**BỘ** **GIÁO** **DỤC** **VÀ** **ĐÀO** **TẠO**



**TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP.HCM**

**KHOA CÔNG NGHỆ THÔNG TIN**

**MÔN:** **THIÊT KẾ MẠNG**

**BÁO CÁO LAB 02:**

**THIẾT LẬP & CẤU HÌNH MẠNG LAN THEO MÔ HÌNH PHÂN LỚP CHO CÔNG TY CỔ PHẦN MARSU**

**MÃ MÔN HỌC: CNDE430780**

**HỌ VÀ TÊN: NGUYỄN QUỲNH HƯƠNG QUYÊN**

**MSSV: 22162036**

**LỚP: 22162B**

**GVHD: TS. HUỲNH NGUYÊN CHÍNH**

**Tp.** **Hồ** **Chí Minh, tháng 02 năm 2025**

**THUẬT NGỮ**

**vPC (Virtual PortChannel):** công nghệ cho phép nhiều đường kết nối từ 2 switch cùng kết nối với 1 thiết bị thứ 3 bằng cách tạo ra một đường kết nối logic. Điều này giúp nâng cao khả năng dự phòng, băng thông tới thiết bị.

**LAN (Local Area Network):** Mạng cục bộ kết nối các thiết bị trong phạm vi nhỏ như văn phòng, tòa nhà.

**VLAN (Virtual LAN):** Mạng LAN ảo chia một LAN vật lý thành nhiều mạng logic để tăng bảo mật và quản lý.

**WAN (Wide Area Network):** Mạng diện rộng kết nối nhiều LAN qua khoảng cách lớn, như Internet.

**Broadcast Storms:** Hiện tượng gói tin broadcast tràn ngập mạng, gây nghẽn băng thông.

**STP (Spanning Tree Protocol):** Giao thức ngăn chặn loop trong mạng bằng cách vô hiệu hóa các liên kết dư thừa.

**ARP (Address Resolution Protocol):** Giao thức ánh xạ địa chỉ IP sang địa chỉ MAC trong mạng nội bộ, giúp thiết bị giao tiếp với nhau trong cùng một mạng.

**DAI (Dynamic ARP Inspection):** Cơ chế bảo mật ngăn chặn ARP spoofing bằng cách kiểm tra ARP request/response.

**DHCP (Dynamic Host Configuration Protocol):** Giao thức cấp phát IP động cho thiết bị trong mạng.

**DHCP Snooping:** Cơ chế bảo mật kiểm soát DHCP để ngăn chặn DHCP giả mạo.

**Storm Control:** Cơ chế giới hạn lưu lượng broadcast, multicast và unicast không xác định để tránh nghẽn mạng.

**OSPF (Open Shortest Path First):** Giao thức định tuyến link-state tìm đường đi ngắn nhất trong mạng IP.

**NAT (Network Address Translation):** Cơ chế chuyển đổi địa chỉ IP riêng thành địa chỉ IP công cộng để truy cập Internet.

**VPN (Virtual Private Network):** Kết nối bảo mật giữa các mạng qua Internet bằng cách mã hóa dữ liệu.

**SNMP (Simple Network Management Protocol):** Giao thức giám sát và quản lý thiết bị mạng từ xa.

**DMZ (Demilitarized Zone):** Vùng mạng trung gian giữa mạng nội bộ và Internet, thường dùng cho máy chủ công khai.

**QoS (Quality of Service):** là thuật ngữ dùng trong lĩnh vực viễn thông. QoS cho phép điều khiển dòng thông tin ở mục độ căn bản, xác định phương thức để dòng thông tin của một ứng dụng nào đó đi qua các bộ định tuyến và chuyển mạch của mạng.

1. **GIỚI THIỆU**

Hệ thống mạng là nền tảng quan trọng trong hạ tầng công nghệ thông tin của mọi tổ chức, đóng vai trò kết nối, truyền tải dữ liệu và đảm bảo tính sẵn sàng của các dịch vụ. Một thiết kế mạng hiệu quả không chỉ giúp tối ưu hóa hiệu suất hoạt động mà còn tăng cường khả năng bảo mật, quản lý dễ dàng và hỗ trợ mở rộng trong tương lai. Với sự phát triển của công nghệ và nhu cầu ngày càng cao về băng thông, tính ổn định và an toàn thông tin, việc xây dựng một hệ thống mạng có kiến trúc hợp lý là yếu tố then chốt để đảm bảo hoạt động của tổ chức diễn ra suôn sẻ.

Mô hình phân lớp là một trong những phương pháp thiết kế mạng phổ biến, giúp tổ chức hệ thống một cách khoa học và tối ưu. Bằng cách chia mạng thành các lớp như ***Core*** (Lõi), ***Distribution*** (Phân phối) và ***Access*** (Truy cập), mô hình này giúp quản lý lưu lượng hiệu quả, giảm tắc nghẽn và tăng tính linh hoạt. Ngoài ra, việc phân tách VLAN cho phép kiểm soát truy cập tốt hơn, tăng cường bảo mật và giảm thiểu rủi ro lây lan sự cố trong hệ thống. Với những ưu điểm này, mô hình phân lớp không chỉ giúp nâng cao hiệu suất của hệ thống mạng mà còn đảm bảo khả năng mở rộng và bảo trì dễ dàng trong tương lai.

1. **MỤC TIÊU THIẾT KẾ**

Tài liệu thiết kế này trình bày thiết kế và triển khai một hệ thống mạng LAN theo mô hình phân lớp, với mục tiêu chính là xây dựng một hệ thống mạng có khả năng mở rộng linh hoạt, bảo mật cao và hiệu suất tối ưu. Hệ thống được thiết kế để hỗ trợ kết nối ổn định giữa các thiết bị, đảm bảo truy cập nhanh chóng, bảo vệ thông tin khỏi các mối đe dọa an ninh, đồng thời dễ dàng mở rộng khi có nhu cầu nâng cấp hoặc bổ sung thiết bị.

Thiết kế mạng tập trung vào việc chia mạng thành các VLAN nhằm tối ưu hóa lưu lượng, giảm xung đột dữ liệu và nâng cao khả năng quản lý mạng. Mô hình này giúp cô lập các nhóm thiết bị theo từng phòng ban hoặc khu vực, đồng thời tăng cường bảo mật nội bộ. Hệ thống firewall được tích hợp để kiểm soát truy cập, ngăn chặn các truy cập trái phép và bảo vệ hệ thống khỏi các cuộc tấn công mạng. Ngoài ra, việc triển khai DHCP giúp tự động cấp phát địa chỉ IP cho các thiết bị, giảm công tác quản trị và tránh tình trạng xung đột địa chỉ IP.

Bên cạnh đó, hệ thống còn bao gồm một vùng DMZ nhằm quản lý các dịch vụ công cộng như Web Server và Mail Server, đảm bảo các dịch vụ này có thể truy cập từ bên ngoài mà không ảnh hưởng đến vùng mạng nội bộ. DMZ giúp nâng cao bảo mật bằng cách tạo một vùng đệm giữa hệ thống bên trong và Internet, hạn chế rủi ro khi bị tấn công từ bên ngoài.

Với thiết kế này, hệ thống mạng sẽ đáp ứng tốt nhu cầu sử dụng của tổ chức, hỗ trợ các dịch vụ quan trọng, đảm bảo hoạt động trơn tru và dễ dàng mở rộng trong tương lai.

1. **PHÂN TÍCH YÊU CẦU THIẾT KẾ**

* ***Phạm vi dự án***

Dự án này tập trung vào việc thiết kế một hệ thống mạng LAN phân lớp cho một tòa nhà văn phòng gồm nhiều phòng ban. Hệ thống mạng sẽ bao phủ toàn bộ hai tòa nhà với kiến trúc bao gồm các switch core, switch distribution, switch access, firewall, router, và các server quan trọng.

Hệ thống mạng sẽ hỗ trợ các dịch vụ nội bộ, kết nối Internet, và truy cập từ xa qua VPN. Toàn bộ kiến trúc được chia thành các vùng chính như sau:

* Building 1 (VLAN 10 – 16)
* Building 2 (VLAN 20 – 26)
* DMZ: Chứa Web Server và Mail Server, đảm bảo các dịch vụ có thể truy cập từ bên ngoài mà vẫn giữ được bảo mật.
* Mạng nội bộ: Chứa DHCP Server và DNS Server để hỗ trợ quản lý mạng tự động.
* ***Mục tiêu kỹ thuật***

Hệ thống mạng cần đáp ứng các tiêu chí kỹ thuật quan trọng để đảm bảo hoạt động ổn định, bảo mật và hiệu suất cao. Dưới đây là các tiêu chí chính được cân nhắc trong thiết kế:

1. *Khả năng mở rộng*

* Hệ thống mạng được thiết kế theo mô hình phân lớp (Core, Distribution, Access), giúp dễ dàng mở rộng khi cần bổ sung thiết bị hoặc mở rộng hệ thống.
* Sử dụng VLAN và VTP để dễ dàng thêm hoặc quản lý các nhóm thiết bị mà không cần thay đổi cấu trúc vật lý của mạng.
* EtherChannel giúp tăng băng thông và hỗ trợ mở rộng mà không làm giảm hiệu suất mạng.

1. *Tính sẵn sàng*

* Cấu hình dự phòng trên switch core và switch distribution giúp duy trì kết nối khi một thiết bị gặp sự cố.
* Firewall bảo vệ hệ thống và kiểm soát luồng dữ liệu ra vào mạng.
* Cấu hình DHCP và DNS giúp đảm bảo hệ thống có thể phục hồi nhanh chóng khi xảy ra lỗi.

1. *Hiệu suất mạng*

* EtherChannel tăng tốc độ truyền tải giữa các thiết bị quan trọng.
* Trunking giữa các switch giúp giảm bớt tắc nghẽn mạng.
* Cấu hình QoS (Quality of Service) để ưu tiên lưu lượng quan trọng, đảm bảo hiệu suất cho các ứng dụng nhạy cảm với độ trễ như VoIP và truyền tải dữ liệu.

1. *Bảo mật*

* Tường lửa (Firewall) bảo vệ mạng nội bộ khỏi các cuộc tấn công từ bên ngoài.
* VLAN giúp cô lập các nhóm thiết bị, tránh nguy cơ lây lan tấn công trong nội bộ.
* VPN được thiết lập để bảo mật kết nối từ xa, tránh rủi ro rò rỉ dữ liệu.
* Access Control Lists (ACLs) kiểm soát quyền truy cập vào các tài nguyên quan trọng.

1. *Khả năng quản lý*

* VTP giúp quản lý VLAN dễ dàng hơn giữa các switch.
* SNMP (Simple Network Management Protocol) hỗ trợ giám sát mạng, phát hiện lỗi nhanh chóng.
* DHCP Server tự động cấp phát IP, giúp giảm thiểu lỗi nhập thủ công và đơn giản hóa việc quản lý.

1. *Khả năng thích ứng*

* Hệ thống mạng hỗ trợ IPv4 và IPv6, đảm bảo khả năng tương thích với công nghệ mới.
* Cấu trúc mở và linh hoạt, có thể tích hợp thêm các công nghệ bảo mật như IDS/IPS (Intrusion Detection/Prevention Systems) trong tương lai.
* Hỗ trợ truy cập từ xa qua VPN mà không ảnh hưởng đến bảo mật mạng nội bộ.

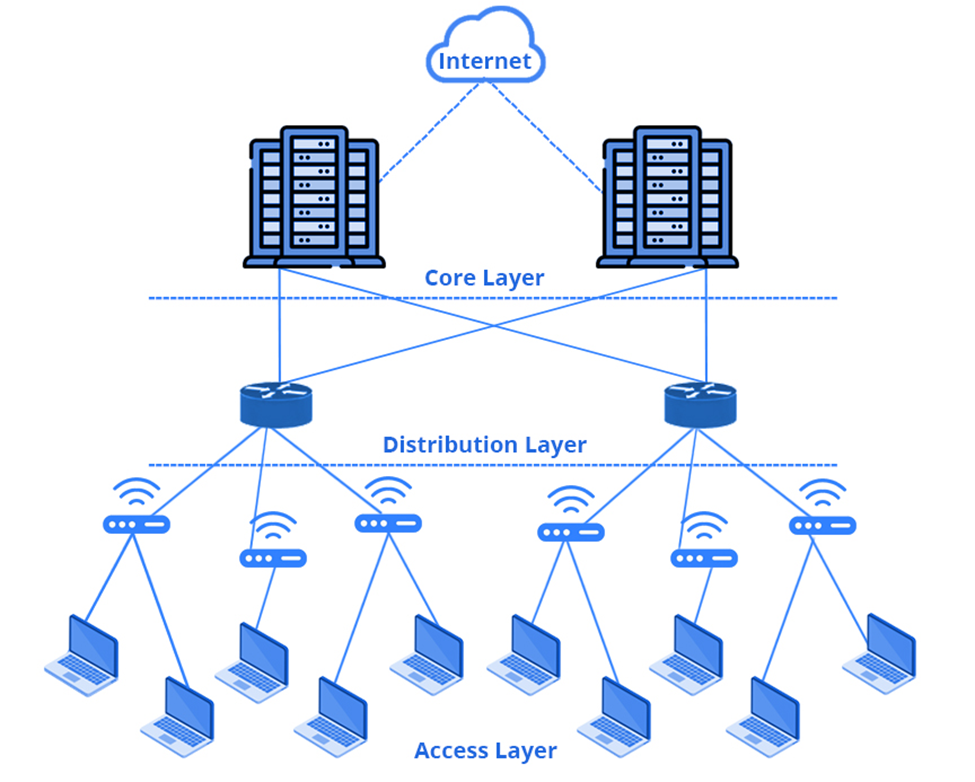
1. *Khả năng tài chính*

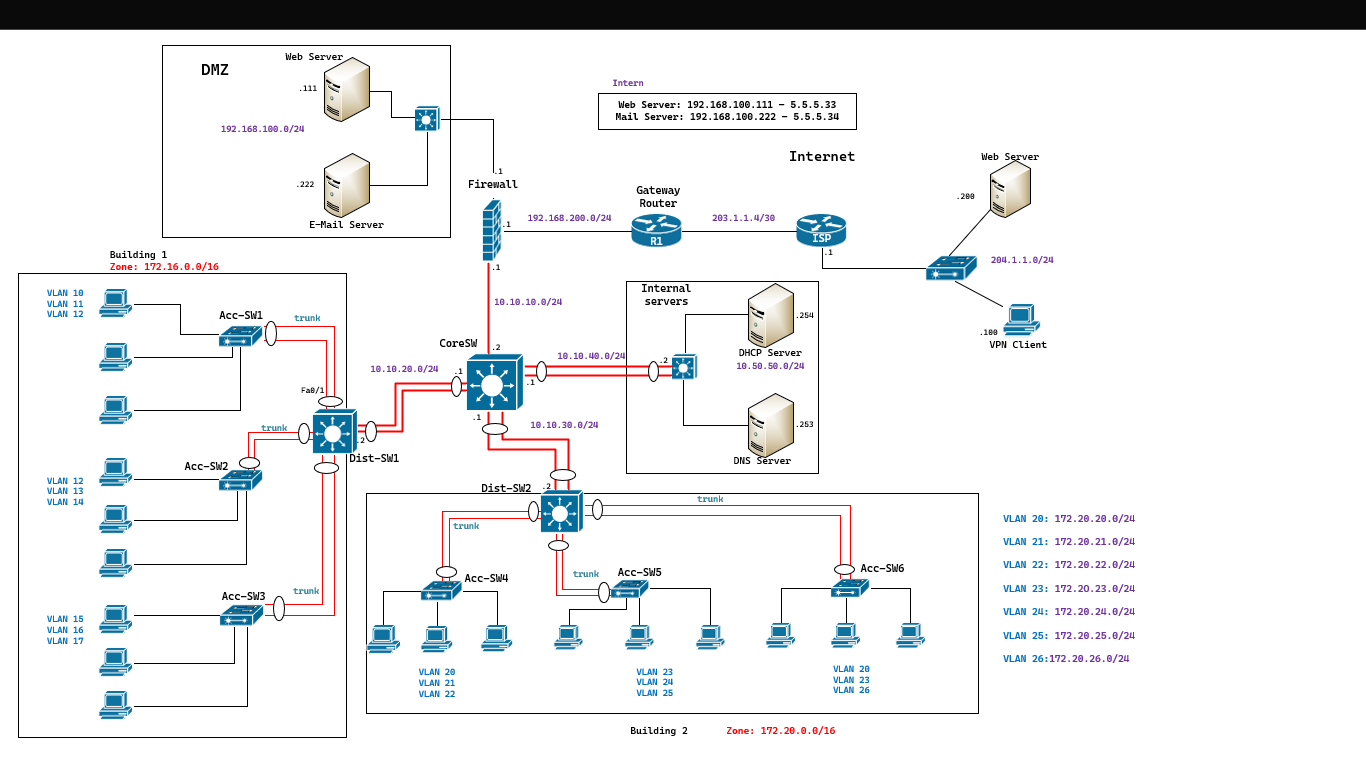
* Hệ thống mạng được thiết kế với chi phí hợp lý, sử dụng thiết bị có hiệu năng cao nhưng vẫn trong giới hạn ngân sách.
* Ưu tiên sử dụng các thiết bị có khả năng mở rộng thay vì phải thay thế toàn bộ hệ thống khi mở rộng.
* Cấu trúc mạng tối ưu hóa số lượng switch, router và firewall, giúp giảm chi phí triển khai và bảo trì trong dài hạn.

1. **SƠ ĐỒ MẠNG**

***Mô hình phân lớp (layered network architecture)*** được sử dụng phổ biến trong thiết kế hệ thống mạng nhằm tổ chức và quản lý hiệu quả hơn các thành phần của mạng.

* Cấu trúc phân lớp bao gồm :
* Tầng lõi (Core Layer) :  cung cấp khả năng chuyển mạch tốc độ cao.
* Tầng phân phối( Distribution Layer): cung cấp các chính sách kết nối.
* Tầng truy cập (Access Layer): Kết nối các thiết bị đầu cuối .

****

****

1. **QUY HOẠCH ĐỊA CHỈ IP**

Quy hoạch địa chỉ IP là một bước quan trọng trong thiết kế và triển khai hệ thống mạng. Việc quy hoạch giúp quản trị viên dễ dàng giám sát và bảo trì hệ thống, dễ dàng xác định vị trí của thiết bị thông qua sơ đồ địa chỉ IP. Ngoài ra còn giúp cải thiện hiệu suất, tối ưu tài nguyên, đảm bảo tính bảo mật và hỗ trợ mở rộng mạng trong tương lai.

* **Hệ thống mạng lõi (Core)**

Hệ thống mạng lõi (Core) có vai trò trung tâm trong toàn bộ hệ thống hạ tầng mạng (network backbone). Hệ thống core layer có tốc độ chuyển mạch cao nhất trong các thành phần thiết kế.

Hệ thống hạ tầng mạng lõi có thể xem xét là thành phần từ router gateway vào firewall, đến core switch và đến khu vực server (bao gồm khu vực DMZ và Internal server).

|  |  |
| --- | --- |
| **TÊN PHÒNG BAN** | **DẢI IP** |
| CoreSW kết nối Firewall | 10.10.10.0/24 |
| CoreSW kết nối Dist-SW1 | 10.20.10.0/24 |
| CoreSW kết nối Dist-SW2 | 10.30.10.0/24 |
| CoreSW kết nối Internal server | 10.40.10.0/24 |

* **Hệ thống mạng phân phối**

Là khu vực trung gian giữa tầng lõi và tầng truy cập. Tầng phân phối có thể gồm nhiều chức năng như:

* Thiết lập các chính sách kết nối, định tuyến
* Khả năng dự phòng và chia tải lưu lượng dữ liệu
* Điểm tập trung các kết nối từ các LAN
* Điểm tập trung cho các kết nối WAN
* Các chính sách về QoS
* Security filtering
* Tóm tắt địa chỉ đến core layer (route summarization)
* Định tuyến cho các VLAN
* Nơi thực hiện các chức năng định tuyến theo chính sách hay phân phối giữa các giao thức định tuyến

|  |  |
| --- | --- |
| **TÊN PHÒNG BAN** | **DẢI IP** |
| Building 1 | 172.16.0.0/24 |
| Building 2 | 172.20.0.0/24 |

* **Hệ thống mạng truy cập**

Lớp truy cập cung cấp cho người dùng truy xuất vào hệ thống mạng, thông thường sử dụng các switch L2. Các chức năng:

1. Chuyển mạch layer 2
2. Khả năng sẵn sàng cao
3. Port security
4. Giới hạn miền quảng bá
5. Kiểm tra ARP
6. VACL (VLAN access control lists)
7. STP
8. PoE
9. Giới hạn tốc độ
10. Phân loại mức độ tin cậy

Thành phần lớp truy cập liên quan đến các switch layer 2 kết nối các các thiết bị người dùng cuối.

**Building 1** (Zone: 172.16.0.0/24)

|  |  |  |
| --- | --- | --- |
| **VLAN** | **TÊN PHÒNG BAN** | **DẢI IP** |
| VLAN 10 | PHÒNG TÀI CHÍNH | 172.16.10.0/24 |
| VLAN 11 | PHÒNG NHÂN SỰ | 172.16.11.0/24 |
| VLAN 12 | PHÒNG IT | 172.16.12.0/24 |
| VLAN 13 | PHÒNG KINH DOANH | 172.16.13.0/24 |
| VLAN 14 | PHÒNG MARKETING | 172.16.14.0/24 |
| VLAN 15 | PHÒNG KỸ THUẬT | 172.16.15.0/24 |
| VLAN 16 | PHÒNG CÔNG ĐOÀN | 172.16.16.0/24 |

**Building 2 (Zone: 172.20.0.0/24)**

|  |  |  |
| --- | --- | --- |
| **VLAN** | **TÊN PHÒNG BAN** | **DẢI IP** |
| VLAN 20 | PHÒNG ĐIỀU HÀNH | 172.20.20.0/24 |
| VLAN 21 | PHÒNG BẢO AN | 172.20.21.0/24 |
| VLAN 22 | PHÒNG KỸ SƯ | 172.20.22.0/24 |
| VLAN 23 | PHÒNG CHĂM SÓC KHÁCH HÀNG | 172.20.23.0/24 |
| VLAN 24 | PHÒNG LOGISTICS | 172.20.24.0/24 |
| VLAN 25 | PHÒNG LAB | 172.20.25.0/24 |
| VLAN 26 | PHÒNG Y TẾ | 172.20.26.0/24 |

**Internal Servers** (10.50.50.0/24)

|  |  |
| --- | --- |
| **THIẾT BỊ** | **ĐỊA CHỈ IP** |
| DNS Server | 10.50.50.253 |
| DHCP Server | 10.50.50.254 |

* **Vùng mạng DMZ** (192.168.100.0/24)

|  |  |
| --- | --- |
| **THIẾT BỊ** | **ĐỊA CHỈ IP** |
| Web Server | 192.168.100.111 |
| Web Server | 192.168.100.222 |

* **Vùng Internet Pool**

|  |  |
| --- | --- |
| **TÊN PHÒNG BAN/ THIẾT BỊ** | **DẢI IP** |
| Firewall nối với Gateway Router | 192.168.200.0/24 |
| Gateway Router nối với Internet | 203.1.1.4/30 |
| Internet | 204.1.1.0/24 |
| VPN Client | 204.1.1.100/24 |
| Web Server | 204.1.1.200/24 |
| Web Server (public) | 5.5.5.33 |
| Mail Server (public) | 5.5.5.34 |

1. **CÁC KỸ THUẬT TRIỂN KHAI**
2. *Cấu hình EtherChannel, Trunking, VLAN (VTP), IP cho các interface VLAN*

**Cấu hình EtherChannel**

**(i) - (iii) Cấu hình L3 EtherChannel trên Core-SW**

**L3 EtherChannel yêu cầu bật chế độ no switchport và gán địa chỉ IP.**

Core-SW(config)# interface range GigabitEthernet1/0/1 - 2

Core-SW(config-if-range)# channel-group 11 mode active

Core-SW(config-if-range)# exit

Core-SW(config)# interface Port-channel 11

Core-SW(config-if)# no switchport

Core-SW(config-if)# ip address 10.1.1.1 255.255.255.0

Core-SW(config-if)# exit

**Lặp lại với các nhóm khác:**

**Po12 (Core-SW ↔ Dist-SW2)**

**Po13 (Core-SW ↔ Server-SW1)**

**(iv) - (v) Cấu hình L2 EtherChannel trên Dist-SW1 & Dist-SW2**

**L2 EtherChannel giữa switchport để truyền VLAN.**

Dist-SW1(config)# interface range GigabitEthernet1/0/1 - 2

Dist-SW1(config-if-range)# channel-group 1 mode active

Dist-SW1(config-if-range)# exit

Dist-SW1(config)# interface Port-channel 1

Dist-SW1(config-if)# switchport mode trunk

Dist-SW1(config-if)# exit

**Lặp lại với Po2, Po3 trên Dist-SW1 và Po4, Po5, Po6 trên Dist-SW2.**

**Cấu hình đường trunk**

**Trunking cho phép nhiều VLAN chạy qua.**

Dist-SW1(config)# interface range GigabitEthernet1/0/3 - 5

Dist-SW1(config-if-range)# switchport mode trunk

Dist-SW1(config-if-range)# switchport trunk allowed vlan all

Dist-SW1(config-if-range)# exit

**Lặp lại trên Dist-SW2.**

**Cấu hình VLAN (VTP)**

**VTP giúp quản lý VLAN tập trung.**

(i) Building 1

Dist-SW1(config)# vtp domain HCMUS1

Dist-SW1(config)# vtp mode server

Dist-SW1(config)# vtp password secret123

Trên Acc-SW1, Acc-SW2, Acc-SW3:

Acc-SW1(config)# vtp domain HCMUS1

Acc-SW1(config)# vtp mode client

Acc-SW1(config)# vtp password secret123

**Tạo VLAN:**

Dist-SW1(config)# vlan 10

Dist-SW1(config-vlan)# name Sales

Dist-SW1(config-vlan)# vlan 11

Dist-SW1(config-vlan)# name HR

**Lặp lại cho VLAN 12 - 16.**

**(ii) Building 2**

**Tương tự với vtp domain HCMUS2 trên Dist-SW2 và các Access Switch.**

*b.**Cấu hình định tuyến cho hệ thống mạng nội bộ*

**(i) Định tuyến trên Firewall**

Firewall(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1

**(ii) Định tuyến trên Core-SW, Dist-SW, Server-SW**

**Sử dụng OSPF để quảng bá mạng.**

Core-SW(config)# router ospf 1

Core-SW(config-router)# network 10.1.1.0 0.0.0.255 area 0

Core-SW(config-router)# exit

**Lặp lại trên Dist-SW1, Dist-SW2 với network tương ứng.**

*c. Cấu hình dịch vụ mạng*

**(i) DHCP cấp IP**

**Trên Core-SW:**

Core-SW(config)# ip dhcp pool VLAN10

Core-SW(dhcp-config)# network 192.168.10.0 255.255.255.0

Core-SW(dhcp-config)# default-router 192.168.10.1

Core-SW(dhcp-config)# exit

**Lặp lại cho các VLAN khác.**

**(ii) Cấu hình local DNS**

**Trên DNS Server:**

DNS(config)# ip host www.xyz.net 192.168.10.100

DNS(config)# ip host mail.xyz.net 192.168.20.100

*d. Cấu hình NAT*

**(i) Cấu hình Router ISP**

ISP-Router(config)# ip route 5.5.5.32 255.255.255.248 192.168.100.1

**(ii) Cấu hình NAT trên Router Gateway R1**

**Cấu hình NAT tĩnh cho DMZ:**

R1(config)# ip nat inside source static 192.168.100.2 5.5.5.33

R1(config)# ip nat inside source static 192.168.100.3 5.5.5.34

**Cấu hình PAT cho mạng nội bộ ra Internet:**

R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255

R1(config)# ip nat inside source list 1 interface GigabitEthernet0/0 overload

**Xác định interface:**

R1(config)# interface GigabitEthernet0/0

R1(config-if)# ip nat outside

R1(config-if)# exit

R1(config)# interface GigabitEthernet0/1

R1(config-if)# ip nat inside

1. **DANH MỤC THIẾT BỊ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **TÊN THIẾT BỊ** | **THÔNG SỐ**  **KỸ THUẬT** | **ĐƠN VỊ TÍNH** | **SỐ LƯỢNG** | **GIÁ TIỀN** |
| **I.                   SWITCH** | | | | | |
| 1 | Cisco Catalyst 9500-40X-E (CoreSW) | Download links total 10/100/1000 or PoE + Copper ports, 40 ports data | Cái | 1 | 630.120.000đ |
| 2 | Aruba ​J9821A  (DistSW) | Layer 3 Advanced (OSPF, BGP, VRRP, PIM), 6 open module slots, Supports 10/100/1000 ports or 144 SFP ports or 48 SFP+ ports or 48 HPE Smart Rate Multi-Gigabit or 12 40GbE ports, or a combination | Cái | 2 | 63.128.000đ |
| 3 | CISCO CATALYST 9200L-24T-4GE  (AccessSW, InternalServerSW, DMZ-SW) | 24 cổng 10/100/1000 Mbps và 4 cổng 1G SFP, ác tính năng layer 3 như OSPF, EIGRP, ISIS, RIP | Cái | 3 | 25.473.000đ |
| **II. ROUTER** | | | | | |
| 4 | Cisco ASR 1001 | 4 cổng 1GbE SFP, 1 cổng 10GbE SFP+ tích hợp, Throughput: 2.5 Gbps (mặc định), nâng cấp lên 5 Gbps với license,Hỗ trợ NAT, PAT, DMZ, OSPF, BGP. | Cái | 1 | 62.000.000đ |
| **III. FIREWALL** | | | | | |
| 6 | Fortigate FG-100D-BDL | 20 x GE RJ45 (bao gồm 1 DMZ, 1 Mgmt, 2 HA, 16 Internal Switch ports,2 x Shared Media Pairs (2 x GE RJ45 + 2 x GE SFP,32GB onboard storage | Cái | 1 | 68.000.000đ |
| **IV. SERVER** | | | | | |
| 7 | Dell PowerEdge R350 (DHCP&DNS Server) | Xeon E-2300, 16GB RAM, 512GB SSD | Cái | 2 | 69.900.000đ |
| **TỔNG: 1.150.595.000đ** | | | | | |

1. **DỰ TOÁN ĐẦU TƯ**
2. **KẾT LUẬN**