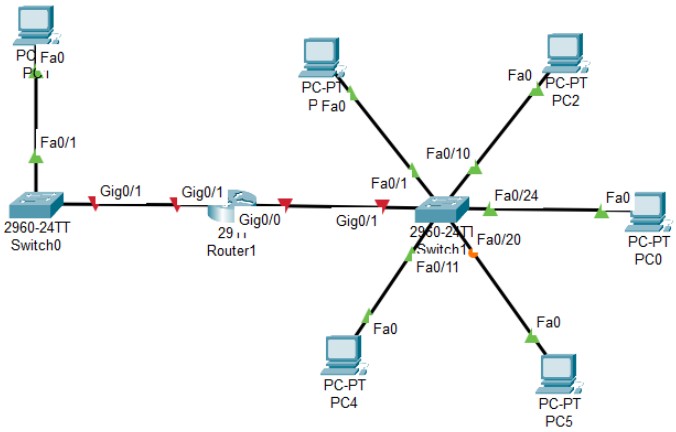
TỔNG HỢP CẤU HÌNH
THIẾT BỊ MẠNG - FULL LỆNH

TỔNG HỢP CẤU HÌNH SWITCH LAYER 2 -ROUTER

1. SƠ ĐỒ



Cấu hình thiết bị trên sơ đồ mạng trên , biết:

- ✓ Router (subinterface))
  - Gig0/0.1 Vlan 1 (10.0.1.1/24)
  - Gig0/0.20 Vlan 20 (10.0.20.1/24)
  - Gig0/0.30 Vlan (30 10.0.30.1/24)
  - Gig0/1 nối Switch1 (L2) mạng server 10.0.100.0/24;
- ✓ Switch1: Vlan 1 (Fa0/21-24); Vlan 20 (Fa0/1-10); Vlan 30 (Fa0/11-20); Gig0/1 trunk Gig0/2 Router
- ✓ Switch0: Vlan 100 (IP 10.0.100.0/24; all port vlan 100); gig0/1 nối Gig0/1 Router

II. YÊU CẦU:

1. Trên Router R1:

- ✓ Đổi tên thiết bị: hostname R1.
- ✓ Cấu hình IP cho các subinterface:
  - Gig0/1.1 gắn với VLAN 1: 10.0.1.1/24
  - Gig0/1.20 gắn với VLAN 20: 10.0.20.1/24
  - Gig0/1.30 gắn với VLAN 30: 10.0.30.1/24
- ✓ Gig0/1 là cổng trunk kết nối đến Switch1.
- ✓ Cấu hình IP cho Gig0/0 (kết nối Switch0): 10.0.100.1/24

2. Trên Switch1 (chia VLAN):

- ✓ Đổi tên thiết bị: hostname Switch1.
- ✓ Tạo các VLAN:
  - VLAN 1: Kỹ thuật
  - VLAN 20: Kinh doanh
  - VLAN 30: Nhân sự
- ✓ Gán port cho từng VLAN:
- ✓ VLAN 1: Fa0/21 – Fa0/24
- ✓ VLAN 20: Fa0/1 – Fa0/10
- ✓ VLAN 30: Fa0/11 – Fa0/20

- ✓ Cấu hình trunk trên cổng Gig0/1 (nối R1).

3. Trên Switch0 (không chia VLAN):

- ✓ Đổi tên thiết bị: hostname Switch0.
- ✓ Giữ nguyên VLAN mặc định (hoặc dùng VLAN 100 cho dễ nhận diện).
- ✓ Tất cả các cổng thuộc cùng một mạng: 10.0.100.0/24.
- ✓ Kết nối Gig0/1 lên Router R1 (Gig0/0).

4. Kiểm tra

- ✓ PC trong cùng VLAN ping được nhau.
- ✓ PC khác VLAN ping được nhau thông qua Router.
- ✓ Các thiết bị thuộc mạng Switch0 ping được đến các VLAN khác và ngược lại.

III. CÂU LỆNH

1. CẤU HÌNH ROUTER R1 (KHÔNG VLAN)

```
Router> enable {Vào chế độ EXEC đặc quyền}
Router# configure terminal {Vào chế độ cấu hình toàn cục}
Router(config)# hostname R1 {Đặt tên thiết bị}
R1(config)# interface GigabitEthernet0/0
R1(config-subif)# ip address 10.0.1.1 255.255.255.0 {Gán ip cổng gig0/0}
R1(config-if)# no shutdown {Bật cổng}
R1(config-subif)# exit
R1(config)# interface GigabitEthernet0/1
R1(config-if)# ip address 10.0.100.1 255.255.255.0 {Gán ip cổng gig0/1}
R1(config-if)# no shutdown {Bật cổng}
R1(config-if)# exit
R1(config)# router rip { định tuyến động}
R1(config-router)#version 2
R1(config-router)#network 10.0.1.0
R1(config-router)#network 10.0.100.0
R1(config-router)#exit
R1(config)#end
R1(config)# ip route 203.0.0.0 255.255.255.0 10.0.100.2 { định tuyến tĩnh ra địa chỉ mạng đích
203.0.0.0 255.255.255.0  qua cổng  10.0.100.2 router kế tiếp}
R1(config)#end
R1# write memory {Lưu cấu hình}
```

1. CẤU HÌNH ROUTER R1 (SUBINTERFACE)

```
Router> enable {Vào chế độ EXEC đặc quyền}
Router# configure terminal {Vào chế độ cấu hình toàn cục}
Router(config)# hostname R1 {Đặt tên thiết bị}
R1(config)# interface GigabitEthernet0/0.1 {Subinterface cho VLAN 1}
R1(config-subif)# encapsulation dot1Q 1 {Gán VLAN ID 1}
R1(config-subif)# ip address 10.0.1.1 255.255.255.0 {Đặt IP cho VLAN 1}
R1(config-subif)# exit
R1(config)# interface GigabitEthernet0/0.20 {Subinterface cho VLAN 20}
R1(config-subif)# encapsulation dot1Q 20 {Gán VLAN ID 20}
R1(config-subif)# ip address 10.0.20.1 255.255.255.0 {Đặt IP cho VLAN 20}
R1(config-subif)# exit
R1(config)# interface GigabitEthernet0/0.30 {Subinterface cho VLAN 30}
R1(config-subif)# encapsulation dot1Q 30 {Gán VLAN ID 30}
R1(config-subif)# ip address 10.0.30.1 255.255.255.0 {Đặt IP cho VLAN 30}
R1(config-subif)# exit
```

R1(config)# interface GigabitEthernet0/0 *{Cổng chính chứa các subinterface}*
R1(config-if)# no shutdown *{Bật cổng}*
R1(config-if)# exit
R1(config)# interface GigabitEthernet0/1 *{Kết nối Switch0 (mạng không chia VLAN)}*
R1(config-if)# ip address 10.0.100.1 255.255.255.0 *{Đặt IP cho mạng Server}*
R1(config-if)# no shutdown *{Bật cổng}*
R1(config-if)# exit
R1(config)# ip routing *{Thiết lập tuyến nội bộ}*
R1(config)# ip route 0.0.0.0 0.0.0.0 10.0.100.2 *{Thiết lập tuyến mặc định ra Internet qua cổng 10.0.100.2 của router kế tiếp}*
R1#end
R1# write memory *{Lưu cấu hình}*

2. CẤU HÌNH SWITCH1 (CHIA VLAN)

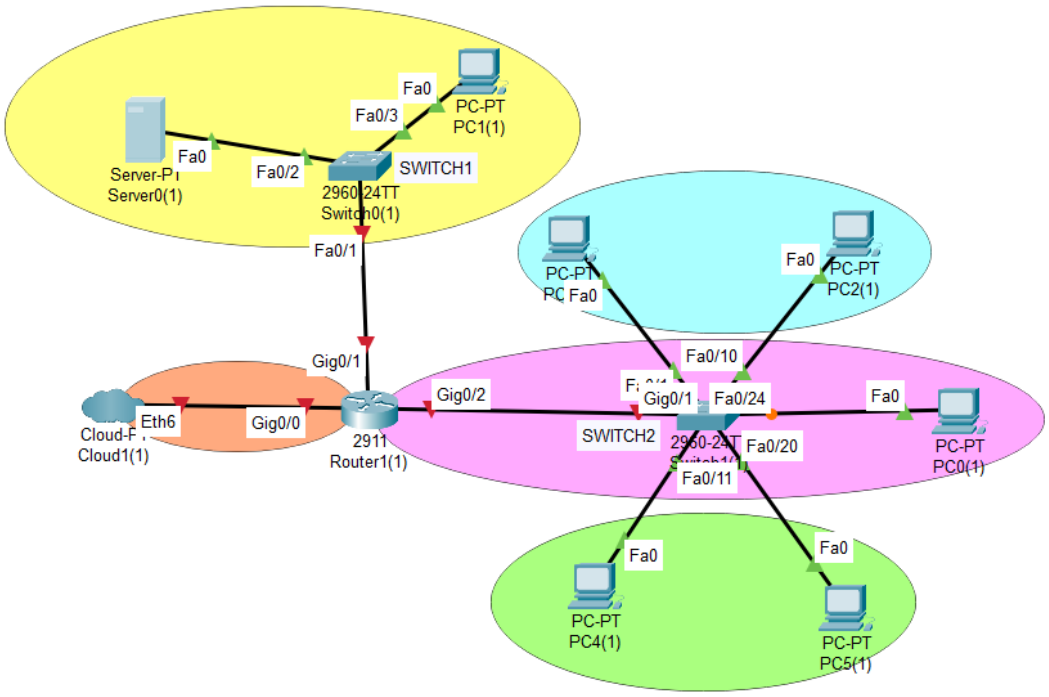
Switch>enable *{Vào chế độ EXEC đặc quyền}*
Switch# configure terminal *{Vào chế độ cấu hình}*
Switch(config)# hostname SW1 *{Đặt tên thiết bị}*
SW2(config)# vlan 1 *{Tạo VLAN 1}*
SW2(config-vlan)# exit
SW2(config)# vlan 20 *{Tạo VLAN 20}*
SW2(config-vlan)# exit
SW2(config)# vlan 30 *{Tạo VLAN 30}*
SW2(config-vlan)# exit
SW2(config)# interface range Fa0/1 - 10 *{Gán các cổng vào VLAN 20}*
SW2(config-if-range)# switchport mode access
SW2(config-if-range)# switchport access vlan 20
SW2(config-if-range)# exit
SW2(config)# interface range Fa0/11 - 20 *{Gán các cổng vào VLAN 30}*
SW2(config-if-range)# switchport mode access
SW2(config-if-range)# switchport access vlan 30
SW2(config-if-range)# exit
SW2(config)# interface range Fa0/21 - 24 *{Gán các cổng vào VLAN 1}*
SW2(config-if-range)# switchport mode access
SW2(config-if-range)# switchport access vlan 1
SW2(config-if-range)# exit
SW2(config)# interface GigabitEthernet0/1 *{Kết nối trunk đến Router (R1)}*
SW2(config-if)# switchport trunk encapsulation dot1q
SW2(config-if)# switchport mode trunk
SW2(config-if)# exit
SW2# write memory *{Lưu cấu hình}*

3. CẤU HÌNH SWITCH0 (KHÔNG CHIA VLAN)

Switch>enable *{Vào chế độ EXEC đặc quyền}*
Switch# configure terminal *{Vào chế độ cấu hình}*
Switch(config)# hostname SW1 *{Đặt tên thiết bị}*
SW1(config)# interface range fa0/1 - 24 *{Tất cả các cổng vào VLAN mặc định}*
SW1(config-if-range)# switchport mode access
SW1(config-if-range)# exit
SW1(config)# interface GigabitEthernet0/1 *{Kết nối đến R1}*
SW1(config-if)# switchport mode access
SW1(config-if)# exit
SW1# write memory *{Lưu cấu hình}*

TỔNG HỢP CẤU HÌNH ROUTER

1. SƠ ĐỒ



Cấu hình mạng biết:

- ✓ Router (subinterface))
  - Gig0/2.1 Vlan 1 (10.0.1.1/24)
  - Gig0/2.20 Vlan 20 (10.0.20.1/24)
  - Gig0/2.30 Vlan (30 10.0.30.1/24)
  - Gig0/1 Van 100 (10.0.100.1/24)
  - Gig0/1 nối Switch1 (L2) mạng server 10.0.100.0/24;
  - Gig0/2 nối Switch2 (L2) mạng Vlan1/20/30;
  - Gig0/0 nối Cloud Ett6 (10.0.0.0/24)
- ✓ Switch2: Vlan 1 (Fa0/21-24); Vlan 20 (Fa0/1-10); Vlan 30 (Fa0/11-20); Gig0/1 trunk Gig0/2 Router
- ✓ Switch1: Vlan 100 (IP 10.0.100.0/24; all port vlan 100); Fa0/1 nối Gig0/1 Router

II. YÊU CẦU

1. Cấu hình Router R1 và các Subinterface

- ✓ Đổi tên thiết bị Router thành R1
- ✓ Cấu hình các subinterface trên cổng GigabitEthernet0/0 để định tuyến cho các VLAN:
  - Gig0/0.1 – VLAN 1 (10.0.1.1/24)
  - Gig0/0.20 – VLAN 20 (10.0.20.1/24)
  - Gig0/0.30 – VLAN 30 (10.0.30.1/24)
- ✓ Gán địa chỉ IP cho từng subinterface tương ứng với mỗi VLAN.
- ✓ Cấu hình lệnh ip helper-address 10.0.100.2 để chuyển tiếp gói broadcast đến DHCP Server đặt tại mạng Server.
- ✓ Bật cổng vật lý GigabitEthernet0/0 để kích hoạt các subinterface.

2. Kết nối mạng Server và ra Internet

- ✓ Cấu hình cổng GigabitEthernet0/1 kết nối với Switch1 (mạng Server - 10.0.100.0/24), đặt IP 10.0.100.1/24.
- ✓ Cấu hình cổng FastEthernet0/1 kết nối ra Internet (giả lập Cloud) với IP 10.0.0.1/24.

- ✓ Định danh vùng NAT:
  - NAT Inside: Gig0/0.x và Gig0/1
  - NAT Outside: Fa0/1

3. Cấu hình NAT Overload

- ✓ Tạo access-list 1 để cho phép NAT cho tất cả các mạng nội bộ (10.0.0.0/8 hoặc 10.0.0.0/16).
- ✓ Cấu hình NAT Overload để các mạng nội bộ truy cập được Internet.
- ✓ Thiết lập tuyến mặc định ra Internet qua địa chỉ gateway 10.0.0.2.

4. Cấu hình ACL kiểm soát truy cập

- ✓ ACL 100: Chặn truy cập từ Internet đến VLAN 1 (phòng kỹ thuật), cho phép truy cập các mạng còn lại.
- ✓ ACL 110: Chặn các IP 10.0.x.254 truy cập cổng Web (80) của Web Server nội bộ 10.0.100.2.
- ✓ ACL 120: Chỉ cho phép máy 10.0.1.100 sử dụng dịch vụ DHCP từ 10.0.100.2, chặn truy cập khác.
- ✓ ACL 130: Chặn các máy 10.0.x.253 truy cập toàn bộ mạng Server (10.0.100.0/24).
- ✓ ACL 140: Chặn máy 10.0.100.254 (từ mạng Server) truy cập các VLAN 1, 20, 30.
- ✓ ACL 150: Chỉ cho phép máy 10.0.100.253 giao tiếp trong mạng nội bộ Server, chặn ra ngoài.
- ✓ ACL 160: Từ Internet chỉ cho phép địa chỉ IP 203.11.1.1 truy cập Web Server (port 80), chặn tất cả dịch vụ khác và mạng khác.

5. NAT tĩnh cho Web Server

- ✓ Cấu hình NAT tĩnh ánh xạ cổng TCP 80 từ địa chỉ công cộng (giao diện FastEthernet0/1) đến máy chủ nội bộ 10.0.100.2.

6. Kiểm tra kết nối

- ✓ Các PC thuộc VLAN 1, 20, 30 và thiết bị trong mạng Server có thể ping qua lại và ra Internet.
- ✓ Internet có thể ping vào các mạng nội bộ (nếu được phép).
- ✓ Chỉ truy cập Web nội bộ từ IP 203.11.1.1 (các IP khác bị chặn).

7. Lưu cấu hình

- ✓ Sau khi hoàn tất cấu hình, lưu lại với lệnh:

III. CÂU LỆNH

1. CẤU HÌNH ROUTER R1 VÀ CÁC SUBINTERFACE

```
Router> enable
Rouuter# configure terminal
Router(config)# hostname R1 {Đổi tên thiết bị thành R1}
R1(config)# interface GigabitEthernet0/0.1
R1(config-subif)# encapsulation dot1Q 1
R1(config-subif)# ip address 10.0.1.1 255.255.255.0
R1(config-subif)# ip helper-address 10.0.100.2 {chuyển tiếp DHCP về server}
R1(config)# interface GigabitEthernet0/0.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 10.0.20.1 255.255.255.0
R1(config-subif)# ip helper-address 10.0.100.2 { chuyển tiếp DHCP về server}
R1(config)# interface GigabitEthernet0/0.30
R1(config-subif)# encapsulation dot1Q 30
R1(config-subif)# ip address 10.0.30.1 255.255.255.0
R1(config-subif)# ip helper-address 10.0.100.2 {chuyển tiếp DHCP về server}
R1(config)# interface GigabitEthernet0/0
R1(config-if)# no shutdown
 {Kích hoạt cổng vật lý để các subinterface hoạt động}
```

2. KẾT NỐI MẠNG SERVER VÀ INTERNET

```
R1(config)# interface GigabitEthernet0/1
R1(config-if)# ip address 10.0.100.1 255.255.255.0
```

R1(config-if)# no shutdown
{Kết nối mạng Server}
R1(config)# interface FastEthernet0/1
R1(config-if)# ip address 10.0.0.1 255.255.255.0
R1(config-if)# no shutdown
{Kết nối ra Internet (Cloud)}

3. CẤU HÌNH NAT OVERLOAD

R1(config)# access-list 1 permit 10.0.0.0 0.255.255.255 *{Cho phép NAT các mạng nội bộ lớp A}*
R1(config)# ip nat inside source list 1 interface FastEthernet0/1 overload *{Cấu hình NAT Overload}*
R1(config)# interface GigabitEthernet0/0.1
R1(config-if)# ip nat inside
R1(config)# interface GigabitEthernet0/0.20
R1(config-if)# ip nat inside
R1(config)# interface GigabitEthernet0/0.30
R1(config-if)# ip nat inside
R1(config)# interface GigabitEthernet0/1
R1(config-if)# ip nat inside
R1(config)# interface FastEthernet0/1
R1(config-if)# ip nat outside
{Định danh vùng NAT}
R1(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.2
{Thiết lập tuyến mặc định ra Internet}

4. CẤU HÌNH ACL KIỂM SOÁT TRUY CẬP

R1(config)# access-list 100 deny ip any 10.0.1.0 0.0.0.255
R1(config)# access-list 100 permit ip any any
{ACL 100 – Chặn Internet truy cập VLAN 1}
R1(config)# access-list 110 deny tcp 10.0.0.0 0.255.255.255 host 10.0.100.2 eq 80
R1(config)# access-list 110 permit ip any any
{ACL 110 – Chặn IP .254 truy cập Web Server nội bộ}
R1(config)# access-list 120 permit udp host 10.0.1.100 host 10.0.100.2 eq 67
R1(config)# access-list 120 deny udp any host 10.0.100.2 eq 67
R1(config)# access-list 120 permit ip any any
{ACL 120 – Chỉ cho máy 10.0.1.100 dùng DHCP}
R1(config)# access-list 130 deny ip 10.0.0.253 0.0.0.0 10.0.100.0 0.0.0.255
R1(config)# access-list 130 permit ip any any
{ACL 130 – Chặn IP .253 truy cập Server}
R1(config)# access-list 140 deny ip host 10.0.100.254 10.0.0.0 0.0.255.255
R1(config)# access-list 140 permit ip any any
{ACL 140 – Chặn Server .254 truy cập VLAN 1,20,30}
R1(config)# access-list 150 permit ip host 10.0.100.253 10.0.100.0 0.0.0.255
R1(config)# access-list 150 deny ip host 10.0.100.253 any
R1(config)# access-list 150 permit ip any any
{ACL 150 – Chỉ cho phép Server .253 giao tiếp nội bộ}
R1(config)# access-list 160 permit tcp host 203.11.1.1 host 10.0.100.2 eq 80
R1(config)# access-list 160 deny ip any any
{ACL 160 – Chỉ cho IP 203.11.1.1 truy cập Web Server}

5. NAT TĨNH CHO WEB SERVER

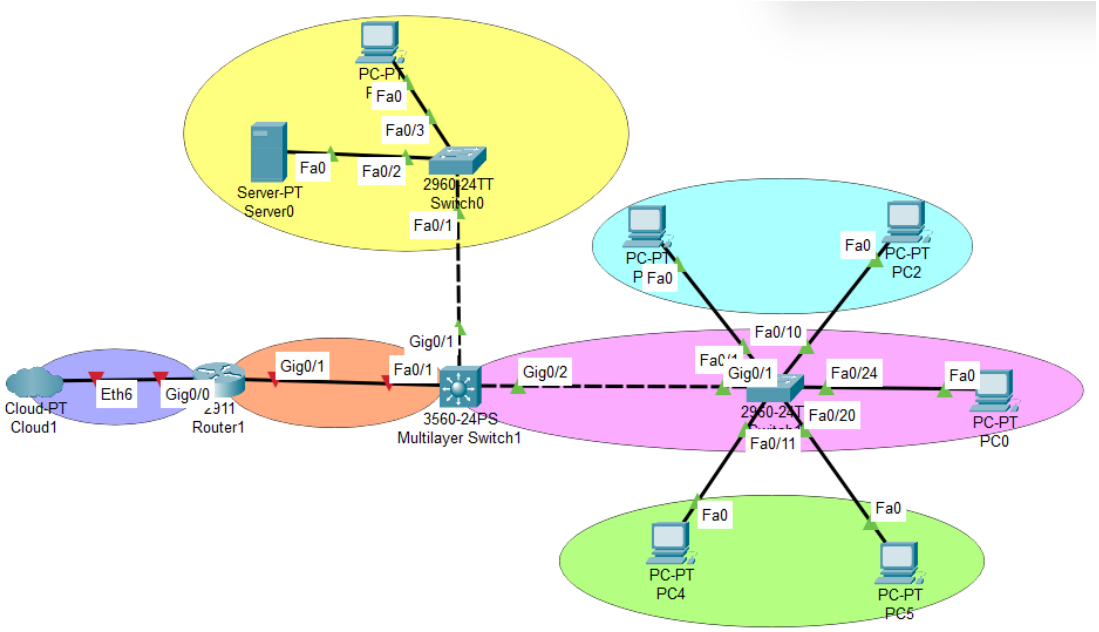
R1(config)# ip nat inside source static tcp 10.0.100.2 80 interface FastEthernet0/1 80
{Ánh xạ NAT tĩnh dịch vụ Web ra Internet}

6. LƯU CẤU HÌNH

R1# copy running-config startup-config
{Lưu cấu hình}

TỔNG HỢP CẤU HÌNH SWITCH LAYER 3

1. SƠ ĐỒ



Cấu hình mạng biết:

- ✓ Switch L3 (Chế độ SVI))
  - Vlan 1 (10.0.1.1/24)
  - Vlan 20 (10.0.20.1/24)
  - Vlan (30 10.0.30.1/24)
  - Van 100 (10.0.100.1/24)
  - Gig0/1 nối Switch1 (L2) mạng server 10.0.100.0/24;
  - Gig0/2 nối Switch2 (L2) mạng Vlan1/20/30;
  - Fa0/1 nối gig0/1 router (10.0.0.0/24)
- ✓ Switch2: Vlan 1 (Fa0/21-24); Vlan 20 (Fa0/1-10); Vlan 30 (Fa0/11-20); Gig0/1 trunk Gig0/2 Switch L3
- ✓ Switch1: Vlan 100 (IP 10.0.100.0/24; all port vlan 100); Fa0/1 nối Gig0/1 Switch L3
- ✓ Router: Gig0/0 nối Internet (cloud); Gig0/1 nối Fa0/1 Switch L3

II. YÊU CẦU

1. Cấu hình Switch Layer 3 (SWL3)

- ✓ Đổi tên thiết bị Switch Layer 3 thành SWL3.
- ✓ Tạo các VLAN nội bộ gồm: VLAN 20, VLAN 30 và VLAN 100. (VLAN 1 mặc định không cần tạo lại).
- ✓ Cấu hình các interface VLAN (SVI) tương ứng với các VLAN trên, gán địa chỉ IP như sau:
  - VLAN 1: 10.0.1.1/24
  - VLAN 20: 10.0.20.1/24
  - VLAN 30: 10.0.30.1/24
  - VLAN 100: 10.0.100.1/24
- ✓ Bật chức năng định tuyến bằng lệnh: ip routing.
- ✓ Cấu hình lệnh ip helper-address 10.0.100.2 trên các SVI để chuyển tiếp các gói broadcast DHCP đến DHCP Server nội bộ.
- ✓ Cấu hình trunk các cổng:
  + GigabitEthernet0/1: trunk kết nối đến Switch1 (mạng server – VLAN 100)
  + GigabitEthernet0/2: trunk kết nối đến Switch2 (VLAN 1, 20, 30)

- ✓ Cấu hình cổng FastEthernet0/1 là cổng routing, gán IP 10.0.0.2/24, kết nối với Router để truy cập Internet.

II. Cấu hình Router (R1)

- ✓ Đổi tên thiết bị thành R1.
- ✓ Gán IP cho các cổng:
- ✓ GigabitEthernet0/0: nhận IP từ DHCP, cấu hình là NAT outside (kết nối ra Internet
- ✓ GigabitEthernet0/1: IP 10.0.0.1/24, NAT inside (kết nối về nội bộ).
- ✓ Cấu hình NAT Overload để các mạng nội bộ (VLAN 1, 20, 30, 100) có thể truy cập Internet.
- ✓ Thiết lập tuyến mặc định để định tuyến ra Internet, ví dụ: ip route 0.0.0.0 0.0.0.0 203.11.1.254

III. Kiểm tra kết nối hệ thống

- ✓ Kiểm tra các PC thuộc VLAN 1, 20, 30 và các thiết bị trong mạng server VLAN 100 có thể:
- ✓ Ping được nhau.
- ✓ Ping được Web Server tại 10.0.100.2.
- ✓ Ping ra Internet (ví dụ: 8.8.8.8).
- ✓ Từ mạng ngoài (Internet – ví dụ IP 203.11.1.1) có thể:
- ✓ Ping đến các địa chỉ trong mạng nội bộ.
- ✓ Truy cập Web Server nội bộ tại 10.0.100.2 (port 80).

IV. Thiết lập ACL bảo mật trên SWL3

- ✓ Chặn các địa chỉ IP sau truy cập vào Web Server (cổng 80): 10.0.1.254, 10.0.20.254, 10.0.30.254
- ✓ Chặn các địa chỉ IP sau truy cập vào toàn bộ mạng server (10.0.100.0/24): 10.0.1.253, 10.0.20.253, 10.0.30.253
- ✓ Chặn máy 10.0.100.254 từ VLAN 100 truy cập các VLAN 1, 20, 30.
- ✓ Chỉ cho phép máy 10.0.100.253 giao tiếp trong mạng server (10.0.100.0/24), chặn toàn bộ truy cập ra ngoài.
- ✓ Chỉ cho phép địa chỉ WAN 203.11.1.1 truy cập cổng Web (80) của Web Server, chặn toàn bộ các dịch vụ khác.
- ✓ Chặn truy cập từ Internet đến VLAN 1 (phòng kỹ thuật), cho phép truy cập các mạng còn lại.

V. Lưu cấu hình

- ✓ Trên cả Switch L3 và Router, lưu cấu hình sau khi hoàn tất:

III. CẤU HÌNH

I. Cấu hình SWL3 (Switch Layer 3 – SVI)

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SWL3
SWL3(config)#ip routing  {Bật định tuyến giữa các VLAN}
SWL3(config)#vlan 20
SWL3(config-vlan)#exit
SWL3(config)#vlan 30
SWL3(config-vlan)#exit
SWL3(config)#vlan 100
SWL3(config-vlan)#exit
SWL3(config)#interface vlan 1
SWL3(config-if)#ip address 10.0.1.1 255.255.255.0
SWL3(config-if)#ip helper-address 10.0.100.2  {Chuyển tiếp DHCP đến server trong VLAN}
SWL3(config-if)#no shutdown
SWL3(config-if)#exit
SWL3(config)#interface vlan 20
SWL3(config-if)#ip address 10.0.20.1 255.255.255.0
SWL3(config-if)#ip helper-address 10.0.100.2
```

```
SWL3(config-if)#no shutdown
SWL3(config-if)#exit
SWL3(config)#interface vlan 30
SWL3(config-if)#ip address 10.0.30.1 255.255.255.0
SWL3(config-if)#ip helper-address 10.0.100.2
SWL3(config-if)#no shutdown
SWL3(config-if)#exit
SWL3(config)#interface vlan 100
SWL3(config-if)#ip address 10.0.100.1 255.255.255.0
SWL3(config-if)#ip helper-address 10.0.100.2
SWL3(config-if)#no shutdown
SWL3(config-if)#exit
SWL3(config)#interface gigabitEthernet0/1
SWL3(config-if)#switchport mode trunk
SWL3(config-if)#no shutdown
SWL3(config-if)#exit
SWL3(config)#interface gigabitEthernet0/2
SWL3(config-if)#switchport mode trunk
SWL3(config-if)#no shutdown
SWL3(config-if)#exit
SWL3(config)#interface fastEthernet0/1
SWL3(config-if)#no switchport
SWL3(config-if)#ip address 10.0.0.2 255.255.255.0
SWL3(config-if)#no shutdown
SWL3(config-if)#exit
```

2. Cấu hình Router R1

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#interface gigabitEthernet0/0
R1(config-if)#ip address dhcp
R1(config-if)#ip nat outside
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface gigabitEthernet0/1
R1(config-if)#ip address 10.0.0.1 255.255.255.0
R1(config-if)#ip nat inside
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#access-list 1 permit 10.0.1.0 0.0.0.255
R1(config)#access-list 1 permit 10.0.20.0 0.0.0.255
R1(config)#access-list 1 permit 10.0.30.0 0.0.0.255
R1(config)#access-list 1 permit 10.0.100.0 0.0.0.255
R1(config)#ip nat inside source list 1 interface gigabitEthernet0/0 overload  {NAT Overload cho mạng nội bộ}
R1(config)#ip route 0.0.0.0 0.0.0.0 203.11.1.254  {Tuyến mặc định ra Internet}
```

3. ACL Bảo mật trên SWL3

```
SWL3(config)#ip access-list extended BLOCK_WEBSERVER
SWL3(config-ext-nacl)#deny tcp host 10.0.1.254 any eq 80
SWL3(config-ext-nacl)#deny tcp host 10.0.20.254 any eq 80
SWL3(config-ext-nacl)#deny tcp host 10.0.30.254 any eq 80
```

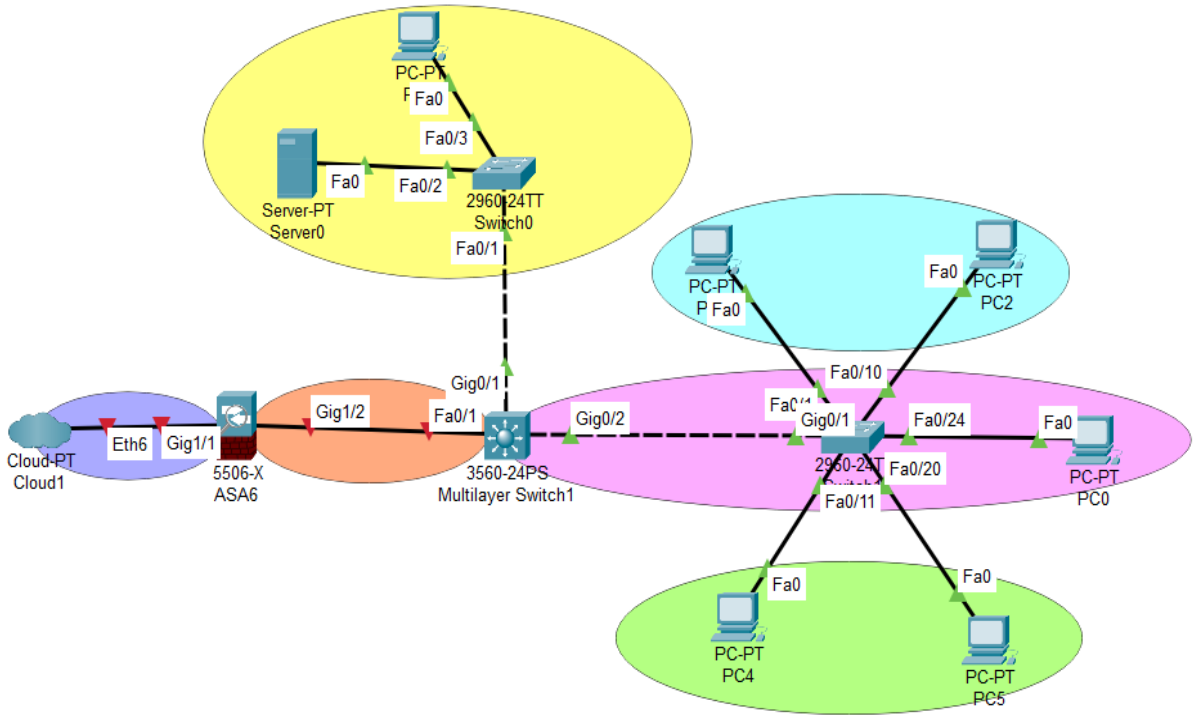
```
SWL3(config-ext-nacl)#permit ip any any
SWL3(config-ext-nacl)#exit
SWL3(config)#ip access-list extended BLOCK_SERVER
SWL3(config-ext-nacl)#deny ip host 10.0.1.253 10.0.100.0 0.0.0.255
SWL3(config-ext-nacl)#deny ip host 10.0.20.253 10.0.100.0 0.0.0.255
SWL3(config-ext-nacl)#deny ip host 10.0.30.253 10.0.100.0 0.0.0.255
SWL3(config-ext-nacl)#permit ip any any
SWL3(config-ext-nacl)#exit
SWL3(config)#ip access-list extended BLOCK_100_OUT
SWL3(config-ext-nacl)#deny ip host 10.0.100.254 10.0.1.0 0.0.0.255
SWL3(config-ext-nacl)#deny ip host 10.0.100.254 10.0.20.0 0.0.0.255
SWL3(config-ext-nacl)#deny ip host 10.0.100.254 10.0.30.0 0.0.0.255
SWL3(config-ext-nacl)#permit ip any any
SWL3(config-ext-nacl)#exit
SWL3(config)#ip access-list extended ONLY_253_INTERNAL
SWL3(config-ext-nacl)#permit ip host 10.0.100.253 10.0.100.0 0.0.0.255
SWL3(config-ext-nacl)#deny ip host 10.0.100.253 any
SWL3(config-ext-nacl)#permit ip any any
SWL3(config-ext-nacl)#exit
SWL3(config)#interface vlan 100
SWL3(config-if)#ip access-group BLOCK_WEBSERVER in
SWL3(config-if)#ip access-group BLOCK_SERVER in
SWL3(config-if)#ip access-group BLOCK_100_OUT in
SWL3(config-if)#ip access-group ONLY_253_INTERNAL in
```

4. Lưu cấu hình

```
SWL3(config-if)#end
SWL3#write memory
```

TỔNG HỢP CẤU HÌNH FIREWALL(ASA)

I. SƠ ĐỒ



Cấu hình mạng biết:

- ✓ Switch L3 (Chế độ SVI))
  - Vlan 1 (10.0.1.1/24)
  - Vlan 20 (10.0.20.1/24)
  - Vlan (30 10.0.30.1/24)
  - Van 100 (10.0.100.1/24)
  - Gig0/1 nối Switch1 (L2) mạng server 10.0.100.0/24;
  - Gig0/2 nối Switch2 (L2) mạng Vlan1/20/30;
  - Fa0/1 nối gig0/1 router (10.0.0.0/24)
- ✓ Switch2: Vlan 1 (Fa0/21-24); Vlan 20 (Fa0/1-10); Vlan 30 (Fa0/11-20); Gig0/1 trunk Gig0/2 Switch L3
- ✓ Switch1: Vlan 100 (IP 10.0.100.0/24; all port vlan 100); Fa0/1 nối Gig0/1 Switch L3
- ✓ Firewall(ASA 5506-X): Gig1/1 nối Internet (cloud); Gig1/2 nối Fa0/1 Switch L3

II. YÊU CẦU

1. Cấu hình cơ bản Firewall ASA (ASA6)

- ✓ Đổi tên thiết bị Firewall thành ASA6.
- ✓ Cấu hình các giao diện:

  + GigabitEthernet1/1 (kết nối Internet/Cloud):
    - Đặt nameif là outside
    - Đặt security-level 0
    - Nhận IP động từ DHCP

  + GigabitEthernet1/2 (kết nối vào mạng nội bộ – SWL3):
    - Đặt nameif là inside
    - Đặt security-level 100
    - IP tĩnh: 10.0.0.2/24

- ✓ Thiết lập tuyến mặc định ra Internet bằng lệnh: route outside 0.0.0.0 0.0.0.0 dhcp

2. Cấu hình NAT Overload (PAT)

- ✓ Tạo NAT động để chuyển đổi địa chỉ toàn bộ mạng nội bộ (10.0.0.0/24) ra Internet qua địa chỉ IP của outside.'
  - ví dụ:

```
object network obj-inside
 subnet 10.0.0.0 255.255.255.0
 nat (inside,outside) dynamic interface
```

3. Cấu hình ACL cơ bản

- ✓ Cho phép các dịch vụ cơ bản truy cập từ Internet vào nội bộ (nếu cần), bao gồm:
  + HTTP (port 80)
  + HTTPS (port 443)
  + ICMP (ping)

4. Cấu hình kiểm tra dịch vụ ICMP/DNS

- ✓ Đảm bảo các máy trong mạng có thể sử dụng ping và phân giải tên miền:

5. Cấu hình ACL nâng cao

1. Chỉ cho phép địa chỉ IP WAN cụ thể (203.11.1.1) truy cập Web Server nội bộ (10.0.100.2) qua cổng 80.
2. Chặn truy cập từ Internet đến toàn bộ các mạng VLAN nội bộ (VLAN 1, 20, 30, 100).
3. Cho phép ICMP (ping) từ Internet vào Web Server.
4. Chặn các máy nội bộ sau truy cập Web Server (port 80): 10.0.1.254, 10.0.20.254, 10.0.30.254.
5. Chặn các IP sau truy cập toàn bộ mạng Server (10.0.100.0/24): 10.0.1.253, 10.0.20.253, 10.0.30.253.
6. Chỉ cho phép máy 10.0.100.253 giao tiếp nội bộ trong mạng Server (10.0.100.0/24).
7. Chặn máy 10.0.100.254 không được phép truy cập các VLAN 1, 20, 30.
8. Gắn các ACL vào các interface tương ứng (inside hoặc outside) đúng theo chiều truy cập.

6. Lưu cấu hình

Sau khi hoàn tất cấu hình,

III. CẤU HÌNH

I. Cấu hình cơ bản Firewall ASA

```
ASA6(config)# hostname ASA6
ASA6(config)# interface GigabitEthernet1/1
ASA6(config-if)# nameif outside
ASA6(config-if)# security-level 0
ASA6(config-if)# ip address dhcp setroute
ASA6(config-if)# no shutdown
ASA6(config)# interface GigabitEthernet1/2
ASA6(config-if)# nameif inside
ASA6(config-if)# security-level 100
ASA6(config-if)# ip address 10.0.0.2 255.255.255.0
ASA6(config-if)# no shutdown
ASA6(config)# route outside 0.0.0.0 0.0.0.0 dhcp  {<Thiết lập default route ra Internet>}
```

2. Cấu hình NAT Overload (PAT)

```
ASA6(config)# object network obj-inside
ASA6(config-network-object)# subnet 10.0.0.0 255.255.255.0
ASA6(config-network-object)# nat (inside,outside) dynamic interface  {<NAT Overload toàn bộ mạng nội bộ>}
```

3. Cấu hình ACL cơ bản

```
ASA6(config)# access-list OUTSIDE-IN extended permit tcp any host 10.0.100.2 eq 80  {<Cho phép HTTP>}
```

ASA6(config)# access-list OUTSIDE-IN extended permit tcp any host 10.0.100.2 eq 443 *{<Cho phép HTTPS>}*
ASA6(config)# access-list OUTSIDE-IN extended permit icmp any host 10.0.100.2 *{<Cho phép ICMP ping>}*
ASA6(config)# access-group OUTSIDE-IN in interface outside

V. Cấu hình ACL nâng cao

ASA6(config)# access-list OUTSIDE-IN extended permit tcp host 203.11.1.1 host 10.0.100.2 eq 80
ASA6(config)# access-list OUTSIDE-IN extended deny ip any 10.0.1.0 255.255.255.0
ASA6(config)# access-list OUTSIDE-IN extended deny ip any 10.0.20.0 255.255.255.0
ASA6(config)# access-list OUTSIDE-IN extended deny ip any 10.0.30.0 255.255.255.0
ASA6(config)# access-list OUTSIDE-IN extended permit icmp any host 10.0.100.2
ASA6(config)# access-list INSIDE-IN extended deny tcp host 10.0.1.254 host 10.0.100.2 eq 80
ASA6(config)# access-list INSIDE-IN extended deny tcp host 10.0.20.254 host 10.0.100.2 eq 80
ASA6(config)# access-list INSIDE-IN extended deny tcp host 10.0.30.254 host 10.0.100.2 eq 80
ASA6(config)# access-list INSIDE-IN extended deny ip host 10.0.1.253 10.0.100.0 255.255.255.0
ASA6(config)# access-list INSIDE-IN extended deny ip host 10.0.20.253 10.0.100.0 255.255.255.0
ASA6(config)# access-list INSIDE-IN extended deny ip host 10.0.30.253 10.0.100.0 255.255.255.0
ASA6(config)# access-list INSIDE-IN extended permit ip host 10.0.100.253 10.0.100.0 255.255.255.0
ASA6(config)# access-list INSIDE-IN extended deny ip host 10.0.100.254 10.0.1.0 255.255.255.0
ASA6(config)# access-list INSIDE-IN extended deny ip host 10.0.100.254 10.0.20.0 255.255.255.0
ASA6(config)# access-list INSIDE-IN extended deny ip host 10.0.100.254 10.0.30.0 255.255.255.0
ASA6(config)# access-group INSIDE-IN in interface inside

VI. Lưu cấu hình

ASA6# write memory *{<Lưu cấu hình vào bộ nhớ>}*

CẤU HÌNH SWITCH L3 VÀ SWITCH L2 (SƠ ĐỒ ASA)

I. SWITCH LAYER 3 – SW_L3

Switch>enable
Switch#configure terminal
Switch(config)#hostname SW_L3
SW_L3(config)#ip routing
SW_L3(config)#vlan 1
SW_L3(config-vlan)#exit
SW_L3(config)#vlan 20
SW_L3(config-vlan)#exit
SW_L3(config)#vlan 30
SW_L3(config-vlan)#exit
SW_L3(config)#vlan 100
SW_L3(config-vlan)#exit
SW_L3(config)#interface vlan 1
SW_L3(config-if)#ip address 10.0.1.1 255.255.255.0 {Đặt IP cho VLAN 1}
SW_L3(config-if)#no shutdown
SW_L3(config-if)#exit
SW_L3(config)#interface vlan 20
SW_L3(config-if)#ip address 10.0.20.1 255.255.255.0 {Đặt IP cho VLAN 20}
SW_L3(config-if)#no shutdown
SW_L3(config-if)#exit
SW_L3(config)#interface vlan 30
SW_L3(config-if)#ip address 10.0.30.1 255.255.255.0 {Đặt IP cho VLAN 30}
SW_L3(config-if)#no shutdown
SW_L3(config-if)#exit

```
SW_L3(config)#interface vlan 100
SW_L3(config-if)#ip address 10.0.100.1 255.255.255.0    {Đặt IP cho mạng Server}
SW_L3(config-if)#no shutdown
SW_L3(config-if)#exit
SW_L3(config)#ip routing    {Bật định tuyến để các VLAN liên lạc}
SW_L3(config)#interface gig0/1
SW_L3(config-if)#switchport mode trunk
SW_L3(config-if)#no shutdown
SW_L3(config-if)#exit
SW_L3(config)#interface gig0/2
SW_L3(config-if)#switchport mode trunk
SW_L3(config-if)#no shutdown
SW_L3(config-if)#exit
```

II. SWITCH LAYER 2 – SW_L2

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW_L2
SW_L2(config)#vlan 1
SW_L2(config-vlan)#exit
SW_L2(config)#vlan 20
SW_L2(config-vlan)#exit
SW_L2(config)#vlan 30
SW_L2(config-vlan)#exit
SW_L2(config)#interface range fa0/1 - 10
SW_L2(config-if-range)#switchport mode access
SW_L2(config-if-range)#switchport access vlan 20
SW_L2(config-if-range)#exit
SW_L2(config)#interface range fa0/11 - 20
SW_L2(config-if-range)#switchport mode access
SW_L2(config-if-range)#switchport access vlan 30
SW_L2(config-if-range)#exit
SW_L2(config)#interface range fa0/21 - 24
SW_L2(config-if-range)#switchport mode access
SW_L2(config-if-range)#switchport access vlan 1
SW_L2(config-if-range)#exit
SW_L2(config)#interface gig0/1
SW_L2(config-if)#description  Trunk to SW_L3
SW_L2(config-if)#switchport mode trunk
SW_L2(config-if)#no shutdown
SW_L2(config-if)#exit
```