NETWORK SYSTEM DESIGN PROJECT

Thiết kế & triển khai hệ thống mạng doanh nghiệp quy mô vừa

Vị trí định hướng: Network Engineer / System Admin (Intern)

Thời gian thực hiện: 2025

Người thực hiện: Chu Trọng Việt

1.Giới thiệu chung về Dự Án

- Project được xây dựng nhằm mô phỏng hệ thống mạng của một doanh nghiệp quy mô vừa (30-50 users), với yêu cầu phân chia phòng ban, quản lý tập trung, đảm bảo hiệu năng và mức độ bảo mật cơ bản được xây dựng trên nguyên tắc mạng doanh nghiệp 2 lớp (2-Tier Architecture)
- Dự án được thực hiện độc lập nhằm củng cố kiến thức CCNA và rèn luyện tư duy thiết kế mạng thực tế

2. Yêu cầu hệ thống & mục tiêu

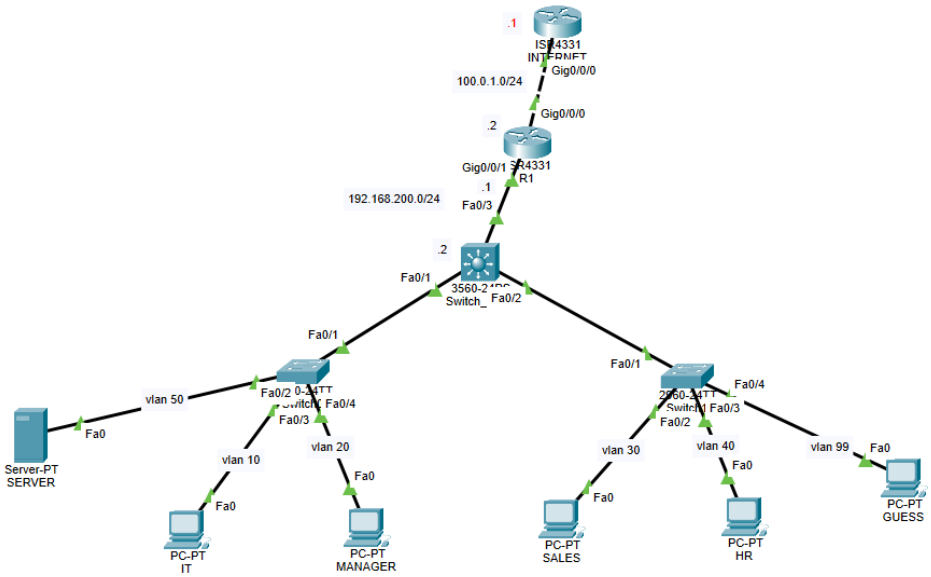
2.1. Yêu cầu hệ thống

- Phân chia phòng ban với các VLAN
- Giao tiếp giữa các phòng ban sử dụng Inter-Vlan
- Cấp IP tự động bằng DHCP
- Truy cập Internet bởi NAT
- Kiểm soát truy cập với ACL
- Bảo mật thiết bị, dữ liệu bằng Port-Security
- Ghi nhận truy cập thiết bị bằng Syslog Server

2.2. Mục tiêu

- Biết các cấu hình và áp dụng VLAN, SVI cho các phòng ban
- Biết cách cấu hình và áp dụng DHCP, NAT cho hệ thống mạng
- Cấu hình ACL, Port-Security, Syslog server đảm bảo yêu cầu hệ thống mạng

3.Sơ đồ mạng tổng thể



Mô tả mô hình: Hệ thống mạng Doanh Nghiệp Kinh Doanh có 2 khu vực làm việc riêng biệt, 1 khu vực dành cho các văn phòng quản lí như: IT, MANAGER và Server lưu trữ dữ liệu toàn công ty, 1 khu vực dành cho các văn phòng làm việc: Sales, Hr và các máy khách Guess**.** Các phòng ban được kết nối tới các Switch Layer 2 và các Switch Layer 2 được kết nối tới Switch Core Layer 3 trung tâm theo kiến trúc mạng doanh nghiệp 2 lớp, toàn bộ hệ thống mạng được kết nối với Internet thông qua 1 Router biên

3.1. Vai trò của các thiết bị mạng trong các tầng của hệ thống mạng

- Switch layer 2 (2960):

+ Kết nối tới các thiết bị đầu cuối như PC của các phòng ban: IT, HR, Sales, Server, Manager, Guess
+ Cấu hình bảo mật thiết bị Port-security
+ Gán cổng access cho các Vlan
+ Giảm tải lưu lượng cho Switch Core

- Switch Core Layer 3 (3560):

+ Inter-Vlan Routing : Tạo SVI cho từng VLAN
+ Cấu hình ACLs cho hệ thống mạng
+ DHCP Replay

- Router biên (4331):

+ Default route ra Internet
+ NAT: chuyển IP private thành IP public
+ DHCP cấp IP động cho hệ thống

- Router Internet:

+ Giả lập Internet

4.Thiết kế VLAN & IP

4.1 Danh sách VLAN

VLAN	Name	Host
10	IT	192.168.10.0/24
20	MANAGER	192.168.20.0/24
30	SALES	192.168.30.0/24
40	HR	192.168.40.0/24
50	SERVER	192.168.50.0/24
99	GUESS	192.168.99.0/24
100	MGMT	192.168.100.0/24

- VLAN 10: Các máy tính phòng kỹ thuật- IT
- VLAN 20: Các máy tính phòng Quản lí- Manager
- VLAN 30: Các máy tính phòng nhân viên kinh doanh- SALES
- VLAN 40: Các máy tính phòng nhân sự- HR
- VLAN 50: Máy chủ Server- lưu dữ liệu và ghi nhận sự kiện syslog
- VLAN 99: Các máy khách dùng cho khách hàng- GUESS
- VLAN 100: Vlan quản trị chung cho hệ thống mạng- MGMT

5.Giải pháp kỹ thuật & cấu hình

5.1 VLAN & Trunk

- Để đáp ứng yêu cầu phân chia mạng theo phòng ban, hệ thống được thiết kế sử dụng công nghệ VLAN (Virtual LAN) nhằm tách biệt các nhóm người dùng, phòng ban trong cùng hạ tầng hệ thống mạng doanh nghiệp
- Với việc sử dụng các VLAN giúp cho hệ thống mạng đảm bảo được các lợi ích:
  + Giảm broadcast traffic trong mạng
  + Dễ dàng quản lý và mở rộng hệ thống
  + Tăng tính bảo mật giữa các phòng ban

Các cổng kết nối giữa Switch Layer 2 và Switch Core được cấu hình ở chế độ Trunk, cho phép truyền nhiều VLAN trên cùng một đường truyền vật lý

```
SW_Core#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/2       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30,40,50,99,100
Fa0/2       1,10,20,30,40,50,99,100

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,30,40,50,99,100
Fa0/2       1,10,20,30,40,50,99,100
```

5.2 Inter-VLAN Routing (SVI-Switch Virtual Interface)

- Với yêu cầu hệ thống mạng doanh nghiệp là quản lí tập trung hiệu quả và hiệu năng cao, đồng thời khả năng mở rộng linh hoạt thì SVI là biện pháp tối ưu cho việc định tuyến giữa các Vlan hiệu quả và phù hợp với kiến trúc mạng doanh nghiệp hiện đại
- SVI (Switch Virtual Interface) là một interface logic đại diện cho một VLAN trên Switch Layer 3. Mỗi SVI được gán một địa chỉ IP và đóng vai trò là default gateway cho VLAN tương ứng

Trong mô hình này:

- SVI đóng vai trò là cổng Layer 3 (gateway) cho từng VLAN
- Thực hiện định tuyến giữa các VLAN trong Switch Layer 3
- Đường trunk được sử dụng để truyền nhiều VLAN giữa các switch

Vlan	Default-Gateway
10	192.168.10.1/24
20	192.168.20.1/24
30	192.168.30.1/24
40	192.168.40.1/24
50	192.168.50.1/24
99	192.168.99.1/24
100	192.168.100.1/24

Giải pháp SVI có ưu điểm:

- Hiệu năng cao: Việc định tuyến giữa các VLAN được thực hiện trực tiếp bên trong switch Layer 3 thông qua phần cứng (ASIC), giúp giảm độ trễ và tránh hiện tượng nghẽn traffic như mô hình Router-on-a-Stick (ROAS)
- Quản lí tập trung và dễ dàng mở rộng

```
Vlan1                  unassigned      YES unset  administratively down down
Vlan10                 192.168.10.1    YES manual up                    up
Vlan20                 192.168.20.1    YES manual up                    up
Vlan30                 192.168.30.1    YES manual up                    up
Vlan40                 192.168.40.1    YES manual up                    up
Vlan50                 192.168.50.1    YES manual up                    up
Vlan99                 192.168.99.1    YES manual up                    up
Vlan100                192.168.100.1   YES manual up                    up
```

5.3 DHCP trên Router

Hệ thống sử dụng DHCP Server tích hợp trên router để cấp phát địa chỉ IP động cho các máy trạm và server trong từng VLAN

Lý do lựa chọn DHCP trên router:

- Tiết kiệm chi phí triển khai thêm máy chủ riêng
- Phù hợp với quy mô mạng doanh nghiệp vừa
- Dễ quản lý và cấu hình tập trung

Mỗi VLAN được cấu hình một DHCP pool riêng, bao gồm:

- Network address
- Default gateway
- DNS server

Giải pháp này với ưu điểm đảm bảo các thiết bị trong mạng có thể tự động nhận IP hợp lệ mà không cần cấu hình thủ công trên từng thiết bị

```
ip dhcp pool VLAN10_IT
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 8.8.8.8
ip dhcp pool VLAN20_MANAGER
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 8.8.8.8
ip dhcp pool VLAN30_SALES
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 8.8.8.8
ip dhcp pool VLAN40_HR
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 8.8.8.8
ip dhcp pool VLAN50_SERVER
 network 192.168.50.0 255.255.255.0
 default-router 192.168.50.1
 dns-server 8.8.8.8
ip dhcp pool VLAN99_GUESS
 network 192.168.99.0 255.255.255.0
 default-router 192.168.99.1
 dns-server 8.8.8.8
```

- Ngoài ra, vì có một số thiết bị cần phải cấu hình IP tĩnh nên phải dự phòng 10 địa chỉ đầu tiên trên mỗi subnet không cho DHCP cấp tránh trường hợp xung đột IP

```
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp excluded-address 192.168.20.1 192.168.20.10
ip dhcp excluded-address 192.168.30.1 192.168.30.10
ip dhcp excluded-address 192.168.40.1 192.168.40.10
ip dhcp excluded-address 192.168.50.1 192.168.50.10
ip dhcp excluded-address 192.168.99.1 192.168.99.10
```

5.4 NAT Overload

Để cho phép các thiết bị trong mạng LAN truy cập Internet, router biên được cấu hình NAT Overload (Port Address Translation)

NAT Overload được lựa chọn cấu hình vì các nguyên lí hoạt động ưu việt:

- Nhiều địa chỉ IP private trong mạng LAN dùng chung một địa chỉ IP public
- Router phân biệt các phiên kết nối dựa trên số hiệu cổng (port)

Với cách thức hoạt động trên, NAT Overload là lựa chọn tốt nhất:

- Tiết kiệm địa chỉ IP public
- Phù hợp với hầu hết hệ thống mạng doanh nghiệp
- Đáp ứng tốt nhu cầu truy cập Internet đồng thời của nhiều người dùng

NAT được cấu hình tại router biên và cần phải xác định rõ:

- Inside interface (LAN)
- Outside interface (WAN/Internet)

```
R1#  show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 100.0.1.2:1       192.168.99.11:1    8.8.8.8:1          8.8.8.8:1
icmp 100.0.1.2:2       192.168.99.11:2    8.8.8.8:2          8.8.8.8:2
icmp 100.0.1.2:3       192.168.99.11:3    8.8.8.8:3          8.8.8.8:3
icmp 100.0.1.2:4       192.168.99.11:4    8.8.8.8:4          8.8.8.8:4
```

5.5 ACL (Access Control List)

Để tăng cường bảo mật và nghiệp vụ trong công ty hệ thống áp dụng Access Control List (ACL) nhằm kiểm soát luồng lưu thông giữa các VLAN và giữa các VLAN với Internet

ACL được đặt trên router tại các vị trí có lưu lượng cần kiểm soát, theo nguyên tắc:

- Chỉ đặt ACL tại nơi có gói tin đi qua
- Áp dụng ACL theo hướng in hoặc out phù hợp với luồng traffic

Mục đích của ACL trong hệ thống:

- Hạn chế quyền truy cập không cần thiết giữa các phòng ban
- Bảo vệ VLAN Server khỏi các truy cập trái phép
- Đảm bảo chỉ các VLAN được phép mới có thể truy cập tài nguyên quan trọng

```
SW_Core#show ip access-lists
Extended IP access list guess
    10 permit udp any eq bootpc any eq bootps (2 match(es))
    20 permit udp any eq bootps any eq bootpc
    30 permit icmp 192.168.99.0 0.0.0.255 192.168.10.0 0.0.0.255 echo-reply (4 match(es))
    40 deny ip 192.168.99.0 0.0.0.255 192.168.0.0 0.0.255.255
    50 permit ip any any (4 match(es))
Extended IP access list SALES
    10 permit icmp 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255 echo-reply
    20 permit icmp 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255 echo-reply
    30 permit ip 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255
    40 deny ip 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255
    50 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
    60 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
    70 permit ip any any (6 match(es))
Extended IP access list HR
    10 permit icmp 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255 echo-reply
    20 permit icmp 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255 echo-reply
    30 permit ip 192.168.40.0 0.0.0.255 192.168.50.0 0.0.0.255
    40 deny ip 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255 (8 match(es))
    50 deny ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255
    60 deny ip 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255
    70 permit ip any any (22 match(es))
Extended IP access list VLAN_MGMT
    10 permit tcp 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 22
    15 permit tcp 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 443
    20 permit udp 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255 eq snmp
    30 deny ip any 192.168.100.0 0.0.0.255 (4 match(es))
    40 permit ip any any
```

Các luật ACL được cấu hình trong hệ thống:

+ IT và Manager được quyền Full access

+ Các máy khách (Guess) chỉ được quyền truy cập Internet và không được phép truy cập mạng LAN.Tuy nhiên phòng IT có thể kiểm tra được các máy Guess

+ Phòng Sales được phép truy cập Server và Internet.Không được truy cập tới các phòng ban như Manager, IT, HR nhưng phòng IT và Manager được phép truy cập tới Sales

+ Phòng HR được phép truy cập Server và Internet. Không được truy cập tới các phòng ban như Manager, IT, Sales nhưng phòng IT và Manager được phép truy cập tới HR

+ VLAN MGMT chỉ được duy nhất phòng IT sử dụng trong việc theo dõi, quản lí, và truy nhập từ xa vào hệ thống mạng, ngoài ra các máy trạm khác không được phép truy cập vào VLAN này ví lí do bảo mật

5.6 Port-Security trên Switch

Tại các cổng access kết nối đến máy người dùng, đặc biệt là VLAN IT, tính năng Port Security được triển khai để ngăn chặn thiết bị trái phép truy cập vào mạng nội bộ

Các cổng access được cấu hình:

- Giới hạn số lượng MAC address tối đa
- Sử dụng MAC address sticky để switch tự động học MAC hợp lệ
- Áp dụng chế độ xử lý vi phạm (violation) nhằm chặn các thiết bị không hợp lệ

Port Security giúp:

- Ngăn chặn việc cắm thiết bị lạ vào mạng
- Giảm nguy cơ tấn công từ bên trong hệ thống
- Nâng cao mức độ bảo mật lớp truy cập (Access Layer)

Trong dự án, port-security được cấu hình trên cổng access ở phòng IT lí do là bởi phòng IT luôn là cửa ngõ cho các đợt tấn công đánh cắp dữ liệu

```
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0001.C793.6EC2
```

5.7. Syslog Server

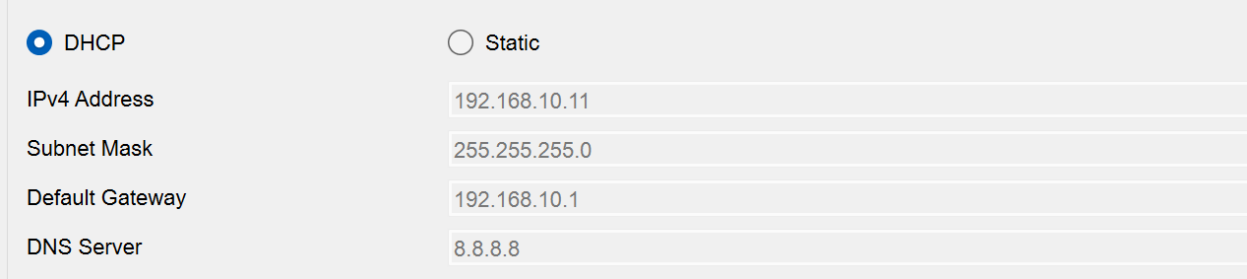
- Syslog được cấu hình để linh hoạt trong việc kiểm tra, giám sát hệ thống mạng nhanh chóng và dễ dàng. Syslog server được đặt trong Vlan Server (VLAN 50) để thu thập log từ Router biên, Switch Core, Switch Access để tiện theo dõi, phân tích và xử lí sự cố

```
SW_Core# show running-config | include logging
logging trap debugging
logging 192.168.50.11
```

6. Kiểm tra & kết quả

Sau khi hoàn tất quá trình cấu hình hệ thống mạng, các bước kiểm tra (testing) được thực hiện nhằm đảm bảo toàn bộ chức năng hoạt động đúng theo yêu cầu ban đầu. Kiểm tra tập trung vào các thành phần chính như VLAN, Inter-VLAN routing, DHCP, NAT, ACL và Port Security, Syslog.

6.1 Kiểm tra cấp phát IP (DHCP)



Các PC trong từng VLAN nhận được địa chỉ IP đúng dải mạng đã thiết kế
Default gateway nhận đúng địa chỉ IP của sub-interface tương ứng trên router
DNS server được cấu hình đúng theo DHCP pool

- Dịch vụ DHCP trên router hoạt động ổn định và đáp ứng đúng yêu cầu cấp phát IP tự động cho hệ thống

+ Các dải địa chỉ đã được DHCP cung cấp:

```
R1#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.10.11    0001.C793.6EC2           --                     Automatic
192.168.20.11    0000.0C87.4991           --                     Automatic
192.168.30.11    0007.EC44.884C           --                     Automatic
192.168.40.11    0060.5CBD.3D31           --                     Automatic
192.168.50.11    00D0.588E.1DD4           --                     Automatic
192.168.99.11    0060.3E26.A09E           --                     Automatic
```

6.2 Kiểm tra kết nối trong cùng VLAN và trong Inter-Vlan Routing

Các máy trạm nằm trong cùng một VLAN và thuộc các VLAN khác nhau được kiểm tra khả năng kết nối với nhau thông qua lệnh ping

```
C:\>ping 192.168.40.11

Pinging 192.168.40.11 with 32 bytes of data:

Reply from 192.168.40.11: bytes=32 time<1ms TTL=127
Reply from 192.168.40.11: bytes=32 time<1ms TTL=127
Reply from 192.168.40.11: bytes=32 time<1ms TTL=127
Reply from 192.168.40.11: bytes=32 time<1ms TTL=127
```

Kết quả kiểm tra:

- Các PC trong cùng VLAN ping thành công lẫn nhau
- Các VLAN được phép giao tiếp theo đúng chính sách ACL đã cấu hình
- Không xảy ra hiện tượng mất gói tin

Cấu hình VLAN và các cổng access trên switch hoạt động chính xác. Chức năng Inter-VLAN routing thông qua SVI hoạt động đúng thiết kế và tuân thủ các chính sách bảo mật

6.3 Kiểm tra truy cập Internet (NAT Overload)

Các PC trong mạng LAN được kiểm tra khả năng truy cập Internet bằng cách ping tới địa chỉ IP public (ví dụ: 8.8.8.8)

```
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<1ms TTL=254
Reply from 8.8.8.8: bytes=32 time<1ms TTL=254
Reply from 8.8.8.8: bytes=32 time<1ms TTL=254
Reply from 8.8.8.8: bytes=32 time<1ms TTL=254
```

```
R1#  show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 100.0.1.2:1       192.168.99.11:1    8.8.8.8:1          8.8.8.8:1
icmp 100.0.1.2:2       192.168.99.11:2    8.8.8.8:2          8.8.8.8:2
icmp 100.0.1.2:3       192.168.99.11:3    8.8.8.8:3          8.8.8.8:3
icmp 100.0.1.2:4       192.168.99.11:4    8.8.8.8:4          8.8.8.8:4
```

Kết quả kiểm tra:

- Router biên ping thành công ra Internet
- Các PC trong LAN ping thành công ra Internet thông qua NAT Overload
- Các phiên truy cập Internet được dịch địa chỉ IP và port chính xác

Cấu hình NAT Overload hoạt động tốt, cho phép toàn bộ mạng LAN truy cập Internet thông qua một địa chỉ IP public

6.4 Kiểm tra Access Control List (ACL)

ACL được kiểm tra bằng cách mô phỏng các tình huống truy cập hợp lệ và không hợp lệ giữa các VLAN

6.4.1. ACL SALES

```
Extended IP access list SALES
    8 permit icmp 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255 echo-reply (4 match(es))
    9 permit icmp 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255 echo-reply
    10 permit ip 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255 (4 match(es))
    11 deny ip 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255 (4 match(es))
    12 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255 (4 match(es))
    13 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255 (8 match(es))
    20 permit ip any any (4 match(es))
```

```
C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\>ping 192.168.50.11

Pinging 192.168.50.11 with 32 bytes of data:

Reply from 192.168.50.11: bytes=32 time<1ms TTL=127
Reply from 192.168.50.11: bytes=32 time<1ms TTL=127
Reply from 192.168.50.11: bytes=32 time<1ms TTL=127
Reply from 192.168.50.11: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.50.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- ACL SALES đã đảm bảo cấu hình và thực hiện chính xác theo yêu cầu hệ thống

6.4.2. ACL HR

```
Extended IP access list HR
    8 permit icmp 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255 echo-reply (4 match(es))
    9 permit icmp 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255 echo-reply (4 match(es))
    10 permit ip 192.168.40.0 0.0.0.255 192.168.50.0 0.0.0.255 (8 match(es))
    11 deny ip 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255
    12 deny ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255 (12 match(es))
    13 deny ip 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255 (4 match(es))
    20 permit ip any any (4 match(es))
```

```
C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.40.1: Destination host unreachable.
Reply from 192.168.40.1: Destination host unreachable.
Reply from 192.168.40.1: Destination host unreachable.
Reply from 192.168.40.1: Destination host unreachable.

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
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<1ms TTL=254
Reply from 8.8.8.8: bytes=32 time<1ms TTL=254
Reply from 8.8.8.8: bytes=32 time<1ms TTL=254
Reply from 8.8.8.8: bytes=32 time<1ms TTL=254

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- ACL HR đã đảm bảo chạy đúng với các yêu cầu hệ thống

6.4.3 ACL Guess

```
Extended IP access list guess
    5 permit udp any eq bootpc any eq bootps (5 match(es))
    6 permit udp any eq bootps any eq bootpc
    7 permit icmp 192.168.99.0 0.0.0.255 192.168.10.0 0.0.0.255 echo-reply (4 match(es))
    10 deny ip 192.168.99.0 0.0.0.255 192.168.0.0 0.0.255.255 (32 match(es))
    20 permit ip any any (8 match(es))
```

```
C:\>ping 192.168.50.11

Pinging 192.168.50.11 with 32 bytes of data:

Reply from 192.168.99.1: Destination host unreachable.
Reply from 192.168.99.1: Destination host unreachable.
Reply from 192.168.99.1: Destination host unreachable.
Reply from 192.168.99.1: Destination host unreachable.

Ping statistics for 192.168.50.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

6.4.4 Một số yêu cầu của ACL khác

- Văn phòng IT và Manager được phép truy cập vào các máy tính ở các phòng ban còn lại, tuy nhiên các phòng ban không thể truy cập tới phòng IT và Manager

+ Hình ảnh máy Guess ping tới máy phòng IT lập tức bị từ chối truy cập:

```
C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.99.1: Destination host unreachable.
Reply from 192.168.99.1: Destination host unreachable.
Reply from 192.168.99.1: Destination host unreachable.
Reply from 192.168.99.1: Destination host unreachable.

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Tuy nhiên, phòng IT vẫn được truy cập tới máy khác Guess:

```
C:\>ping 192.168.99.11

Pinging 192.168.99.11 with 32 bytes of data:

Reply from 192.168.99.11: bytes=32 time<1ms TTL=127
Reply from 192.168.99.11: bytes=32 time<1ms TTL=127
Reply from 192.168.99.11: bytes=32 time<1ms TTL=127
Reply from 192.168.99.11: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.99.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Kết quả kiểm tra tổng thể:

- Các VLAN được phép có thể truy cập tài nguyên theo đúng thiết kế
- Các VLAN bị hạn chế không thể truy cập VLAN Server hoặc các VLAN khác
- ACL không ảnh hưởng tới lưu lượng Internet hợp lệ

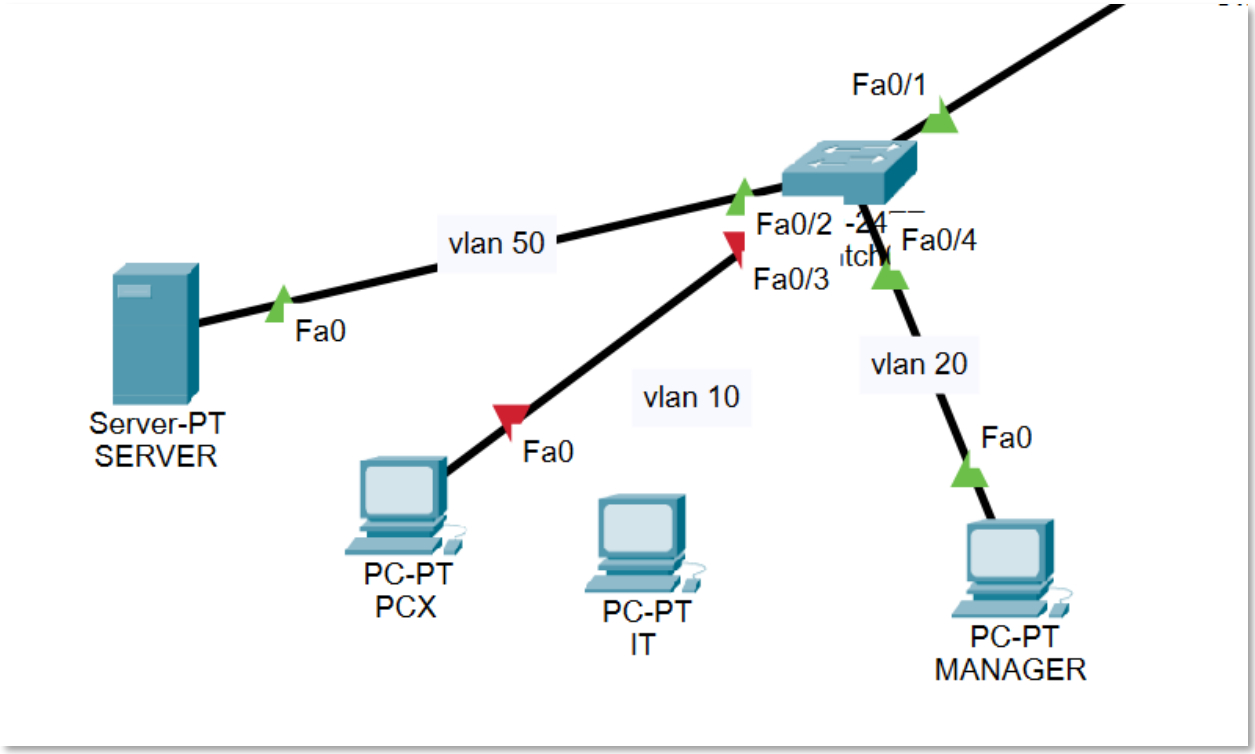
ACL được đặt đúng vị trí và hoạt động chính xác, giúp tăng cường bảo mật cho hệ thống mạng

6.5 Kiểm tra Port Security

Port Security được kiểm tra bằng cách:

- Kết nối thiết bị hợp lệ đã được học MAC address
- Thử kết nối thiết bị khác vào cùng cổng switch đã bật Port Security

```
SW_Left#show port-security interface fa0/3
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0060.3ED4.887D:10
Security Violation Count   : 1
```



Kết quả kiểm tra:

- Switch cho phép thiết bị hợp lệ truy cập mạng
- Khi cắm thiết bị lạ, cổng switch bị hạn chế hoặc shutdown
- MAC address sticky được switch học và lưu lại sau khi phát sinh lưu lượng

Port Security hoạt động đúng chức năng, giúp ngăn chặn các thiết bị không được phép truy cập vào mạng LAN

6.6. Syslog Server

- Syslog được kiểm tra bằng cách đăng nhập vào thiết bị ở các chế độ config terminal và đăng xuất để kiểm tra thời gian và sự ghi chép của server

	Time	HostName	Message
1	03.01.1993 01:34:34.245 AM	192.168.50.1	%SYS-5-CONFIG_I: Configured from console by…
2	03.01.1993 01:35:14.509 AM	192.168.200.1	%SYS-5-CONFIG_I: Configured from console by…
3	03.01.1993 01:35:38.161 AM	192.168.100.3	%SYS-5-CONFIG_I: Configured from console by…
4	03.01.1993 01:35:46.711 AM	192.168.100.2	%SYS-5-CONFIG_I: Configured from console by…

- Các thiết bị mạng như Switch, Router khi đăng nhập vào chế độ config terminal thì server sẽ ghi chép sự kiện với ngày giờ, địa chỉ IP và nội dung mức độ của sự kiện

7.Khó khăn và hướng phát triển

7.1 Khó khăn trong cấu hình NAT

Một trong những khó khăn lớn nhất là tình huống router ping được Internet nhưng các PC trong mạng LAN không truy cập được Internet

Nguyên nhân chính sau khi tìm hiểu:

- Chưa xác định đúng interface inside và outside cho NAT
- Sai cấu hình default route
- Route trả về từ phía Internet/ISP chưa đúng

Cách khắc phục:

- Kiểm tra lại cấu hình NAT (inside/outside)
- Kiểm tra bảng định tuyến (show ip route)
- Đảm bảo có default route trỏ về phía ISP
- Kiểm tra luồng gói tin từ LAN ra Internet và chiều ngược lại

7.2. Khó khăn trong triển khai Port Security

Trong quá trình cấu hình Port Security với MAC address sticky, switch không ngay lập tức hiển thị địa chỉ MAC trong cấu hình.

Nguyên nhân sau khi tìm hiểu:

- Switch chỉ học MAC address khi có lưu lượng (traffic) đi qua cổng
- Khi chưa phát sinh gói tin, MAC sticky chưa được cập nhật

Cách khắc phục:

- Tạo lưu lượng bằng cách ping hoặc truy cập mạng từ PC
- Kiểm tra bảng MAC address (show mac address-table)
- Chờ switch cập nhật sticky MAC

7.3. Khó khăn trong việc đặt ACL

- Trong quá trình triển khai ACL, việc đặt ACL sai vị trí hoặc sai hướng (in/out) có thể dẫn đến:
  - Chặn toàn bộ lưu lượng mạng
  - Ảnh hưởng đến các dịch vụ hợp lệ như DHCP hoặc Internet

Cách khắc phục:

- Xác định chính xác luồng đi của gói tin
- Áp dụng ACL tại các vị trí cần kiểm soát
- Kiểm tra từng rule trước khi áp dụng toàn bộ

- Ngoài ra, trong quá trình đặt ACL cho máy Guess, vô tình đặt ACL deny ip truy cập vào mạng LAN dẫn đến việc DHCP không thể cấp ip cho các máy khách, cách khắc phục là chúng ta permit các gói Discover và Offer của client (udp 68) và server (udp 67):

permit udp any eq 68 any eq 67
permit udp any eq 67 any eq 68

7.4. Khó khăn trong việc cấu hình syslog server trên Switch Layer 2

- Vì Switch Layer 2 không có khả năng định tuyến khác VLAN nên khi Server khác VLAN thì Switch layer 2 không thể gửi log tới server được do không có default-gateway và địa chỉ IP cụ thể
- Giải pháp được đưa ra là cấu hình SVI cho VLAN 100 MGMT và cấu hình default-gateway để VLAN 100 có thể ping được tới Server Syslog
- Bên cạnh đó, để hỗ trợ cho vấn đề bảo mật, theo dõi và phân luồng của người quản trị và người dùng thì hệ thống mạng cần có một VLAN để quản lí trong hệ thống mạng.Vì vậy chúng ta cần phải có VLAN 100 để quản lí riêng biệt dành cho việc quản trị

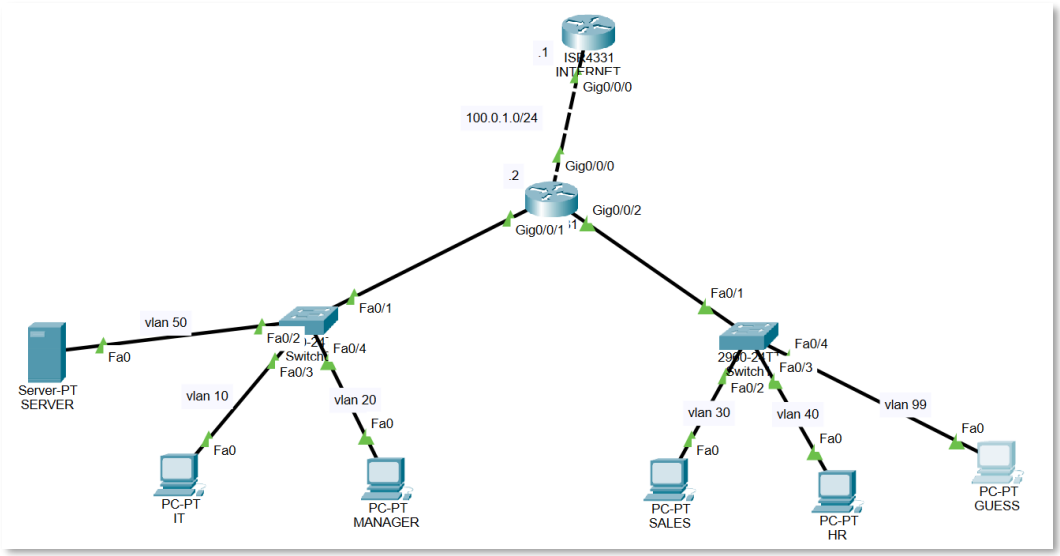
+ Eq 22 cho phép VLAN IT truy cập SSH vào thiết bị
+ Eq 443 cho phép truy cập web HTTPS (Web Management) của các thiết bị
+ Eq 161 cho phép thu nhập các sự cố, các thay đổi của CPU, Interface status…

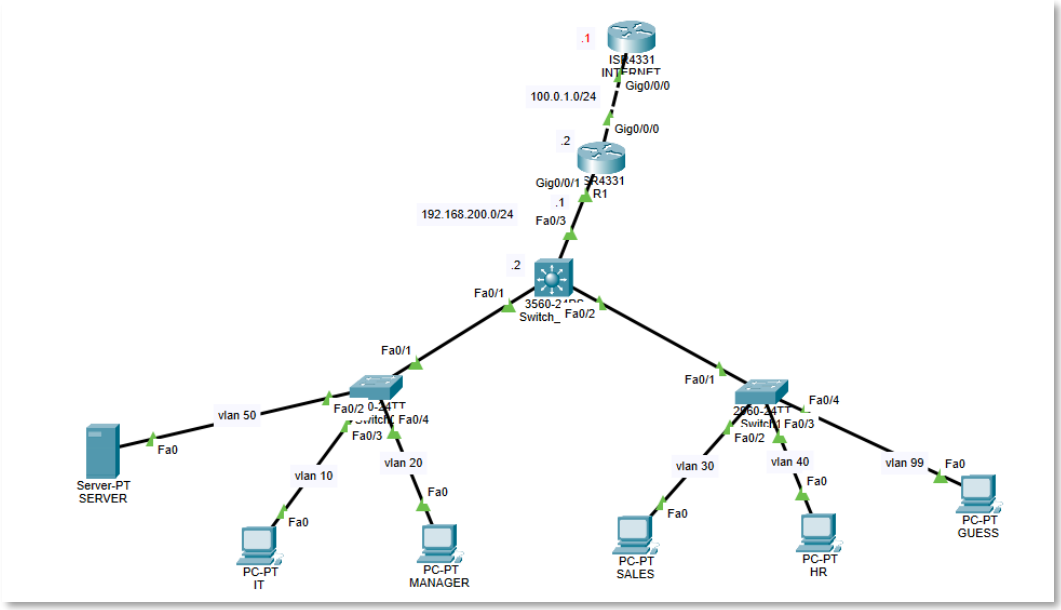
```
ip access-list extended VLAN_MGMT
 permit tcp 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 22
 permit tcp 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 443
 permit udp 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255 eq snmp
 deny ip any 192.168.100.0 0.0.0.255
 permit ip any any
```

- VLAN 100 chỉ được truy cập khi cần thiết thông qua các giao thức truy cập SSH, Web và SNMP ở phòng IT còn lại tất cả gói tin khác đều phải bị chặn

7.5. Khó khăn trong nâng cấp hệ thống mạng

- Hệ thống mạng ban đầu được thiết kế với số lượng VLAN ít vì vậy để tiết kiệm thì Inter-Vlan được cấu hình Router-on-a-stick (ROAS).Tuy nhiên, khi hệ thống đã lớn dần thì không thể sử dụng Roas để Vlan routing được nữa vì nó sẽ gây ra tắc nghẽn dữ liệu nếu nhiều gói tin được gửi cùng lúc, vì vậy để khắc phục hạn chế này hệ thống sẽ cần phải đầu tư thêm Switch Core Layer 3 với công nghệ SVI để sử dụng tốt hiệu năng Inter-Vlan Routing vì SW layer 3 có VSIC hỗ trợ việc định tuyến giữa các VLAN mà không cần phải qua CPU như Router
- Việc cấu hình lại các VLAN, ACL, DHCP relay và các route đòi hỏi phải có hiểu biết các tính năng cần thiết đi kèm sự cẩn thận nhất định trong lúc cấu hình và vẽ lại hệ thống để các thiết bị có thể giao tiếp được với nhau hoàn chỉnh, hạn chế các lỗi làm trì hoãn quá trình làm việc





7.6. Hạn chế của hệ thống hiện tại

Mặc dù hệ thống đáp ứng tốt yêu cầu ban đầu, vẫn tồn tại một số hạn chế:

- Hệ thống hiện tại chỉ mô phỏng một site, chưa có chi nhánh
- Chưa triển khai giao thức định tuyến động OSPF
- Chưa có firewall chuyên dụng kiểm soát truy cập
- Chưa có cơ chế dự phòng (redundancy) cho các thiết bị quan trọng phòng trường hợp bất khả kháng

7.7. Hướng phát triển trong tương lai

Trong tương lai, hệ thống có thể được nâng cấp và mở rộng theo các hướng sau:

- Triển khai mô hình đa chi nhánh, kết nối các site thông qua WAN
- Sử dụng OSPF để tự động định tuyến giữa các router
- Triển khai Firewall nhằm nâng cao mức độ bảo mật, kiểm soát truy cập
- Bổ sung DHCP Failover để tăng tính sẵn sàng khi gặp trường hợp lỗi cấp phát ip
- Áp dụng các giải pháp giám sát mạng (monitoring) và logging để kiểm tra hệ thống

HỆ THỐNG VẪN CÒN ĐƯỢC TIẾP TỤC ĐƯỢC NÂNG CẤP TRONG TƯƠNG LAI
