phát cho host có MAC nào, thuộc VLAN nào và kết nối trên cổng nào của switch.

Đến đây chúng ta đã hoàn thành khảo sát tính năng DHCP snooping của switch.

2. Dynamic ARP Inspection (DAI):

Cấu hình:

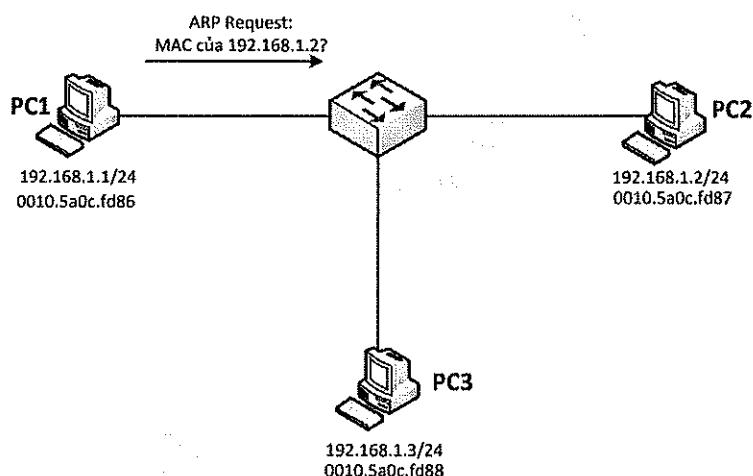
Ta thực hiện bật tính năng DAI trên switch:

```
SW(config)#ip arp inspection vlan 1
SW(config)#interface e0/0
SW(config-if)#ip arp inspection trust
SW(config-if)#exit
```

Ghi chú:

Tính năng DAI – Dynamic ARP Inspection giúp switch chống lại hoạt động tấn công giả mạo ARP trên các VLAN. Với phương thức tấn công giả mạo ARP, kẻ tấn công sẽ phát ra các gói tin ARP giả mạo phân giải địa chỉ IP thành một MAC sai lệch từ đó thực hiện đánh cắp dữ liệu người dùng hoặc ngăn chặn người dùng truy nhập các tài nguyên mạng. Ta cùng điểm qua một vài nét chính của phương thức tấn công này.

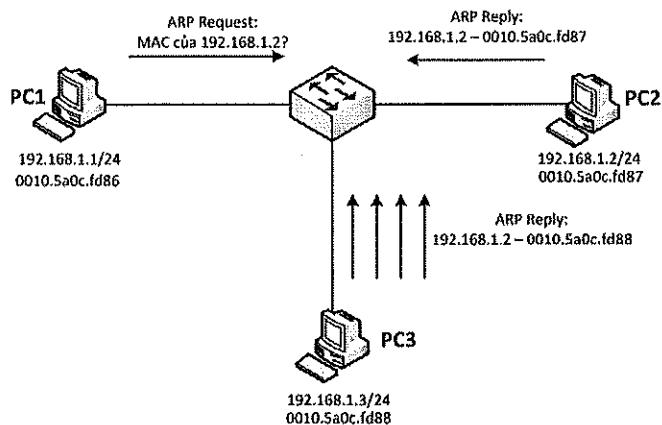
Xét một sơ đồ mạng đơn giản trên hình 2:



Hình 2 – Sơ đồ mạng ví dụ của tấn công ARP.

Sơ đồ mạng trên hình 2 gồm các PC với quy hoạch IP và có địa chỉ MAC được chỉ ra như trên hình vẽ. Giả sử PC1 muốn gửi dữ liệu đến PC2 ở địa chỉ IP 192.168.1.2, nó cần phải có được địa chỉ MAC của PC2 để đóng frame các dữ liệu này nhằm truyền trên data link Ethernet tới tay PC2. Như chúng ta đã biết, để có thể có được MAC của PC2, PC1 thực hiện phát broadcast gói tin ARP Request để hỏi xem máy mang địa chỉ IP 192.168.1.2 sẽ có địa chỉ MAC là gì. Đúng nguyên tắc, PC2 sẽ trả lời ARP reply để cho biết địa chỉ MAC của nó chính là địa chỉ MAC của máy mang địa chỉ 192.168.1.2 và PC1 khi nhận được gói ARP reply từ PC2 sẽ thực hiện cập nhật MAC của PC2.

Tuy nhiên, nếu như PC3 là một kẻ tấn công thực hiện giả mạo ARP, kẻ tấn công này sẽ thực hiện phát ra liên tục các gói ARP Reply báo rằng MAC tương ứng với IP 192.168.1.2 là MAC của PC3 (tức là MAC của kẻ tấn công) (hình 3):



Hình 3 – PC3 phát ra gói ARP giả mạo.

Kết quả của điều này là PC1 sẽ cập nhật bảng ARP của nó là 192.168.1.2 lại tương ứng với MAC của PC3 – MAC của kẻ tấn công. Từ đó, mọi lưu lượng gửi đến địa chỉ 192.168.1.2 của PC2 sẽ đều được hệ thống switch ở giữa forward đến PC3 của kẻ tấn công chứ không chuyển đến được đúng tay người nhận. Kẻ tấn công có thể đọc toàn bộ dữ liệu nhận được này rồi chuyển đi tiếp đến PC2 (kiểu tấn công Man – in – the – middle) hoặc drop bỏ dữ liệu này khiến PC1 và PC2 không trao đổi dữ liệu với nhau được.

Để chống lại kiểu tấn công giả mạo ARP này, chúng ta thực hiện bật tính năng *DAI – Dynamic ARP Inspection* trên switch. Tính năng này hoạt động như sau:

- Các cổng trên switch được chia thành hai loại: trusted port và untrusted port (lưu ý phân biệt với trusted port và untrusted port của tính năng DHCP snooping).
- Tính năng DAI sẽ kiểm tra mọi gói tin ARP trên các untrusted port. Cặp địa chỉ phân giải Sender – MAC và sender – IP trong các gói ARP reply đi vào untrusted port phải khớp với thông tin tương ứng về MAC và IP trong bảng DHCP snooping binding. Nếu cặp này không khớp, gói tin được cho là giả mạo và sẽ bị DAI drop bỏ. Ta thấy, với cách hoạt động như vậy, nếu user kết nối vào một untrusted port, user sẽ không thể phát đi được gói ARP reply phân giải cho một địa chỉ MAC không phải của mình và như vậy hoạt động giả mạo ARP của kẻ tấn công đã bị ngăn chặn.

Ta cũng thấy rằng để tính năng DAI hoạt động, trước đó chúng ta cần phải cấu hình DHCP snooping trên VLAN để switch có được bảng DHCP snooping binding nhằm kiểm tra tính hợp lệ của gói ARP.

- Để cấu hình bật tính năng DAI trên một VLAN của switch, chúng ta sử dụng lệnh:

```
SW(config)#ip arp inspection vlan-id
```

- Để chỉ định một cổng là trusted port, chúng ta sử dụng lệnh (mặc định, các cổng tham gia DAI đều là untrusted port):

```
SW(config-if)#ip arp inspection trust
```

- Để kiểm tra các thông số của DAI:

```
SW#show ip arp inspection
```

Kiểm tra:

Ta quan sát lại bảng DHCP snooping binding được xây dựng bởi tính năng DHCP snooping ở trên:

SW#show ip dhcp snooping binding					
MacAddress	IpAddress	Lease (sec)	Type	VLAN	Interface
AA:BB:CC:00:30:00	192.168.1.3	86333	dhcp-snooping	1	Ethernet0/3
AA:BB:CC:00:10:00	192.168.1.2	86331	dhcp-snooping	1	Ethernet0/1
Total number of bindings: 2					

Căn cứ theo bảng này, mọi gói tin ARP reply cho địa chỉ IP 192.168.1.3 của Host3 phải có kết quả địa chỉ MAC là “AA:BB:CC:00:30:00”. Mọi kết quả phân giải địa chỉ khác với kết quả này đều được xem là không hợp lệ và sẽ bị switch drop bỏ.

Ta thử giả lập một cuộc tấn công ARP đến từ Host2 bằng cách đổi địa chỉ IP trên Host2 thành địa chỉ của Host3:

```
Host2(config)#interface e0/0
Host2(config-if)#ip address 192.168.1.3 255.255.255.0
Host2(config-if)#exit
```

Khi chúng ta thay đổi địa chỉ IP như vừa thực hiện, host sẽ lập tức phát ra một gói ARP đặc biệt có tên là *Gratuitous ARP* để thông báo cho các host khác trên mạng LAN về vấn đề chuyển đổi địa chỉ này nhằm tránh trùng lặp địa chỉ IP trên mạng. Về bản chất, gói *Gratuitous ARP* là một gói *ARP Reply* với nội dung cho tương ứng địa chỉ MAC của host với địa chỉ IP vừa thay đổi; trong trường hợp này, gói sẽ báo rằng địa chỉ IP 192.168.1.3 sẽ tương ứng với MAC của cổng E0/0 trên Host2. Điều này tương đương với việc Host2 phát ra bản tin ARP sai lệch để khiến cho các host khác cập nhật lại MAC tương ứng với địa chỉ 192.168.1.3 của Host3 thành địa chỉ MAC của mình → Một cuộc tấn công ARP được giả lập.

SW đã được cấu hình tính năng DAI nên nó lập tức phát hiện ra gói ARP không hợp lệ này:

```
*Aug 31 04:12:45.739: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Res) on Et0/2, vlan 1. ([aabb.cc00.2000/192.168.1.3/ffff.ffff/192.168.1.3/06:12:45 EET Tue Aug 31 2021])
```

SW thấy rằng gói này thông tin rằng địa chỉ 192.168.1.3 tương ứng với MAC “aabb.cc00.2000”, trong khi nếu đổi chiều theo bảng DHCP snooping binding ở trên thì địa chỉ này phải tương ứng với MAC “aabb.cc00.3000”. SW thực hiện drop bỏ các gói ARP Reply vừa nêu và cuộc tấn công bị vô hiệu hóa.

Sau khi kiểm tra xong, chúng ta cấu hình để Host2 nhận IP một cách hợp lệ từ DHCP:

```
Host2(config)#interface e0/0
Host2(config-if)#ip address dhcp client-id e0/0
Host2(config-if)#exit
*Aug 31 07:44:58.421: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0/0 assigned DHCP address 192.168.1.4, mask 255.255.255.0, hostname Host2
```

3. Port – security:

Cấu hình:

Trước hết, chúng ta kiểm tra địa chỉ MAC trên cổng E0/0 của Host1:

```
Host1#show interfaces e0/0 | inc bia
Hardware is AmdP2, address is aabb.cc00.1000 (bia aabb.cc00.1000)
```

Ta thấy địa chỉ MAC trên card mạng của Host1 là “aabb.cc00.1000”. Ta sẽ cấu hình tính năng Port – security trên cổng E0/1 của switch để chỉ cho phép địa chỉ MAC này được quyền truy nhập cổng, mọi địa chỉ MAC khác nếu xuất hiện trên cổng sẽ khiến cổng bị shutdown:

```
SW(config)#interface e0/1
SW(config-if)#shutdown
SW(config-if)#switchport mode access
SW(config-if)#switchport port-security
SW(config-if)#switchport port-security mac-address aabb.cc00.1000
SW(config-if)#no shutdown
SW(config-if)#exit
```

Ghi chú:

Port – security là một tính năng ở lớp 2 cho phép áp một giới hạn về số lượng địa chỉ MAC được phép truy nhập trên một cổng. Hai mục đích chính của port – security là ngăn chặn việc truy nhập không hợp lệ trên cổng (chỉ những MAC nào được phép mới được đi vào cổng) và chống tấn công MAC – flooding. Kiểu tấn công MAC – flooding được thực hiện bằng cách tạo ra rất nhiều frame với source MAC khác nhau rồi đẩy vào switch khiến cho bảng địa chỉ MAC của switch bị tràn từ đó switch sẽ hoạt động như một thiết bị hub với các thiết bị kết nối sau này.

Tính năng port – security chỉ hoạt động trên các port được cấu hình là static access hoặc static trunk, không hoạt động trên các dynamic port (auto hoặc desirable). Trình tự cấu hình tính năng này trên một cổng switch có thể được tiến hành như sau:

- Bật tính năng Port – security trên cổng:

```
SW(config-if)#switchport port-security
```

- Cấu hình số lượng địa chỉ MAC tối đa được đi vào cổng:

```
SW(config-if)#switchport port-security maximum n
```

Trong đó: “n” là số địa chỉ tối đa, nằm trong dải từ 1 đến 132, mặc định bằng 1.

- Cấu hình khai báo các địa chỉ MAC được phép xuất hiện trên cổng:

```
SW(config-if)#switchport port-security mac-address {Địa_chi_MAC | sticky}
```

Sau khi cấu hình số lượng địa chỉ tối đa được phép đi vào cổng, chúng ta phải khai báo tường minh từng địa chỉ MAC được phép này. Lưu ý rằng, nếu cho phép bao nhiêu địa chỉ, chúng ta phải khai báo cho đủ số lượng bấy nhiêu, nếu khai báo thiếu, “vị trí còn trống” này có thể được sử dụng bởi bất kỳ địa chỉ MAC nào khác khiến cho cấu hình Port – security kiểm soát truy nhập trở nên vô nghĩa.

Bên cạnh việc khai báo địa chỉ MAC tường minh, chúng ta có thể sử dụng tùy chọn “sticky” của câu lệnh này. Tùy chọn “sticky” sẽ khiến cho switch tự động học địa chỉ MAC của thiết bị gắn trên cổng cho đến khi đủ số lượng. Hơn nữa, các địa chỉ MAC học được còn được tự động lưu vào trong file cấu hình “running-config” của switch và sẽ được lưu lại cố định cho sau này nếu chúng ta thực

hiện lưu cấu hình thành file “startup-config” (“SW#write memory” hoặc “SW#copy running-config startup-config”).

- Chọn phương thức xử phạt vi phạm:

```
SW(config-if)#switchport port-security violation {shutdown | restrict | protect}
```

Trong đó:

- “shutdown”: cổng sẽ bị shutdown nếu xuất hiện frame vi phạm. Thực ra, là cổng được đưa vào một trạng thái đặc biệt có tên gọi là “err – disabled”. Ở trạng thái này, cổng bị cho down vật lý, giống như bị shutdown. Để khắc phục, chúng ta cần đảm bảo địa chỉ MAC xuất hiện trên cổng phải là địa chỉ hợp lệ và thực hiện reset lại cổng bằng cách tắt rồi mở lại cổng với các lệnh “shutdown/no shutdown”.
- “restrict” và “protect”: ở các chế độ xử phạt này, switch không shutdown cổng mà chỉ drop các frame không hợp lệ (source MAC không đúng). Điểm khác biệt của hai mode này là: với “restrict”, switch sẽ phát cảnh báo về sự vi phạm, còn với “protect”, switch không phát cảnh báo gì cả.
- Mode mặc định được sử dụng là “shutdown”.

Ta nên shutdown cổng trước khi cấu hình Port – security trên cổng ấy. Sau khi hoàn tất cấu hình, ta thực hiện no shutdown cổng trở lại.

Kiểm tra:

Hiện tại, sau khi cấu hình xong Port – security, Host1 sử dụng MAC hợp lệ nên vẫn truy nhập mạng bình thường:

```
Host1#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 = 1/1/2 ms
```

Ta kiểm tra rằng switch đã ghi nhận địa chỉ của Host1 cho hoạt động Port – security:

```
SW#show port-security address
      Secure Mac Address Table
-----
Vlan   Mac Address       Type           Ports      Remaining Age
                  (mins)
-----
1      aabb.cc00.1000    SecureConfigured  Et0/1      -
-----
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

Ta có thể xem thêm một số thông tin khác về Port – security đã cấu hình trên cổng E0/1:

```
SW#show port-security interface e0/1
Port Security          : Enabled
Port Status              : Secure-up
Violation Mode          : Shutdown
Aging Time               : 0 mins
Aging Type               : Absolute
```

```
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan 1:aabb.cc00.1000:1
Security Violation Count  : 0
```

Tiếp theo, ta thực hiện đổi địa chỉ MAC trên cổng E0/0 của Host1 thành một địa chỉ khác để kiểm tra hoạt động của tính năng Port – security:

```
Host1(config)#interface e0/0
Host1(config-if)#mac-address 0010.5a0c.fd86
Host1(config-if)#end

Host1#show interfaces e0/0 | inc bia
    Hardware is AmdP2, address is 0010.5a0c.fd86 (bia aabb.cc00.1000)
```

Khi địa chỉ MAC được thay đổi thành một địa chỉ không hợp lệ, một số lưu lượng xuất phát từ Host1 đi lên switch sẽ sử dụng source MAC mới (ví dụ: lưu lượng ARP), Port – security trên switch sẽ phát hiện được điều này và thực hiện phản ứng:

```
SW#
*Aug 31 08:58:52.090: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/1,
putting Et0/1 in err-disable state
SW#
*Aug 31 08:58:52.090: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 0010.5a0c.fd86 on port Ethernet0/1.
*Aug 31 08:58:53.096: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1,
changed state to down
SW#
*Aug 31 08:58:54.091: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to down
```

Cổng E0/1 bị đưa vào trạng thái “err – disable” và bị shutdown:

```
SW#show interfaces e0/1 status

Port      Name          Status      Vlan      Duplex  Speed Type
Et0/1           err-disabled  1         auto    auto unknown

SW#show ip interface brief e0/1
Interface      IP-Address      OK? Method Status      Protocol
Ethernet0/1    unassigned     YES unset  down        down
```

Host1 lúc này không thể truy nhập mạng được nữa vì cổng của switch nối đến nó đã bị shutdown.

Tiếp theo, ta trả địa chỉ MAC của Host1 về lại địa chỉ cũ:

```
Host1(config)#interface e0/0
Host1(config-if)#no mac-address 0010.5a0c.fd86
Host1(config-if)#end
```

```
Host1#show interfaces e0/0 | inc bia
Hardware is AmdP2, address is aabb.cc00.1000 (bia aabb.cc00.1000)
```

Cổng E0/1 lúc này vẫn ở trạng thái err – disable và vẫn bị shutdown:

```
SW#show interfaces e0/1 status
Port      Name          Status      Vlan      Duplex    Speed Type
Et0/1           err-disabled 1        auto      auto unknown
SW#show ip interface brief e0/1
Interface      IP-Address      OK? Method Status      Protocol
Ethernet0/1     unassigned      YES unset   down      down
```

Ta cần reset lại cổng bằng cách tắt rồi mở cổng lại:

```
SW(config)#interface e0/1
SW(config-if)#shutdown
SW(config-if)#no shutdown
SW(config-if)#exit
```

Cổng đã được mở ra trở lại:

```
SW#show interfaces e0/1 status
Port      Name          Status      Vlan      Duplex    Speed Type
Et0/1           connected    1        auto      auto unknown
SW#show ip interface brief e0/1
Interface      IP-Address      OK? Method Status      Protocol
Ethernet0/1     unassigned      YES unset   up       up
```

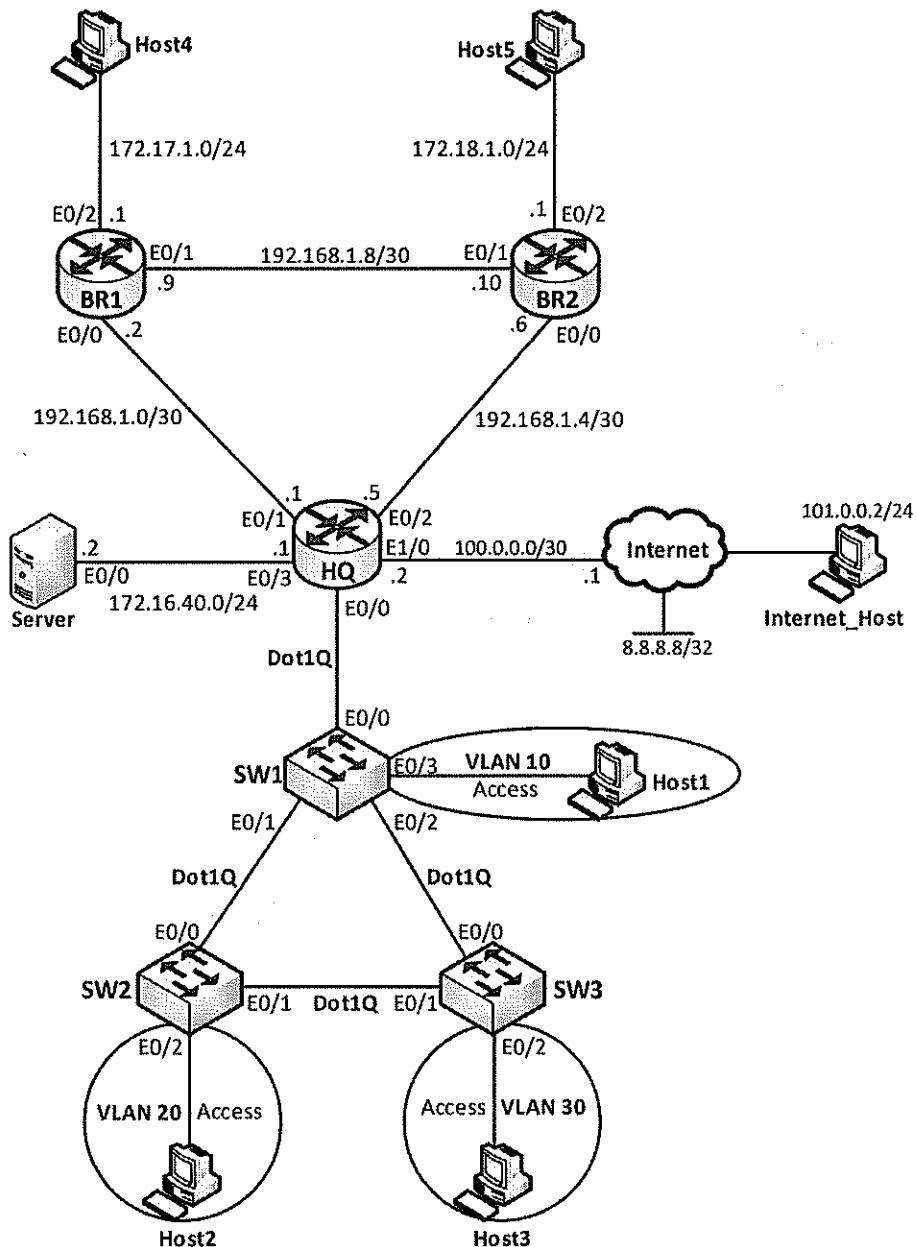
Host1 có thể truy nhập mạng trở lại:

```
Host1#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 80 percent (4/5), round-trip min/avg/max = 2/2/3 ms
```

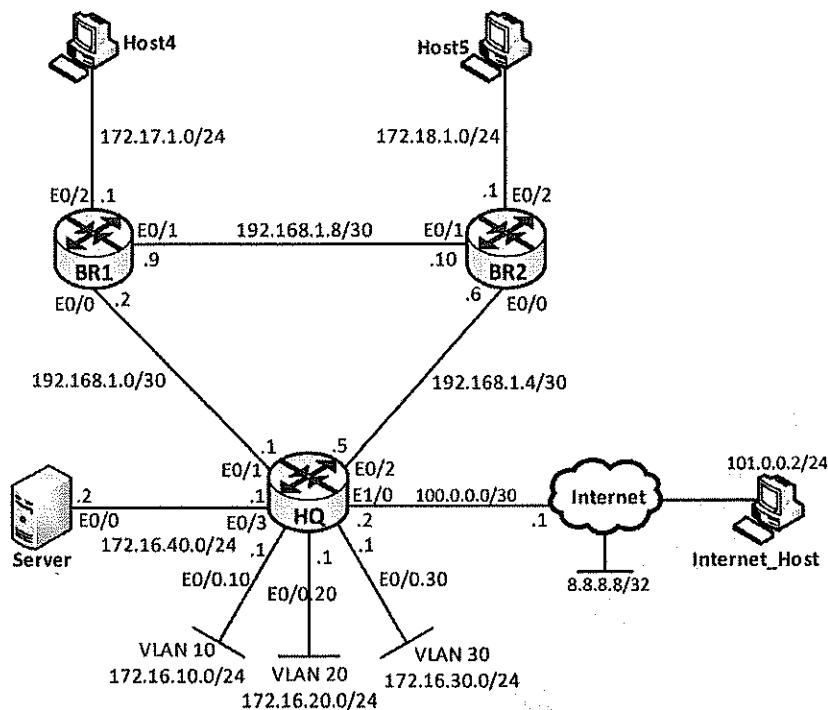
Đến đây, chúng ta đã hoàn thành các yêu cầu đặt ra của bài lab.

Lab 27 – Tổng hợp ôn tập – Bài số 1

Sơ đồ:



Hình 1 – Sơ đồ đấu nối giữa các thiết bị.



Hình 2 – Sơ đồ layer 3.

Mô tả:

- Bài lab giả lập kịch bản một mạng doanh nghiệp có 3 khu vực: Headquarters (HQ), chi nhánh 1 (BR1) và chi nhánh 2 (BR2). Tại khu vực HQ, có 3 switch đầu nối mạng cho 3 site, tạo thành một sơ đồ dạng vòng (Ring topology) layer 2.
- Thông qua bài lab này, các bạn học viên thực hiện ôn tập lại một số chủ đề cơ bản và trọng tâm của chương trình CCNA.
- Các thiết bị đều đã được cấu hình sẵn Hostname và địa chỉ IP (ngoại trừ các sub-interface của router HQ), các bạn học viên không cần phải cấu hình lại các thông số này.
- Trong suốt quá trình làm bài lab, các bạn học viên không can thiệp vào cấu hình các thiết bị: Server, router giả lập Internet, router giả lập một host trên Internet (Internet_Host).

Yêu cầu:**1. Trunking:**

- Thực hiện cấu hình tất cả các đường link kết nối giữa các switch thành các đường trunk.
- Các đường trunk này sử dụng phương pháp trunking Dot1Q, thiết lập tĩnh (mode ON).

2. VTP, VLAN:

- Cấu hình để 3 switch của HQ (SW1, SW2, SW3) tham gia VTP với các thông số như sau:
 - VTP domain: waren.
 - VTP password: cisco.
 - SW1: Server; SW2, SW3: Client.

- Trên SW1, tạo cấu hình VLAN gồm các VLAN 10, 20, 30. Kiểm tra xác nhận rằng cấu hình VLAN đã lan truyền đầy đủ đến các switch SW2 và SW3.
- Trên các switch, thực hiện gán cổng vào các VLAN đã tạo như được chỉ ra trên hình 1.

3. STP:

- Hãy cấu hình hiệu chỉnh STP trên các VLAN 10, 20 và 30 một cách thích hợp đảm bảo rằng không một đường link nào giữa các switch bị khóa hoàn toàn.
- Việc hiệu chỉnh này chỉ giới hạn trong hoạt động cấu hình root switch cho các VLAN.
- Trên các cổng access của các switch, thực hiện cấu hình tính năng để các cổng kết nối đến các end – user (Host1, Host2, Host3) chuyển qua hoạt động ngay lập tức, bỏ qua các trạng thái trung gian STP.

4. Định tuyến giữa các VLAN:

- Trên router HQ và SW1, thực hiện cấu hình để router HQ đảm nhận nhiệm vụ định tuyến giữa các VLAN theo phương pháp “Router on a Stick”.
- Các bạn học viên căn cứ vào sơ đồ hình 2 để tạo các sub – interface và đặt IP thích hợp trên các sub – interface này.

5. Cấu hình OSPF:

- Thực hiện cấu hình OSPF Area 0 trên các router đảm bảo mọi địa chỉ IP Private trên sơ đồ mạng thấy nhau (các bạn học viên nên sử dụng sơ đồ hình 2 để cấu hình yêu cầu này).

6. Hiệu chỉnh OSPF:

- Thực hiện hiệu chỉnh router – id cho các router chạy OSPF thành các giá trị như sau:
 - HQ: 10.0.0.1.
 - BR1: 10.0.0.2.
 - BR2: 10.0.0.3.
- Thực hiện hiệu chỉnh thích hợp đảm bảo dữ liệu xuất phát từ mạng LAN của BR1 đi bất cứ đâu cũng đều phải được trung chuyển qua router BR2.

7. DHCP:

- Cấu hình tại các vị trí thích hợp đảm bảo các host thuộc các VLAN 10, 20, 30 có thể nhận được cấu hình IP từ DHCP server đặt tại Server 172.16.40.2.
- Bên cạnh đó, hãy cấu hình để các router BR1 và BR2 đảm nhận vai trò DHCP server cấp phát IP cho các thiết bị Host5 và Host6 (xem hình 2).

8. Internet:

- Cấu hình trên router HQ đảm bảo các user thuộc các mạng LAN có thể truy nhập Internet thông qua IP mặt ngoài của router (100.0.0.2).
- Cấu hình hosting thiết bị Server lên môi trường Internet bằng địa chỉ 200.0.0.1 được cấp phát từ ISP.

9. Access – list:

Cấu hình access – list theo chiều out trên cổng E0/3 của router HQ thực hiện một số “rule” như sau cho các dữ liệu đi đến Server:

- Chỉ cho phép Server ping đi các thiết bị khác, không cho các thiết bị khác ping đến Server.
- Chỉ cho phép các user thuộc VLAN 10, 20, 30 truy nhập Web đến Server.
- Chỉ cho phép các user thuộc VLAN 10 được Telnet đến Server.
- Cấm tất cả các lưu lượng khác đi đến Server.

Thực hiện:**1. Trunking:****Cấu hình:**

Trên SW1:

```
SW1(config)#interface range e0/1 - 2
SW1(config-if-range)#switchport trunk encapsulation dot1q
SW1(config-if-range)#switchport mode trunk
```

Trên SW2, SW3:

```
SW2-3(config)#interface range e0/0 - 1
SW2-3(config-if-range)#switchport trunk encapsulation dot1q
SW2-3(config-if-range)#switchport mode trunk
```

Kiểm tra:

Ta thực hiện kiểm tra để xác nhận rằng các đường trunk giữa các switch đã được thiết lập đúng theo yêu cầu:

SW1#show interfaces trunk				
Port	Mode	Encapsulation	Status	Native vlan
Et0/1	on	802.1q	trunking	1
Et0/2	on	802.1q	trunking	1
(...)				

SW2-3#show interfaces trunk				
Port	Mode	Encapsulation	Status	Native vlan
Et0/0	on	802.1q	trunking	1
Et0/1	on	802.1q	trunking	1
(...)				

2. VTP, VLAN:**Cấu hình:**

Trên cả ba switch, cấu hình để chúng tham gia VTP với domain là “waren” và password là “cisco”:

```
SW1-2-3(config)#vtp domain waren
SW1-2-3(config)#vtp password cisco
```

SW1 mặc định đã hoạt động ở mode Server nên ta không cần phải cấu hình gì thêm. Ta cấu hình chuyển mode của SW2 và SW3 sang mode Client:

```
SW2(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
```

Trên SW1, ta tạo các VLAN 10, 20 và 30:

```
SW1(config)#vlan 10,20,30
```

Kiểm tra và gán cổng vào các VLAN:

Trước hết, ta kiểm tra các thông số VTP trên các switch.

Trên SW1:

```
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                : aabb.cc80.7000
Configuration last modified by 0.0.0.0 at 6-15-20 04:52:35
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    : 1
MD5 digest               : 0xA2 0xD2 0xA8 0x3E 0x0B 0x29 0xBB 0x80
                           0x7C 0x9F 0xF9 0x1A 0x1B 0xF4 0xFC 0xCD

SW1#show vtp password
VTP Password: cisco
```

Trên SW2 và SW3:

```
SW2-3#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                : aabb.cc80.8000
Configuration last modified by 0.0.0.0 at 6-15-20 04:52:35

Feature VLAN:
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 8
Configuration Revision    : 1
MD5 digest               : 0xA2 0xD2 0xA8 0x3E 0x0B 0x29 0xBB 0x80
                           0x7C 0x9F 0xF9 0x1A 0x1B 0xF4 0xFC 0xCD

SW2-3#show vtp password
VTP Password: cisco
```

Kết quả show ở trên cho thấy các switch đã được thiết lập đúng đắn các thông số VTP. Bên cạnh đó, chúng ta để ý rằng hai thông số là “Number of existing VLANs” và “Configuration Revision” trên các switch hoàn toàn giống nhau, điều này cho thấy cấu hình VLAN đã được đồng bộ giữa chúng. Chúng ta tiếp tục kiểm tra cấu hình VLAN trên các switch để xác nhận sự đồng bộ vừa nêu.

Trên SW1:

```
SW1#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Et0/0, Et0/3
10 VLAN0010	active	
20 VLAN0020	active	
30 VLAN0030	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Trên SW2 và SW3:

```
SW2-3#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Et0/2, Et0/3
10 VLAN0010	active	
20 VLAN0020	active	
30 VLAN0030	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Cấu hình VLAN đã được đồng bộ giữa các switch, chúng ta thực hiện gán các cổng vào các VLAN như được chỉ ra trên hình 1.

Trên SW1:

```
SW1(config)#interface e0/3
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
```

Trên SW2:

```
SW2(config)#interface e0/2
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 20
```

Trên SW3:

```
SW3(config)#interface e0/2
SW3(config-if)#switchport mode access
SW3(config-if)#switchport access vlan 30
```

Ta xác nhận rằng các cổng đã được gán đúng đắn trên các VLAN:

SW1#show vlan brief

VLAN	Name	Status	Ports
1	default	active	Et0/0
10	VLAN0010	active	Et0/3
20	VLAN0020	active	
30	VLAN0030	active	
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

SW2#show vlan brief

VLAN	Name	Status	Ports
1	default	active	Et0/3
10	VLAN0010	active	
20	VLAN0020	active	Et0/2
30	VLAN0030	active	
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

SW3#show vlan brief

VLAN	Name	Status	Ports
1	default	active	Et0/3
10	VLAN0010	active	
20	VLAN0020	active	
30	VLAN0030	active	Et0/2
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Đến đây, chúng ta đã hoàn tất yêu cầu về VTP và VLAN của bài lab.

3. STP:

Cấu hình:

Để đảm bảo yêu cầu không để một đường link nào bị khóa hoàn toàn, chúng ta thực hiện hiệu chỉnh để mỗi switch sẽ đảm nhận vai trò root switch cho một VLAN trong số các VLAN 10, 20 và 30;

```
SW1(config) #spanning-tree vlan 10 root primary
SW2(config) #spanning-tree vlan 20 root primary
SW3(config) #spanning-tree vlan 30 root primary
```

Ngoài ra, để các access – port trên các switch chuyển sang trạng thái hoạt động ngay lập tức, bỏ qua các trạng thái trung gian của STP, chúng ta sử dụng tính năng Portfast trên các cổng này.

Trên SW1:

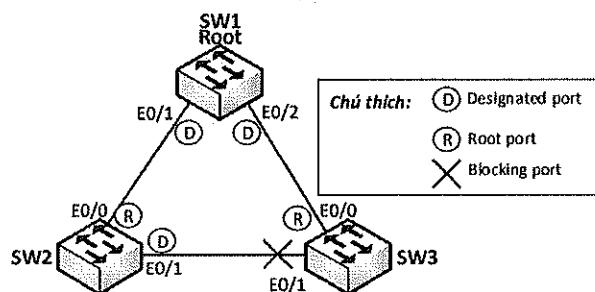
```
SW1(config) #interface e0/3
SW1(config-if) #spanning-tree portfast
```

Trên SW2 và SW3:

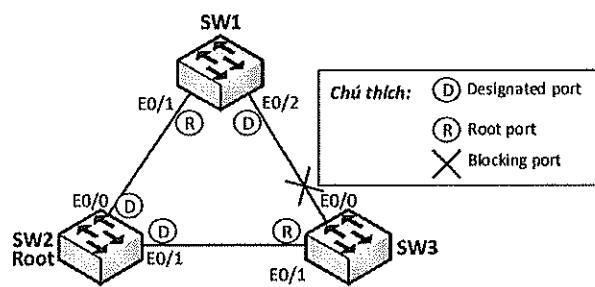
```
SW2-3(config) #interface e0/2
SW2-3(config-if) #spanning-tree portfast
```

Kiểm tra:

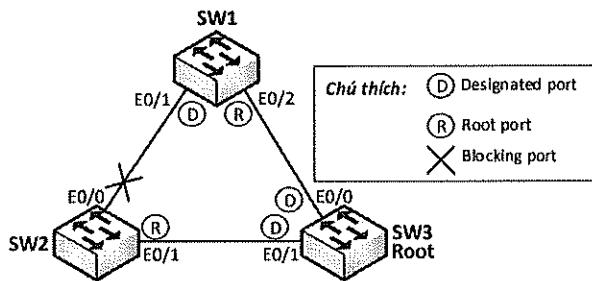
Với cấu hình STP đã thực hiện ở trên, sơ đồ layer 2 trên các VLAN hội tụ như trên các hình 3, 4 và 5 ở dưới đây:



Hình 3 – Kết quả hội tụ STP trên VLAN 10.



Hình 2 – Kết quả hội tụ STP trên VLAN 20.



Hình 5 – Kết quả hội tụ STP trên VLAN 30.

Từ các sơ đồ hội tụ ở trên ta thấy không có một đường link nào giữa các switch bị khóa hoàn toàn.

Ta có thể thực hiện kiểm tra các kết quả này bằng cách quan sát thông số STP trên các switch, ví dụ, trên VLAN 10:

```
SW1#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
              Address     aabb.cc00.7000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24586  (priority 24576 sys-id-ext 10)
              Address     aabb.cc00.7000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time   300 sec

  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----
  Et0/1          Desg FWD 100      128.2      Shr
  Et0/2          Desg FWD 100      128.3      Shr
  Et0/3          Desg FWD 100      128.4      Shr Edge

SW2#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
              Address     aabb.cc00.7000
              Cost        100
              Port        1 (Ethernet0/0)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
              Address     aabb.cc00.8000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time   300 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Et0/0	Root	FWD	100	128.1	Shr
Et0/1	Desg	FWD	100	128.2	Shr
SW3#show spanning-tree vlan 10					
VLAN0010					
Spanning tree enabled protocol ieee					
Root ID	Priority	24586			
	Address	aabb.cc00.7000			
	Cost	100			
	Port	1 (Ethernet0/0)			
	Hello Time	2 sec	Max Age 20 sec	Forward Delay 15 sec	
Bridge ID	Priority	32778 (priority 32768 sys-id-ext 10)			
	Address	aabb.cc00.9000			
	Hello Time	2 sec	Max Age 20 sec	Forward Delay 15 sec	
	Aging Time	300 sec			
Interface	Role	Sts	Cost	Prio.Nbr	Type
Et0/0	Root	FWD	100	128.1	Shr
Et0/1	Altn	BLK	100	128.2	Shr

Ta cũng có thể kiểm tra rằng các cổng access của các switch đã được bật Portfast:

```
SW1#show spanning-tree interface e0/3 portfast
VLAN0010      enabled
SW2#show spanning-tree interface e0/2 portfast
VLAN0020      enabled
SW3#show spanning-tree interface e0/2 portfast
VLAN0030      enabled
```

4. Định tuyến giữa các VLAN:

Cấu hình:

Trên HQ:

```
HQ(config)#interface e0/0
HQ(config-if)#no shutdown
HQ(config-if)#exit
HQ(config)#interface e0/0.10
HQ(config-subif)#encapsulation dot1Q 10
HQ(config-subif)#ip address 172.16.10.1 255.255.255.0
HQ(config-subif)#exit
HQ(config)#interface e0/0.20
HQ(config-subif)#encapsulation dot1Q 20
HQ(config-subif)#ip address 172.16.20.1 255.255.255.0
HQ(config-subif)#exit
```

```
HQ(config)#interface e0/0.30
HQ(config-subif)#encapsulation dot1q 30
HQ(config-subif)#ip address 172.16.30.1 255.255.255.0
HQ(config-subif)#exit
```

Trên SW1:

```
SW1(config)#interface e0/0
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
```

Kiểm tra:

```
HQ#show ip interface brief
Interface IP-Address OK? Method Status Protocol
Ethernet0/0 unassigned YES TFTP up up
Ethernet0/0.10 172.16.10.1 YES manual up up
Ethernet0/0.20 172.16.20.1 YES manual up up
Ethernet0/0.30 172.16.30.1 YES manual up up
Ethernet0/1 192.168.1.1 YES TFTP up up
Ethernet0/2 192.168.1.5 YES TFTP up up
Ethernet0/3 172.16.40.1 YES TFTP up up
Ethernet1/0 100.0.0.2 YES TFTP up up
Ethernet1/1 unassigned YES TFTP administratively down down
Ethernet1/2 unassigned YES TFTP administratively down down
Ethernet1/3 unassigned YES TFTP administratively down down

SW1#show interfaces trunk
Port Mode Encapsulation Status Native vlan
Et0/0 on 802.1q trunking 1
Et0/1 on 802.1q trunking 1
Et0/2 on 802.1q trunking 1
(...)
```

Các bạn học viên có thể cấu hình địa chỉ IP tĩnh trên các host thuộc các VLAN 10, 20, 30 và thực hiện ping giữa các host này để kiểm tra rằng router đã thực hiện được định tuyến VLAN, hoặc cũng có thể để đến khi hoàn thành yêu cầu về DHCP rồi mới tiến hành kiểm tra. Solution này sẽ để đến khi hoàn thành các yêu cầu về DHCP rồi mới thực hiện kiểm tra.

5. Cấu hình OSPF:

Cấu hình:

Trên HQ:

```
HQ(config)#router ospf 1
HQ(config-router)#network 172.16.10.1 0.0.0.0 area 0
HQ(config-router)#network 172.16.20.1 0.0.0.0 area 0
HQ(config-router)#network 172.16.30.1 0.0.0.0 area 0
HQ(config-router)#network 172.16.40.1 0.0.0.0 area 0
HQ(config-router)#network 192.168.1.1 0.0.0.0 area 0
HQ(config-router)#network 192.168.1.5 0.0.0.0 area 0
```

Trên BR1:

```
BR1(config)#router ospf 1
BR1(config-router)#network 172.17.1.1 0.0.0.0 area 0
BR1(config-router)#network 192.168.1.2 0.0.0.0 area 0
BR1(config-router)#network 192.168.1.9 0.0.0.0 area 0
```

Trên BR2:

```
BR2(config)#router ospf 1
BR2(config-router)#network 172.18.1.1 0.0.0.0 area 0
BR2(config-router)#network 192.168.1.6 0.0.0.0 area 0
BR2(config-router)#network 192.168.1.10 0.0.0.0 area 0
```

Kiểm tra:

Ta kiểm tra rằng định tuyến đã hội tụ trên các router:

```
HQ#show ip route ospf
(...)
  172.17.0.0/24 is subnetted, 1 subnets
O    172.17.1.0 [110/20] via 192.168.1.2, 00:07:29, Ethernet0/1
  172.18.0.0/24 is subnetted, 1 subnets
O    172.18.1.0 [110/20] via 192.168.1.6, 00:04:32, Ethernet0/2
  192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O      192.168.1.8/30 [110/20] via 192.168.1.6, 00:04:32, Ethernet0/2
          [110/20] via 192.168.1.2, 00:03:48, Ethernet0/1
BR1#show ip route ospf
(...)
  172.16.0.0/24 is subnetted, 4 subnets
O    172.16.10.0 [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0
O    172.16.20.0 [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0
O    172.16.30.0 [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0
O    172.16.40.0 [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0
  172.18.0.0/24 is subnetted, 1 subnets
O    172.18.1.0 [110/20] via 192.168.1.10, 00:03:52, Ethernet0/1
  192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O      192.168.1.4/30 [110/20] via 192.168.1.10, 00:03:52, Ethernet0/1
          [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0
BR2#show ip route ospf
(...)
  172.16.0.0/24 is subnetted, 4 subnets
O    172.16.10.0 [110/20] via 192.168.1.5, 00:04:43, Ethernet0/0
O    172.16.20.0 [110/20] via 192.168.1.5, 00:04:43, Ethernet0/0
O    172.16.30.0 [110/20] via 192.168.1.5, 00:04:43, Ethernet0/0
O    172.16.40.0 [110/20] via 192.168.1.5, 00:04:43, Ethernet0/0
  172.17.0.0/24 is subnetted, 1 subnets
O    172.17.1.0 [110/20] via 192.168.1.9, 00:03:58, Ethernet0/1
  192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O      192.168.1.0/30 [110/20] via 192.168.1.9, 00:03:58, Ethernet0/1
          [110/20] via 192.168.1.5, 00:04:43, Ethernet0/0
```

6. Hiệu chỉnh OSPF:

Hiệu chỉnh Router – id:

Ta quan sát router – id của các router trước khi được hiệu chỉnh:

```
HQ#show ip ospf
  Routing Process "ospf 1" with ID 192.168.1.5
  (...)

BR1#show ip ospf
  Routing Process "ospf 1" with ID 192.168.1.9
  (...)

BR2#show ip ospf
  Routing Process "ospf 1" with ID 192.168.1.10
  (...)
```

Thực hiện hiệu chỉnh router – id của các router:

```
HQ(config)#router ospf 1
HQ(config-router)#router-id 10.0.0.1
% OSPF: Reload or use "clear ip ospf process" command, for this to take effect
HQ#clear ip ospf process
Reset ALL OSPF processes? [no]: y

BR1(config)#router ospf 1
BR1(config-router)#router-id 10.0.0.2
% OSPF: Reload or use "clear ip ospf process" command, for this to take effect
BR1#clear ip ospf process
Reset ALL OSPF processes? [no]: y

BR2(config)#router ospf 1
BR2(config-router)#router-id 10.0.0.3
% OSPF: Reload or use "clear ip ospf process" command, for this to take effect
BR2#clear ip ospf process
Reset ALL OSPF processes? [no]: y
```

Sau khi tiến trình OSPF trên các router được reset, giá trị router – id đã được cập nhật:

```
HQ#show ip ospf
  Routing Process "ospf 1" with ID 10.0.0.1
  (...)

BR1#show ip ospf
  Routing Process "ospf 1" with ID 10.0.0.2
  (...)

BR2#show ip ospf
  Routing Process "ospf 1" with ID 10.0.0.3
  (...)
```

Hiệu chỉnh đường đi:

Trước khi hiệu chỉnh đường đi, BR1 sẽ chọn đường đi đến các subnet trong mạng theo một trong hai next – hop: HQ (192.168.1.1) hoặc BR2 (192.168.1.10):

```
BR1#show ip route ospf
(...)
  172.16.0.0/24 is subnetted, 4 subnets
O    172.16.10.0 [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0
O    172.16.20.0 [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0
O    172.16.30.0 [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0
O    172.16.40.0 [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0
  172.18.0.0/24 is subnetted, 1 subnets
O    172.18.1.0 [110/20] via 192.168.1.10, 00:03:52, Ethernet0/1
  192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O      192.168.1.4/30 [110/20] via 192.168.1.10, 00:03:52, Ethernet0/1
          [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0
```

Để BR1 luôn chọn đường đi đến mọi đích đến chỉ theo next – hop BR2 (192.168.1.10), ta chỉnh lại giá trị cost trên cổng E0/0 nối đến HQ cao hơn tổng cost của hai cổng E0/1 (của BR1) và E0/0 (của BR2) cộng lại:

```
BR1(config)#interface e0/0
BR1(config-if)#ip ospf cost 21
```

Lúc này, BR1 đã chọn đường đi đến mọi đích đến chỉ còn thông qua next – hop BR2 (192.168.1.10):

```
BR1#show ip route ospf
(...)
  172.16.0.0/24 is subnetted, 4 subnets
O    172.16.10.0 [110/30] via 192.168.1.10, 00:01:27, Ethernet0/1
O    172.16.20.0 [110/30] via 192.168.1.10, 00:01:27, Ethernet0/1
O    172.16.30.0 [110/30] via 192.168.1.10, 00:01:27, Ethernet0/1
O    172.16.40.0 [110/30] via 192.168.1.10, 00:01:27, Ethernet0/1
  172.18.0.0/24 is subnetted, 1 subnets
O    172.18.1.0 [110/20] via 192.168.1.10, 00:10:08, Ethernet0/1
  192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O      192.168.1.4/30 [110/20] via 192.168.1.10, 00:10:08, Ethernet0/1
```

7. DHCP:

Cấu hình:

Trên thiết bị Server đã thực hiện cấu hình sẵn chức năng DHCP server để cấp phát IP động cho các user thuộc các VLAN 10, 20, 30 (các bạn học viên có thể quan sát cấu hình này bằng cách truy nhập vào thiết bị Server – thực ra là một router giả lập vai trò của một server). Chúng ta cấu hình thêm tính năng DHCP Relay Agent trên các cổng sub – interface của router HQ để các host thuộc các VLAN vừa nêu có thể nhận được cấu hình IP:

```
HQ(config)#interface e0/0.10
HQ(config-subif)#ip helper-address 172.16.40.2
HQ(config-subif)#exit
HQ(config)#interface e0/0.20
HQ(config-subif)#ip helper-address 172.16.40.2
HQ(config-subif)#exit
HQ(config)#interface e0/0.30
HQ(config-subif)#ip helper-address 172.16.40.2
HQ(config-subif)#exit
```

Bên cạnh đó, chúng ta cấu hình các router BR1 và BR2 cấp phát IP xuống cho các host của mình theo quy hoạch IP đã chỉ ra trên hình 2:

```
BR1(config)#ip dhcp excluded-address 172.17.1.1
BR1(config)#ip dhcp pool BR1_LAN
BR1(dhcp-config)#network 172.17.1.0 /24
BR1(dhcp-config)#default-router 172.17.1.1
BR1(dhcp-config)#exit

BR2(config)#ip dhcp excluded-address 172.18.1.1
BR2(config)#ip dhcp pool BR2_LAN
BR2(dhcp-config)#network 172.18.1.0 /24
BR2(dhcp-config)#default-router 172.18.1.1
BR2(dhcp-config)#exit
```

Kiểm tra:

Ta kiểm tra rằng các host trên sơ đồ đều đã nhận được cấu hình IP từ DHCP:

```
Host1> dhcp -r
DDORA IP 172.16.10.2/24 GW 172.16.10.1

Host2> dhcp -r
DDORA IP 172.16.20.2/24 GW 172.16.20.1

Host3> dhcp -r
DDORA IP 172.16.30.2/24 GW 172.16.30.1

Host4> dhcp -r
DDORA IP 172.17.1.2/24 GW 172.17.1.1

Host5> dhcp -r
DDORA IP 172.18.1.2/24 GW 172.18.1.1
```

Bảng DHCP Binding trên các DHCP Server cho thấy các server này đã thực sự làm nhiệm vụ cấp phát IP:

Server#show ip dhcp binding			
Bindings from all pools not associated with VRF:			
IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
172.16.10.2	0100.5079.6668.0a	Jun 16 2020 11:37 AM	Automatic
172.16.20.2	0100.5079.6668.0b	Jun 16 2020 11:37 AM	Automatic
172.16.30.2	0100.5079.6668.0c	Jun 16 2020 11:37 AM	Automatic

BR1#show ip dhcp binding			
Bindings from all pools not associated with VRF:			
IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
172.17.1.2	0100.5079.6668.0d	Jun 16 2020 11:37 AM	Automatic

BR2#show ip dhcp binding			
Bindings from all pools not associated with VRF:			
IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
172.18.1.2	0100.5079.6668.0e	Jun 16 2020 11:37 AM	Automatic

Khi các host Host1, Host2, Host3 đã có IP, ta kiểm tra lại hoạt động định tuyến giữa các VLAN bằng cách cho các host này ping lẫn nhau:

```
Host1> ping 172.16.20.2
84 bytes from 172.16.20.2 icmp_seq=1 ttl=63 time=8.791 ms
84 bytes from 172.16.20.2 icmp_seq=2 ttl=63 time=5.556 ms

Host1> ping 172.16.30.2
84 bytes from 172.16.30.2 icmp_seq=1 ttl=63 time=10.738 ms
84 bytes from 172.16.30.2 icmp_seq=2 ttl=63 time=3.911 ms

Host2> ping 172.16.30.2
84 bytes from 172.16.30.2 icmp_seq=1 ttl=63 time=5.822 ms
84 bytes from 172.16.30.2 icmp_seq=2 ttl=63 time=7.434 ms
```

Kết quả ping thành công cho thấy cấu hình định tuyến VLAN thực hiện ở trên đã hoạt động tốt.

8. Internet:

Cấu hình:

Trước hết, router HQ cần có một default – route đi Internet và phải thực hiện lan truyền default – route này vào mạng bên trong:

```
HQ(config)#ip route 0.0.0.0 0.0.0.0 100.0.0.1
HQ(config)#router ospf 1
HQ(config-router)#default-information originate
```

Tiếp theo, ta thực hiện cấu hình NAT overload để các host thuộc các mạng LAN có thể truy nhập Internet thông qua IP mặt ngoài trên cổng E1/0 của router HQ:

```
HQ(config)#access-list 1 permit 172.16.10.0 0.0.0.255
HQ(config)#access-list 1 permit 172.16.20.0 0.0.0.255
HQ(config)#access-list 1 permit 172.16.30.0 0.0.0.255
HQ(config)#access-list 1 permit 172.17.1.0 0.0.0.255
HQ(config)#access-list 1 permit 172.18.1.0 0.0.0.255

HQ(config)#ip nat inside source list 1 interface e1/0 overload

HQ(config)#interface e0/0.10
HQ(config-subif)#ip nat inside
HQ(config-subif)#exit
HQ(config)#interface e0/0.20
HQ(config-subif)#ip nat inside
HQ(config-subif)#exit
HQ(config)#interface e0/0.30
HQ(config-subif)#ip nat inside
HQ(config-subif)#exit
HQ(config)#interface e0/1
HQ(config-if)#ip nat inside
HQ(config-if)#exit
HQ(config)#interface e0/2
HQ(config-if)#ip nat inside
HQ(config-if)#exit
```

```
HQ(config)#interface e1/0
HQ(config-if)#ip nat outside
HQ(config-if)#exit
```

Tiếp theo, ta cấu hình Static NAT để NAT địa chỉ Private của Server thành địa chỉ public 200.0.0.1 do ISP cấp phát cho doanh nghiệp:

```
HQ(config)#ip nat inside source static 172.16.40.2 200.0.0.1
HQ(config)#interface e0/3
HQ(config-if)#ip nat inside
HQ(config-if)#exit
```

Kiểm tra:

Ta kiểm tra rằng các host đều đã có thể truy nhập được Internet. Việc kiểm tra được thực hiện bằng cách ping đến địa chỉ 8.8.8.8 hoặc đến Internet_Host (ở đây ta chọn ping đến 8.8.8.8):

```
Host1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=3.411 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=3.069 ms
(...)

Host2> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=5.243 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=3.577 ms
(...)

Host3> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=3.810 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=4.190 ms
(...)

Host4> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=4.859 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=3.527 ms
(...)

Host5> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=3.476 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=2.915 ms
(...)
```

Bảng NAT của router HQ cho thấy hoạt động NAT overload đã diễn ra:

HQ#show ip nat translations				
Pro	Inside global	Inside local	Outside local	Outside global
icmp	100.0.0.2:8764	172.16.10.2:8764	8.8.8.8:8764	8.8.8.8:8764
icmp	100.0.0.2:9276	172.16.20.2:9276	8.8.8.8:9276	8.8.8.8:9276
icmp	100.0.0.2:9532	172.16.30.2:9532	8.8.8.8:9532	8.8.8.8:9532
---	200.0.0.1	172.16.40.2	---	---
icmp	100.0.0.2:10044	172.17.1.2:10044	8.8.8.8:10044	8.8.8.8:10044
icmp	100.0.0.2:10556	172.18.1.2:10556	8.8.8.8:10556	8.8.8.8:10556

Tiếp theo, ta thử từ Internet_Host, là một thiết bị giả lập một user trên Internet truy nhập đến thiết bị Server nằm bên trong mạng:

```
Internet_Host#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:
!!!!! <- Ping thành công đến Server bên trong
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

Internet_Host#telnet 200.0.0.1
Trying 200.0.0.1 ... Open <- Telnet thành công đến Server bên trong

Password required, but none set

[Connection to 200.0.0.1 closed by foreign host]

Internet_Host#telnet 200.0.0.1 80
Trying 200.0.0.1, 80 ... Open <- Truy nhập HTTP thành công đến Server bên trong
exit
HTTP/1.1 400 Bad Request
Date: Tue, 16 Jun 2020 03:30:31 GMT
Server: cisco-IOS
Accept-Ranges: none
400 Bad Request
[Connection to 200.0.0.1 closed by foreign host]
Internet_Host#
```

Kết quả phản hồi từ HTTP Server

Bảng NAT của router HQ cho thấy hoạt động Static NAT đã diễn ra phù hợp cho các truy nhập vừa thực hiện từ Internet_Host đến Server:

HQ#show ip nat translations				
Pro	Inside global	Inside local	Outside local	Outside global
icmp	200.0.0.1:0	172.16.40.2:0	101.0.0.2:0	101.0.0.2:0
tcp	200.0.0.1:23	172.16.40.2:23	101.0.0.2:17005	101.0.0.2:17005
tcp	200.0.0.1:80	172.16.40.2:80	101.0.0.2:44149	101.0.0.2:44149
---	200.0.0.1	172.16.40.2	---	---

Đến đây, chúng ta đã cấu hình và kiểm tra thành công hoạt động NAT trên router HQ.

9. Access – list:

Cấu hình:

Trước hết, để chỉ cho phép ping một chiều từ Server ra ngoài, ta chỉ cho phép lưu lượng ICMP Echo – Reply đi ra khỏi cổng E0/3 của HQ để đi đến Server (lưu lượng này chính là kết quả trả về cho hoạt động ping thành công từ Server):

```
HQ(config)#ip access-list extended FIREWALL
HQ(config-ext-nacl)#permit icmp any host 172.16.40.2 echo-reply
```

Tiếp theo, ta chỉ cho phép lưu lượng TCP đi đến port 80 (HTTP) của Server mà xuất phát từ các subnet được cho phép (gồm: 172.16.10.0/24 – VLAN 10, 172.16.20.0/24 – VLAN 20, 172.16.30.0/24 – VLAN 30):

```
HQ(config-ext-nacl)#permit tcp 172.16.10.0 0.0.0.255 host 172.16.40.2 eq 80
HQ(config-ext-nacl)#permit tcp 172.16.20.0 0.0.0.255 host 172.16.40.2 eq 80
HQ(config-ext-nacl)#permit tcp 172.16.30.0 0.0.0.255 host 172.16.40.2 eq 80
```

Cuối cùng, ta cho phép lưu lượng TCP đi đến port 23 (Telnet) của Server mà xuất phát từ subnet 172.16.10.0/24 (VLAN 10):

```
HQ(config-ext-nacl)#permit tcp 172.16.10.0 0.0.0.255 host 172.16.40.2 eq 23
HQ(config-ext-nacl)#exit
```

Các lưu lượng khác sẽ bị chặn lại bởi entry ngầm định “deny ip any any” của access – list “FIREWALL” vừa cấu hình ở trên.

Sau khi cấu hình access – list, ta thực hiện đặt nó lên cổng E0/3 của HQ theo chiều out như yêu cầu đặt ra:

```
HQ(config)#interface e0/3
HQ(config-if)#ip access-group FIREWALL out
HQ(config-if)#exit
```

Kiểm tra:

Ta kiểm tra lại nội dung của access – list vừa cấu hình:

```
HQ#show access-lists FIREWALL
Extended IP access list FIREWALL
 10 permit icmp any host 172.16.40.2 echo-reply
 20 permit tcp 172.16.10.0 0.0.0.255 host 172.16.40.2 eq www
 30 permit tcp 172.16.20.0 0.0.0.255 host 172.16.40.2 eq www
 40 permit tcp 172.16.30.0 0.0.0.255 host 172.16.40.2 eq www
 50 permit tcp 172.16.10.0 0.0.0.255 host 172.16.40.2 eq telnet
```

Access – list này đã được đặt trên cổng E0/3 đúng theo yêu cầu:

```
HQ#show ip interface e0/3 | inc access list
Outgoing access list is FIREWALL
Inbound access list is not set
```

Ta bắt đầu kiểm tra hoạt động của access – list.

Đầu tiên, ta thử rằng Server có thể ping đến các host khác nhưng các host khác không thể ping Server, ví dụ, Host1 và Internet_Host:

```
Server#ping 172.16.10.2 <- Server ping thành công Host1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

Host1> ping 172.16.40.2 <- Host1 không ping được Server
*172.16.10.1 icmp_seq=1 ttl=255 time=3.041 ms (ICMP type:3, code:13, Communication administratively prohibited)
*172.16.10.1 icmp_seq=2 ttl=255 time=2.544 ms (ICMP type:3, code:13, Communication administratively prohibited)
(...)
```

Tiếp theo, ta kiểm tra rằng chỉ có những subnet được cho phép mới được phép truy nhập Web đến Server, ví dụ, Host2:

```
Host2> ping 172.16.40.2 -P 6 -p 80 <- Host2 truy nhập HTTP thành công đến Server
Connect 80@172.16.40.2 seq=1 ttl=254 time=2.469 ms
SendData 80@172.16.40.2 seq=1 ttl=254 time=2.844 ms
Close    80@172.16.40.2 seq=1 ttl=254 time=4.893 ms
(...)

Host4> ping 172.16.40.2 -P 6 -p 80 <- Host4 bị chặn truy nhập HTTP đến Server
*192.168.1.5 tcp_seq=1 ttl=254 time=2.685 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.1.5 tcp_seq=3 ttl=254 time=2.711 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.1.5 tcp_seq=5 ttl=254 time=2.907 ms (ICMP type:3, code:13, Communication administratively prohibited)
```

Ghi chú:

Các host trên các mạng LAN trong bài lab này được giả lập bằng chương trình VPC trên phần mềm EVE. Trên chương trình này không tích hợp telnet nên ta sử dụng lệnh ping đến 172.16.40.2 với protocol – ID = 6 (“-P 6”), chính là protocol – ID của TCP và destination port = 80 (“-p 80”), chính là port TCP của ứng dụng HTTP.

Tiếp theo, ta kiểm tra “rule” Telnet (chỉ có các host thuộc VLAN 10 và subnet 101.0.0.0/24 mới có thể telnet đến Server):

```
Host1> ping 172.16.40.2 -P 6 -p 23 <- Host1 Telnet được đến Server
Connect 23@172.16.40.2 seq=1 ttl=254 time=2.549 ms
SendData 23@172.16.40.2 seq=1 ttl=254 time=2.565 ms
Close    23@172.16.40.2 timeout(16.601ms)
(...)

Host5> ping 172.16.40.2 -P 6 -p 23 <- Host5 bị chặn Telnet đến Server
*192.168.1.5 tcp_seq=1 ttl=254 time=1.573 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.1.5 tcp_seq=3 ttl=254 time=2.620 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.1.5 tcp_seq=5 ttl=254 time=1.542 ms (ICMP type:3, code:13, Communication administratively prohibited)
```

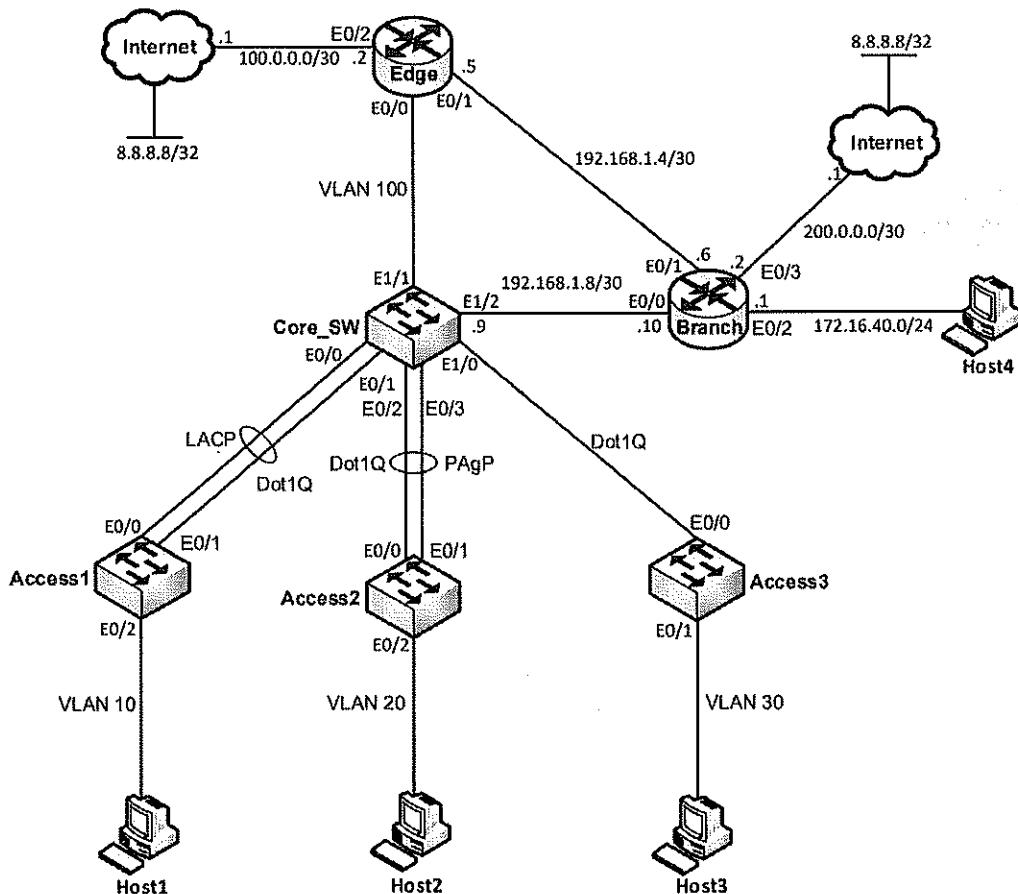
Kết quả kiểm tra access – list FIREWALL trên router HQ cho thấy các “rule” đã hoạt động:

```
HQ#show access-lists FIREWALL
Extended IP access list FIREWALL
  10 permit icmp any host 172.16.40.2 echo-reply (10 matches)
  20 permit tcp 172.16.10.0 0.0.0.255 host 172.16.40.2 eq www
  30 permit tcp 172.16.20.0 0.0.0.255 host 172.16.40.2 eq www (25 matches)
  40 permit tcp 172.16.30.0 0.0.0.255 host 172.16.40.2 eq www
  50 permit tcp 172.16.10.0 0.0.0.255 host 172.16.40.2 eq telnet (28 matches)
```

Đến đây, chúng ta đã hoàn tất cấu hình và kiểm tra tác vụ về access – list của bài lab.

Lab 28 – Tổng hợp ôn tập – Bài số 2

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Bài lab gồm các thiết bị được kết nối với nhau theo sơ đồ được chỉ ra trong hình 1. Trong sơ đồ này, hệ thống switch và router Edge đóng vai trò là các thiết bị của trung tâm của một mạng doanh nghiệp, router Branch đóng vai trò là router tại một trung tâm chi nhánh của doanh nghiệp này.
- Trong bài lab này, các bạn học viên sẽ thực hành ôn tập lại các vấn đề về Ethernet switching, định tuyến OSPF cũng như một số dịch vụ mạng như DHCP và Internet.
- Trên bài lab này, các thiết bị đều đã được thiết lập sẵn hostname; ngoài ra, các router còn được cấu hình sẵn địa chỉ IP trên các cổng; các bạn học viên không cần phải thiết lập lại các thông số này. Bên cạnh đó, trong suốt quá trình thực hiện bài lab, các bạn học viên không can thiệp vào thiết bị già lập Internet.

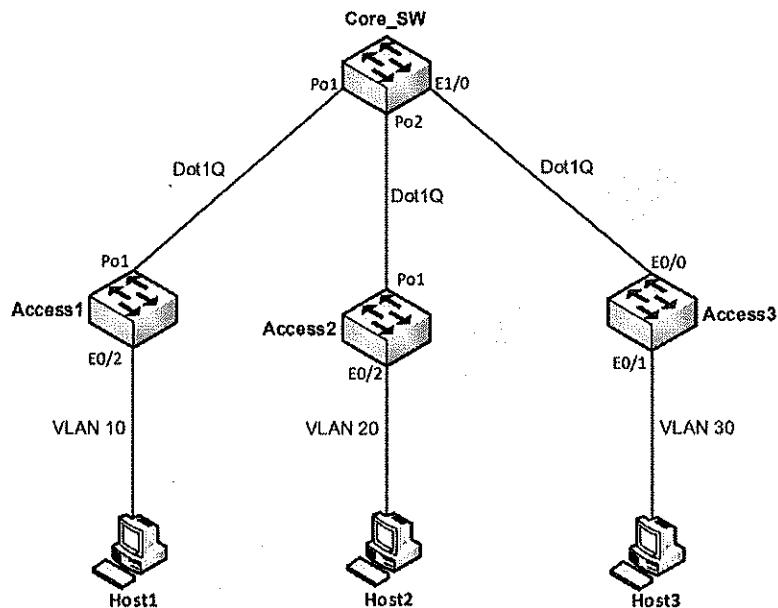
Yêu cầu:**1. Etherchannel:**

Thực hiện cấu hình các đường Etherchannel như được mô tả trong hình 1, trong đó:

- Đường Etherchannel nối giữa Core_SW và Access1 sử dụng phương thức thiết lập channel LACP.
- Đường Etherchannel nối giữa Core_SW và Access2 sử dụng phương thức thiết lập channel PAgP.

2. Trunking:

- Sau khi thiết lập xong Etherchannel, đầu nối giữa các switch có thể được mô tả lại như trên sơ đồ hình 2 dưới đây:



Hình 2 – Kết nối giữa các switch.

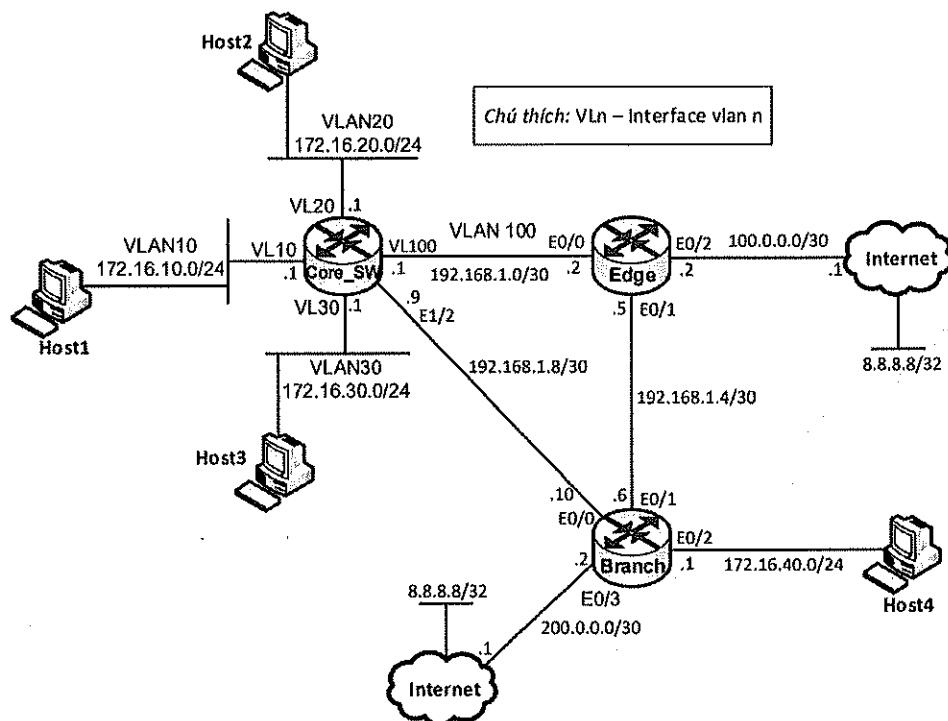
- Hãy thực hiện cấu hình các link giữa các switch thành các đường Trunking Dot1Q.

3. VTP, VLAN:

- Thực hiện cho các switch tham gia VTP với các thông số như sau:
 - VTP domain: *waren*.
 - VTP password: *cisco*.
 - Core_SW: Server; Access1, Access2, Access3: Client.
- Thực hiện tạo các VLAN 10, 20, 30 trên Core_SW, kiểm tra rằng cấu hình VLAN này được tự động đồng bộ xuống các switch Access1, Access2, Access3.
- Trên các switch access, thực hiện gán cổng vào các VLAN như được chỉ ra trên các sơ đồ ở trên.

4. Xây dựng layer 3 topology:

- Cấu hình switch Core_SW thực hiện định tuyến giữa các VLAN theo các thông số như được chỉ ra trên sơ đồ layer 3 ở hình 3:



Hình 3 – Layer 3 topology.

- Ngoài ra, cũng trên Core_SW, thực hiện tạo thêm VLAN 100 cùng SVI tương ứng và chuyển cổng E1/2 thành cổng layer 3 để tạo kết nối IP đến các router như mô tả trên hình 3. Các bạn học viên cũng cần phải đặt địa chỉ IP cho các cổng layer 3 mới tạo ra này theo quy hoạch IP được chỉ ra trên hình 3.

5. Định tuyến OSPF:

Thực hiện cấu hình định tuyến OSPF Area 0 giữa các router và switch layer 3 trên hình 3 đảm bảo mọi địa chỉ trên sơ đồ thấy nhau.

6. DHCP:

- Thực hiện cấu hình router Edge làm DHCP server cấp phát IP cho các host thuộc các VLAN 10, 20, và 30.
- Cấu hình router Branch cấp phát IP cho Host4.

7. Hiệu chỉnh đường đi:

Hãy hiệu chỉnh OSPF đảm bảo hoạt động trao đổi dữ liệu giữa các host thuộc hai chi nhánh đều phải thông qua router Edge, đường link nối giữa Core_SW và Branch chỉ sử dụng để dự phòng.

8. Internet:

Thực hiện cấu hình hoạt động truy nhập Internet cho các host của doanh nghiệp này theo yêu cầu sau:

- Các host thuộc trụ sở chính (các VLAN 10, 20, 30) sẽ đi Internet theo đường truyền Internet tại router Edge của trụ sở chính.

- Các host thuộc chi nhánh (mạng LAN 172.16.40.0/24) sẽ đi Internet theo đường truyền Internet tại chi nhánh.
- Hoạt động truy nhập Internet vừa nêu trên hai trụ sở sẽ được sử dụng để dự phòng lẫn nhau: trụ sở nào bị mất kết nối Internet sẽ truy nhập Internet thông qua đường truyền của trụ sở còn lại; nếu đường chính được khôi phục sẽ lại truy nhập Internet theo đường chính trên chi nhánh của mình.

Thực hiện:

1. Etherchannel:

Cấu hình:

Trước hết, chúng ta thiết lập Etherchannel giữa Core_SW và Access1 bằng giao thức LACP.

Trên Core_SW:

```
Core_SW(config)#interface range e0/0 - 1
Core_SW(config-if-range)#shutdown
Core_SW(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1

Core_SW(config-if-range)#no shutdown
```

Trên Access1:

```
Access1(config)#interface range e0/0 - 1
Access1(config-if-range)#shutdown
Access1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1

Access1(config-if-range)#no shutdown
```

Tiếp theo, chúng ta thiết lập Etherchannel nối giữa Core_SW và Access2 bằng PAgP.

Trên Core_SW:

```
Core_SW(config)#interface range e0/2 - 3
Core_SW(config-if-range)#shutdown
Core_SW(config-if-range)#channel-group 2 mode desirable
Creating a port-channel interface Port-channel 2

Core_SW(config-if-range)#no shutdown
```

Trên Access2:

```
Access2(config)#interface range e0/0 - 1
Access2(config-if-range)#shutdown
Access2(config-if-range)#channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1

Access2(config-if-range)#no shutdown
```

Kiểm tra:

Chúng ta kiểm tra rằng các đường Etherchannel đã được thiết lập đúng theo yêu cầu.

Trên Core_SW:

```
Core_SW#show etherchannel summary
Flags: D - down      P - bundled in port-channel
       I - stand-alone S - suspended
       H - Hot-standby (LACP only)
       R - Layer3      S - Layer2
       U - in use       N - not in use, no aggregation
       f - failed to allocate aggregator

       M - not in use, minimum links not met
       m - not in use, port not aggregated due to minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

       A - formed by Auto LAG

Number of channel-groups in use: 3
Number of aggregators: 3

Group Port-channel Protocol Ports
-----+-----+-----+
1    Po1 (SU)     LACP    Et0/0 (P)  Et0/1 (P)
2    Po2 (SU)     PAgP    Et0/2 (P)  Et0/3 (P)
```

Trên Access1:

```
Access1#show etherchannel summary
Flags: D - down      P - bundled in port-channel
       I - stand-alone S - suspended
       H - Hot-standby (LACP only)
       R - Layer3      S - Layer2
       U - in use       N - not in use, no aggregation
       f - failed to allocate aggregator

       M - not in use, minimum links not met
       m - not in use, port not aggregated due to minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

       A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators: 1
```

Group	Port-channel	Protocol	Ports
1	Pol(SU)	LACP	Et0/0(P) Et0/1(P)

Trên Access2:

```
Access2#show etherchannel summary
Flags:  D - down          P - bundled in port-channel
       I - stand-alone  S - suspended
       H - Hot-standby (LACP only)
       R - Layer3         S - Layer2
       U - in use         N - not in use, no aggregation
       f - failed to allocate aggregator

       M - not in use, minimum links not met
       m - not in use, port not aggregated due to minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

       A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:           1

Group Port-channel Protocol Ports
-----+-----+-----+
1     Pol(SU)      PAgP    Et0/0(P) Et0/1(P)
```

2. Trunking:

Cấu hình:

Trên Core_SW:

```
Core_SW(config)#interface range po 1 - 2,e1/0
Core_SW(config-if-range)#switchport trunk encapsulation dot1q
Core_SW(config-if-range)#switchport mode trunk
```

Cấu hình trunking trên các cổng Po1 của các switch access:

```
Access1-2(config)#interface po 1
Access1-2(config-if)#switchport trunk encapsulation dot1q
Access1-2(config-if)#switchport mode trunk
```

Trên Access3:

```
Access3(config)#interface e0/0
Access3(config-if)#switchport trunk encapsulation dot1q
Access3(config-if)#switchport mode trunk
```

Kiểm tra:

Trên Core_SW:

```
Core_SW#show interfaces trunk

Port      Mode          Encapsulation  Status      Native vlan
Et1/0     on           802.1q        trunking   1
Po1       on           802.1q        trunking   1
Po2       on           802.1q        trunking   1

Port      Vlans allowed on trunk
Et1/0     1-4094
Po1       1-4094
Po2       1-4094

Port      Vlans allowed and active in management domain
Et1/0     1
Po1       1
Po2       1

Port      Vlans in spanning tree forwarding state and not pruned
Et1/0     1
Po1       1
Po2       1
```

Trên các switch Access1 và Access2:

```
Access1-2#show interfaces trunk

Port      Mode          Encapsulation  Status      Native vlan
Po1       on           802.1q        trunking   1

Port      Vlans allowed on trunk
Po1       1-4094

Port      Vlans allowed and active in management domain
Po1       1

Port      Vlans in spanning tree forwarding state and not pruned
Po1       1
```

Trên Access3:

```
Access3#show interfaces trunk

Port      Mode          Encapsulation  Status      Native vlan
Et0/0    on           802.1q        trunking   1

Port      Vlans allowed on trunk
Et0/0    1-4094

Port      Vlans allowed and active in management domain
```

```
Et0/0      1
Port        Vlans in spanning tree forwarding state and not pruned
Et0/0      1
```

3. VTP, VLAN:

Cấu hình VTP và VLAN:

Thực hiện cấu hình cho các switch tham gia VTP. Trên cả 4 switch (mode config):

```
vtp domain waren
vtp password cisco
```

Trên các switch access:

```
Access1-2-3(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
```

Thực hiện tạo VLAN trên Core_SW theo yêu cầu đặt ra:

```
Core_SW(config)#vlan 10,20,30
Core_SW(config-vlan)#exit
```

Kiểm tra và gán cổng vào các VLAN:

Ta kiểm tra rằng thông số VTP đã được thiết lập đúng đắn trên các switch.

Trên Core_SW:

```
Core_SW#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                   : aabb.cc80.1000
Configuration last modified by 0.0.0.0 at 11-11-20 13:52:06
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       : 1
MD5 digest                  : 0x9D 0x26 0x16 0x09 0x69 0xC6 0x5C 0xFD
                                0x65 0x35 0x59 0xE1 0x8A 0x32 0xD4 0x63

Core_SW#show vtp password
VTP Password: cisco
```

Trên các switch access, kiểm tra ví dụ trên switch Access1:

```
Access1#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                    : aabb.cc80.2000
Configuration last modified by 0.0.0.0 at 11-11-20 13:52:06

Feature VLAN:
-----
VTP Operating Mode           : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs      : 8
Configuration Revision        : 1
MD5 digest                   : 0x9D 0x26 0x16 0x09 0x69 0xC6 0x5C 0xFD
                                0x65 0x35 0x59 0xE1 0x8A 0x32 0xD4 0x63
Access1#show vtp password
VTP Password: cisco
```

Ta có thể thực hiện kiểm tra VTP tương tự trên các switch access còn lại.

Tiếp theo, ta thực hiện kiểm tra rằng cấu hình VLAN mới tạo ra đã được đồng bộ giữa các switch.

Trên Core_SW:

```
Core_SW#show vlan brief
VLAN Name                  Status    Ports
----- -----
1  default                  active    Et1/1, Et1/2, Et1/3
10 VLAN0010                active
20 VLAN0020                active
30 VLAN0030                active
1002 fddi-default          act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default         act/unsup
```

Trên Access1 và Access2:

```
Access1-2#show vlan brief
VLAN Name                  Status    Ports
----- -----
1  default                  active    Et0/2, Et0/3, Et1/0, Et1/1
                                         Et1/2, Et1/3
10 VLAN0010                active
20 VLAN0020                active
30 VLAN0030                active
1002 fddi-default          act/unsup
```

1003 token-ring-default	act/unsup
1004 fddinet-default	act/unsup
1005 trnet-default	act/unsup

Trên Access3:

Access3#show vlan brief

VLAN Name	Status	Ports
1 default	active	Et0/1, Et0/2, Et0/3, Et1/0 Et1/1, Et1/2, Et1/3
10 VLAN0010	active	
20 VLAN0020	active	
30 VLAN0030	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Cuối cùng, ta thực hiện gán các cổng vào các VLAN như được chỉ ra trên sơ đồ:

```
Access1(config) #interface e0/2
Access1(config-if)#switchport mode access
Access1(config-if)#switchport access vlan 10

Access2(config) #interface e0/2
Access2(config-if)#switchport mode access
Access2(config-if)#switchport access vlan 20

Access3(config) #interface e0/1
Access3(config-if)#switchport mode access
Access3(config-if)#switchport access vlan 30
```

4. Xây dựng layer 3 topology:

Cấu hình:

Trước hết, trên Core_SW, ta tạo VLAN 100 và interface vlan 100 để kết nối IP đến router Edge:

```
Core_SW(config) #vlan 100
Core_SW(config-vlan)#name TO_EDGE
Core_SW(config-vlan)#exit
Core_SW(config) #interface e1/1
Core_SW(config-if)#switchport mode access
Core_SW(config-if)#switchport access vlan 100
Core_SW(config-if)#exit
Core_SW(config) #interface vlan 100
Core_SW(config-if)#description TO EDGE
Core_SW(config-if)#no shutdown
Core_SW(config-if)#ip address 192.168.1.1 255.255.255.252
Core_SW(config-if)#exit
```

```
Core_SW(config)#interface e1/2
Core_SW(config-if)#description TO BRANCH
Core_SW(config-if)#no switchport
Core_SW(config-if)#ip address 192.168.1.9 255.255.255.252
Core_SW(config-if)#exit
```

Tiếp theo, ta tạo các SVI (interface VLAN) kết nối đến các VLAN 10, 20 và 30 để thực hiện định tuyến VLAN giữa các VLAN này:

```
Core_SW(config)#interface vlan 10
Core_SW(config-if)#no shutdown
Core_SW(config-if)#ip address 172.16.10.1 255.255.255.0
Core_SW(config-if)#exit
Core_SW(config)#interface vlan 20
Core_SW(config-if)#no shutdown
Core_SW(config-if)#ip address 172.16.20.1 255.255.255.0
Core_SW(config-if)#exit
Core_SW(config)#interface vlan 30
Core_SW(config-if)#ip address 172.16.30.1 255.255.255.0
Core_SW(config-if)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng các cổng layer 3 đã được tạo đầy đủ trên Core_SW:

Core_SW#show ip interface brief					
Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	unassigned	YES	unset	up	up
Ethernet0/1	unassigned	YES	unset	up	up
Ethernet0/2	unassigned	YES	unset	up	up
Ethernet0/3	unassigned	YES	unset	up	up
Ethernet1/0	unassigned	YES	unset	up	up
Ethernet1/1	unassigned	YES	unset	up	up
Ethernet1/2	192.168.1.9	YES	manual	up	up
Ethernet1/3	unassigned	YES	unset	up	up
Port-channel1	unassigned	YES	unset	up	up
Port-channel2	unassigned	YES	unset	up	up
Vlan10	172.16.10.1	YES	manual	up	up
Vlan20	172.16.20.1	YES	manual	up	up
Vlan30	172.16.30.1	YES	manual	up	up
Vlan100	192.168.1.1	YES	manual	up	up

Ta kiểm tra rằng Switch đã thông suốt kết nối IP với hai router Edge và Branch:

```
Core_SW#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 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms
```

```
Core_SW#ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Đến đây, chúng ta đã xây dựng xong sơ đồ layer 3 ở hình 3. Tiếp theo, chúng ta thực hiện cấu hình định tuyến đảm bảo full – reachability cho sơ đồ này.

5. Định tuyến OSPF:

Cấu hình:

Trên Core_SW:

```
Core_SW(config)#ip routing
Core_SW(config)#router ospf 1
Core_SW(config-router)#network 172.16.10.0 0.0.0.255 area 0
Core_SW(config-router)#network 172.16.20.0 0.0.0.255 area 0
Core_SW(config-router)#network 172.16.30.0 0.0.0.255 area 0
Core_SW(config-router)#network 192.168.1.0 0.0.0.3 area 0
Core_SW(config-router)#network 192.168.1.8 0.0.0.3 area 0
Core_SW(config-router)#exit
```

Trên Edge:

```
Edge(config)#router ospf 1
Edge(config-router)#network 192.168.1.0 0.0.0.3 area 0
Edge(config-router)#network 192.168.1.4 0.0.0.3 area 0
Edge(config-router)#exit
```

Trên Branch:

```
Branch(config)#router ospf 1
Branch(config-router)#network 172.16.40.0 0.0.0.255 area 0
Branch(config-router)#network 192.168.1.4 0.0.0.3 area 0
Branch(config-router)#network 192.168.1.8 0.0.0.3 area 0
Branch(config-router)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng định tuyến OSPF đã hội tụ trên sơ đồ:

```
Core_SW#show ip route ospf
(...)
    172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
O        172.16.40.0/24 [110/20] via 192.168.1.10, 00:02:28, Ethernet1/2
          192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O        192.168.1.4/30 [110/11] via 192.168.1.2, 00:01:51, Vlan100
Edge#show ip route ospf
(...)
    172.16.0.0/24 is subnetted, 4 subnets
O        172.16.10.0 [110/11] via 192.168.1.1, 00:03:14, Ethernet0/0
O        172.16.20.0 [110/11] via 192.168.1.1, 00:03:14, Ethernet0/0
```

```
O      172.16.30.0 [110/11] via 192.168.1.1, 00:03:14, Ethernet0/0
O      172.16.40.0 [110/20] via 192.168.1.6, 00:02:00, Ethernet0/1
      192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O      192.168.1.8/30 [110/20] via 192.168.1.6, 00:02:00, Ethernet0/1
                  [110/20] via 192.168.1.1, 00:03:14, Ethernet0/0
Branch#show ip route ospf
(...)
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O      172.16.10.0/24 [110/11] via 192.168.1.9, 00:02:40, Ethernet0/0
O      172.16.20.0/24 [110/11] via 192.168.1.9, 00:02:40, Ethernet0/0
O      172.16.30.0/24 [110/11] via 192.168.1.9, 00:02:40, Ethernet0/0
      192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O      192.168.1.0/30 [110/11] via 192.168.1.9, 00:02:40, Ethernet0/0
```

Việc kiểm tra rằng các host có thể đi đến nhau được sẽ được thực hiện sau câu DHCP.

6. DHCP:

Cấu hình:

Trước hết, ta thực hiện cấu hình để router Edge có thể cấp phát IP được cho các host thuộc các VLAN 10, 20, 30 của trụ sở chính:

```
Edge(config)#ip dhcp pool VLAN10
Edge(dhcp-config)#network 172.16.10.0 /24
Edge(dhcp-config)#default-router 172.16.10.1
Edge(dhcp-config)#exit
Edge(config)#ip dhcp pool VLAN20
Edge(dhcp-config)#network 172.16.20.0 /24
Edge(dhcp-config)#default-router 172.16.20.1
Edge(dhcp-config)#exit
Edge(config)#ip dhcp pool VLAN30
Edge(dhcp-config)#network 172.16.30.0 /24
Edge(dhcp-config)#default-router 172.16.30.1
Edge(dhcp-config)#exit

Core_SW(config)#interface vlan 10
Core_SW(config-if)#ip helper-address 192.168.1.2
Core_SW(config-if)#exit
Core_SW(config)#interface vlan 20
Core_SW(config-if)#ip helper-address 192.168.1.2
Core_SW(config-if)#exit
Core_SW(config)#interface vlan 30
Core_SW(config-if)#ip helper-address 192.168.1.2
Core_SW(config-if)#exit
```

Tiếp theo, ta cấu hình để router Branch cấp phát IP cho các host thuộc mạng LAN của chi nhánh:

```
Branch(config)#ip dhcp pool BRANCH
Branch(dhcp-config)#network 172.16.40.0 /24
Branch(dhcp-config)#default-router 172.16.40.1
Branch(dhcp-config)#exit
```

Kiểm tra:

Ta kiểm tra rằng các host đều đã nhận được IP từ DHCP:

```
Host1> dhcp -r
DDORA IP 172.16.10.2/24 GW 172.16.10.1

Host2> dhcp -r
DDORA IP 172.16.20.2/24 GW 172.16.20.1

Host3> dhcp -r
DDORA IP 172.16.30.2/24 GW 172.16.30.1

Host4> dhcp -r
DDORA IP 172.16.40.2/24 GW 172.16.40.1
```

Ta cũng kiểm tra rằng các router Edge và Branch đã thực hiện cấp phát các IP ở trên xuống cho các host:

```
Edge#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/           Lease expiration      Type
                  Hardware address/
                  User name
172.16.10.2        0100.5079.6668.09   Nov 17 2020 09:50 AM Automatic
172.16.20.2        0100.5079.6668.0a   Nov 17 2020 09:50 AM Automatic
172.16.30.2        0100.5079.6668.0b   Nov 17 2020 09:50 AM Automatic

Branch#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/           Lease expiration      Type
                  Hardware address/
                  User name
172.16.40.2        0100.5079.6668.0c   Nov 17 2020 09:51 AM Automatic
```

Các host này đã có thể đi đến được nhau cho thấy hoạt động định tuyến giữa các VLAN cũng như định tuyến giữa hai chi nhánh đã thông suốt:

```
Host1> ping 172.16.20.2
84 bytes from 172.16.20.2 icmp_seq=1 ttl=63 time=3.134 ms
84 bytes from 172.16.20.2 icmp_seq=2 ttl=63 time=4.894 ms

Host1> ping 172.16.30.2
84 bytes from 172.16.30.2 icmp_seq=1 ttl=63 time=3.837 ms
84 bytes from 172.16.30.2 icmp_seq=2 ttl=63 time=4.035 ms

Host1> ping 172.16.40.2
84 bytes from 172.16.40.2 icmp_seq=1 ttl=62 time=4.301 ms
84 bytes from 172.16.40.2 icmp_seq=2 ttl=62 time=1.537 ms

Host2> ping 172.16.30.2
84 bytes from 172.16.30.2 icmp_seq=1 ttl=63 time=5.743 ms
84 bytes from 172.16.30.2 icmp_seq=2 ttl=63 time=1.993 ms

Host2> ping 172.16.40.2
84 bytes from 172.16.40.2 icmp_seq=1 ttl=62 time=4.153 ms
84 bytes from 172.16.40.2 icmp_seq=2 ttl=62 time=4.199 ms
```

```
Host3> ping 172.16.40.2
84 bytes from 172.16.40.2 icmp_seq=1 ttl=62 time=4.211 ms
84 bytes from 172.16.40.2 icmp_seq=2 ttl=62 time=3.909 ms
```

7. Hiệu chỉnh đường đi:

Cấu hình:

Hiện tại, nếu quan sát bảng định tuyến của switch Core_SW và router Branch, ta sẽ thấy rằng hai chi nhánh đang đi đến nhau theo đường link kết nối trực tiếp giữa Core_SW và router Branch:

```
Core_SW#show ip route ospf
(...)
 172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
O      172.16.40.0/24 [110/20] via 192.168.1.10, 00:02:28, Ethernet1/2
      192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O      192.168.1.4/30 [110/11] via 192.168.1.2, 00:01:51, Vlan100
Branch#show ip route ospf
(...)
 172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O      172.16.10.0/24 [110/11] via 192.168.1.9, 00:02:40, Ethernet0/0
O      172.16.20.0/24 [110/11] via 192.168.1.9, 00:02:40, Ethernet0/0
O      172.16.30.0/24 [110/11] via 192.168.1.9, 00:02:40, Ethernet0/0
      192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O      192.168.1.0/30 [110/11] via 192.168.1.9, 00:02:40, Ethernet0/0
```

Để hai router này dẫn đường dữ liệu đi đến nhau thông qua router Edge, ta thực hiện chỉnh cost của đường link trực tiếp lên cao hơn so với tổng cost của lô tuyến đi qua router Edge:

```
Core_SW(config)#interface e1/2
Core_SW(config-if)#ip ospf cost 100
Branch(config)#interface e0/0
Branch(config-if)#ip ospf cost 100
```

Kiểm tra:

Ta kiểm tra xác nhận rằng, sau khi chỉnh cost, hai chi nhánh đã chọn đường đi đến nhau thông qua router Edge:

```
Core_SW#show ip route ospf
(...)
 172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
O      172.16.40.0/24 [110/21] via 192.168.1.2, 00:01:32, Vlan100
      192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O      192.168.1.4/30 [110/11] via 192.168.1.2, 00:16:15, Vlan100
Branch#show ip route ospf
(...)
 172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O      172.16.10.0/24 [110/21] via 192.168.1.5, 00:01:21, Ethernet0/1
O      172.16.20.0/24 [110/21] via 192.168.1.5, 00:01:21, Ethernet0/1
O      172.16.30.0/24 [110/21] via 192.168.1.5, 00:01:21, Ethernet0/1
```

```
192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O     192.168.1.0/30 [110/20] via 192.168.1.5, 00:01:21, Ethernet0/1
```

Ta có thể xác nhận thêm điều này bằng cách trace giữa hai chi nhánh:

```
Host1> trace 172.16.40.2
trace to 172.16.40.2, 8 hops max, press Ctrl+C to stop
 1  172.16.10.1    1.547 ms  1.419 ms  1.614 ms
 2  192.168.1.2    2.065 ms  2.322 ms  2.355 ms
 3  192.168.1.6    2.525 ms  2.399 ms  1.833 ms
 4  *172.16.40.2   3.787 ms (ICMP type:3, code:3, Destination port unreachable)

Host4> trace 172.16.10.2
trace to 172.16.10.2, 8 hops max, press Ctrl+C to stop
 1  172.16.40.1    1.387 ms  1.119 ms  0.762 ms
 2  192.168.1.5    2.200 ms  2.474 ms  2.187 ms
 3  192.168.1.1    3.650 ms  1.760 ms  1.378 ms
 4  *172.16.10.2   2.597 ms (ICMP type:3, code:3, Destination port unreachable)
```

Kết quả Trace chỉ ra rằng lưu lượng giữa hai host trên hai chi nhánh đã di chuyển ngang qua router Edge.

8. Internet:

Cấu hình:

Để thực hiện cho phép truy nhập Internet cho mỗi chi nhánh đồng thời dự phòng Internet lẫn nhau, tại mỗi chi nhánh, ta thực hiện cấu hình default – route tĩnh đi Internet, track giám sát đường đi này, đồng thời thực hiện lan truyền default – route vừa tạo vào mạng bên trong bằng OSPF. Mỗi router biên (Edge, Branch) sẽ có được hai default route (một route tĩnh và một route nhận từ OSPF do router kia gửi qua), nhưng sẽ luôn chọn static default – route vì AD của static route nhỏ hơn AD của OSPF; các router biên này sẽ chỉ sử dụng default – route do OSPF cung cấp nếu static default – route down.

Trên Edge:

```
Edge(config)#ip sla 1
Edge(config-ip-sla)#icmp-echo 100.0.0.1 source-ip 100.0.0.2
Edge(config-ip-sla-echo)#frequency 5
Edge(config-ip-sla-echo)#exit
Edge(config)#ip sla schedule 1 start-time now life forever
Edge(config)#track 1 ip sla 1
Edge(config-track)#exit
Edge(config)#ip route 0.0.0.0 0.0.0.0 100.0.0.1 track 1
Edge(config)#router ospf 1
Edge(config-router)#default-information originate
Edge(config-router)#exit
Edge(config)#access-list 1 permit 172.16.10.0 0.0.0.255
Edge(config)#access-list 1 permit 172.16.20.0 0.0.0.255
Edge(config)#access-list 1 permit 172.16.30.0 0.0.0.255
Edge(config)#access-list 1 permit 172.16.40.0 0.0.0.255
Edge(config)#ip nat inside source list 1 interface e0/2 overload
```

```
Edge(config)#interface range e0/0 - 1
Edge(config-if-range)#ip nat inside
Edge(config-if-range)#exit
Edge(config)#interface e0/2
Edge(config-if)#ip nat outside
Edge(config-if)#exit
```

Trên Branch:

```
Branch(config)#ip sla 1
Branch(config-ip-sla)#icmp-echo 200.0.0.1 source-ip 200.0.0.2
Branch(config-ip-sla-echo)#frequency 5
Branch(config-ip-sla-echo)#exit
Branch(config)#ip sla schedule 1 start-time now life forever

Branch(config)#track 1 ip sla 1
Branch(config-track)#exit

Branch(config)#ip route 0.0.0.0 0.0.0.0 200.0.0.1 track 1
Branch(config)#router ospf 1
Branch(config-router)#default-information originate
Branch(config-router)#exit

Branch(config)#access-list 1 permit 172.16.10.0 0.0.0.255
Branch(config)#access-list 1 permit 172.16.20.0 0.0.0.255
Branch(config)#access-list 1 permit 172.16.30.0 0.0.0.255
Branch(config)#access-list 1 permit 172.16.40.0 0.0.0.255

Branch(config)#ip nat inside source list 1 interface e0/3 overload

Branch(config)#interface range e0/0 - 2
Branch(config-if-range)#ip nat inside
Branch(config-if-range)#exit
Branch(config)#interface e0/3
Branch(config-if)#ip nat outside
Branch(config-if)#exit
```

Kiểm tra:

Ta kiểm tra rằng hiện tại các router/switch layer 3 tại mỗi chi nhánh sẽ chọn đường đi Internet (default – route) theo đường truyền Internet tại chi nhánh ấy:

```
Core_SW#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
Known via "ospf 1", distance 110, metric 1, candidate default path
Tag 1, type extern 2, forward metric 1
Last update from 192.168.1.2 on Vlan100, 00:00:06 ago
Routing Descriptor Blocks:
* 192.168.1.2, from 192.168.1.5, 00:00:06 ago, via Vlan100
    Route metric is 1, traffic share count is 1
    Route tag 1
```

```
Edge#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
Known via "static", distance 1, metric 0, candidate default path
Routing Descriptor Blocks:
* 100.0.0.1
    Route metric is 0, traffic share count is 1
Branch#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
Known via "static", distance 1, metric 0, candidate default path
Routing Descriptor Blocks:
* 200.0.0.1
    Route metric is 0, traffic share count is 1
```

Ta kiểm tra hướng đi Internet bằng cách trace từ các host:

```
Host1> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
1 172.16.10.1 1.027 ms 1.274 ms 1.123 ms
2 192.168.1.2 3.117 ms 2.407 ms 2.188 ms
3 *100.0.0.1 3.991 ms (ICMP type:3, code:3, Destination port unreachable) *
Host2> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
1 172.16.20.1 5.495 ms 0.946 ms 1.136 ms
2 192.168.1.2 1.937 ms 1.678 ms 1.599 ms
3 *100.0.0.1 2.734 ms (ICMP type:3, code:3, Destination port unreachable) *
Host3> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
1 172.16.30.1 0.836 ms 0.675 ms 0.618 ms
2 192.168.1.2 1.905 ms 1.621 ms 1.365 ms
3 *100.0.0.1 1.669 ms (ICMP type:3, code:3, Destination port unreachable) *
Host4> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
1 172.16.40.1 0.329 ms 0.285 ms 0.261 ms
2 *200.0.0.1 0.742 ms (ICMP type:3, code:3, Destination port unreachable) *
```

Ta thấy các host thuộc các VLAN 10, 20, 30 đang đi Internet theo link Internet trên router Edge của trụ sở chính và Host4 đang đi Internet theo link Internet của router Branch đúng như yêu cầu.

Ta thực hiện kiểm tra rằng nếu đường truyền Internet trên trụ sở chính down, các host trên các VLAN sẽ chuyển qua đi Internet thông qua router Branch.

Đầu tiên, ta thực hiện down đường link Internet kết nối đến router Edge:

```
Internet(config)#interface e0/0
Internet(config-if)#shutdown
```

Lúc này router Edge đã chuyển hướng Internet theo default – route OSPF học được từ router Branch:

```
Edge#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
Known via "ospf 1", distance 110, metric 1, candidate default path
Tag 1, type extern 2, forward metric 10
```

```
Last update from 192.168.1.6 on Ethernet0/1, 00:00:53 ago
```

```
Routing Descriptor Blocks:
```

```
* 192.168.1.6, from 200.0.0.2, 00:00:53 ago, via Ethernet0/1
```

```
    Route metric is 1, traffic share count is 1
```

```
    Route tag 1
```

Ta thực hiện trace từ các host thuộc các VLAN 10, 20 và 30 để xác nhận rằng lần này chúng đi Internet thông qua router Branch:

```
Host1> trace 8.8.8.8
```

```
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
```

```
 1  172.16.10.1  1.109 ms  1.006 ms  0.746 ms  
 2  192.168.1.2  1.409 ms  1.246 ms  1.256 ms  
 3  192.168.1.6  3.424 ms  2.716 ms  2.611 ms
```

```
 4  *200.0.0.1   3.451 ms (ICMP type:3, code:3, Destination port unreachable)
```

```
Host2> trace 8.8.8.8
```

```
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
```

```
 1  172.16.20.1  1.858 ms  0.899 ms  1.060 ms  
 2  192.168.1.2  1.918 ms  1.453 ms  5.786 ms  
 3  192.168.1.6  2.481 ms  2.238 ms  2.308 ms
```

```
 4  *200.0.0.1   4.172 ms (ICMP type:3, code:3, Destination port unreachable) *
```

```
Host3> trace 8.8.8.8
```

```
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
```

```
 1  172.16.30.1  1.336 ms  3.187 ms  2.033 ms  
 2  192.168.1.2  2.656 ms  7.348 ms  3.542 ms  
 3  192.168.1.6  4.677 ms  4.470 ms  2.152 ms
```

```
 4  *200.0.0.1   2.153 ms (ICMP type:3, code:3, Destination port unreachable) *
```

Sau khi kiểm tra dự phòng xong, ta nhớ no shutdown đường Link Internet của router Edge lại như cũ:

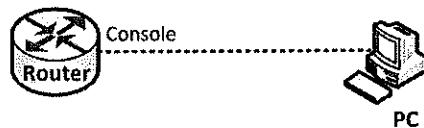
```
Internet(config)#interface e0/0
```

```
Internet(config-if)#no shutdown
```

Ta có thể thực hiện kiểm tra tương tự với đi Internet ngược lại từ phía chi nhánh.

Phụ lục 1 – Khôi phục mật khẩu cho router

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

Như ta biết, để thực hiện bảo mật cho thiết bị, người quản trị thường cài đặt các password như *enable password*, *console password* hay *telnet password* để ngăn chặn việc truy nhập không hợp lệ vào thiết bị. Tuy nhiên, vì một số lý do nào đó, người quản trị có thể quên mất các password này hoặc cấu hình sai một vài ký tự nào đó khi thiết lập các password dẫn đến không thể đăng nhập được vào thiết bị.

Chúng ta cùng nhau điểm qua cách thức khôi phục lại mật khẩu của Router trong những trường hợp như trên, giúp người quản trị có thể truy nhập lại được thiết bị của mình khi gặp sự cố.

Thực hiện:

Đầu tiên, giả sử rằng, ta có dự định đặt password enable cho Router là “cisco”, tuy nhiên, vì thao tác gõ bàn phím không cẩn thận, ta lại gõ thành “ciscowrong” và lưu password sai này vào file cấu hình:

```
R1(config)#enable password ciscowrong
R1(config)#exit
*Feb 25 03:03:39.603: %SYS-5-CONFIG_I: Configured from console by console
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Sau một thời gian, khi từ mode User đi vào mode Privilege, ta được hỏi về enable password, vì đã ghi chú lại trong tài liệu về thiết bị rằng enable password là “cisco” nên ta đăng nhập bằng password này. Tuy nhiên, như đã đề cập ở trên, trước đó ta cấu hình sai nên Router không chấp nhận password đúng mà ta nhập:

```
R1>enable
Password:
Password:
Password:
% Bad password

R1>
```

Ta đã không thể đăng nhập được vào Router do mình quản lý. Vì vậy, ta phải thực hiện thao tác khôi phục mật khẩu cho Router.

Quy trình khôi phục mật khẩu cho Router được thực hiện dựa trên việc thay đổi giá trị của thanh ghi cấu hình để tác động đến bước thứ 4 trong tiến trình khởi động của Router. *Thanh ghi cấu hình (Configuration Register)* là một thanh ghi mềm 16 bit lưu trên bộ nhớ NVRAM của Router, thay đổi giá trị thanh ghi này sẽ ảnh hưởng đến một số hoạt động của Router. Một số giá trị tiêu biểu của thanh ghi cấu hình thường được sử dụng: 0x2102, 0x2142,... (kí hiệu “0x” chỉ ra rằng đây là giá trị Hexa).

Tiến trình khởi động của Router gồm các bước như sau:

1. **Bước 1 – P.O.S.T (Power On Self Test):** Tại bước đầu tiên này, khi Router mới được bật lên, nó chạy một chương trình kiểm tra phần cứng (Hardware Diagnostic) kiểm tra tình trạng của mọi module phần cứng của Router. Khi mọi module đều qua được kỳ kiểm tra này, Router mới tiến hành chuyển sang bước thứ 2.
2. **Bước 2 – Load chương trình Bootstraps từ bộ nhớ ROM vào RAM:** Chương trình này chịu trách nhiệm tìm kiếm và load IOS để vận hành Router.
3. **Bước 3 – Load IOS cho Router:**
Chương trình bootstraps sẽ thực hiện load IOS cho Router.
4. **Bước 4 – Load file cấu hình cho Router:**
Tùy thuộc vào giá trị của bit thứ 6 của thanh ghi cấu hình mà Router sẽ thực hiện các phương thức load cấu hình khác nhau.
 - Nếu bit 6 = 0 (vd: 0x2102): load file startup-config trong NVRAM vào RAM thành running-config để chạy.
 - Nếu bit 6 = 1 (vd: 0x2142): bỏ qua file startup-config trong NVRAM, load vào một cấu hình trắng.

Nguyên tắc khôi phục mật khẩu cho Router là đổi bit 6 của thanh ghi cấu hình thành 1 (sử dụng giá trị thanh ghi là 0x2142) từ đó bỏ qua file cấu hình của Router khi khởi động. Vì file cấu hình lưu password nên nếu ta bỏ qua file cấu hình thì ta cũng bỏ qua được password trong quá trình đăng nhập Router.

Các bước thực hiện như sau:

Bước 1: Tắt/mở Router

Ta thực hiện tắt/cắt Router bằng công tắc nguồn rồi bật lại công tắc nguồn để khởi động lại Router. Chú ý rằng, để đảm bảo an toàn điện cho Router, sau khi tắt xong, ta chờ một khoảng thời gian từ 15 đến 30 giây rồi hãy mở lại Router.

Bước 2: Sử dụng tổ hợp phím ngắt để đưa Router vào mode ROMMON

Trong khi Router đang khởi động, ta nhấn tổ hợp phím ngắt “Ctrl – Break” để đưa Router vào mode ROMMON. Ta không nên nhấn ngắt quá sớm vì điều này có thể gây treo Router mà nên chờ khi màn hình Console hiện ra kích thước bộ nhớ chính thì hãy thực hiện ngắt.

```
System Bootstrap, Version 12.4(13r)T11, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2009 by cisco Systems, Inc.

Initializing memory for ECC
...
This platform does not support 1 GB Memory
Total Memory is Restricted to 768 MB

c2811 platform with 786432 Kbytes of main memory
Main memory is configured to 64 bit mode with ECC enabled

(Nhấn "Ctrl - Break" tại đây)

Upgrade ROMMON initialized
PC = 0xbfc0d54, Cause = 0x2000, Status Reg = 0x3040a803
rommon 1 >
```

Bước 3: Thay đổi giá trị thanh ghi cấu hình

Tại mode ROMMON, ta thực hiện thay đổi giá trị của thanh ghi cấu hình từ giá trị mặc định là 0x2102 thành giá trị mới là 0x2142 để đảm bảo bit 6 được chuyển thành giá trị 1. Câu lệnh để thiết lập giá trị thanh ghi cấu hình ở ROMMON là “confreg”. Sau khi thay đổi xong, ta phải thực hiện khởi động lại Router để giá trị mới được áp dụng. Câu lệnh để khởi động lại Router ở ROMMON là “reset”.

```
rommon 1 > confreg 0x2142 <-Đổi giá trị thanh ghi thành 0x2142
```

You must reset or power cycle for new config to take effect

```
rommon 2 > reset <-Khởi động lại Router
```

c2811 platform with 786432 Kbytes of main memory

Main memory is configured to 64 bit mode with ECC enabled

(...)

Bước 4: Chính sửa password

Sau khi khởi động lại, vì giá trị thanh ghi cấu hình đã được đổi thành 0x2142 với bit số 6 = 1 nên ở bước thứ 4, Router sẽ bỏ qua file startup-config và đưa ra câu hỏi để chọn setup mode hoặc load vào một cấu hình trắng, ta chọn “no” như thường lệ để load vào một cấu hình trắng:

```
--- System Configuration Dialog ---  
Would you like to enter the initial configuration dialog? [yes/no]: no  
Press RETURN to get started!  
*Feb 25 04:04:04.663: %VPN_HW-6-INFO_LOC: Crypto engine: onboard 0 State changed to:  
Initialized  
*Feb 25 04:04:04.667: %VPN_HW-6-INFO_LOC: Crypto engine: onboard 0 State changed to:  
Enabled  
*Feb 25 04:04:06.075: %LINEPROTO-5-UPDOWN: Line protocol on Interface VoIP-Null0,  
changed state to up  
*Feb 25 04:04:06.075: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up  
*Feb 25 04:04:06.075: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up  
  
(Đã bỏ bớt một số dòng trong kết quả hiển thị)  
  
Router>  
Router>enable  
Router# <- Đã được vào mode Privilege mà không bị hỏi password
```

Như trên ta thấy, ta đã bỏ qua được file cấu hình cũ có lưu password và đi được vào mode Privilege của Router khi sử dụng cấu hình trắng. Để thực hiện sửa lại password cũ cho đúng, chúng ta thực hiện load file cấu hình cũ vào Router bằng lệnh “copy startup-config running-config”:

```
Router#copy startup-config running-config  
Destination filename [running-config]?  
1527 bytes copied in 0.552 secs (2766 bytes/sec)  
R1#
```

Ta thấy, cấu hình cũ đã được load lại vào thành running-config (kết quả chỉ rõ có bao nhiêu byte cấu hình đã được copy và tên của Router đổi lại từ tên mặc định là “Router” thành tên đã lưu từ trước ở file cấu hình là “R1”).

Ta tiến hành sửa lại password cho đúng, sau khi sửa xong, nhớ thực hiện lưu password mới này lại:

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#enable password cisco
R1(config)#exit
R1#
*Feb 25 04:23:54.031: %SYS-5-CONFIG_I: Configured from console by console
R1#write memory
Building configuration...
[OK]
R1#
```

Bước 5: Trả lại giá trị thanh ghi cấu hình về mặc định

Sau khi hoàn tất xong việc chỉnh sửa password, ta thực hiện trả lại giá trị thanh ghi cấu hình về mặc định (0x2102). Câu lệnh để thay đổi lại giá trị thanh ghi cấu hình là “config-register” ở mode Global Configuration.

```
R1(config)#config-register 0x2102
```

Ta có thể kiểm tra sự thay đổi này bằng lệnh “show version” ở mode Privilege:

```
R1#show version
(Đã bỏ bớt một số dòng trong kết quả hiển thị)

Cisco 2811 (revision 53.50) with 774144K/12288K bytes of memory.
Processor board ID FTX1412AKYT
2 FastEthernet interfaces
8 Low-speed serial(sync/async) interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
253008K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2142 (will be 0x2102 at next reload)
```

Ta thấy rằng giá trị của thanh ghi cấu hình vẫn là 0x2142, nhưng sẽ được đổi thành 0x2102 ở lần khởi động kế tiếp. Vì vậy, để hoàn tất tiến trình khôi phục mật khẩu cho Router, ta cần thực hiện lưu cấu hình rồi khởi động lại Router.

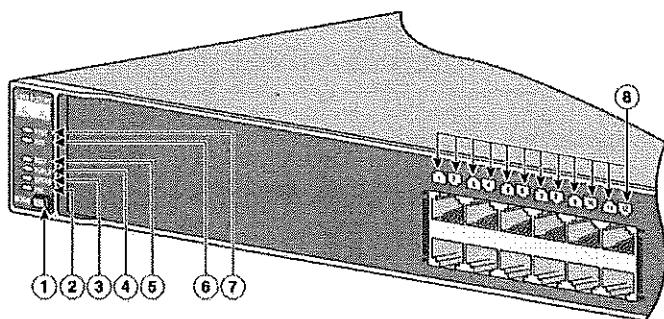
Bài lab trên đây được thực hiện trên dòng Router được sử dụng rất phổ biến hiện nay là dòng 2800. Cách khôi phục mật khẩu trên các dòng Router khác có thể có một vài khác biệt nhưng nguyên tắc cơ bản thì vẫn giống như đã trình bày.

Phụ lục 2 – Khôi phục mật khẩu cho switch

Trong phụ lục 1, chúng ta đã đề cập đến cách thức để khôi phục mật khẩu cho router Cisco. Trong phụ lục 2, chúng ta tiếp tục trao đổi về cách khôi phục mật khẩu trên switch Cisco. Chúng ta sẽ cùng thực hành tiến trình này trên dòng switch rất phổ biến là dòng switch 3560 của Cisco. Việc khôi phục mật khẩu này có thể được thực hiện tương tự trên các dòng switch khác.

Tương tự như với router, để đảm bảo một mức độ bảo mật cơ bản cho switch, chúng ta thường cấu hình các password để giới hạn quyền truy nhập vào switch. Các password này có thể bị thiết lập sai trong quá trình cấu hình hoặc bị quên, mất do những thiếu sót của quy trình quản trị và dẫn đến thiết bị không thể đăng nhập vào được. Trong trường hợp này, chúng ta phải thực hiện tiến trình khôi phục mật khẩu cho switch.

Trước khi đi vào các bước của tiến trình, chúng ta cùng điểm qua một vài thành phần phần cứng của switch 3560 (hình 1):



Hình 1 – Các đèn LED ở mặt trước một switch 3560.

1. Vị trí 1 – Phím “MODE”:

Các đèn LED trên các port của switch có thể cho ta biết trạng thái Duplex (DUPLX) hoặc tốc độ cổng (SPEED) hoặc trạng thái kết nối (STAT) hoặc trạng thái PoE (PoE) của chúng. Để quyết định các đèn LED hiển thị thông tin nào trong các thông tin trên, chúng ta sử dụng phím “MODE”. Mặc định, các đèn LED trên các cổng hiển thị thông tin về trạng thái kết nối của các port (STAT):

- Xanh (Green): port đang kết nối.
- Xanh nhấp nháy (Blinking Green): đang truyền dữ liệu.
- Hổ phách (Amber): đang bị khóa bởi tiến trình Spanning Tree trên switch và không forward dữ liệu được.
- Thay đổi liên tục giữa Green và Amber: Bị lỗi trên link.

Nếu ta chuyển chế độ hiển thị sang DUPLX:

- Tắt: Port đang hoạt động ở chế độ Half – duplex.
- Bật lên màu xanh (Green): Port đang hoạt động ở chế độ Full – duplex.

Nếu ta chuyển sang chế độ SPEED (xét các loại port 10/100 và 10/100/1000):

- Tắt: port hoạt động ở tốc độ 10Mbps.
- Xanh (Green): port hoạt động ở tốc độ 100Mbps.
- Xanh nhấp nháy (Blinking Green): port hoạt động ở tốc độ 1000Mbps.

Nếu ta chuyển sang chế độ PoE:

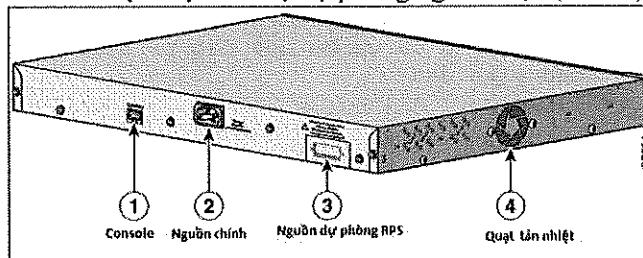
- Tắt: PoE hiện không hoạt động trên cổng.
 - Xanh (Green): port đang hoạt động PoE và đang cấp nguồn cho thiết bị kết nối.
 - Thay đổi liên tục giữa Green và Amber: PoE từ chối cấp nguồn cho thiết bị kết nối vì quỹ công suất của switch cho PoE đã bị sử dụng hết.
 - Amber nhấp nháy: PoE bị tắt trên cổng do có lỗi xảy ra, ví dụ: sử dụng cáp hoặc thiết bị không phù hợp.
 - Amber: PoE cho port đã bị tắt, mặc định PoE được bật trên cổng.
- Ghi chú:* PoE là tính năng cấp nguồn cho thiết bị thông qua cổng Ethernet LAN. Tính năng này thường được sử dụng để cấp nguồn cho các IP Phone hay các Access – point.

2. Các vị trí 2, 3, 4, 5:

Là các đèn PoE, SPEED, DUPLEX, STAT. Các đèn này cho biết ta đã chọn chế độ hiển thị như thế nào cho LED của các port bằng phím MODE: ta chọn chế độ nào thì đèn tương ứng của chế độ ấy sẽ sáng lên màu xanh (GREEN). Mặc định, chế độ hiện thị trạng thái kết nối của port được chọn nên đèn STAT sẽ sáng.

3. Vị trí số 6 – Đèn RPS:

RPS – Redundancy Power System là thiết bị cấp nguồn dự phòng chuyên dụng của Cisco. Các switch 3560 ngoài việc lấy nguồn từ nguồn điện chính, có thể đấu nối thêm bằng cổng nguồn RPS ở mặt sau đèn thiết bị RPS của Cisco để thực hiện chế độ dự phòng nguồn điện (hình 2):



Hình 2 – Mặt sau của các switch dòng 3560 – 24PS và 3560 – 48PS.

Đèn RPS sẽ cho biết hoạt động sử dụng nguồn dự phòng có diễn ra bình thường không. Khi nguồn dự phòng đang hoạt động bình thường, đèn này sẽ sáng màu xanh (Green) còn khi cổng RPS không kết nối đến nguồn dự phòng, đèn này sẽ tắt.

4. Vị trí số 7 – đèn SYSTEM LED:

Đèn này cho biết trạng thái của thiết bị:

- Xanh (Green): Thiết bị hoạt động bình thường.
- Hồ phách (Amber): Thiết bị đã được cấp nguồn nhưng hoạt động chưa đúng.
- Tắt: Thiết bị chưa được cấp nguồn.

5. Vị trí số 8: là các đèn LED hiển thị thông tin về các port mạng của switch. Thông tin do các đèn này cung cấp được quy định bởi việc nhấn phím MODE (xem phần về phím MODE).

Sau khi đi kèm qua về các đèn LED của switch, chúng ta đi vào vấn đề chính: Recovery password cho switch.

Hoạt động recovery password cho switch được thực hiện dựa vào phím MODE trên mặt trước của switch. Các bước thao tác được tiến hành như sau:

Bước 1: Khởi động lại switch về một cấu hình trắng

Nhấn phím MODE ở mặt trước của switch, ta sẽ thấy các đèn STAT, DUPLEX và SPEED nhấp nháy xanh. Ta giữ chặt phím MODE cho đến khi cả 3 đèn này ngừng nhấp nháy và chuyển sang màu xanh huyền thì thả phím MODE. Động tác này khiến cho switch khởi động lại và nạp vào một cấu hình trắng.

Bước 2: Load và sửa password trên cấu hình cũ

Switch lưu hai file phục vụ cho hoạt động lưu cấu hình của switch là file *config.text* và *vlan.dat*: file *config.text* chứa cấu hình cũ của switch và file *vlan.dat* chứa cấu hình VLAN trên switch. Trong quá trình khởi động, switch sẽ load nội dung của hai file này để hoạt động; nội dung của file *config.text* sẽ được đưa vào *running-config* để chạy và nội dung của file *vlan.dat* sẽ được dùng để khởi tạo cấu hình VLAN trên switch.

Khi ta thực hiện thao tác với phím MODE như ở bước 1, switch sẽ thực hiện di chuyển toàn bộ nội dung của file *config.text* sang file *config.text.renamed* và nội dung của file *vlan.dat* sang file *vlan.dat.renamed*. Nội dung của các file *config.text* và *vlan.dat* lúc này được đưa về mặc định: cấu hình trắng và các VLAN cơ bản mặc định của switch. Do đó, sau khi khởi động lại xong với phím MODE, chúng ta đã bỏ qua được các password trong cấu hình cũ:

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>enable
Switch#
```

Để sửa chữa các password và lấy lại cấu hình cũ, chúng ta thực hiện di chuyển ngược lại nội dung của các file: *config.text.renamed* → *running-config* và *vlan.dat.renamed* → *vlan.dat*:

```
Switch#copy config.text.renamed running-config <-Lấy lại cấu hình cũ
Destination filename [running-config]?
2531 bytes copied in 6.685 secs (379 bytes/sec)
SW# <- Đã lấy lại được cấu hình cũ và bỏ qua các password
SW#copy vlan.dat.renamed vlan.dat
Destination filename [vlan.dat]?
Copy in progress...C
676 bytes copied in 0.025 secs (27040 bytes/sec)
SW#
```

Bắt đầu từ đây, chúng ta thực hiện các thao tác chỉnh sửa password và lưu lại password mới:

```
SW#configure terminal
SW(config)#enable password cisco
SW(config)#exit
SW#wr
Building configuration...
[OK]
SW#
```

Cuối cùng, để file *vlan.dat* được load lại vào RAM nhằm xây dựng lại cấu hình VLAN, chúng ta khởi động lại switch hoàn tất tiến trình recovery password:

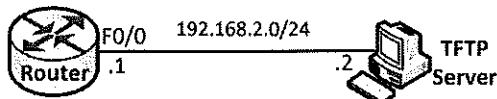
```
SW#reload
Proceed with reload? [confirm]

*Mar 1 00:03:52.708: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload command.
```

Khi switch khởi động lại xong, chúng ta nhận được cấu hình đầy đủ với các password lỗi đã được sửa và cấu hình VLAN đã thực hiện trên switch trước đó. Thao tác khôi phục mật khẩu cho switch đã được hoàn tất.

Phụ lục 3 – Thao tác với file IOS trên Router

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

Bài lab này hướng dẫn các bạn học viên một số thao tác cơ bản với file IOS của một router Cisco. Các thao tác này bao gồm:

- Sao lưu file IOS từ router ra bên ngoài để dự phòng.
- Chép file IOS từ một máy tính bên ngoài vào router.
- Cài mới một IOS lên router khi router này bị mất file IOS.

Yêu cầu:

1. Đầu nối dây cáp mạng giữa PC và Router; thực hiện đặt địa chỉ IP trên Router và PC như hình 1.
2. Cài đặt chương trình giả lập TFTP Server trên PC.
3. Thực hiện copy IOS trên Router ra TFTP Server.
4. Thực hiện copy ngược lại từ TFTP Server vào Router.
5. Xóa IOS trên Flash của Router.
6. Thực hiện load IOS từ TFTP Server vào Flash của Router.

Thực hiện:

Bước 1: Đầu nối dây giữa Router và PC, đặt địa chỉ IP

Thực hiện cắm dây như trên sơ đồ được chỉ ra trên hình 1.

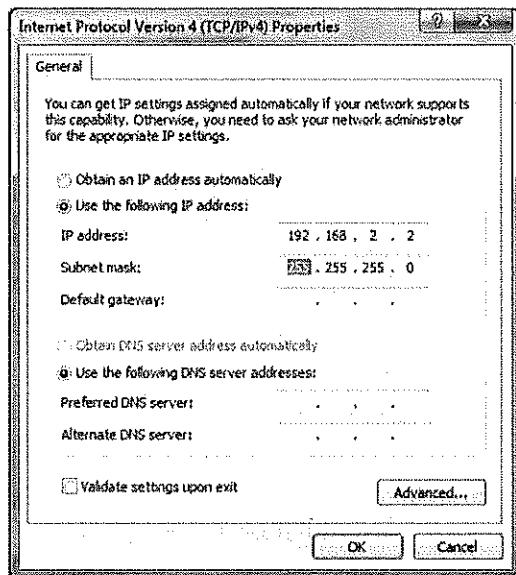
Sau khi cắm dây cáp mạng, ta thực hiện đặt địa chỉ IP trên Router như hình 1 đã chỉ ra:

```
Router(config)#interface f0/0
Router(config-if)#no shutdown
Router(config-if)#
*Feb 24 07:17:20.731: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Feb 24 07:17:21.731: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#exit
Router(config)#

```

Ta cũng vào card mạng của PC và đặt địa chỉ IP theo yêu cầu (hình 2):



Hình 2 – Đặt IP trên PC.

Thực hiện ping kiểm tra để đảm bảo chắc chắn Router và IP đã thông kết nối IP:

```
Router#ping 192.168.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms
Router#
```

Sau khi đảm bảo kết nối giữa Router và PC đã thông suốt, chúng ta chuyển qua bước tiếp theo.

Bước 2: Copy IOS từ Router ra TFTP Server

Khi quản trị một thiết bị mạng của Cisco, người quản trị cần phải nắm vững cách thức sao chép và nâng cấp hệ điều hành của thiết bị để có thể quản trị thật tốt thiết bị này.

Có nhiều cách để thực hiện sao chép và nâng cấp IOS nhưng cách thông dụng nhất là sử dụng giao thức truyền file TFTP. Ta có thể dựng hẳn một server TFTP để thực hiện hoặc cũng có thể chỉ cần cài đặt một phần mềm giả lập TFTP Server trên PC là cũng có thể thực hiện được tác vụ.

Điều kiện để Router có thể sao chép IOS của mình ra một TFTP Server hoặc chép IOS từ TFTP Server vào Flash (nâng cấp IOS) là Router và TFTP Server phải đi đến được nhau và TFTP Server phải còn đủ bộ nhớ cũng như chỉ các đường dẫn đúng đến nơi lưu file của mình.

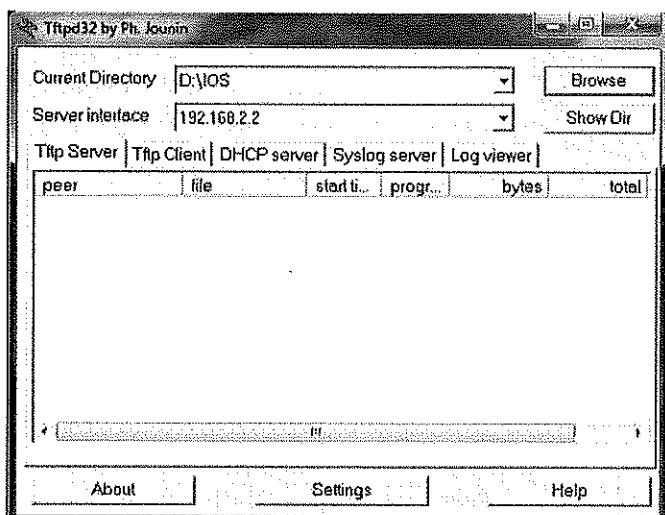
Trong bài lab này, ta sẽ sử dụng một PC thông thường để làm TFTP Server. Ở bước thứ nhất của bài lab, ta đã đảm bảo được Router và PC đi đến được nhau thông qua một kết nối IP của mạng 192.168.2.0/24. Tiếp theo, ta sẽ giả lập PC thành TFTP Server bằng cách cài đặt phần mềm TFTPd32 lên PC. Phần mềm này có thể được download miễn phí từ địa chỉ <http://tftp32.jounin.net/>. Việc cài đặt được thực hiện một cách bình

thường trên Window. Sau khi cài đặt xong, trên màn hình desktop xuất hiện biểu tượng của TFTPD32 (hình 3), ta double click vào biểu tượng này để chạy phần mềm.



Hình 3 – Biểu tượng của phần mềm TFTPD32.

Giao diện của phần mềm TFTPD32 (hình 4):



Hình 4 – Giao diện chương trình TFTPD32.

Chúng ta thiết lập một vài thông số trên giao diện này:

- *Current Directory*: Sử dụng phím “Browse” để chọn đường dẫn đến thư mục mà chúng ta sử dụng để chứa IOS (ví dụ ở trên hình 4 là “D:\IOS”).
- *Server interface*: Ta click vào dấu mũi tên ở ô này để chọn đúng địa chỉ mà ta muốn làm địa chỉ của TFTP Server (trong bài lab này là “192.168.2.2”).

Sau khi thiết lập xong các bước trên, ta đã có một TFTP Server sẵn sàng cho việc backup IOS từ Router ra ngoài.

Ta kiểm tra IOS đang có trên Flash của Router bằng lệnh “show flash:” ở mode Privilege:

```
Router#show flash:  
--length-- -----date/time----- path  
1      39868440 May  4 2010 22:33:02 +00:00 c2800nm-adventerprisek9-mz.124-23a.bin  
2      2900 May   4 2010 22:33:58 +00:00 cpconfig-2811.cfg  
3      2324992 May  4 2010 22:34:20 +00:00 cpexpress.tar  
4      1038 May   4 2010 22:34:28 +00:00 home.shtml  
5      115712 May  4 2010 22:34:36 +00:00 home.tar  
6      527849 May  4 2010 22:34:50 +00:00 128MB.sdf  
7      1697952 May  4 2010 22:35:06 +00:00 securedesktop-ios-3.1.1.45-k9.pkg  
8      415956 May  4 2010 22:35:14 +00:00 sslclient-win-1.1.4.176.pkg  
9      23205 May  31 2013 15:28:02 +00:00 crashinfo_20130531-152803
```

```
10      23216 May 31 2013 15:29:40 +00:00 crashinfo_20130531-152940
```

```
213635072 bytes available (45019136 bytes used)
```

```
Router#
```

Từ kết quả show, ta thấy IOS được sử dụng và đang được lưu trong bộ nhớ Flash là “c2800nm-adventerprisek9-mz.124-23a.bin”. Ta sẽ thực hiện copy IOS này ra TFTP Server cho mục đích dự phòng:

```
Router#copy flash: tftp:
```

```
Source filename []? c2800nm-adventerprisek9-mz.124-23a.bin <-Tên file được copy
```

```
Address or name of remote host []? 192.168.2.2 <-Địa chỉ IP của TFTP Server
```

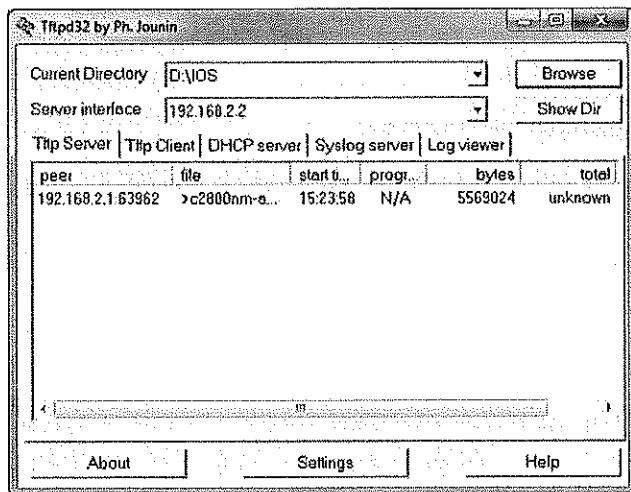
```
Destination filename [c2800nm-adventerprisek9-mz.124-23a.bin]? <-Tên của file tại đích  
đến, nếu không muốn sửa tên file, ta chỉ cần gõ Enter tại đây
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
39868440 bytes copied in 144.280 secs (276327 bytes/sec)
```

```
Router#
```

Trong quá trình sao chép, màn hình giao diện của TFTPD32 cũng hiển thị các thông số của kết nối TFTP (hình 5):



Hình 5 – Giao diện TFTPD32 hiển thị các thông số.

Sau khi thực hiện copy xong file IOS từ Flash của Router ra TFTP Server bên ngoài, ta có thể kiểm tra lại bằng cách vào thư mục đường dẫn đã chỉ ra để thấy rằng file đã được sao chép lên server.

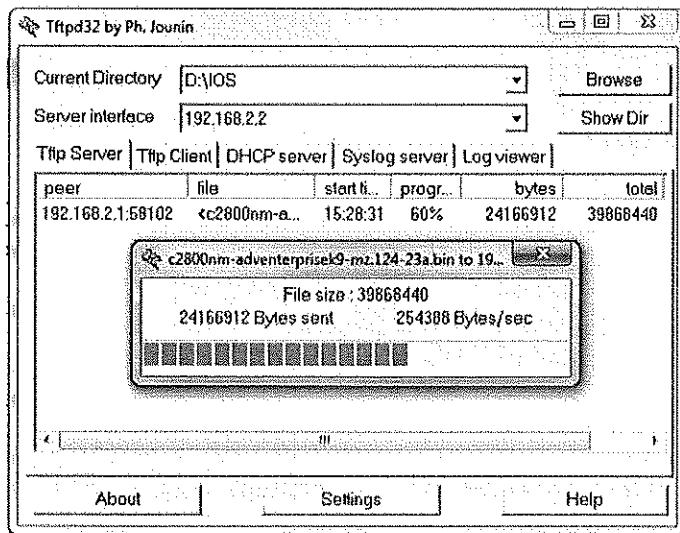
Bước 3: Copy file từ TFTP Server vào Flash

Ở bước này, chúng ta sẽ thực hiện thao tác ngược lại với bước thứ 2 là chép ngược lại file từ TFTP Server vào Flash. Thao tác này thường được sử dụng khi người quản trị muốn nâng cấp IOS của Router lên một IOS mới có nhiều tính năng hơn.

Thực hiện bằng lệnh “copy tftp: flash:” trên mode Privilege của Router:

```
Router#copy tftp flash:  
Address or name of remote host []? 192.168.2.2 <-Địa chỉ TFTP Server  
Source filename []? c2800nm-adventureprisek9-mz.124-23a.bin <-Tên file muốn copy  
Destination filename [c2800nm-adventureprisek9-mz.124-23a.bin]? <-Tên file tại đích đến (là Flash). Nếu không muốn đổi tên, ta chỉ cần gõ Enter tại đây  
%Warning:There is a file already existing with this name <-Cảnh báo có file trùng tên đang tồn tại trên Flash  
Do you want to over write? [confirm] <-Xác nhận có ghi đè  
Accessing tftp://192.168.2.2/c2800nm-adventureprisek9-mz.124-23a.bin...  
Loading c2800nm-adventureprisek9-mz.124-23a.bin from 192.168.2.2 (via FastEthernet0/0):  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
[OK - 39868440 bytes]  
  
39868440 bytes copied in 167.704 secs (237731 bytes/sec)  
Router#
```

Giao diện TFTPD32 cũng hiển thị thông tin cho quá trình sao chép từ Server xuống Router (hình 6):



Hình 6 – Giao diện TFTPD32 khi copy từ Server vào Router.

```
TFTP_SERVER: 192.168.2.2
TFTP_FILE: c2800nm-adventerprisek9-mz.124-23a.bin
TFTP_VERBOSE: Progress
TFTP_RETRY_COUNT: 18
TFTP_TIMEOUT: 7200
TFTP_CHECKSUM: Yes
TFTP_MACADDR: 00:26:99:93:39:80
FE_PORT: Fast Ethernet 0
FE_SPEED_MODE: Auto
```

Invoke this command for disaster recovery only.

WARNING: all existing data in all partitions on flash will be lost!

Do you wish to continue? y/n: [n]: y <- Chọn "y" để bắt đầu

Receiving c2800nm-adventerprisek9-mz.124-23a.bin from 192.168.2.2

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

(Đã bỏ bớt một số dòng cho gọn)

File reception completed.

Validating checksum.

Copying file c2800nm-adventerprisek9-mz.124-23a.bin to flash:.
program load complete, entry point: 0x8000f000, size: 0xcb80

Format: All system sectors written. OK...

Format: Operation completed successfully.

Format of flash: complete

program load complete, entry point: 0x8000f000, size: 0xcb80

rommon 8 >

Đến đây, IOS đã được load vào Flash. Ta thực hiện khởi động lại Router, câu lệnh khởi động lại Router ở ROMMON là “reset”:

rommon 8 > reset

Router sẽ khởi động lại bình thường và đưa chúng ta vào mode cấu hình đầu tiên của Router là mode User:

Router>

Ta đã hoàn tất tiến trình load IOS cho Router khi Router bị mất IOS bằng cách sử dụng các lệnh của mode ROMMON.

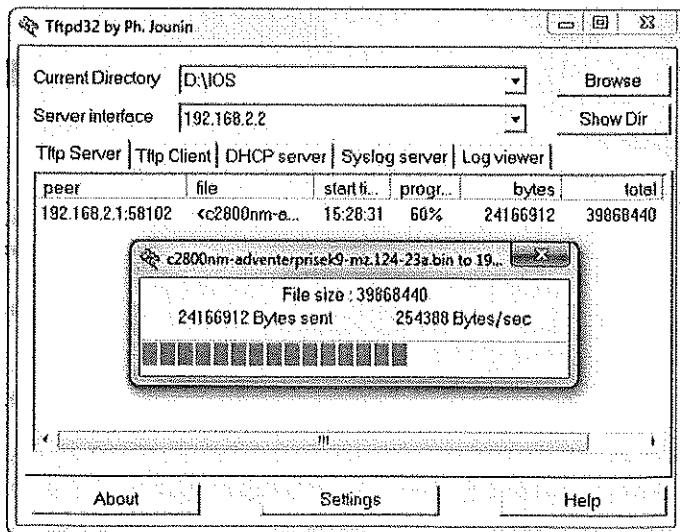
Bước 3: Copy file từ TFTP Server vào Flash

Ở bước này, chúng ta sẽ thực hiện thao tác ngược lại với bước thứ 2 là chép ngược lại file từ TFTP Server vào Flash. Thao tác này thường được sử dụng khi người quản trị muốn nâng cấp IOS của Router lên một IOS mới có nhiều tính năng hơn.

Thực hiện bằng lệnh “copy tftp: flash:” trên mode Privilege của Router:

```
Router#copy tftp flash:  
Address or name of remote host []? 192.168.2.2 <-Địa chỉ TFTP Server  
Source filename []? c2800nm-adventureprisek9-mz.124-23a.bin <-Tên file muốn copy  
Destination filename [c2800nm-adventureprisek9-mz.124-23a.bin]? <-Tên file tại đích đến (là Flash). Nếu không muốn đổi tên, ta chỉ cần gõ Enter tại đây  
%Warning:There is a file already existing with this name <-Cảnh báo có file trùng tên đang tồn tại trên Flash  
Do you want to over write? [confirm] <-Xác nhận có ghi đè  
Accessing tftp://192.168.2.2/c2800nm-adventureprisek9-mz.124-23a.bin...  
Loading c2800nm-adventureprisek9-mz.124-23a.bin from 192.168.2.2 (via FastEthernet0/0):  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
[OK - 39868440 bytes]  
39868440 bytes copied in 167.704 secs (237731 bytes/sec)  
Router#
```

Giao diện TFTPD32 cũng hiển thị thông tin cho quá trình sao chép từ Server xuống Router (hình 6):



Hình 6 – Giao diện TFTPD32 khi copy từ Server vào Router.

Trên đây là các thao tác copy IOS từ trong ra ngoài và từ ngoài vào trong được thực hiện bằng chính các lệnh của IOS trên Router nên được sử dụng cho mục đích backup một IOS và nâng cấp một IOS.

Tuy nhiên, trong nhiều trường hợp, ta phải thực hiện copy một IOS cho Router khi mà Router bị mất IOS trên Flash. Khi Router bị mất IOS, tiến trình khởi động của Router sẽ đưa Router vào một mode đặc biệt gọi là ROMMON. Mode này sử dụng hệ điều hành dự phòng lưu trên bộ nhớ ROM của Router để chạy, hệ điều hành dự phòng này chỉ hỗ trợ một vài tính năng rất cơ bản để duy trì hoạt động của Router và thường được sử dụng cho mục đích phục hồi Router khi bị lỗi. Các bước tiếp theo của bài lab sẽ hướng dẫn chúng ta cách load IOS bằng cách sử dụng hệ điều hành dự phòng này.

Bước 4: Xóa IOS trên Flash và khởi động lại Router

Ta thực hiện xóa IOS hiện có trên Flash và khởi động lại Router. Trong quá trình khởi động, chương trình Boottrap của tiến trình khởi động của Router sẽ thực hiện tìm kiếm IOS trong Flash của Router và load vào bộ nhớ RAM để chạy. Tuy nhiên, vì IOS đã bị xóa nên Router sẽ báo lỗi và load hệ điều hành phụ từ bộ nhớ ROM vào RAM để vận hành Router.

Xóa IOS trên Flash và khởi động lại:

```
Router#delete flash:c2800nm-adventuresek9-mz.124-23a.bin
Delete filename [c2800nm-adventuresek9-mz.124-23a.bin]?
Delete flash:/c2800nm-adventuresek9-mz.124-23a.bin? [confirm] <-Gõ Enter để xác nhận
xóa file
Router#
Router#reload
System configuration has been modified. Save? [yes/no]: n
Proceed with reload? [confirm] <-Gõ Enter để xác nhận khởi động lại
*Feb 24 09:00:46.103: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.

System Bootstrap, Version 12.4(13r)T11, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2009 by cisco Systems, Inc.

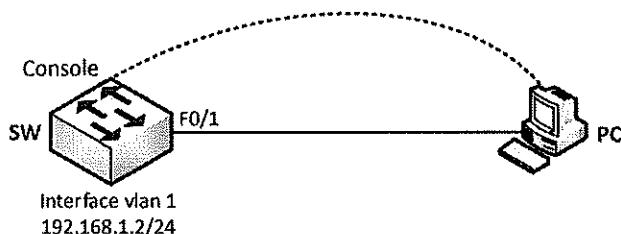
Initializing memory for ECC
....
This platform does not support 1 GB Memory
Total Memory is Restricted to 768 MB

c2811 platform with 786432 Kbytes of main memory
Main memory is configured to 64 bit mode with ECC enabled

Upgrade ROMMON initialized
program load complete, entry point: 0x8000f000, size: 0xcb80
program load complete, entry point: 0x8000f000, size: 0xcb80
loadprog: bad file magic number:      0x0
boot: cannot load "flash:" <-Báo lỗi không tìm thấy IOS trong Flash
c2811 platform with 786432 Kbytes of main memory
```

Phụ lục 4 – Thao tác với file IOS trên Switch

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

Bài lab này hướng dẫn các bạn học viên một số thao tác cơ bản với file IOS của một switch dòng Catalyst của Cisco. Các thao tác này bao gồm:

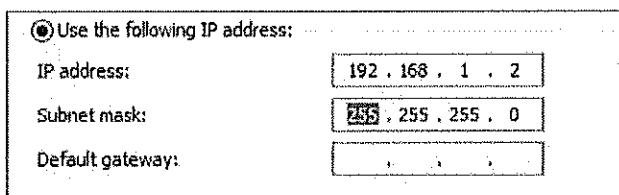
- Sao lưu file IOS từ switch ra bên ngoài để dự phòng.
- Chép file IOS từ một máy tính bên ngoài vào switch.
- Cài mới một IOS lên switch khi switch này bị mất file IOS.

Thực hiện:

Bước 1: Cấu hình IP cho PC và Switch

Trong bước này, chúng ta thực hiện kết nối dây giữa PC và switch như được chỉ ra trên hình 1. Tiếp đó, chúng ta thực hiện cấu hình địa chỉ IP cho PC và switch để có thể thực hiện các thao tác với IOS trên thiết bị như đã chỉ ra.

Đặt IP trên PC là 192.168.1.2 (hình 2):



Hình 2 – Cấu hình IP trên PC.

Đặt IP trên interface vlan 1 của switch:

```
SW(config)#interface vlan 1
SW(config-if)#no shutdown
SW(config-if)#ip address 192.168.1.2 255.255.255.0
```

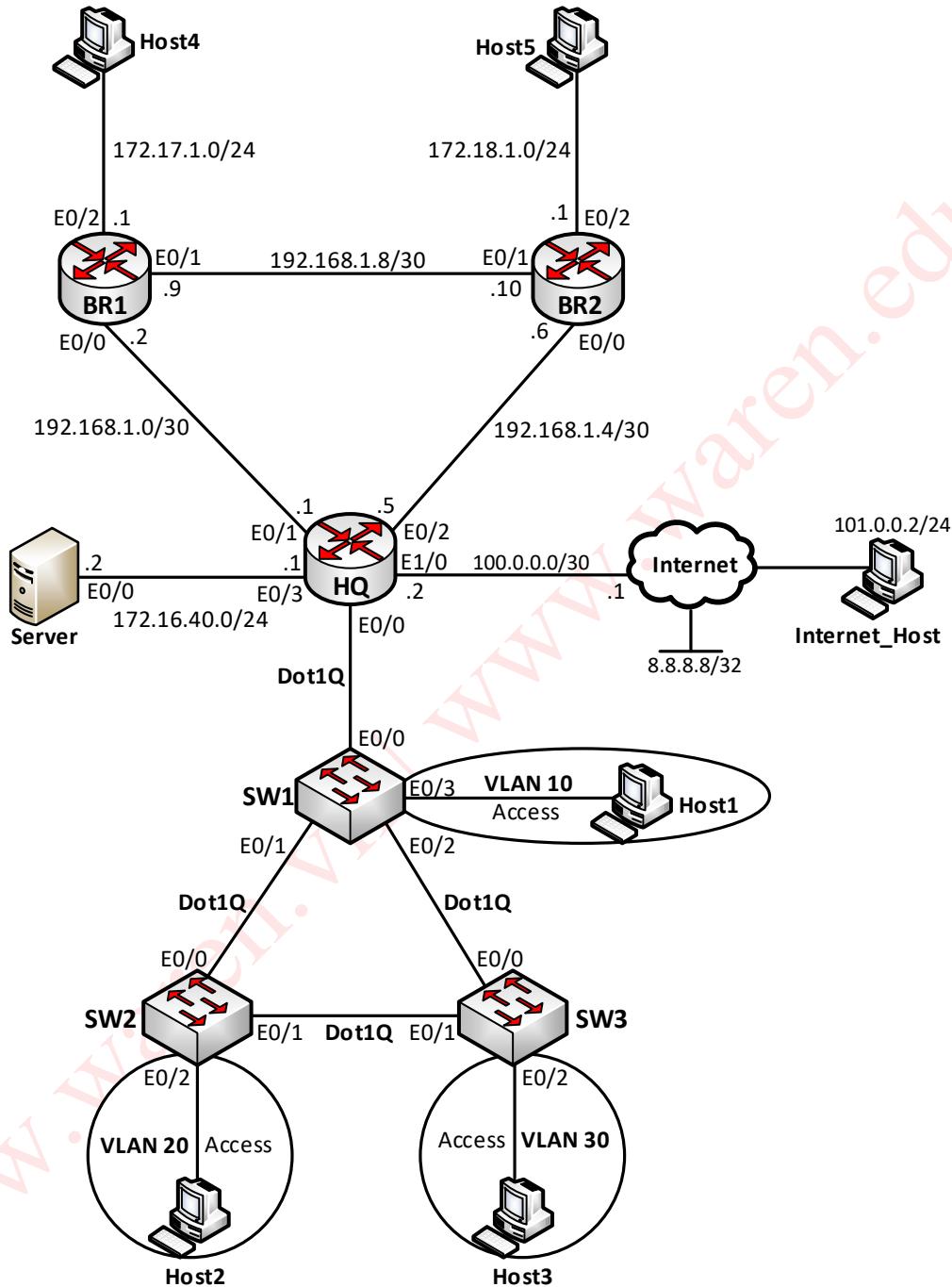
Ta kiểm tra lại rằng interface vlan 1 đã up/up:

```
SW#show ip interface brief vlan 1
Interface          IP-Address      OK? Method Status        Protocol
Vlan1              192.168.1.2    YES manual up
```

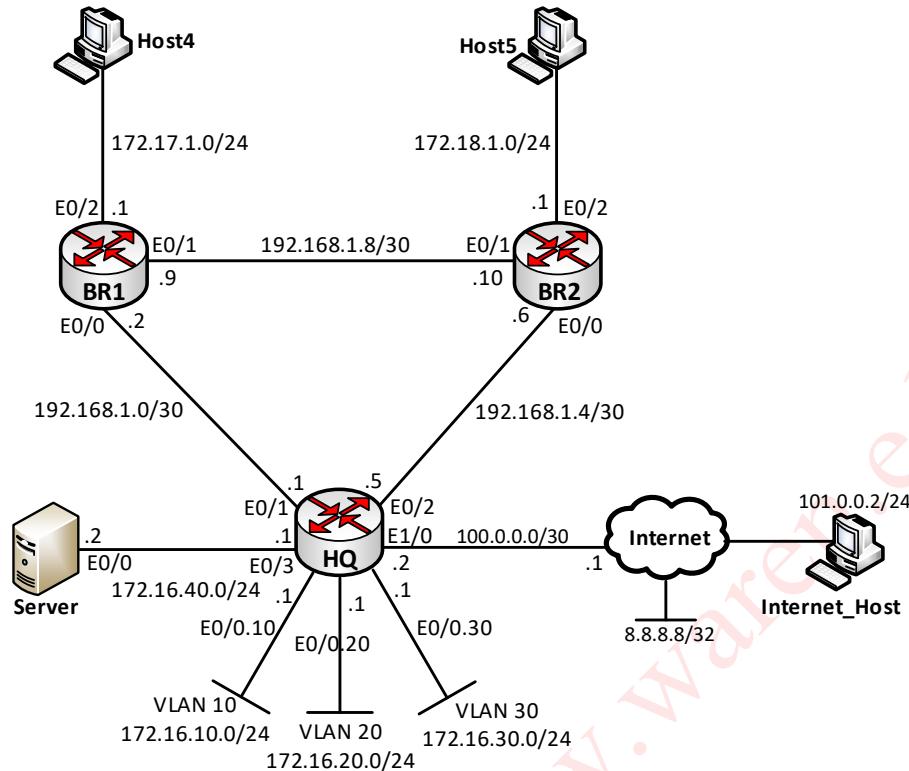


Lab 27 – Tổng hợp ôn tập – Bài số 1

Sơ đồ:



Hình 1 – Sơ đồ đấu nối giữa các thiết bị.



Hình 2 – Sơ đồ layer 3.

Mô tả:

- Bài lab giả lập kịch bản một mạng doanh nghiệp có 3 khu vực: Headquarters (HQ), chi nhánh 1 (BR1) và chi nhánh 2 (BR2). Tại khu vực HQ, có 3 switch đấu nối mạng cho 3 site, tạo thành một sơ đồ dạng vòng (Ring topology) layer 2.
- Qua bài lab này, các bạn học viên thực hiện ôn tập lại một số chủ đề cơ bản và trọng tâm của chương trình CCNA.
- Các thiết bị đều đã được cấu hình sẵn Hostname và địa chỉ IP (ngoại trừ các sub-interface của router HQ), các bạn học viên không cần phải cấu hình lại các thông số này.
- Trong suốt quá trình làm bài lab, các bạn học viên không can thiệp vào cấu hình các thiết bị: Server, router giả lập Internet, router giả lập một host trên Internet (Internet_Host).

Yêu cầu:**1. Trunking:**

- Thực hiện cấu hình tất cả các đường link kết nối giữa các switch thành các đường trunk.
- Các đường trunk này sử dụng phương pháp trunking Dot1Q, thiết lập tĩnh (mode ON).

2. VTP, VLAN:

- Cấu hình để 3 switch của HQ (SW1, SW2, SW3) tham gia VTP với các thông số như sau:
 - VTP domain: waren.
 - VTP password: cisco.
 - SW1: Server; SW2, SW3: Client.

- Trên SW1, tạo cấu hình VLAN gồm các VLAN 10, 20, 30. Kiểm tra xác nhận rằng cấu hình VLAN đã lan truyền đầy đủ đến các switch SW2 và SW3.
- Trên các switch, thực hiện gán cổng vào các VLAN đã tạo như được chỉ ra trên hình 1.

3. STP:

- Hãy cấu hình hiệu chỉnh STP trên các VLAN 10, 20 và 30 một cách thích hợp đảm bảo rằng không một đường link nào giữa các switch bị khóa hoàn toàn.
- Việc hiệu chỉnh này chỉ giới hạn trong hoạt động cấu hình root switch cho các VLAN.
- Trên các cổng access của các switch, thực hiện cấu hình tính năng để các cổng kết nối đến các end – user (Host1, Host2, Host3) chuyển qua hoạt động ngay lập tức, bỏ qua các trạng thái trung gian STP.

4. Định tuyến giữa các VLAN:

- Trên router HQ và SW1, thực hiện cấu hình để router HQ đảm nhận nhiệm vụ định tuyến giữa các VLAN theo phương pháp “Router on a Stick”.
- Các bạn học viên căn cứ vào sơ đồ hình 2 để tạo các sub – interface và đặt IP thích hợp trên các sub – interface này.

5. Cấu hình OSPF:

- Thực hiện cấu hình OSPF Area 0 trên các router đảm bảo mọi địa chỉ IP Private trên sơ đồ mạng thấy nhau (các bạn học viên nên sử dụng sơ đồ hình 2 để cấu hình yêu cầu này).

6. Hiệu chỉnh OSPF:

- Thực hiện hiệu chỉnh router – id cho các router chạy OSPF thành các giá trị như sau:
 - HQ: 10.0.0.1.
 - BR1: 10.0.0.2.
 - BR2: 10.0.0.3.
- Thực hiện hiệu chỉnh thích hợp đảm bảo dữ liệu xuất phát từ mạng LAN của BR1 đi bất cứ đâu cũng đều phải được trung chuyển qua router BR2.

7. DHCP:

- Cấu hình tại các vị trí thích hợp đảm bảo các host thuộc các VLAN 10, 20, 30 có thể nhận được cấu hình IP từ DHCP server đặt tại Server 172.16.40.2.
- Bên cạnh đó, hãy cấu hình để các router BR1 và BR2 đảm nhận vai trò DHCP server cấp phát IP cho các thiết bị Host5 và Host6 (xem hình 2).

8. Internet:

- Cấu hình trên router HQ đảm bảo các user thuộc các mạng LAN có thể truy nhập Internet thông qua IP mặt ngoài của router (100.0.0.2).
- Cấu hình hosting thiết bị Server lên môi trường Internet bằng địa chỉ 200.0.0.1 được cấp phát từ ISP.

9. Access – list:

Cấu hình access – list theo chiều out trên cổng E0/3 của router HQ thực hiện một số “rule” như sau cho các dữ liệu đi đến Server:

- Chỉ cho phép Server ping đi các thiết bị khác, không cho các thiết bị khác ping đến Server.
- Chỉ cho phép các user thuộc VLAN 10, 20, 30 truy nhập Web đến Server.
- Chỉ cho phép các user thuộc VLAN 10 được Telnet đến Server.
- Cấm tất cả các lưu lượng khác đi đến Server.

Thực hiện:**1. Trunking:****Cấu hình:**

Trên SW1:

```
SW1(config)#interface range e0/1 - 2
SW1(config-if-range)#switchport trunk encapsulation dot1q
SW1(config-if-range)#switchport mode trunk
```

Trên SW2, SW3:

```
SW2-3(config)#interface range e0/0 - 1
SW2-3(config-if-range)#switchport trunk encapsulation dot1q
SW2-3(config-if-range)#switchport mode trunk
```

Kiểm tra:

Ta thực hiện kiểm tra để xác nhận rằng các đường trunk giữa các switch đã được thiết lập đúng theo yêu cầu:

```
SW1#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Et0/1	on	802.1q	trunking	1
Et0/2	on	802.1q	trunking	1
(...)				

```
SW2-3#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Et0/0	on	802.1q	trunking	1
Et0/1	on	802.1q	trunking	1
(...)				

2. VTP, VLAN:**Cấu hình:**

Trên cả ba switch, cấu hình để chúng tham gia VTP với domain là “waren” và password là “cisco”:

```
SW1-2-3(config)#vtp domain waren
SW1-2-3(config)#vtp password cisco
```

SW1 mặc định đã hoạt động ở mode Server nên ta không cần cấu hình gì thêm. Ta cấu hình chuyển mode của SW2 và SW3 sang mode Client:

```
SW2(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
```

Trên SW1, ta tạo các VLAN 10, 20 và 30:

```
SW1(config)#vlan 10,20,30
```

Kiểm tra và gán cổng vào các VLAN:

Trước hết, ta kiểm tra các thông số VTP trên các switch.

Trên SW1:

```
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                     : aabb.cc80.7000
Configuration last modified by 0.0.0.0 at 6-15-20 04:52:35
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       : 1
MD5 digest                    : 0xA2 0xD2 0xA8 0x3E 0x0B 0x29 0xBB 0x80
                                0x7C 0x9F 0xF9 0x1A 0x1B 0xF4 0xFC 0xCD

SW1#show vtp password
VTP Password: cisco
```

Trên SW2 và SW3:

```
SW2-3#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                     : aabb.cc80.8000
Configuration last modified by 0.0.0.0 at 6-15-20 04:52:35

Feature VLAN:
-----
VTP Operating Mode          : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs       : 8
Configuration Revision       : 1
MD5 digest                    : 0xA2 0xD2 0xA8 0x3E 0x0B 0x29 0xBB 0x80
                                0x7C 0x9F 0xF9 0x1A 0x1B 0xF4 0xFC 0xCD

SW2-3#show vtp password
VTP Password: cisco
```

Kết quả show ở trên cho thấy các switch đã được thiết lập đúng đắn các thông số VTP. Bên cạnh đó, chúng ta để ý rằng hai thông số là “Number of existing VLANs” và “Configuration Revision” trên các switch hoàn toàn giống nhau, điều này cho thấy cấu hình VLAN đã được đồng bộ giữa chúng. Chúng ta tiếp tục kiểm tra cấu hình VLAN trên các switch để xác nhận sự đồng bộ vừa nêu.

Trên SW1:

```
SW1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Et0/0, Et0/3
10	VLAN0010	active	
20	VLAN0020	active	
30	VLAN0030	active	
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Trên SW2 và SW3:

```
SW2-3#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Et0/2, Et0/3
10	VLAN0010	active	
20	VLAN0020	active	
30	VLAN0030	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 đã được đồng bộ giữa các switch, chúng ta thực hiện gán các cổng vào các VLAN như được chỉ ra trên hình 1.

Trên SW1:

```
SW1(config)#interface e0/3
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
```

Trên SW2:

```
SW2(config)#interface e0/2
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 20
```

Trên SW3:

```
SW3(config)#interface e0/2
SW3(config-if)#switchport mode access
SW3(config-if)#switchport access vlan 30
```

Ta xác nhận rằng các cổng đã được gán đúng đắn trên các VLAN:

SW1#show vlan brief

VLAN	Name	Status	Ports
1	default	active	Et0/0
10	VLAN0010	active	Et0/3
20	VLAN0020	active	
30	VLAN0030	active	
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

SW2#show vlan brief

VLAN	Name	Status	Ports
1	default	active	Et0/3
10	VLAN0010	active	
20	VLAN0020	active	Et0/2
30	VLAN0030	active	
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

SW3#show vlan brief

VLAN	Name	Status	Ports
1	default	active	Et0/3
10	VLAN0010	active	
20	VLAN0020	active	
30	VLAN0030	active	Et0/2
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Đến đây, chúng ta đã hoàn tất yêu cầu về VTP và VLAN của bài lab.

3. STP:

Cấu hình:

Để đảm bảo yêu cầu không để một đường link nào bị khóa hoàn toàn, chúng ta thực hiện hiệu chỉnh để mỗi switch sẽ đảm nhận vai trò root switch cho một VLAN trong số các VLAN 10, 20 và 30:

```
SW1(config)#spanning-tree vlan 10 root primary
SW2(config)#spanning-tree vlan 20 root primary
SW3(config)#spanning-tree vlan 30 root primary
```

Ngoài ra, để các access – port trên các switch chuyển sang trạng thái hoạt động ngay lập tức, bỏ qua các trạng thái trung gian của STP, chúng ta sử dụng tính năng Portfast trên các cổng này.

Trên SW1:

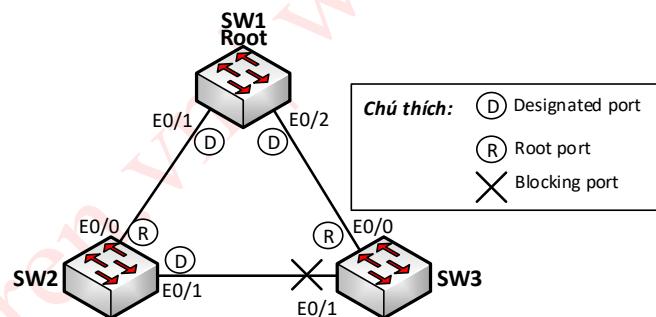
```
SW1(config)#interface e0/3
SW1(config-if)#spanning-tree portfast
```

Trên SW2 và SW3:

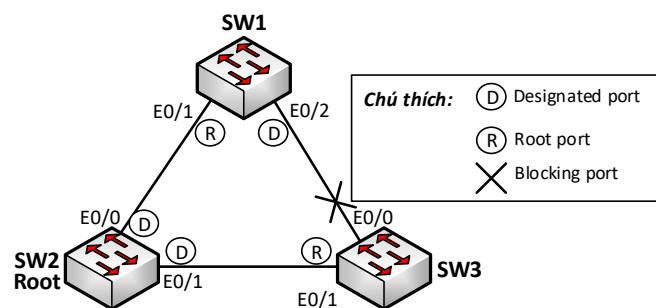
```
SW2-3(config)#interface e0/2
SW2-3(config-if)#spanning-tree portfast
```

Kiểm tra:

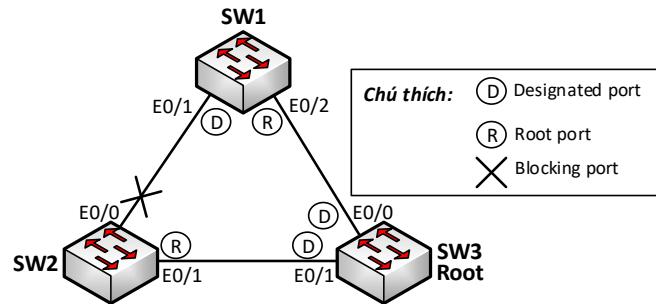
Với cấu hình STP đã thực hiện ở trên, sơ đồ layer 2 trên các VLAN hội tụ như trên các hình 3, 4 và 5 ở dưới đây:



Hình 3 – Kết quả hội tụ STP trên VLAN 10.



Hình 2 – Kết quả hội tụ STP trên VLAN 20.



Hình 5 – Kết quả hội tụ STP trên VLAN 30.

Từ các sơ đồ hội tụ ở trên ta thấy không có một đường link nào giữa các switch bị khóa hoàn toàn.

Ta có thể thực hiện kiểm tra các kết quả này bằng cách quan sát thông số STP trên các switch, ví dụ, trên VLAN 10:

```
SW1#show spanning-tree vlan 10
VLAN0010
Spanning tree enabled protocol ieee
Root ID    Priority    24586
Address    aabb.cc00.7000
This bridge is the root
Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    24586  (priority 24576 sys-id-ext 10)
Address    aabb.cc00.7000
Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time 300 sec

Interface      Role Sts Cost      Prio.Nbr Type
-----+-----+-----+-----+-----+-----+
Et0/1          Desg FWD 100      128.2      Shr
Et0/2          Desg FWD 100      128.3      Shr
Et0/3          Desg FWD 100      128.4      Shr Edge
```

```
SW2#show spanning-tree vlan 10
VLAN0010
Spanning tree enabled protocol ieee
Root ID    Priority    24586
Address    aabb.cc00.7000
Cost      100
Port      1 (Ethernet0/0)
Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
Address    aabb.cc00.8000
Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time 300 sec
```

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Et0/0	Root	FWD	100	128.1		Shr
Et0/1	Desg	FWD	100	128.2		Shr

SW3#show spanning-tree vlan 10

VLAN0010

Spanning tree enabled protocol ieee

Root ID	Priority	24586
	Address	aabb.cc00.7000
	Cost	100
	Port	1 (Ethernet0/0)
	Hello Time	2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID	Priority	32778 (priority 32768 sys-id-ext 10)
	Address	aabb.cc00.9000
	Hello Time	2 sec Max Age 20 sec Forward Delay 15 sec
	Aging Time	300 sec

Interface Role Sts Cost Prio.Nbr Type

Et0/0	Root	FWD	100	128.1		Shr
Et0/1	Altn	BLK	100	128.2		Shr

Ta cũng có thể kiểm tra rằng các cổng access của các switch đã được bật Portfast:

```
SW1#show spanning-tree interface e0/3 portfast
VLAN0010          enabled
SW2#show spanning-tree interface e0/2 portfast
VLAN0020          enabled
SW3#show spanning-tree interface e0/2 portfast
VLAN0030          enabled
```

4. Định tuyến giữa các VLAN:

Cấu hình:

Trên HQ:

```
HQ(config)#interface e0/0
HQ(config-if)#no shutdown
HQ(config-if)#exit
HQ(config)#interface e0/0.10
HQ(config-subif)#encapsulation dot1Q 10
HQ(config-subif)#ip address 172.16.10.1 255.255.255.0
HQ(config-subif)#exit
HQ(config)#interface e0/0.20
HQ(config-subif)#encapsulation dot1Q 20
HQ(config-subif)#ip address 172.16.20.1 255.255.255.0
HQ(config-subif)#exit
```

```
HQ(config)#interface e0/0.30
HQ(config-subif)#encapsulation dot1Q 30
HQ(config-subif)#ip address 172.16.30.1 255.255.255.0
HQ(config-subif)#exit
```

Trên SW1:

```
SW1(config)#interface e0/0
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
```

Kiểm tra:

HQ#show ip interface brief					
Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	unassigned	YES	TFTP	up	up
Ethernet0/0.10	172.16.10.1	YES	manual	up	up
Ethernet0/0.20	172.16.20.1	YES	manual	up	up
Ethernet0/0.30	172.16.30.1	YES	manual	up	up
Ethernet0/1	192.168.1.1	YES	TFTP	up	up
Ethernet0/2	192.168.1.5	YES	TFTP	up	up
Ethernet0/3	172.16.40.1	YES	TFTP	up	up
Ethernet1/0	100.0.0.2	YES	TFTP	up	up
Ethernet1/1	unassigned	YES	TFTP	administratively down	down
Ethernet1/2	unassigned	YES	TFTP	administratively down	down
Ethernet1/3	unassigned	YES	TFTP	administratively down	down

SW1#show interfaces trunk					
Port	Mode	Encapsulation	Status	Native	vlan
Et0/0	on	802.1q	trunking	1	
Et0/1	on	802.1q	trunking	1	
Et0/2	on	802.1q	trunking	1	
(...)					

Các bạn học viên có thể cấu hình địa chỉ IP tĩnh trên các host thuộc các VLAN 10, 20, 30 và thực hiện ping giữa các host này để kiểm tra rằng router đã thực hiện được định tuyến VLAN, hoặc cũng có thể để đến khi hoàn thành yêu cầu về DHCP rồi mới tiến hành kiểm tra. Solution này sẽ để đến khi hoàn thành các yêu cầu về DHCP rồi mới thực hiện kiểm tra.

5. Cấu hình OSPF:

Cấu hình:

Trên HQ:

```
HQ(config)#router ospf 1
HQ(config-router)#network 172.16.10.1 0.0.0.0 area 0
HQ(config-router)#network 172.16.20.1 0.0.0.0 area 0
HQ(config-router)#network 172.16.30.1 0.0.0.0 area 0
HQ(config-router)#network 172.16.40.1 0.0.0.0 area 0
HQ(config-router)#network 192.168.1.1 0.0.0.0 area 0
HQ(config-router)#network 192.168.1.5 0.0.0.0 area 0
```

Trên BR1:

```
BR1(config)#router ospf 1
BR1(config-router)#network 172.17.1.1 0.0.0.0 area 0
BR1(config-router)#network 192.168.1.2 0.0.0.0 area 0
BR1(config-router)#network 192.168.1.9 0.0.0.0 area 0
```

Trên BR2:

```
BR2(config)#router ospf 1
BR2(config-router)#network 172.18.1.1 0.0.0.0 area 0
BR2(config-router)#network 192.168.1.6 0.0.0.0 area 0
BR2(config-router)#network 192.168.1.10 0.0.0.0 area 0
```

Kiểm tra:

Ta kiểm tra rằng định tuyến đã hội tụ trên các router:

```
HQ#show ip route ospf
(...)
  172.17.0.0/24 is subnetted, 1 subnets
O    172.17.1.0 [110/20] via 192.168.1.2, 00:07:29, Ethernet0/1
  172.18.0.0/24 is subnetted, 1 subnets
O    172.18.1.0 [110/20] via 192.168.1.6, 00:04:32, Ethernet0/2
  192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O      192.168.1.8/30 [110/20] via 192.168.1.6, 00:04:32, Ethernet0/2
          [110/20] via 192.168.1.2, 00:03:48, Ethernet0/1

BR1#show ip route ospf
(...)
  172.16.0.0/24 is subnetted, 4 subnets
O    172.16.10.0 [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0
O    172.16.20.0 [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0
O    172.16.30.0 [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0
O    172.16.40.0 [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0
  172.18.0.0/24 is subnetted, 1 subnets
O    172.18.1.0 [110/20] via 192.168.1.10, 00:03:52, Ethernet0/1
  192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O      192.168.1.4/30 [110/20] via 192.168.1.10, 00:03:52, Ethernet0/1
          [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0

BR2#show ip route ospf
(...)
  172.16.0.0/24 is subnetted, 4 subnets
O    172.16.10.0 [110/20] via 192.168.1.5, 00:04:43, Ethernet0/0
O    172.16.20.0 [110/20] via 192.168.1.5, 00:04:43, Ethernet0/0
O    172.16.30.0 [110/20] via 192.168.1.5, 00:04:43, Ethernet0/0
O    172.16.40.0 [110/20] via 192.168.1.5, 00:04:43, Ethernet0/0
  172.17.0.0/24 is subnetted, 1 subnets
O    172.17.1.0 [110/20] via 192.168.1.9, 00:03:58, Ethernet0/1
  192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O      192.168.1.0/30 [110/20] via 192.168.1.9, 00:03:58, Ethernet0/1
          [110/20] via 192.168.1.5, 00:04:43, Ethernet0/0
```

6. Hiệu chỉnh OSPF:

Hiệu chỉnh Router – id:

Ta quan sát router – id của các router trước khi được hiệu chỉnh:

```
HQ#show ip ospf
Routing Process "ospf 1" with ID 192.168.1.5
(...)

BR1#show ip ospf
Routing Process "ospf 1" with ID 192.168.1.9
(...)

BR2#show ip ospf
Routing Process "ospf 1" with ID 192.168.1.10
(...)
```

Thực hiện hiệu chỉnh router – id của các router:

```
HQ(config)#router ospf 1
HQ(config-router)#router-id 10.0.0.1
% OSPF: Reload or use "clear ip ospf process" command, for this to take effect
HQ#clear ip ospf process
Reset ALL OSPF processes? [no]: y

BR1(config)#router ospf 1
BR1(config-router)#router-id 10.0.0.2
% OSPF: Reload or use "clear ip ospf process" command, for this to take effect
BR1#clear ip ospf process
Reset ALL OSPF processes? [no]: y

BR2(config)#router ospf 1
BR2(config-router)#router-id 10.0.0.3
% OSPF: Reload or use "clear ip ospf process" command, for this to take effect
BR2#clear ip ospf process
Reset ALL OSPF processes? [no]: y
```

Sau khi tiến trình OSPF trên các router được reset, giá trị router – id đã được cập nhật:

```
HQ#show ip ospf
Routing Process "ospf 1" with ID 10.0.0.1
(...)

BR1#show ip ospf
Routing Process "ospf 1" with ID 10.0.0.2
(...)

BR2#show ip ospf
Routing Process "ospf 1" with ID 10.0.0.3
(...)
```

Hiệu chỉnh đường đi:

Trước khi hiệu chỉnh đường đi, BR1 sẽ chọn đường đi đến các subnet trong mạng theo một trong hai next – hop: HQ (192.168.1.1) hoặc BR2 (192.168.1.10):

BR1#show ip route ospf

```
(...)  
    172.16.0.0/24 is subnetted, 4 subnets  
O      172.16.10.0 [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0  
O      172.16.20.0 [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0  
O      172.16.30.0 [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0  
O      172.16.40.0 [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0  
    172.18.0.0/24 is subnetted, 1 subnets  
O      172.18.1.0 [110/20] via 192.168.1.10, 00:03:52, Ethernet0/1  
192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks  
O          192.168.1.4/30 [110/20] via 192.168.1.10, 00:03:52, Ethernet0/1  
                  [110/20] via 192.168.1.1, 00:07:36, Ethernet0/0
```

Để BR1 luôn chọn đường đi đến mọi đích đến chỉ theo next – hop BR2 (192.168.1.10), ta chỉnh lại giá trị cost trên cổng E0/0 nối đến HQ cao hơn tổng cost của hai cổng E0/1 (của BR1) và E0/0 (của BR2) cộng lại:

```
BR1(config)#interface e0/0  
BR1(config-if)#ip ospf cost 21
```

Lúc này, BR1 đã chọn đường đi đến mọi đích đến chỉ còn thông qua next – hop BR2 (192.168.1.10):

BR1#show ip route ospf

```
(...)  
    172.16.0.0/24 is subnetted, 4 subnets  
O      172.16.10.0 [110/30] via 192.168.1.10, 00:01:27, Ethernet0/1  
O      172.16.20.0 [110/30] via 192.168.1.10, 00:01:27, Ethernet0/1  
O      172.16.30.0 [110/30] via 192.168.1.10, 00:01:27, Ethernet0/1  
O      172.16.40.0 [110/30] via 192.168.1.10, 00:01:27, Ethernet0/1  
    172.18.0.0/24 is subnetted, 1 subnets  
O      172.18.1.0 [110/20] via 192.168.1.10, 00:10:08, Ethernet0/1  
192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks  
O          192.168.1.4/30 [110/20] via 192.168.1.10, 00:10:08, Ethernet0/1
```

7. DHCP:

Cấu hình:

Trên thiết bị Server đã thực hiện cấu hình sẵn chức năng DHCP server để cấp phát IP động cho các user thuộc các VLAN 10, 20, 30 (các bạn học viên có thể quan sát cấu hình này bằng cách truy nhập vào thiết bị Server – thực ra là một router giả lập vai trò của một server). Chúng ta cấu hình thêm tính năng DHCP Relay Agent trên các cổng sub – interface của router HQ để các host thuộc các VLAN vừa nêu có thể nhận được cấu hình IP:

```
HQ(config)#interface e0/0.10  
HQ(config-subif)#ip helper-address 172.16.40.2  
HQ(config-subif)#exit  
HQ(config)#interface e0/0.20  
HQ(config-subif)#ip helper-address 172.16.40.2  
HQ(config-subif)#exit  
HQ(config)#interface e0/0.30  
HQ(config-subif)#ip helper-address 172.16.40.2  
HQ(config-subif)#exit
```

Bên cạnh đó, chúng ta cấu hình các router BR1 và BR2 cấp phát IP xuống cho các host của mình theo quy hoạch IP đã chỉ ra trên hình 2:

```
BR1(config)#ip dhcp excluded-address 172.17.1.1
BR1(config)#ip dhcp pool BR1_LAN
BR1(dhcp-config)#network 172.17.1.0 /24
BR1(dhcp-config)#default-router 172.17.1.1
BR1(dhcp-config)#exit

BR2(config)#ip dhcp excluded-address 172.18.1.1
BR2(config)#ip dhcp pool BR2_LAN
BR2(dhcp-config)#network 172.18.1.0 /24
BR2(dhcp-config)#default-router 172.18.1.1
BR2(dhcp-config)#exit
```

Kiểm tra:

Ta kiểm tra rằng các host trên sơ đồ đều đã nhận được cấu hình IP từ DHCP:

```
Host1> dhcp -r
DDORA IP 172.16.10.2/24 GW 172.16.10.1

Host2> dhcp -r
DDORA IP 172.16.20.2/24 GW 172.16.20.1

Host3> dhcp -r
DDORA IP 172.16.30.2/24 GW 172.16.30.1

Host4> dhcp -r
DDORA IP 172.17.1.2/24 GW 172.17.1.1

Host5> dhcp -r
DDORA IP 172.18.1.2/24 GW 172.18.1.1
```

Bảng DHCP Binding trên các DHCP Server cho thấy các server này đã thực sự làm nhiệm vụ cấp phát IP:

```
Server#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/          Lease expiration      Type
                  Hardware address/
                  User name
172.16.10.2        0100.5079.6668.0a    Jun 16 2020 11:37 AM  Automatic
172.16.20.2        0100.5079.6668.0b    Jun 16 2020 11:37 AM  Automatic
172.16.30.2        0100.5079.6668.0c    Jun 16 2020 11:37 AM  Automatic

BR1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/          Lease expiration      Type
                  Hardware address/
                  User name
172.17.1.2          0100.5079.6668.0d    Jun 16 2020 11:37 AM  Automatic

BR2#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/          Lease expiration      Type
                  Hardware address/
                  User name
172.18.1.2          0100.5079.6668.0e    Jun 16 2020 11:37 AM  Automatic
```

Khi các host Host1, Host2, Host3 đã có IP, ta kiểm tra lại hoạt động định tuyến giữa các VLAN bằng cách cho các host này ping lẫn nhau:

```
Host1> ping 172.16.20.2
84 bytes from 172.16.20.2 icmp_seq=1 ttl=63 time=8.791 ms
84 bytes from 172.16.20.2 icmp_seq=2 ttl=63 time=5.556 ms

Host1> ping 172.16.30.2
84 bytes from 172.16.30.2 icmp_seq=1 ttl=63 time=10.738 ms
84 bytes from 172.16.30.2 icmp_seq=2 ttl=63 time=3.911 ms

Host2> ping 172.16.30.2
84 bytes from 172.16.30.2 icmp_seq=1 ttl=63 time=5.822 ms
84 bytes from 172.16.30.2 icmp_seq=2 ttl=63 time=7.434 ms
```

Kết quả ping thành công cho thấy cấu hình định tuyến VLAN thực hiện ở trên đã hoạt động tốt.

8. Internet:

Cấu hình:

Trước hết, router HQ cần có một default – route đi Internet và phải thực hiện lan truyền default – route này vào mạng bên trong:

```
HQ(config)#ip route 0.0.0.0 0.0.0.0 100.0.0.1
HQ(config)#router ospf 1
HQ(config-router)#default-information originate
```

Tiếp theo, ta thực hiện cấu hình NAT overload để các host thuộc các mạng LAN có thể truy nhập Internet thông qua IP mặt ngoài trên cổng E1/0 của router HQ:

```
HQ(config)#access-list 1 permit 172.16.10.0 0.0.0.255
HQ(config)#access-list 1 permit 172.16.20.0 0.0.0.255
HQ(config)#access-list 1 permit 172.16.30.0 0.0.0.255
HQ(config)#access-list 1 permit 172.17.1.0 0.0.0.255
HQ(config)#access-list 1 permit 172.18.1.0 0.0.0.255

HQ(config)#ip nat inside source list 1 interface e1/0 overload

HQ(config)#interface e0/0.10
HQ(config-subif)#ip nat inside
HQ(config-subif)#exit
HQ(config)#interface e0/0.20
HQ(config-subif)#ip nat inside
HQ(config-subif)#exit
HQ(config)#interface e0/0.30
HQ(config-subif)#ip nat inside
HQ(config-subif)#exit
HQ(config)#interface e0/1
HQ(config-if)#ip nat inside
HQ(config-if)#exit
HQ(config)#interface e0/2
HQ(config-if)#ip nat inside
HQ(config-if)#exit
```

```
HQ(config)#interface e1/0
HQ(config-if)#ip nat outside
HQ(config-if)#exit
```

Tiếp theo, ta cấu hình Static NAT để NAT địa chỉ Private của Server thành địa chỉ public 200.0.0.1 do ISP cấp phát cho doanh nghiệp:

```
HQ(config)#ip nat inside source static 172.16.40.2 200.0.0.1
HQ(config)#interface e0/3
HQ(config-if)#ip nat inside
HQ(config-if)#exit
```

Kiểm tra:

Ta kiểm tra rằng các host đều đã có thể truy nhập được Internet. Việc kiểm tra được thực hiện bằng cách ping đến địa chỉ 8.8.8.8 hoặc đến Internet_Host (ở đây ta chọn ping đến 8.8.8.8):

Host1> ping 8.8.8.8

```
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=3.411 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=3.069 ms
(...)
```

Host2> ping 8.8.8.8

```
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=5.243 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=3.577 ms
(...)
```

Host3> ping 8.8.8.8

```
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=3.810 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=4.190 ms
(...)
```

Host4> ping 8.8.8.8

```
84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=4.859 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=3.527 ms
(...)
```

Host5> ping 8.8.8.8

```
84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=3.476 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=2.915 ms
(...)
```

Bảng NAT của router HQ cho thấy hoạt động NAT overload đã diễn ra:

HQ#show ip nat translations

Pro Inside global	Inside local	Outside local	Outside global
icmp 100.0.0.2:8764	172.16.10.2:8764	8.8.8.8:8764	8.8.8.8:8764
icmp 100.0.0.2:9276	172.16.20.2:9276	8.8.8.8:9276	8.8.8.8:9276
icmp 100.0.0.2:9532	172.16.30.2:9532	8.8.8.8:9532	8.8.8.8:9532
---	172.16.40.2	---	---
icmp 100.0.0.2:10044	172.17.1.2:10044	8.8.8.8:10044	8.8.8.8:10044
icmp 100.0.0.2:10556	172.18.1.2:10556	8.8.8.8:10556	8.8.8.8:10556

Tiếp theo, ta thử từ Internet_Host, là một thiết bị giả lập một user trên Internet truy nhập đến thiết bị Server nằm bên trong mạng:

```
Internet_Host#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:
!!!!! <- Ping thành công đến Server bên trong
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

Internet_Host#telnet 200.0.0.1
Trying 200.0.0.1 ... Open <- Telnet thành công đến Server bên trong

Password required, but none set

[Connection to 200.0.0.1 closed by foreign host]

Internet_Host#telnet 200.0.0.1 80
Trying 200.0.0.1, 80 ... Open <- Truy nhập HTTP thành công đến Server bên trong
exit
HTTP/1.1 400 Bad Request
Date: Tue, 16 Jun 2020 03:30:31 GMT
Server: cisco-IOS
Accept-Ranges: none
}
400 Bad Request
[Connection to 200.0.0.1 closed by foreign host]
Internet_Host#
```

Bảng NAT của router HQ cho thấy hoạt động Static NAT đã diễn ra phù hợp cho các truy nhập vừa thực hiện từ Internet_Host đến Server:

```
HQ#show ip nat translations
Pro Inside global      Inside local        Outside local       Outside global
icmp 200.0.0.1:0        172.16.40.2:0      101.0.0.2:0        101.0.0.2:0
tcp 200.0.0.1:23         172.16.40.2:23      101.0.0.2:17005    101.0.0.2:17005
tcp 200.0.0.1:80         172.16.40.2:80      101.0.0.2:44149    101.0.0.2:44149
--- 200.0.0.1           172.16.40.2        ---               ---
```

Đến đây, chúng ta đã cấu hình và kiểm tra thành công hoạt động NAT trên router HQ.

9. Access – list:

Cấu hình:

Trước hết, để chỉ cho phép ping một chiều từ Server ra ngoài, ta chỉ cho phép lưu lượng ICMP Echo – Reply đi ra khỏi cổng E0/3 của HQ để đi đến Server (lưu lượng này chính là kết quả trả về cho hoạt động ping thành công từ Server):

```
HQ(config)#ip access-list extended FIREWALL
HQ(config-ext-nacl)#permit icmp any host 172.16.40.2 echo-reply
```

Tiếp theo, ta chỉ cho phép lưu lượng TCP đi đến port 80 (HTTP) của Server mà xuất phát từ các subnet được cho phép (gồm: 172.16.10.0/24 – VLAN 10, 172.16.20.0/24 – VLAN 20, 172.16.30.0/24 – VLAN 30):

```
HQ(config-ext-nacl)#permit tcp 172.16.10.0 0.0.0.255 host 172.16.40.2 eq 80
HQ(config-ext-nacl)#permit tcp 172.16.20.0 0.0.0.255 host 172.16.40.2 eq 80
HQ(config-ext-nacl)#permit tcp 172.16.30.0 0.0.0.255 host 172.16.40.2 eq 80
```

Cuối cùng, ta cho phép lưu lượng TCP đi đến port 23 (Telnet) của Server mà xuất phát từ subnet 172.16.10.0/24 (VLAN 10):

```
HQ(config-ext-nacl)#permit tcp 172.16.10.0 0.0.0.255 host 172.16.40.2 eq 23
HQ(config-ext-nacl)#exit
```

Các lưu lượng khác sẽ bị chặn lại bởi entry ngầm định “deny ip any any” của access – list “FIREWALL” vừa cấu hình ở trên.

Sau khi cấu hình access – list, ta thực hiện đặt nó lên cổng E0/3 của HQ theo chiều out như yêu cầu đặt ra:

```
HQ(config)#interface e0/3
HQ(config-if)#ip access-group FIREWALL out
HQ(config-if)#exit
```

Kiểm tra:

Ta kiểm tra lại nội dung của access – list vừa cấu hình:

```
HQ#show access-lists FIREWALL
Extended IP access list FIREWALL
    10 permit icmp any host 172.16.40.2 echo-reply
    20 permit tcp 172.16.10.0 0.0.0.255 host 172.16.40.2 eq www
    30 permit tcp 172.16.20.0 0.0.0.255 host 172.16.40.2 eq www
    40 permit tcp 172.16.30.0 0.0.0.255 host 172.16.40.2 eq www
    50 permit tcp 172.16.10.0 0.0.0.255 host 172.16.40.2 eq telnet
```

Access – list này đã được đặt trên cổng E0/3 đúng theo yêu cầu:

```
HQ#show ip interface e0/3 | inc access list
Outgoing access list is FIREWALL
Inbound access list is not set
```

Ta bắt đầu kiểm tra hoạt động của access – list.

Đầu tiên, ta thử rằng Server có thể ping đến các host khác nhưng các host khác không thể ping Server, ví dụ, Host1 và Internet_Host:

```
Server#ping 172.16.10.2 <- Server ping thành công Host1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

Host1> ping 172.16.40.2 <- Host1 không ping được Server
*172.16.10.1 icmp_seq=1 ttl=255 time=3.041 ms (ICMP type:3, code:13, Communication
administratively prohibited)
*172.16.10.1 icmp_seq=2 ttl=255 time=2.544 ms (ICMP type:3, code:13, Communication
administratively prohibited)
(...)
```

Tiếp theo, ta kiểm tra rằng chỉ có những subnet được cho phép mới được phép truy nhập Web đến Server, ví dụ, Host2:

```
Host2> ping 172.16.40.2 -P 6 -p 80 <- Host2 truy nhập HTTP thành công đến Server
Connect 80@172.16.40.2 seq=1 ttl=254 time=2.469 ms
SendData 80@172.16.40.2 seq=1 ttl=254 time=2.844 ms
Close     80@172.16.40.2 seq=1 ttl=254 time=4.893 ms
(...)

Host4> ping 172.16.40.2 -P 6 -p 80 <- Host4 bị chặn truy nhập HTTP đến Server
*192.168.1.5 tcp_seq=1 ttl=254 time=2.685 ms (ICMP type:3, code:13, Communication
administratively prohibited)
*192.168.1.5 tcp_seq=3 ttl=254 time=2.711 ms (ICMP type:3, code:13, Communication
administratively prohibited)
*192.168.1.5 tcp_seq=5 ttl=254 time=2.907 ms (ICMP type:3, code:13, Communication
administratively prohibited)
```

Ghi chú:

Các host trên các mạng LAN trong bài lab này được giả lập bằng chương trình VPC trên phần mềm EVE. Trên chương trình này không tích hợp telnet nên ta sử dụng lệnh ping đến 172.16.40.2 với protocol – ID = 6 (“-P 6”), chính là protocol – ID của TCP và destination port = 80 (“-p 80”), chính là port TCP của ứng dụng HTTP.

Tiếp theo, ta kiểm tra “rule” Telnet (chỉ có các host thuộc VLAN 10 và subnet 101.0.0.0/24 mới có thể telnet đến Server):

```
Host1> ping 172.16.40.2 -P 6 -p 23 <- Host1 Telnet được đến Server
Connect 23@172.16.40.2 seq=1 ttl=254 time=2.549 ms
SendData 23@172.16.40.2 seq=1 ttl=254 time=2.565 ms
Close     23@172.16.40.2 timeout(16.601ms)
(...)

Host5> ping 172.16.40.2 -P 6 -p 23 <- Host5 bị chặn Telnet đến Server
*192.168.1.5 tcp_seq=1 ttl=254 time=1.573 ms (ICMP type:3, code:13, Communication administratively
prohibited)
*192.168.1.5 tcp_seq=3 ttl=254 time=2.620 ms (ICMP type:3, code:13, Communication administratively
prohibited)
*192.168.1.5 tcp_seq=5 ttl=254 time=1.542 ms (ICMP type:3, code:13, Communication administratively
prohibited)
```

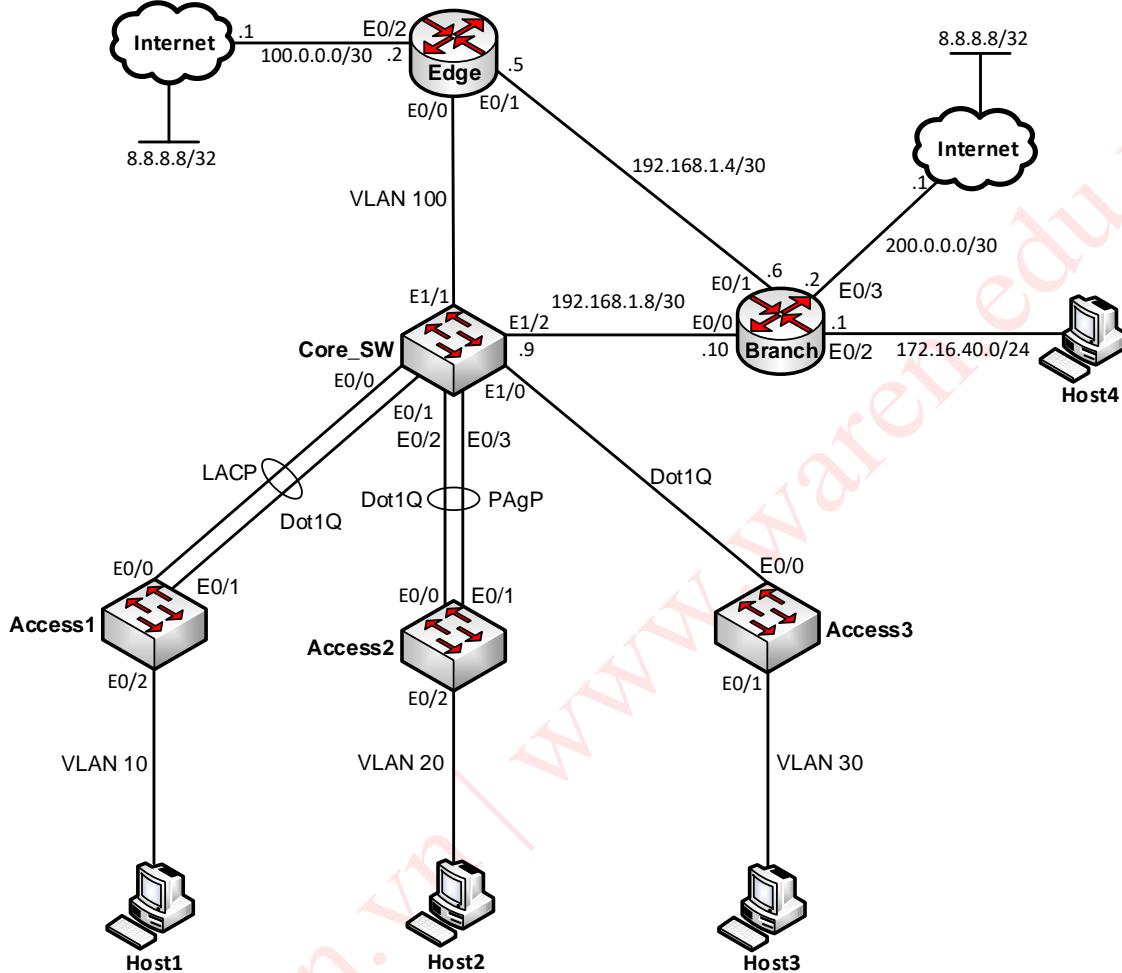
Kết quả kiểm tra access – list FIREWALL trên router HQ cho thấy các “rule” đã hoạt động:

```
HQ#show access-lists FIREWALL
Extended IP access list FIREWALL
  10 permit icmp any host 172.16.40.2 echo-reply (10 matches)
  20 permit tcp 172.16.10.0 0.0.0.255 host 172.16.40.2 eq www
  30 permit tcp 172.16.20.0 0.0.0.255 host 172.16.40.2 eq www (25 matches)
  40 permit tcp 172.16.30.0 0.0.0.255 host 172.16.40.2 eq www
  50 permit tcp 172.16.10.0 0.0.0.255 host 172.16.40.2 eq telnet (28 matches)
```

Đến đây, chúng ta đã hoàn tất cấu hình và kiểm tra tác vụ về access – list của bài lab.

Lab 28 – Tổng hợp ôn tập – Bài số 2

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Bài lab gồm các thiết bị được kết nối với nhau theo sơ đồ được chỉ ra trong hình 1. Trong sơ đồ này, hệ thống switch và router Edge đóng vai trò là các thiết bị của trung tâm của một mạng donut nghiệp, router Branch đóng vai trò là router tại một trung tâm chi nhánh của doanh nghiệp này.
- Trong bài lab này, các bạn học viên sẽ thực hành ôn tập lại các vấn đề về Ethernet switching, định tuyến OSPF cũng như một số dịch vụ mạng như DHCP và Internet.
- Trên bài lab này, các thiết bị đều đã được thiết lập sẵn hostname; ngoài ra, các router còn được cấu hình sẵn địa chỉ IP trên các cổng; các bạn học viên không cần phải thiết lập lại các thông số này. Bên cạnh đó, trong suốt quá trình thực hiện bài lab, các bạn học viên không can thiệp vào thiết bị giả lập Internet.

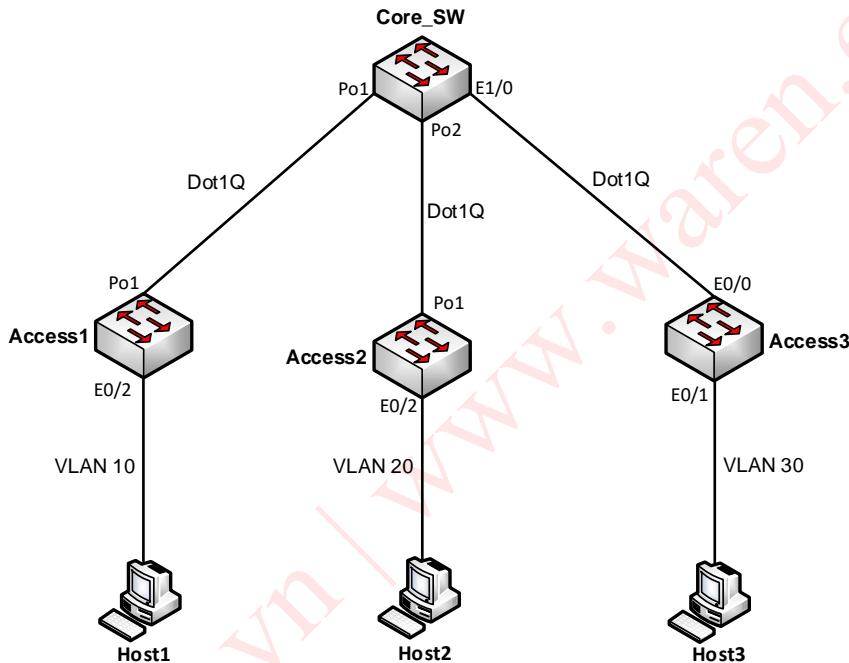
Yêu cầu:**1. Etherchannel:**

Thực hiện cấu hình các đường Etherchannel như được mô tả trong hình 1, trong đó:

- Đường Etherchannel nối giữa Core_SW và Access1 sử dụng phương thức thiết lập channel LACP.
- Đường Etherchannel nối giữa Core_SW và Access2 sử dụng phương thức thiết lập channel PAgP.

2. Trunking:

- Sau khi thiết lập xong Etherchannel, đấu nối giữa các switch có thể được mô tả lại như trên sơ đồ hình 2 dưới đây:



Hình 2 – Kết nối giữa các switch.

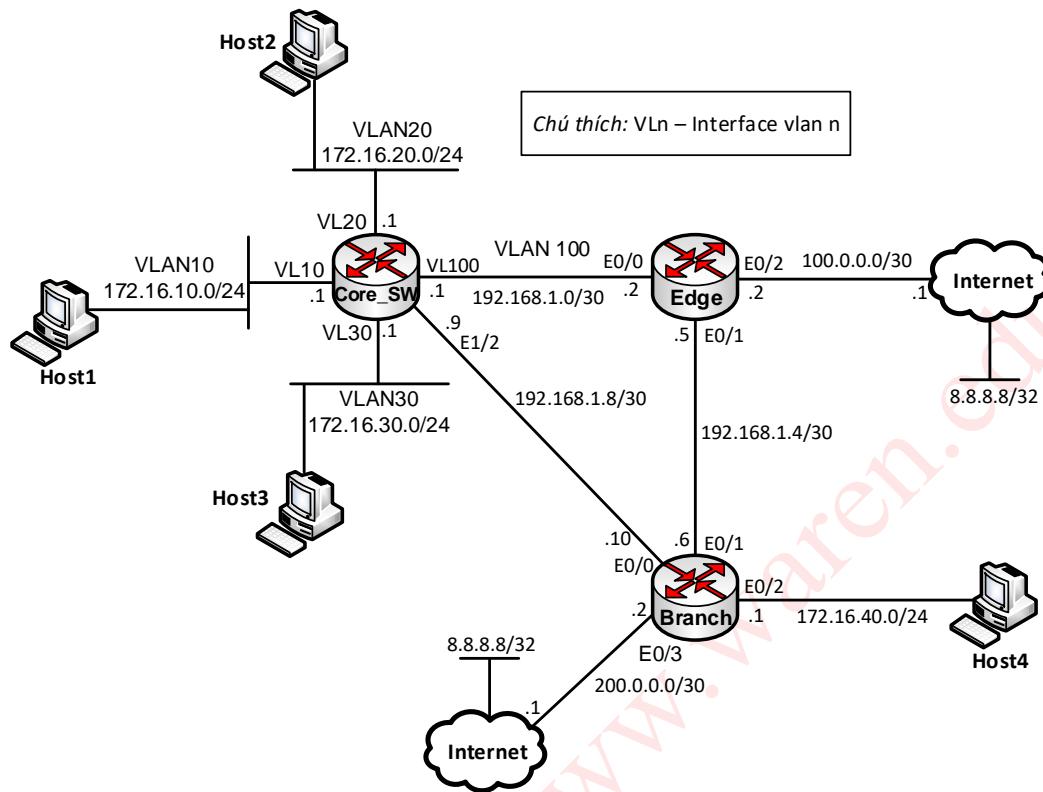
- Hãy thực hiện cấu hình các link giữa các switch thành các đường Trunking Dot1Q.

3. VTP, VLAN:

- Thực hiện cho các switch tham gia VTP với các thông số như sau:
 - VTP domain: *waren*.
 - VTP password: *cisco*.
 - Core_SW: Server; Access1, Access2, Access3: Client.
- Thực hiện tạo các VLAN 10, 20, 30 trên Core_SW, kiểm tra rằng cấu hình VLAN này được tự động đồng bộ xuống các switch Access1, Access2, Access3.
- Trên các switch access, thực hiện gán cổng vào các VLAN như được chỉ ra trên các sơ đồ ở trên.

4. Xây dựng layer 3 topology:

- Cấu hình switch Core_SW thực hiện định tuyến giữa các VLAN theo các thông số như được chỉ ra trên sơ đồ layer 3 ở hình 3:

*Hình 3 – Layer 3 topology.*

- Ngoài ra, cũng trên Core_SW, thực hiện tạo thêm VLAN 100 cùng SVI tương ứng và chuyển cổng E1/2 thành cổng layer 3 để tạo kết nối IP đến các router như mô tả trên hình 3. Các bạn học viên cũng cần phải đặt địa chỉ IP cho các cổng layer 3 mới tạo ra này theo quy hoạch IP được chỉ ra trên hình 3.

5. Định tuyến OSPF:

Thực hiện cấu hình định tuyến OSPF Area 0 giữa các router và switch layer 3 trên hình 3 đảm bảo mọi địa chỉ trên sơ đồ thấy nhau.

6. DHCP:

- Thực hiện cấu hình router Edge làm DHCP server cấp phát IP cho các host thuộc các VLAN 10, 20, và 30.
- Cấu hình router Branch cấp phát IP cho Host4.

7. Hiệu chỉnh đường đi:

Hãy hiệu chỉnh OSPF đảm bảo hoạt động trao đổi dữ liệu giữa các host thuộc hai chi nhánh đều phải thông qua router Edge, đường link nối giữa Core_SW và Branch chỉ sử dụng để dự phòng.

8. Internet:

Thực hiện cấu hình hoạt động truy nhập Internet cho các host của doanh nghiệp này theo yêu cầu sau:

- Các host thuộc trụ sở chính (các VLAN 10, 20, 30) sẽ đi Internet theo đường truyền Internet tại router Edge của trụ sở chính.

- Các host thuộc chi nhánh (mạng LAN 172.16.40.0/24) sẽ đi Internet theo đường truyền Internet tại chi nhánh.
- Hoạt động truy nhập Internet vừa nêu trên hai trụ sở sẽ được sử dụng để dự phòng lẫn nhau: trụ sở nào bị mất kết nối Internet sẽ truy nhập Internet thông qua đường truyền của trụ sở còn lại; nếu đường chính được khôi phục sẽ lại truy nhập Internet theo đường chính trên chi nhánh của mình.

Thực hiện:**1. Etherchannel:****Cấu hình:**

Trước hết, chúng ta thiết lập Etherchannel giữa Core_SW và Access1 bằng giao thức LACP.

Trên Core_SW:

```
Core_SW(config)#interface range e0/0 - 1
Core_SW(config-if-range)#shutdown
Core_SW(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1

Core_SW(config-if-range)#no shutdown
```

Trên Access1:

```
Access1(config)#interface range e0/0 - 1
Access1(config-if-range)#shutdown
Access1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1

Access1(config-if-range)#no shutdown
```

Tiếp theo, chúng ta thiết lập Etherchannel nối giữa Core_SW và Access2 bằng PAgP.

Trên Core_SW:

```
Core_SW(config)#interface range e0/2 - 3
Core_SW(config-if-range)#shutdown
Core_SW(config-if-range)#channel-group 2 mode desirable
Creating a port-channel interface Port-channel 2

Core_SW(config-if-range)#no shutdown
```

Trên Access2:

```
Access2(config)#interface range e0/0 - 1
Access2(config-if-range)#shutdown
Access2(config-if-range)#channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1

Access2(config-if-range)#no shutdown
```

Kiểm tra:

Chúng ta kiểm tra rằng các đường Etherchannel đã được thiết lập đúng theo yêu cầu.

Trên Core_SW:

```
Core_SW#show etherchannel summary
Flags:  D - down          P - bundled in port-channel
        I - stand-alone  S - suspended
        H - Hot-standby (LACP only)
        R - Layer3         S - Layer2
        U - in use         N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG

Number of channel-groups in use: 3
Number of aggregators:          3

Group  Port-channel  Protocol      Ports
-----+-----+-----+
1      Po1(SU)       LACP          Et0/0(P)    Et0/1(P)
2      Po2(SU)       PAgP          Et0/2(P)    Et0/3(P)
```

Trên Access1:

```
Access1#show etherchannel summary
Flags:  D - down          P - bundled in port-channel
        I - stand-alone  S - suspended
        H - Hot-standby (LACP only)
        R - Layer3         S - Layer2
        U - in use         N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:          1
```

Group	Port-channel	Protocol	Ports
1	Po1 (SU)	LACP	Et0/0 (P) Et0/1 (P)

Trên Access2:

```
Access2#show etherchannel summary
Flags: D - down P - bundled in port-channel
      I - stand-alone S - suspended
      H - Hot-standby (LACP only)
      R - Layer3 S - Layer2
      U - in use N - not in use, no aggregation
      f - failed to allocate aggregator

      M - not in use, minimum links not met
      m - not in use, port not aggregated due to minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port

      A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
-----+-----+-----+
1     Po1 (SU)      PAgP    Et0/0 (P)  Et0/1 (P)
```

2. Trunking:

Cấu hình:

Trên Core_SW:

```
Core_SW(config)#interface range po 1 - 2,e1/0
Core_SW(config-if-range)#switchport trunk encapsulation dot1q
Core_SW(config-if-range)#switchport mode trunk
```

Cấu hình trunking trên các cổng Po1 của các switch access:

```
Access1-2(config)#interface po 1
Access1-2(config-if)#switchport trunk encapsulation dot1q
Access1-2(config-if)#switchport mode trunk
```

Trên Access3:

```
Access3(config)#interface e0/0
Access3(config-if)#switchport trunk encapsulation dot1q
Access3(config-if)#switchport mode trunk
```

Kiểm tra:

Trên Core_SW:

```
Core_SW#show interfaces trunk

Port      Mode          Encapsulation  Status      Native vlan
Et1/0     on           802.1q        trunking   1
Po1       on           802.1q        trunking   1
Po2       on           802.1q        trunking   1

Port      Vlans allowed on trunk
Et1/0    1-4094
Po1     1-4094
Po2     1-4094

Port      Vlans allowed and active in management domain
Et1/0    1
Po1     1
Po2     1

Port      Vlans in spanning tree forwarding state and not pruned
Et1/0    1
Po1     1
Po2     1
```

Trên các switch Access1 và Access2:

```
Access1-2#show interfaces trunk

Port      Mode          Encapsulation  Status      Native vlan
Po1       on           802.1q        trunking   1

Port      Vlans allowed on trunk
Po1     1-4094

Port      Vlans allowed and active in management domain
Po1     1

Port      Vlans in spanning tree forwarding state and not pruned
Po1     1
```

Trên Access3:

```
Access3#show interfaces trunk

Port      Mode          Encapsulation  Status      Native vlan
Et0/0    on           802.1q        trunking   1

Port      Vlans allowed on trunk
Et0/0    1-4094

Port      Vlans allowed and active in management domain
```

Et0/0	1
Port	Vlans in spanning tree forwarding state and not pruned
Et0/0	1

3. VTP, VLAN:

Cấu hình VTP và VLAN:

Thực hiện cấu hình cho các switch tham gia VTP. Trên cả 4 switch (mode config):

```
vtp domain waren  
vtp password cisco
```

Trên các switch access:

```
Access1-2-3(config)#vtp mode client  
Setting device to VTP Client mode for VLANS.
```

Thực hiện tạo VLAN trên Core_SW theo yêu cầu đặt ra:

```
Core_SW(config)#vlan 10,20,30  
Core_SW(config-vlan)#exit
```

Kiểm tra và gán cổng vào các VLAN:

Ta kiểm tra rằng thông số VTP đã được thiết lập đúng đắn trên các switch.

Trên Core_SW:

```
Core_SW#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 : aabb.cc80.1000  
Configuration last modified by 0.0.0.0 at 11-11-20 13:52:06  
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 : 1  
MD5 digest : 0x9D 0x26 0x16 0x09 0x69 0xC6 0x5C 0xFD  
0x65 0x35 0x59 0xE1 0x8A 0x32 0xD4 0x63  
  
Core_SW#show vtp password  
VTP Password: cisco
```

Trên các switch access, kiểm tra ví dụ trên switch Access1:

```
Access1#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 : aabb.cc80.2000
Configuration last modified by 0.0.0.0 at 11-11-20 13:52:06

Feature VLAN:
-----
VTP Operating Mode : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs : 8
Configuration Revision : 1
MD5 digest : 0x9D 0x26 0x16 0x09 0x69 0xC6 0x5C 0xFD
               0x65 0x35 0x59 0xE1 0x8A 0x32 0xD4 0x63

Access1#show vtp password
VTP Password: cisco
```

Ta có thể thực hiện kiểm tra VTP tương tự trên các switch access còn lại.

Tiếp theo, ta thực hiện kiểm tra rằng cấu hình VLAN mới tạo ra đã được đồng bộ giữa các switch.

Trên Core_SW:

```
Core_SW#show vlan brief
-----  
VLAN Name          Status      Ports
-----  
1     default       active      Et1/1, Et1/2, Et1/3
10    VLAN0010      active
20    VLAN0020      active
30    VLAN0030      active
1002  fddi-default act/unsup
1003  token-ring-default act/unsup
1004  fddinet-default act/unsup
1005  trnet-default act/unsup
```

Trên Access1 và Access2:

```
Access1-2#show vlan brief
-----  
VLAN Name          Status      Ports
-----  
1     default       active      Et0/2, Et0/3, Et1/0, Et1/1
                                         Et1/2, Et1/3
10    VLAN0010      active
20    VLAN0020      active
30    VLAN0030      active
1002  fddi-default act/unsup
```

1003 token-ring-default	act/unsup
1004 fddinet-default	act/unsup
1005 trnet-default	act/unsup

Trên Access3:

Access3#show vlan brief

VLAN	Name	Status	Ports
1	default	active	Et0/1, Et0/2, Et0/3, Et1/0 Et1/1, Et1/2, Et1/3
10	VLAN0010	active	
20	VLAN0020	active	
30	VLAN0030	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Cuối cùng, ta thực hiện gán các cổng vào các VLAN như được chỉ ra trên sơ đồ:

```
Access1(config)#interface e0/2
Access1(config-if)#switchport mode access
Access1(config-if)#switchport access vlan 10

Access2(config)#interface e0/2
Access2(config-if)#switchport mode access
Access2(config-if)#switchport access vlan 20

Access3(config)#interface e0/1
Access3(config-if)#switchport mode access
Access3(config-if)#switchport access vlan 30
```

4. Xây dựng layer 3 topology:

Cấu hình:

Trước hết, trên Core_SW, ta tạo VLAN 100 và interface vlan 100 để kết nối IP đến router Edge:

```
Core_SW(config)#vlan 100
Core_SW(config-vlan)#name TO_EDGE
Core_SW(config-vlan)#exit
Core_SW(config)#interface e1/1
Core_SW(config-if)#switchport mode access
Core_SW(config-if)#switchport access vlan 100
Core_SW(config-if)#exit
Core_SW(config)#interface vlan 100
Core_SW(config-if)#description TO EDGE
Core_SW(config-if)#no shutdown
Core_SW(config-if)#ip address 192.168.1.1 255.255.255.252
Core_SW(config-if)#exit
```

```
Core_SW(config)#interface e1/2
Core_SW(config-if)#description TO BRANCH
Core_SW(config-if)#no switchport
Core_SW(config-if)#ip address 192.168.1.9 255.255.255.252
Core_SW(config-if)#exit
```

Tiếp theo, ta tạo các SVI (interface VLAN) kết nối đến các VLAN 10, 20 và 30 để thực hiện định tuyến VLAN giữa các VLAN này:

```
Core_SW(config)#interface vlan 10
Core_SW(config-if)#no shutdown
Core_SW(config-if)#ip address 172.16.10.1 255.255.255.0
Core_SW(config-if)#exit
Core_SW(config)#interface vlan 20
Core_SW(config-if)#no shutdown
Core_SW(config-if)#ip address 172.16.20.1 255.255.255.0
Core_SW(config-if)#exit
Core_SW(config)#interface vlan 30
Core_SW(config-if)#ip address 172.16.30.1 255.255.255.0
Core_SW(config-if)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng các cổng layer 3 đã được tạo đầy đủ trên Core_SW:

Core_SW#show ip interface brief	Interface	IP-Address	OK?	Method	Status	Protocol
	Ethernet0/0	unassigned	YES	unset	up	up
	Ethernet0/1	unassigned	YES	unset	up	up
	Ethernet0/2	unassigned	YES	unset	up	up
	Ethernet0/3	unassigned	YES	unset	up	up
	Ethernet1/0	unassigned	YES	unset	up	up
	Ethernet1/1	unassigned	YES	unset	up	up
	Ethernet1/2	192.168.1.9	YES	manual	up	up
	Ethernet1/3	unassigned	YES	unset	up	up
	Port-channel1	unassigned	YES	unset	up	up
	Port-channel2	unassigned	YES	unset	up	up
	Vlan10	172.16.10.1	YES	manual	up	up
	Vlan20	172.16.20.1	YES	manual	up	up
	Vlan30	172.16.30.1	YES	manual	up	up
	Vlan100	192.168.1.1	YES	manual	up	up

Ta kiểm tra rằng Switch đã thông suốt kết nối IP với hai router Edge và Branch:

```
Core_SW#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 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms
```

```
Core_SW#ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Đến đây, chúng ta đã xây dựng xong sơ đồ layer 3 ở hình 3. Tiếp theo, chúng ta thực hiện cấu hình định tuyến đảm bảo full – reachability cho sơ đồ này.

5. Định tuyến OSPF:

Cấu hình:

Trên Core_SW:

```
Core_SW(config)#ip routing
Core_SW(config)#router ospf 1
Core_SW(config-router)#network 172.16.10.0 0.0.0.255 area 0
Core_SW(config-router)#network 172.16.20.0 0.0.0.255 area 0
Core_SW(config-router)#network 172.16.30.0 0.0.0.255 area 0
Core_SW(config-router)#network 192.168.1.0 0.0.0.3 area 0
Core_SW(config-router)#network 192.168.1.8 0.0.0.3 area 0
Core_SW(config-router)#exit
```

Trên Edge:

```
Edge(config)#router ospf 1
Edge(config-router)#network 192.168.1.0 0.0.0.3 area 0
Edge(config-router)#network 192.168.1.4 0.0.0.3 area 0
Edge(config-router)#exit
```

Trên Branch:

```
Branch(config)#router ospf 1
Branch(config-router)#network 172.16.40.0 0.0.0.255 area 0
Branch(config-router)#network 192.168.1.4 0.0.0.3 area 0
Branch(config-router)#network 192.168.1.8 0.0.0.3 area 0
Branch(config-router)#exit
```

Kiểm tra:

Chúng ta kiểm tra rằng định tuyến OSPF đã hội tụ trên sơ đồ:

```
Core_SW#show ip route ospf
(...)
    172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
O        172.16.40.0/24 [110/20] via 192.168.1.10, 00:02:28, Ethernet1/2
    192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O        192.168.1.4/30 [110/11] via 192.168.1.2, 00:01:51, Vlan100
Edge#show ip route ospf
(...)
    172.16.0.0/24 is subnetted, 4 subnets
O        172.16.10.0 [110/11] via 192.168.1.1, 00:03:14, Ethernet0/0
O        172.16.20.0 [110/11] via 192.168.1.1, 00:03:14, Ethernet0/0
```

```
O      172.16.30.0 [110/11] via 192.168.1.1, 00:03:14, Ethernet0/0
O      172.16.40.0 [110/20] via 192.168.1.6, 00:02:00, Ethernet0/1
    192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O      192.168.1.8/30 [110/20] via 192.168.1.6, 00:02:00, Ethernet0/1
                  [110/20] via 192.168.1.1, 00:03:14, Ethernet0/0
Branch#show ip route ospf
(...)
    172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O      172.16.10.0/24 [110/11] via 192.168.1.9, 00:02:40, Ethernet0/0
O      172.16.20.0/24 [110/11] via 192.168.1.9, 00:02:40, Ethernet0/0
O      172.16.30.0/24 [110/11] via 192.168.1.9, 00:02:40, Ethernet0/0
    192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O      192.168.1.0/30 [110/11] via 192.168.1.9, 00:02:40, Ethernet0/0
```

Việc kiểm tra rằng các host có thể đi đến nhau được sẽ được thực hiện sau câu DHCP.

6. DHCP:

Cấu hình:

Trước hết, ta thực hiện cấu hình để router Edge có thể cấp phát IP được cho các host thuộc các VLAN 10, 20, 30 của trụ sở chính:

```
Edge(config)#ip dhcp pool VLAN10
Edge(dhcp-config)#network 172.16.10.0 /24
Edge(dhcp-config)#default-router 172.16.10.1
Edge(dhcp-config)#exit
Edge(config)#ip dhcp pool VLAN20
Edge(dhcp-config)#network 172.16.20.0 /24
Edge(dhcp-config)#default-router 172.16.20.1
Edge(dhcp-config)#exit
Edge(config)#ip dhcp pool VLAN30
Edge(dhcp-config)#network 172.16.30.0 /24
Edge(dhcp-config)#default-router 172.16.30.1
Edge(dhcp-config)#exit

Core_SW(config)#interface vlan 10
Core_SW(config-if)#ip helper-address 192.168.1.2
Core_SW(config-if)#exit
Core_SW(config)#interface vlan 20
Core_SW(config-if)#ip helper-address 192.168.1.2
Core_SW(config-if)#exit
Core_SW(config)#interface vlan 30
Core_SW(config-if)#ip helper-address 192.168.1.2
Core_SW(config-if)#exit
```

Tiếp theo, ta cấu hình để router Branch cấp phát IP cho các host thuộc mạng LAN của chi nhánh:

```
Branch(config)#ip dhcp pool BRANCH
Branch(dhcp-config)#network 172.16.40.0 /24
Branch(dhcp-config)#default-router 172.16.40.1
Branch(dhcp-config)#exit
```

Kiểm tra:

Ta kiểm tra rằng các host đều đã nhận được IP từ DHCP:

```
Host1> dhcp -r
DDORA IP 172.16.10.2/24 GW 172.16.10.1
```

```
Host2> dhcp -r
DDORA IP 172.16.20.2/24 GW 172.16.20.1
```

```
Host3> dhcp -r
DDORA IP 172.16.30.2/24 GW 172.16.30.1
```

```
Host4> dhcp -r
DDORA IP 172.16.40.2/24 GW 172.16.40.1
```

Ta cũng kiểm tra rằng các router Edge và Branch đã thực hiện cấp phát các IP ở trên xuống cho các host:

```
Edge#show ip dhcp binding
```

Bindings from all pools not associated with VRF:

IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
172.16.10.2	0100.5079.6668.09	Nov 17 2020 09:50 AM	Automatic
172.16.20.2	0100.5079.6668.0a	Nov 17 2020 09:50 AM	Automatic
172.16.30.2	0100.5079.6668.0b	Nov 17 2020 09:50 AM	Automatic

```
Branch#show ip dhcp binding
```

Bindings from all pools not associated with VRF:

IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
172.16.40.2	0100.5079.6668.0c	Nov 17 2020 09:51 AM	Automatic

Các host này đã có thể đi đến được nhau cho thấy hoạt động định tuyến giữa các VLAN cũng như định tuyến giữa hai chi nhánh đã thông suốt:

```
Host1> ping 172.16.20.2
84 bytes from 172.16.20.2 icmp_seq=1 ttl=63 time=3.134 ms
84 bytes from 172.16.20.2 icmp_seq=2 ttl=63 time=4.894 ms
```

```
Host1> ping 172.16.30.2
84 bytes from 172.16.30.2 icmp_seq=1 ttl=63 time=3.837 ms
84 bytes from 172.16.30.2 icmp_seq=2 ttl=63 time=4.035 ms
```

```
Host1> ping 172.16.40.2
84 bytes from 172.16.40.2 icmp_seq=1 ttl=62 time=4.301 ms
84 bytes from 172.16.40.2 icmp_seq=2 ttl=62 time=1.537 ms
```

```
Host2> ping 172.16.30.2
84 bytes from 172.16.30.2 icmp_seq=1 ttl=63 time=5.743 ms
84 bytes from 172.16.30.2 icmp_seq=2 ttl=63 time=1.993 ms
```

```
Host2> ping 172.16.40.2
84 bytes from 172.16.40.2 icmp_seq=1 ttl=62 time=4.153 ms
84 bytes from 172.16.40.2 icmp_seq=2 ttl=62 time=4.199 ms
```

```
Host3> ping 172.16.40.2
84 bytes from 172.16.40.2 icmp_seq=1 ttl=62 time=4.211 ms
84 bytes from 172.16.40.2 icmp_seq=2 ttl=62 time=3.909 ms
```

7. Hiệu chỉnh đường đi:

Cấu hình:

Hiện tại, nếu quan sát bảng định tuyến của switch Core_SW và router Branch, ta sẽ thấy rằng hai chi nhánh đang đi đến nhau theo đường link kết nối trực tiếp giữa Core_SW và router Branch:

```
Core_SW#show ip route ospf
(...)
  172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
O    172.16.40.0/24 [110/20] via 192.168.1.10, 00:02:28, Ethernet1/2
      192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O    192.168.1.4/30 [110/11] via 192.168.1.2, 00:01:51, Vlan100
Branch#show ip route ospf
(...)
  172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O    172.16.10.0/24 [110/11] via 192.168.1.9, 00:02:40, Ethernet0/0
O    172.16.20.0/24 [110/11] via 192.168.1.9, 00:02:40, Ethernet0/0
O    172.16.30.0/24 [110/11] via 192.168.1.9, 00:02:40, Ethernet0/0
      192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O    192.168.1.0/30 [110/11] via 192.168.1.9, 00:02:40, Ethernet0/0
```

Để hai router này dẫn đường dữ liệu đi đến nhau thông qua router Edge, ta thực hiện chỉnh cost của đường link trực tiếp lên cao hơn so với tổng cost của lô tuyến đi qua router Edge:

```
Core_SW(config)#interface e1/2
Core_SW(config-if)#ip ospf cost 100
Branch(config)#interface e0/0
Branch(config-if)#ip ospf cost 100
```

Kiểm tra:

Ta kiểm tra xác nhận rằng, sau khi chỉnh cost, hai chi nhánh đã chọn đường đi đến nhau thông qua router Edge:

```
Core_SW#show ip route ospf
(...)
  172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
O    172.16.40.0/24 [110/21] via 192.168.1.2, 00:01:32, Vlan100
      192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O    192.168.1.4/30 [110/11] via 192.168.1.2, 00:16:15, Vlan100
Branch#show ip route ospf
(...)
  172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O    172.16.10.0/24 [110/21] via 192.168.1.5, 00:01:21, Ethernet0/1
O    172.16.20.0/24 [110/21] via 192.168.1.5, 00:01:21, Ethernet0/1
O    172.16.30.0/24 [110/21] via 192.168.1.5, 00:01:21, Ethernet0/1
```

```
192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
O   192.168.1.0/30 [110/20] via 192.168.1.5, 00:01:21, Ethernet0/1
```

Ta có thể xác nhận thêm điều này bằng cách trace giữa hai chi nhánh:

Host1> trace 172.16.40.2

```
trace to 172.16.40.2, 8 hops max, press Ctrl+C to stop
1  172.16.10.1    1.547 ms  1.419 ms  1.614 ms
2  192.168.1.2    2.065 ms  2.322 ms  2.355 ms
3  192.168.1.6    2.525 ms  2.399 ms  1.833 ms
4  *172.16.40.2    3.787 ms (ICMP type:3, code:3, Destination port unreachable)
```

Host4> trace 172.16.10.2

```
trace to 172.16.10.2, 8 hops max, press Ctrl+C to stop
1  172.16.40.1    1.387 ms  1.119 ms  0.762 ms
2  192.168.1.5    2.200 ms  2.474 ms  2.187 ms
3  192.168.1.1    3.650 ms  1.760 ms  1.378 ms
4  *172.16.10.2    2.597 ms (ICMP type:3, code:3, Destination port unreachable)
```

Kết quả Trace chỉ ra rằng lưu lượng giữa hai host trên hai chi nhánh đã di chuyển ngang qua router Edge.

8. Internet:

Cấu hình:

Để thực hiện cho phép truy nhập Internet cho mỗi chi nhánh đồng thời dự phòng Internet lẫn nhau, tại mỗi chi nhánh, ta thực hiện cấu hình default – route tĩnh đi Internet, track giám sát đường đi này, đồng thời thực hiện lan truyền default – route vừa tạo vào mạng bên trong bằng OSPF. Mỗi router biên (Edge, Branch) sẽ có được hai default route (một route tĩnh và một route nhận từ OSPF do router kia gửi qua), nhưng sẽ luôn chọn static default – route vì AD của static route nhỏ hơn AD của OSPF; các router biên này sẽ chỉ sử dụng default – route do OSPF cung cấp nếu static default – route down.

Trên Edge:

```
Edge(config)#ip sla 1
Edge(config-ip-sla)#icmp-echo 100.0.0.1 source-ip 100.0.0.2
Edge(config-ip-sla-echo)#frequency 5
Edge(config-ip-sla-echo)#exit
Edge(config)#ip sla schedule 1 start-time now life forever
Edge(config)#track 1 ip sla 1
Edge(config-track)#exit

Edge(config)#ip route 0.0.0.0 0.0.0.0 100.0.0.1 track 1
Edge(config)#router ospf 1
Edge(config-router)#default-information originate
Edge(config-router)#exit

Edge(config)#access-list 1 permit 172.16.10.0 0.0.0.255
Edge(config)#access-list 1 permit 172.16.20.0 0.0.0.255
Edge(config)#access-list 1 permit 172.16.30.0 0.0.0.255
Edge(config)#access-list 1 permit 172.16.40.0 0.0.0.255

Edge(config)#ip nat inside source list 1 interface e0/2 overload
```

```
Edge(config)#interface range e0/0 - 1
Edge(config-if-range)#ip nat inside
Edge(config-if-range)#exit
Edge(config)#interface e0/2
Edge(config-if)#ip nat outside
Edge(config-if)#exit
```

Trên Branch:

```
Branch(config)#ip sla 1
Branch(config-ip-sla)#icmp-echo 200.0.0.1 source-ip 200.0.0.2
Branch(config-ip-sla-echo)#frequency 5
Branch(config-ip-sla-echo)#exit
Branch(config)#ip sla schedule 1 start-time now life forever
Branch(config)#track 1 ip sla 1
Branch(config-track)#exit

Branch(config)#ip route 0.0.0.0 0.0.0.0 200.0.0.1 track 1
Branch(config)#router ospf 1
Branch(config-router)#default-information originate
Branch(config-router)#exit

Branch(config)#access-list 1 permit 172.16.10.0 0.0.0.255
Branch(config)#access-list 1 permit 172.16.20.0 0.0.0.255
Branch(config)#access-list 1 permit 172.16.30.0 0.0.0.255
Branch(config)#access-list 1 permit 172.16.40.0 0.0.0.255

Branch(config)#ip nat inside source list 1 interface e0/3 overload
Branch(config)#interface range e0/0 - 2
Branch(config-if-range)#ip nat inside
Branch(config-if-range)#exit
Branch(config)#interface e0/3
Branch(config-if)#ip nat outside
Branch(config-if)#exit
```

Kiểm tra:

Ta kiểm tra rằng hiện tại các router/switch layer 3 tại mỗi chi nhánh sẽ chọn đường đi Internet (default – route) theo đường truyền Internet tại chi nhánh ấy:

```
Core_SW#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
Known via "ospf 1", distance 110, metric 1, candidate default path
Tag 1, type extern 2, forward metric 1
Last update from 192.168.1.2 on Vlan100, 00:00:06 ago
Routing Descriptor Blocks:
* 192.168.1.2, from 192.168.1.5, 00:00:06 ago, via Vlan100
    Route metric is 1, traffic share count is 1
    Route tag 1
```

```
Edge#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
Known via "static", distance 1, metric 0, candidate default path
Routing Descriptor Blocks:
* 100.0.0.1
    Route metric is 0, traffic share count is 1

Branch#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
Known via "static", distance 1, metric 0, candidate default path
Routing Descriptor Blocks:
* 200.0.0.1
    Route metric is 0, traffic share count is 1
```

Ta kiểm tra hướng đi Internet bằng cách trace từ các host:

```
Host1> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
1 172.16.10.1 1.027 ms 1.274 ms 1.123 ms
2 192.168.1.2 3.117 ms 2.407 ms 2.188 ms
3 *100.0.0.1 3.991 ms (ICMP type:3, code:3, Destination port unreachable) *

Host2> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
1 172.16.20.1 5.495 ms 0.946 ms 1.136 ms
2 192.168.1.2 1.937 ms 1.678 ms 1.599 ms
3 *100.0.0.1 2.734 ms (ICMP type:3, code:3, Destination port unreachable) *

Host3> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
1 172.16.30.1 0.836 ms 0.675 ms 0.618 ms
2 192.168.1.2 1.905 ms 1.621 ms 1.365 ms
3 *100.0.0.1 1.669 ms (ICMP type:3, code:3, Destination port unreachable) *

Host4> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
1 172.16.40.1 0.329 ms 0.285 ms 0.261 ms
2 *200.0.0.1 0.742 ms (ICMP type:3, code:3, Destination port unreachable) *
```

Ta thấy các host thuộc các VLAN 10, 20, 30 đang đi Internet theo link Internet trên router Edge của trụ sở chính và Host4 đang đi Internet theo link Internet của router Branch đúng như yêu cầu.

Ta thực hiện kiểm tra rằng nếu đường truyền Internet trên trụ sở chính down, các host trên các VLAN sẽ chuyển qua đi Internet thông qua router Branch.

Đầu tiên, ta thực hiện down đường link Internet kết nối đến router Edge:

```
Internet(config)#interface e0/0
Internet(config-if)#shutdown
```

Lúc này router Edge đã chuyển hướng Internet theo default – route OSPF học được từ router Branch:

```
Edge#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
Known via "ospf 1", distance 110, metric 1, candidate default path
Tag 1, type extern 2, forward metric 10
```

```
Last update from 192.168.1.6 on Ethernet0/1, 00:00:53 ago
```

```
Routing Descriptor Blocks:
```

```
* 192.168.1.6, from 200.0.0.2, 00:00:53 ago, via Ethernet0/1
```

```
    Route metric is 1, traffic share count is 1
```

```
    Route tag 1
```

Ta thực hiện trace từ các host thuộc các VLAN 10, 20 và 30 để xác nhận rằng lần này chúng đi Internet thông qua router Branch:

```
Host1> trace 8.8.8.8
```

```
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
```

```
1 172.16.10.1 1.109 ms 1.006 ms 0.746 ms
```

```
2 192.168.1.2 1.409 ms 1.246 ms 1.256 ms
```

```
3 192.168.1.6 3.424 ms 2.716 ms 2.611 ms
```

```
4 *200.0.0.1 3.451 ms (ICMP type:3, code:3, Destination port unreachable)
```

```
Host2> trace 8.8.8.8
```

```
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
```

```
1 172.16.20.1 1.858 ms 0.899 ms 1.060 ms
```

```
2 192.168.1.2 1.918 ms 1.453 ms 5.786 ms
```

```
3 192.168.1.6 2.481 ms 2.238 ms 2.308 ms
```

```
4 *200.0.0.1 4.172 ms (ICMP type:3, code:3, Destination port unreachable) *
```

```
Host3> trace 8.8.8.8
```

```
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
```

```
1 172.16.30.1 1.336 ms 3.187 ms 2.033 ms
```

```
2 192.168.1.2 2.656 ms 7.348 ms 3.542 ms
```

```
3 192.168.1.6 4.677 ms 4.470 ms 2.152 ms
```

```
4 *200.0.0.1 2.153 ms (ICMP type:3, code:3, Destination port unreachable) *
```

Sau khi kiểm tra dự phòng xong, ta nhớ no shutdown đường Link Internet của router Edge lại như cũ:

```
Internet(config)#interface e0/0
Internet(config-if)#no shutdown
```

Ta có thể thực hiện kiểm tra tương tự với đi Internet ngược lại từ phía chi nhánh.