TRƯỜNG ĐẠI HỌC
SƯ PHẠM KỸ THUẬT TP. HỒ CHÍ MINH
HCMC University of Technology and Education
HCMUTE

KHOA CÔNG NGHỆ THÔNG TIN

MÔN: THIẾT KẾ MẠNG

BÁO CÁO ĐỒ ÁN CUỐI KỲ

***

THIẾT KẾ MÔ HÌNH MẠNG LAN ĐẢM BẢO TÍNH SẴN SÀNG CHO CÔNG TY CỔ PHẦN MARSU

GVHD: HUỲNH NGUYÊN CHÍNH

SVTH:

Nguyễn Quỳnh Hương Quyên 22162036

Mã lớp: 242CNDE430780_01

Thành phố Hồ Chí Minh, Tháng 5 Năm 2025

MỤC LỤC

THUẬT NGỮ

VLAN (Virtual Local Area Network): Chia mạng vật lý thành các mạng ảo để tăng bảo mật và tối ưu hiệu suất. Giúp cô lập lưu lượng giữa các nhóm thiết bị mà không cần dùng nhiều switch riêng biệt.

ACL (Access Control List): Danh sách quy tắc kiểm soát quyền truy cập vào mạng. Cho phép hoặc chặn lưu lượng dựa trên IP, cổng, giao thức để bảo vệ hệ thống.

OSPF (Open Shortest Path First): Giao thức định tuyến động tìm đường nhanh nhất trong mạng nội bộ (LAN/WAN). Tự động cập nhật bảng định tuyến khi có thay đổi trong mạng.

BGP (Border Gateway Protocol): Giao thức định tuyến động dùng trên mạng Internet, giúp các ISP và doanh nghiệp kết nối nhiều hệ thống mạng khác nhau. Được sử dụng để định tuyến giữa các nhà cung cấp dịch vụ.

HSRP/VRRP (Hot Standby Router Protocol / Virtual Router Redundancy Protocol): Cơ chế dự phòng giúp tự động chuyển đổi router khi một router chính bị lỗi, đảm bảo tính sẵn sàng. HSRP là giao thức độc quyền của Cisco, còn VRRP là tiêu chuẩn mở.

SD-WAN (Software-Defined Wide Area Network): Công nghệ mạng diện rộng điều khiển bằng phần mềm, cho phép kết hợp nhiều đường truyền (MPLS, Internet, 4G/5G). Giúp cải thiện hiệu suất, tính linh hoạt và giảm chi phí so với MPLS truyền thống.

Cloud Backup: Dịch vụ sao lưu dữ liệu lên nền tảng đám mây, giúp phục hồi nhanh khi có sự cố. Đảm bảo dữ liệu không bị mất ngay cả khi thiết bị hỏng hoặc bị tấn công.

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.

Một hệ thống mạng được thiết kế tối ưu không chỉ cần đáp ứng yêu cầu về hiệu suất mà còn phải đảm bảo tính sẵn sàng cao, giúp giảm thiểu rủi ro gián đoạn dịch vụ. Mô hình phân lớp là một phương pháp tiếp cận phổ biến trong thiết kế mạng, giúp tổ chức hệ thống một cách rõ ràng, tối ưu hóa quản lý và nâng cao tính linh hoạt. Bằng cách phân tách mạng thành các lớp chức năng riêng biệt, mô hình này giúp đơn giản hóa việc triển khai, bảo trì và mở rộng hệ thống. Dựa trên hệ thống mạng đã được thiết kế theo mô hình phân lớp trước đó, bài thiết kế này sẽ đề xuất các cải tiến nhằm nâng cao tính sẵn sàng. Các phương pháp như bổ sung đường truyền dự phòng, tối ưu hóa cân bằng tải, sử dụng tường lửa dự phòng và áp dụng cơ chế bảo vệ mạng sẽ được triển khai để đảm bảo hệ thống có thể hoạt động liên tục ngay cả khi xảy ra sự cố.

Thông qua việc cải tiến này, hệ thống mạng không chỉ duy trì hiệu suất cao mà còn có khả năng phục hồi nhanh chóng trước các sự cố, giảm thiểu tối đa thời gian gián đoạn, đáp ứng tốt hơn nhu cầu của doanh nghiệp và người dùng.

2. MỤC TIÊU THIẾT KẾ

Hệ thống mạng đóng vai trò quan trọng trong việc duy trì hoạt động liên tục của doanh nghiệp. Một thiết kế mạng tốt không chỉ đáp ứng yêu cầu về hiệu suất mà còn phải đảm bảo tính sẵn sàng cao, giúp hệ thống có thể tiếp tục vận hành ngay cả khi một hoặc nhiều thành phần gặp sự cố. Do đó, mục tiêu chính của thiết kế này bao gồm:

- *Đảm bảo tính sẵn sàng cao (High Availability - HA):* Hệ thống phải có khả năng tiếp tục hoạt động ngay cả khi một thành phần gặp sự cố hoặc đang trong quá trình bảo trì. Điều này yêu cầu:
  - Thiết bị dự phòng: Các thành phần quan trọng như switch core, router, firewall phải có phương án dự phòng.
  - Kết nối dự phòng: Sử dụng nhiều đường truyền Internet/mạng nội bộ để tránh sự cố do lỗi một đường truyền.
  - Dịch vụ dự phòng: Các dịch vụ quan trọng như DHCP, DNS, máy chủ ứng dụng cần được nhân bản hoặc chạy chế độ HA.
- *Khả năng cách ly lỗi và cô lập sự cố:* Khi xảy ra lỗi, hệ thống phải có khả năng xác định và cô lập nhanh chóng để giảm thiểu ảnh hưởng đến các thành phần khác. Các phương pháp bao gồm:
  - Cấu trúc phân lớp rõ ràng: Phân chia theo mô hình Core - Distribution - Access để giới hạn phạm vi ảnh hưởng khi xảy ra lỗi.
  - Sử dụng VLAN và ACL để cô lập lưu lượng mạng, ngăn ngừa sự lan truyền lỗi giữa các khu vực.
  - Triển khai giao thức định tuyến động (OSPF, BGP) để tự động chuyển hướng lưu lượng khi có lỗi xảy ra.
- *Khả năng khôi phục và roll-back hệ thống:* Hệ thống cần có các cơ chế khôi phục nhanh chóng khi xảy ra sự cố, bao gồm:
  - Backup & Restore: Thực hiện sao lưu cấu hình thiết bị mạng và dữ liệu định kỳ, đảm bảo khả năng phục hồi nhanh chóng.

- Cấu hình Hot-Standby: Sử dụng HSRP/VRRP để đảm bảo khả năng chuyển đổi nhanh giữa các thiết bị dự phòng.
- Hệ thống giám sát và cảnh báo: Triển khai công cụ giám sát (PRTG, Zabbix, Nagios) để phát hiện lỗi sớm và tự động kích hoạt các phương án khắc phục.

- *Cân bằng giữa tính sẵn sàng và chi phí đầu tư:* Việc triển khai các thiết bị, kết nối và dịch vụ dự phòng giúp tăng tính sẵn sàng nhưng cũng kéo theo chi phí đầu tư và vận hành cao hơn. Do đó, cần:
  - Đánh giá mức độ quan trọng của từng dịch vụ để triển khai dự phòng hợp lý.
  - Sử dụng công nghệ SD-WAN hoặc Cloud Backup để tối ưu hóa chi phí trong khi vẫn đảm bảo hiệu suất.
  - Tự động hóa quản lý hệ thống bằng các công cụ quản trị tập trung để giảm tải công việc cho đội ngũ IT.

3. PHÂN TÍCH YÊU CẦU THIẾT KẾ

- **Phạm vi dự án**

Xác định số VLAN và mỗi VLAN phục vụ bao nhiêu thiết bị:

- Building 1: VLAN 10-17
- Building 2: VLAN 20-26
- Mỗi VLAN có thể chứa nhiều thiết bị đầu cuối (PC, laptop).

Số lượng switch và cổng kết nối:

- 6 switch truy cập (Access-SW1 → Access-SW6), mỗi switch có nhiều kết nối với thiết bị.
- Trung bình một switch có thể hỗ trợ 24-48 thiết bị.

Dự đoán số nhân viên:

- Tối thiểu: Nếu mỗi nhân viên sử dụng một thiết bị, có thể có khoảng 200-300 nhân viên.
- Tối đa: Nếu mỗi nhân viên sử dụng nhiều thiết bị (PC, điện thoại, tablet), hệ thống có thể hỗ trợ 300-500 thiết bị.

- **Mục tiêu kỹ thuật**

Độ tin cậy và khả năng chịu lỗi

- Hệ thống mạng phải có khả năng duy trì hoạt động ngay cả khi một hoặc nhiều thành phần gặp sự cố.
- Đảm bảo thời gian hoạt động (uptime) đạt 99.99%, hạn chế tối đa thời gian gián đoạn.
- Ứng dụng các cơ chế High Availability (HA) để tối ưu hiệu suất và khả năng phục hồi.

Thiết kế dự phòng cho thiết bị và kết nối

- Thiết bị dự phòng:

+ Cấu hình các switch, router, firewall, server dự phòng để thay thế ngay khi có lỗi xảy ra.

+ Triển khai giao thức HSRP/VRRP để đảm bảo chuyển đổi router tự động khi cần.

- Kết nối dự phòng:

+ Kết nối mạng theo mô hình Redundant Link nhằm loại bỏ các điểm đơn lỗi (Single Point of Failure – SPOF).

+ Ứng dụng EtherChannel hoặc LACP để tăng băng thông và tính ổn định.

+ Hỗ trợ Multi-WAN hoặc SD-WAN để tối ưu đường truyền Internet.

Thiết kế cân bằng tải và tối ưu hiệu suất

- Sử dụng Load Balancer để phân phối lưu lượng mạng giữa các thiết bị mạng và dịch vụ, giúp:

+ Tránh tình trạng quá tải ở một nút mạng.

+ Đảm bảo truy cập nhanh và ổn định cho các ứng dụng quan trọng.

- Cấu hình QoS (Quality of Service) để ưu tiên lưu lượng quan trọng như VoIP, Video Conference, ứng dụng doanh nghiệp.
- Hỗ trợ các giao thức định tuyến động như OSPF, BGP để tối ưu đường đi của dữ liệu.

Khả năng khôi phục và cô lập lỗi

- Cách ly lỗi:

+ Khi một thiết bị hoặc kết nối gặp sự cố, hệ thống phải cô lập lỗi để tránh ảnh hưởng lan rộng.

+ Sử dụng cơ chế STP (Spanning Tree Protocol) để ngăn chặn các vòng lặp trong mạng.

- Rollback – Khôi phục nhanh chóng:

+ Hệ thống hỗ trợ backup cấu hình tự động, có thể khôi phục nhanh (rollback) khi gặp sự cố.

+ Triển khai Cloud Backup hoặc On-Premises Backup để sao lưu dữ liệu quan trọng.

Quản trị dễ dàng và bảo mật cao

- Quản lý tập trung thông qua hệ thống giám sát (NMS – Network Monitoring System) để theo dõi hiệu suất và cảnh báo lỗi.
- Tích hợp các giải pháp bảo mật như Firewall, IPS/IDS, ACL để bảo vệ hệ thống trước các cuộc tấn công.

Để đảm bảo hệ thống mạng hoạt động ổn định và có khả năng phục hồi khi gặp sự cố, cần thiết kế các thành phần dự phòng trong nhiều khu vực khác nhau của mạng:

- **Mục tiêu kinh doanh**

Giảm thiểu thời gian gián đoạn dịch vụ

- Hệ thống phải duy trì hoạt động liên tục, đảm bảo khách hàng và nhân viên không bị gián đoạn trong công việc.
- Giảm thiểu thời gian downtime bằng các cơ chế dự phòng và khôi phục nhanh chóng.

Tối ưu chi phí đầu tư và vận hành

- Cân bằng giữa hiệu suất và chi phí, tránh đầu tư quá mức nhưng vẫn đảm bảo hệ thống hoạt động ổn định.
- Áp dụng các công nghệ như ảo hóa (Virtualization), SD-WAN, Cloud Backup để giảm chi phí phần cứng và bảo trì.
- Sử dụng mô hình CAPEX và OPEX để tối ưu chi phí đầu tư và vận hành.

Tăng khả năng mở rộng và linh hoạt

- Hệ thống có thể mở rộng dễ dàng khi số lượng người dùng, chi nhánh hoặc dữ liệu tăng lên.

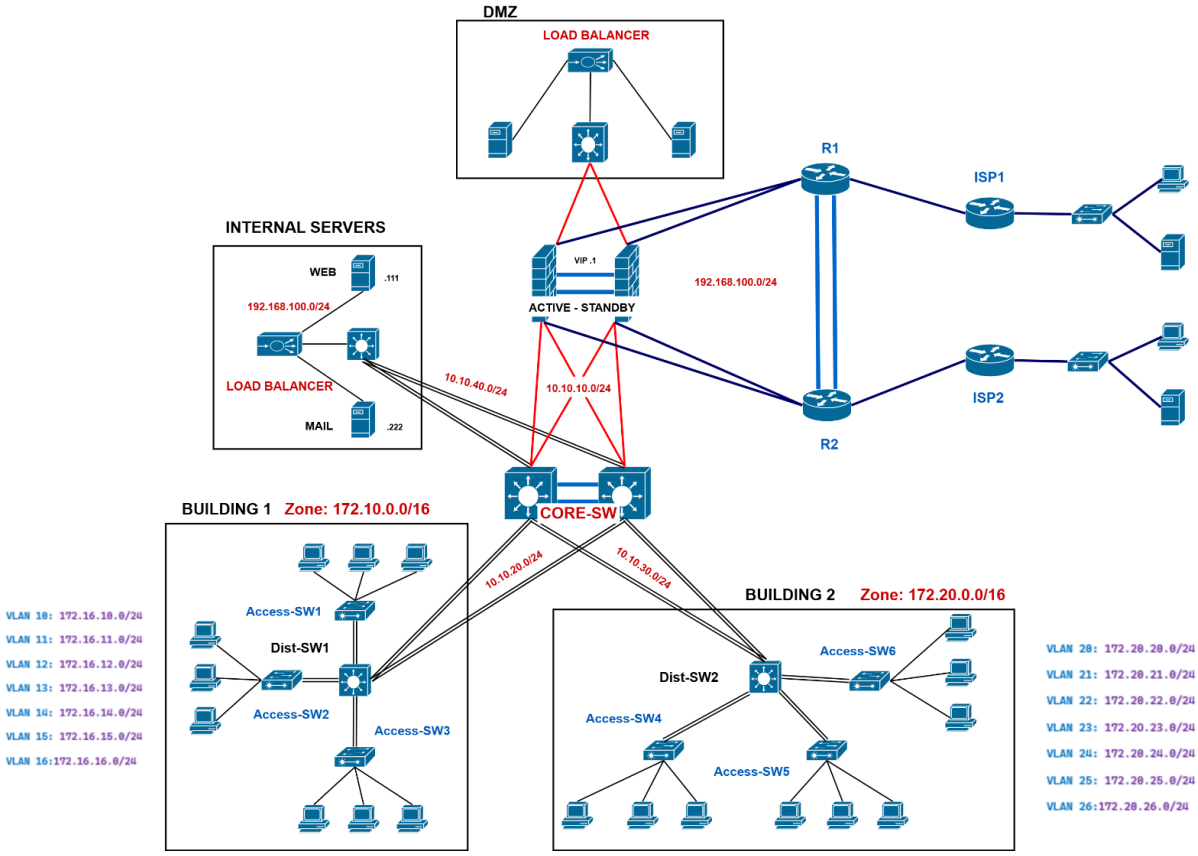
- Hỗ trợ kết nối với các hệ thống Cloud (AWS, Azure, Google Cloud) để mở rộng tài nguyên khi cần.
- Cho phép tích hợp thêm công nghệ mới mà không ảnh hưởng đến hệ thống hiện có.

Đảm bảo an toàn dữ liệu và tuân thủ chính sách

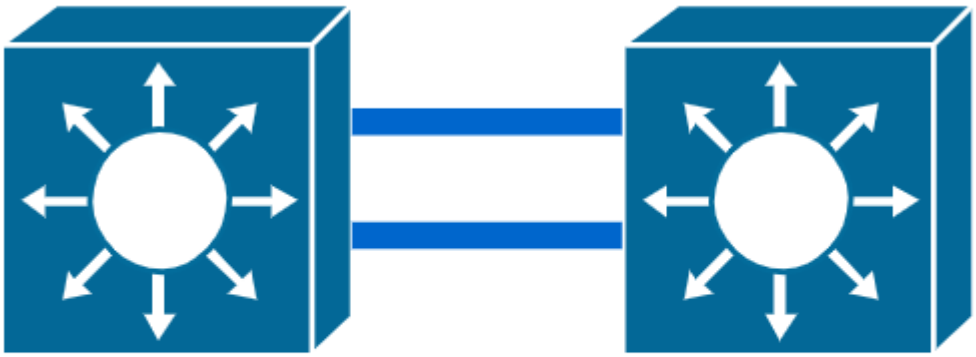
- Hệ thống phải tuân thủ các tiêu chuẩn bảo mật ISO 27001, NIST, GDPR để đảm bảo dữ liệu doanh nghiệp và khách hàng luôn được bảo vệ.
- Hỗ trợ mã hóa dữ liệu (Encryption), bảo mật truy cập (MFA – Multi-Factor Authentication) để tránh rủi ro rò rỉ dữ liệu.
- Triển khai Data Loss Prevention (DLP) để ngăn chặn mất dữ liệu quan trọng.

4. SƠ ĐỒ MẠNG

Tổng Quan



Chi Tiết



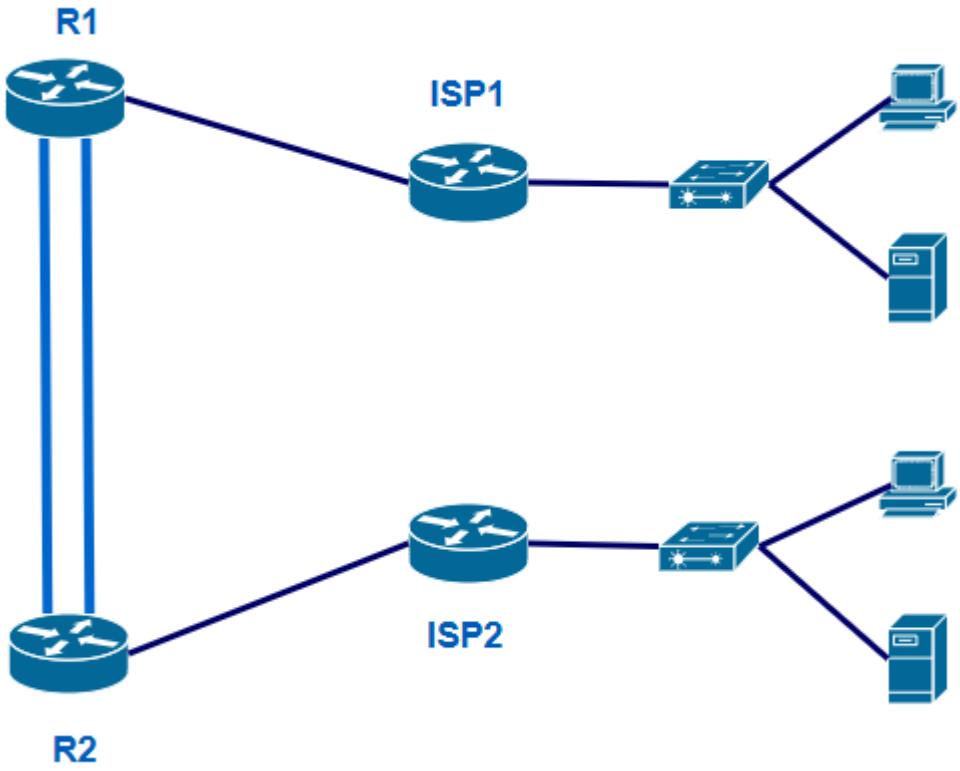
CORE-SW

Mục đích của việc sử dụng 2 CoreSW là để đảm bảo tính sẵn sàng cao HA (High Availability), tính dự phòng (Redundancy), cân bằng tải (Load Balancing) và các yếu tố khác. Việc đảm bảo các yếu tố này giúp cho hệ thống mạng luôn trong trạng thái sẵn sàng, khi một trong 2 thiết bị gặp vấn đề thì thiết bị còn lại sẽ ngay lập tức thay thế để tránh downtime. Ngoài ra, trong trường hợp cần tăng băng thông để đáp ứng nhu cầu của nhiều người dùng cùng một lúc thì 2 CoreSW này sẽ chuyển sang chế độ Active-Active để hoạt động đồng thời. Trong trường hợp cần bảo trì hệ thống hoặc thiết bị thì việc có thiết bị dự phòng sẽ giúp cho hệ thống hoạt động bình thường mà không bị trì trệ.

Tương tự, việc sử dụng 2 firewall cũng nhằm đảm bảo tính sẵn sàng cao HA, tính dự phòng cho hệ thống mạng và tránh Single Point of Failure (SPOF). Firewall đóng vai trò như một *"cửa ngõ"* để các thiết bị bên trong và các dịch vụ bên ngoài có thể giao tiếp với nhau. Do đó, nếu firewall gặp vấn đề trục trặc thì toàn bộ hệ thống mạng có nguy cơ mất kết nối Internet hoặc truy cập các dịch vụ bên ngoài. Để tránh tình trạng này thì việc dự phòng firewall đóng vai trò vô cùng quan trọng. Nó cũng sẽ có 2 chế độ là Active – Standby (máy chính hoạt động, khi máy này gặp vấn đề thì máy dự phòng sẽ thay thế) và chế độ Active – Active

(hai máy sẽ hoạt động cùng lúc, chia tải và cùng xử lý lưu lượng nhưng chế độ này khi cấu hình sẽ phức tạp hơn).

CÔNG NGHỆ	ƯU ĐIỂM	NHƯỢC ĐIỂM
Failover	- Đảm bảo dịch vụ luôn hoạt động khi có lỗi phần cứng/phần mềm - Dễ triển khai, cấu hình	- Phiên kết nối sẽ bị reset nếu không dùng thêm stateful failover - Chuyển đổi có thể gây delay nhỏ
Stateful Failover	- Giữ nguyên phiên kết nối (TCP/UDP) khi chuyển từ Active sang Standby - Trải nghiệm người dùng mượt mà hơn	- Yêu cầu đồng bộ trạng thái thường xuyên giữa 2 firewall (tốn tài nguyên) - Cấu hình phức tạp hơn
VIP (Virtual IP)	- Thiết bị đầu cuối không cần biết firewall nào đang hoạt động - Gateway luôn cố định	- Nếu cấu hình không đúng, có thể xảy ra xung đột IP - Cần cơ chế failover để chuyển đổi IP hiệu quả
Heartbeat/ Sync Link	- Phát hiện lỗi nhanh chóng - Duy trì tính đồng bộ giữa 2 firewall (cấu hình, session)	- Phải có kết nối vật lý riêng biệt giữa 2 firewall - Nếu đường sync bị lỗi có thể gây failover giả (false positive)



Nếu một ISP, thiết bị, hoặc đường truyền gặp sự cố (mất điện, lỗi cáp quang, sự cố hạ tầng), hệ thống vẫn có thể hoạt động nhờ đường Internet từ site dự phòng. Các dịch vụ quan trọng như VPN, email, web server, ứng dụng cloud… không bị gián đoạn, đảm bảo trải nghiệm người dùng và hoạt động doanh nghiệp không bị ảnh hưởng. Khi hoạt động bình thường, cả hai site có thể chia sẻ lưu lượng để tối ưu băng thông và giảm tải cho mỗi đường Internet. Có thể bảo trì một site mà không ảnh hưởng đến kết nối Internet tổng thể của hệ thống. Nếu hệ thống có VPN site-to-site hoặc VPN client-to-site, việc có nhiều site kết nối Internet giúp đảm bảo VPN luôn hoạt động, dù có sự cố ISP hoặc thiết bị ở site chính.

5. 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)

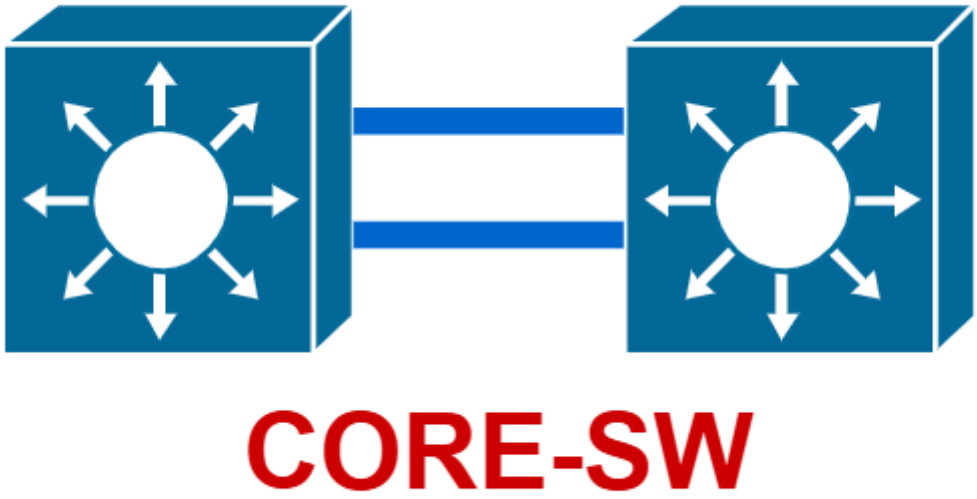
THIẾT BỊ	ĐỊA CHỈ IP
Web Server	192.168.100.111
Web Server	192.168.100.222

- **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 (site 1)	204.1.1.0/24
Internet (site 2)	204.1.2.0/24
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

6. CÁC KỸ THUẬT TRIỂN KHAI

- **Dự phòng CoreSW:**



Dựa trên quy mô của mô hình mạng và yêu cầu của doanh nghiệp, công nghệ ***HSRP (Hot Standby Router Protocol) /VRRP (Virtual Router Redundancy Protocol)*** kết hợp với ***EtherChannel*** mode LACP sẽ được sử dụng để thiết kế dự phòng cho 2 CoreSW này.

HSRP hoặc VRRP cho phép một CoreSW hoạt động chính (Active) và CoreSW còn lại (Standby) sẵn sàng tiếp quản khi Active gặp sự cố. Hai Core Switch chia sẻ một địa chỉ IP ảo (Virtual IP) làm gateway cho các VLAN. Nếu CoreSW Active bị down thì Core Standby tự động trở thành Active giúp đảm bảo tính liên tục cho lưu lượng từ Distribute Switch và Access Switch mà không cần cấu hình lại.

Ngoài ra, EtherChannel giúp tăng băng thông và dự phòng liên kết, dễ triển khai trên hầu hết switch (như Cisco Catalyst). Không phức tạp khi triển khai, phù hợp với mô hình mạng vừa và nhỏ.

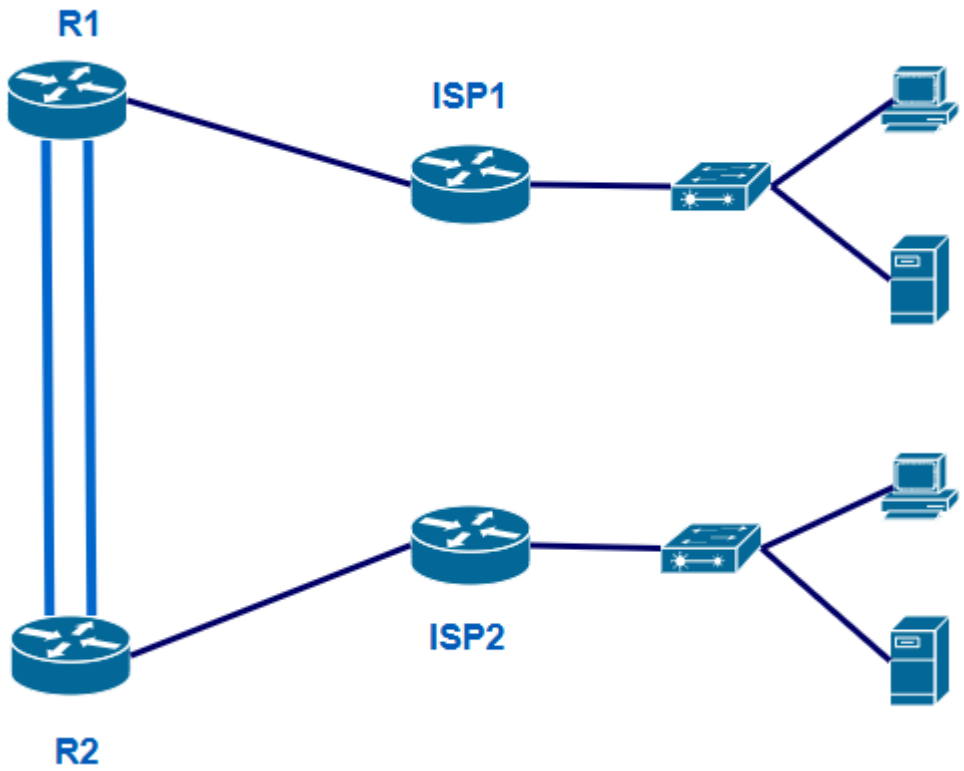
Để kết nối và đảm bảo tính tin cậy và dự phòng cao giữa 2 CoreSW thì sẽ sử dụng StackWise. StackWise sẽ giúp chuyển đổi không gián đoạn (Failover), nó tạo ra một đơn vị logic duy nhất từ hai switch, với một switch hoạt động chính (Active) và switch còn lại sẵn sàng (Standby). Nếu Active Switch gặp sự cố, Standby tự động tiếp quản trong thời gian rất ngắn (thường dưới 1-3 giây), giảm thiểu gián đoạn dịch vụ; đồng bộ cấu hình; dự phòng phần cứng khi một switch trong stack hỏng (do lỗi phần cứng hoặc nguồn), stack vẫn hoạt động với switch còn lại, tăng độ tin cậy cho Core Switch. Ngoài ra còn thuận tiện cho việc quản lý, mở rộng và giảm chi phí vận hành dài hạn.

- **Dự phòng Firewall:**

Active-Standby Failover cho phép 2 Firewall hoạt động như 1 cụm Cluster, trong đó 1 thiết bị hoạt động sẽ có role là Primary, trên firewall trạng thái sẽ là Active, thiết bị này sẽ xử lý toàn bộ traffic trong mạng. Một thiết bị sẽ hoạt động ở chế độ chờ, là Secondary, trên firewall sẽ có role là Standby ready. Secondary sẽ không xử lý traffic, mà chỉ ở chế độ chờ. Khi Primary bị lỗi thì nó sẽ chuyển sang trạng thái active và tiếp tục xử lý dữ liệu. Yêu cầu khi cấu hình HA thì 2 thiết bị phải cùng cấu hình phần cứng, cùng model, có cùng số lượng và loại cổng, cũng như cùng dung lượng RAM.

- Hai thiết bị giao tiếp qua các giao diện heartbeat (thường là cổng chuyên dụng hoặc cổng được chỉ định) để theo dõi trạng thái của nhau. Nếu Primary không phản hồi trong thời gian quy định (heartbeat timeout), Secondary sẽ kích hoạt failover.
- Failover: Khi Primary gặp sự cố (phần cứng, phần mềm, hoặc mất kết nối), Secondary sẽ tự động trở thành Active, nhận các địa chỉ IP và MAC ảo (vMAC) của Primary, thông báo qua ARP để chuyển hướng lưu lượng.
- Session Pickup: Nếu bật tính năng session pickup, các phiên TCP/IP (bao gồm VPN, SIP) có thể được duy trì sau failover, giảm gián đoạn.

- **Dự phòng truy cập Internet cho vùng Internal**



Để đảm bảo dự phòng truy cập Internet cho các site nội bộ, công nghệ ***HSRP (Hot Standby Router Protocol)*** kết hợp với ***IP SLA Tracking*** là lựa chọn phù hợp và dễ triển khai nhất. Lý do là:

- Đơn giản: ***HSRP*** là giao thức phổ biến trên các router/switch Cisco (như Catalyst 9300 hoặc 9200), dễ cấu hình và không yêu cầu sự hợp tác phức tạp với ISP.
- Hiệu quả: ***IP SLA Tracking*** giúp tự động phát hiện sự cố (như mất kết nối ISP1) và kích hoạt failover, giảm phụ thuộc vào thủ công.
- Phù hợp với mô hình: Với hai router (R1, R2) và hai ISP, ***HSRP*** cung cấp dự phòng Active-Standby, đủ cho mạng vừa và nhỏ.

HSRP cho phép R1 hoạt động ở vai trò Active (xử lý lưu lượng ra ISP1), R2 ở vai trò Standby (chờ sẵn sàng). Cả hai chia sẻ một Virtual IP làm default gateway cho các site nội bộ. IP SLA Tracking có chức năng theo dõi trạng thái kết nối đến ISP1 (ví dụ: ping 8.8.8.8). Nếu ISP1 down, IP SLA giảm priority của R1, khiến R2 trở thành Active và chuyển lưu lượng sang ISP2. Chuyển đổi tự động trong vài giây, đảm bảo tính liên tục (Failover).

7. DANH MỤC THIẾT BỊ

- **CoreSW**

C9300-48T-A Specification

Part Number	C9300-48T-A
Product Description	Catalyst 9300 48-port data only, Network Advantage
Total 10/100/1000 or Multigigabit copper ports	48
Default AC power supply	350WAC
Available PoE power	—
Cisco StackWise-480	Yes
Cisco StackPower	Yes
Default power supply	PWR-C1-350WAC
Switching capacity	256 Gbps on 48-port Gigabit Ethernet model
Stacking bandwidth	480 Gbps

Lựa chọn **SWITCH CISCO CATALYST 9300-48T-A** làm CoreSW vì các lý do sau:

- *Hiệu năng cao và khả năng mở rộng*

- Băng thông lớn: Catalyst 9300 cung cấp stacking bandwidth lên đến 480 Gbps (với StackWise-480), đủ để xử lý lưu lượng lớn từ các VLAN, DMZ, và Internal Webs.
- Tùy chọn cổng linh hoạt: Hỗ trợ cổng 1G, 10G, 25G, 40G, và thậm chí 100G (trên các model C9300X), cho phép kết nối EtherChannel hiệu quả với Distribute Switch (như Catalyst 9200).

• *Độ tin cậy và dự phòng cao*

- StackWise: Tích hợp StackWise-480 cho phép hai Core Switch hoạt động như một đơn vị logic, đảm bảo failover nhanh (dưới 1-3 giây) nếu một switch gặp sự cố.
- Cross-Stack EtherChannel: Kết nối EtherChannel giữa các switch trong stack, tăng khả năng dự phòng liên kết.

• Phù hợp với quy mô hệ thống và nhu cầu của doanh nghiệp:

Với vai trò Core Switch, Catalyst 9300 cung cấp hiệu năng và dự phòng vượt trội khi kết hợp với Distribute Switch (như Catalyst 9200) qua EtherChannel và HSRP/VRRP. Hỗ trợ tốt cho các yêu cầu VLAN (311-316), lưu lượng DMZ, và kết nối Internet dự phòng qua R1/R2. Tóm lại, Cisco Catalyst 9300 là lựa chọn lý tưởng nhờ hiệu năng cao, bảo mật mạnh, và khả năng quản lý đơn giản, giúp hệ thống mạng ổn định và sẵn sàng cho việc vận hành.

• **Distribute Switch:**

Switch Cisco C9200-24P-E

Description	Specifications
Performance	
Switching capacity	128 Gbps
Forwarding rate	95.23 Mpps
Virtual Networks	4
Stacking bandwidth	160 Gbps
Features	
Switch fundamentals	Layer 2, Routed Access (RIP, EIGRP Stub, OSPF - 1000 routes), PBR, PIM Stub Multicast (1000 routes), PVLAN, VRRP, PBR, CDP, QoS, FHS, 802.1X, MACsec-128, CoPP, SXP, IP SLA Responder
Connectors	
Connectors and cabling	- 1000BASE-T ports: RJ-45 connectors, 4-pair Cat 5E UTP cabling - 1000BASE-T SFP-based ports: RJ-45 connectors, 4-pair Cat 5E UTP cabling - 100BASE-FX, 1000BASE-SX, -LX/LH, -ZX, -BX10, dense wavelength-division multiplexing (DWDM) and Coarse Wavelength-Division Multiplexing (CWDM) SFP transceivers: LC fiber connectors (single-mode or multimode fiber) - 10GBASE-SR, LR, LRM (only C9200), ER, ZR, DWDM SFP+ transceivers: LC fiber connectors (single-mode or multimode fiber) - SFP+ connector - Cisco StackWise-160 stacking ports: copper-based Cisco StackWise cabling

Hiệu năng phù hợp cho tầng Distribute:

- Băng thông và chuyển tiếp: Catalyst 9200 cung cấp băng thông stacking lên đến 160 Gbps , đủ để xử lý lưu lượng từ các Access Switch trong Building Zone 1 và Zone 2, đồng thời kết nối lên Core Switch (Catalyst 9300) qua EtherChannel.
- Tốc độ cổng: Hỗ trợ cổng 1G (cho Access Switch) và uplink 10G SFP+ (cho Core Switch), phù hợp với yêu cầu băng thông trong hệ thống mạng

Khả năng dự phòng và mở rộng:

- Cross-Stack EtherChannel: Hỗ trợ kết nối EtherChannel với Core Switch (C9300) qua nhiều thành viên stack, tăng khả năng dự phòng liên kết.
- Failover nhanh: Khi stack với Core 9300, thời gian chuyển đổi dưới 1-3 giây, đảm bảo tính liên tục.

Hỗ trợ tính năng Layer 2+

- VLAN và định tuyến tĩnh: Catalyst 9200 quản lý tốt các VLAN (311-316 trong Building Zone 1 và 2) và hỗ trợ định tuyến tĩnh để kết nối với Core Switch, phù hợp cho tầng Distribute.

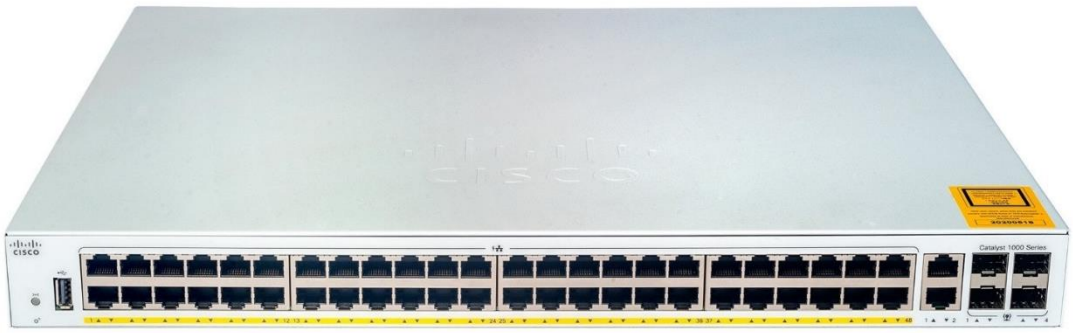
Chi phí hợp lý

- Tiết kiệm hơn 9300/9500: Catalyst 9200 có giá thấp hơn Catalyst 9300 hoặc 9500, phù hợp cho tầng Distribute trong mạng vừa và nhỏ.
- Đầu tư dài hạn: Là dòng switch hiện đại của Cisco, được hỗ trợ lâu dài (IOS XE Dublin 17.12.x, cập nhật gần đây 19/03/2025).

Phù hợp với mô hình

- Catalyst 9200 đáp ứng tốt yêu cầu của Distribute Switch: quản lý VLAN, kết nối EtherChannel với Core Switch, và hỗ trợ lưu lượng từ Access Switch.

- **Access Switch**



SWITCH CISCO C1000-48P-4G-L

C1000-48P-4G-L Datasheet	
Description	Performance
Hardware	
Interface	48x 10/100/1000 Ethernet ports PoE+, 370W PoE budget, 4x 1G SFP uplinks
Console ports	• 1x RJ-45 Ethernet • 1x USB-A port for storage and Bluetooth console
Indicator LEDs	• Per-port status: link integrity, disabled, activity • System status: system
Dimensions (WxDxH in inches)	17.48 x 13.78 x 1.73
Weight	5.43
Memory and processor	
CPU	ARM v7 800 MHz
DRAM	512 MB

Hỗ trợ Power over Ethernet (PoE) mạnh mẽ

- PoE+ (802.3at): C1000-48P-4G-L cung cấp 48 cổng PoE+, mỗi cổng hỗ trợ lên đến 30W, điều này lý tưởng để cấp nguồn cho các thiết bị như:

        - Access Point Wi-Fi (AP) (như Cisco Aironet hoặc Meraki MR series).
        - Camera IP (trong Building Zone 1 và Zone 2).
    - Perpetual PoE: Đảm bảo nguồn PoE không bị gián đoạn ngay cả khi switch khởi động lại, rất hữu ích để duy trì hoạt động của AP hoặc camera.

Hiệu năng phù hợp cho tầng Access

- Số lượng cổng: Cung cấp 48 cổng 1G (RJ45) để kết nối với thiết bị đầu cuối (máy trạm, server, AP, camera) trong Building Zone 1 và Zone 2, đủ cho hầu hết các nhu cầu doanh nghiệp vừa và nhỏ.
- Uplink linh hoạt: Có 4 cổng 1G SFP để kết nối quang hoặc đồng lên Distribute Switch (Catalyst 9200), đáp ứng băng thông 1G cho lưu lượng nội bộ.
- Khả năng chuyển tiếp: Hiệu năng chuyển tiếp đạt 77.38 Mpps, đủ để xử lý lưu lượng Layer 2 từ các VLAN (311-316).

Hỗ trợ tính năng Layer 2 cần thiết

- VLAN: Hỗ trợ tối đa 4094 VLAN, quản lý tốt các VLAN
- Spanning Tree Protocol (STP)
- QoS: Hỗ trợ Quality of Service (QoS) để ưu tiên lưu lượng

Chi phí hợp lý

- Tiết kiệm hơn 9200L: Catalyst 1000 Series có giá thấp hơn Catalyst 9200L, phù hợp cho tầng Access nơi không cần hiệu năng quá cao.
- Đầu tư hiệu quả: Cung cấp PoE+ và tính năng Layer 2 cần thiết với chi phí tối ưu, phù hợp cho mạng vừa và nhỏ.

Quản lý dễ dàng

- Tương thích với Cisco Catalyst Center: Hỗ trợ quản lý tập trung qua Cisco Catalyst Center, đồng bộ với Distribute Switch (C9200) và Core Switch (C9300).

- Giao diện linh hoạt: Quản lý qua CLI, GUI (web), hoặc SNMP, dễ dàng cho quản trị viên.

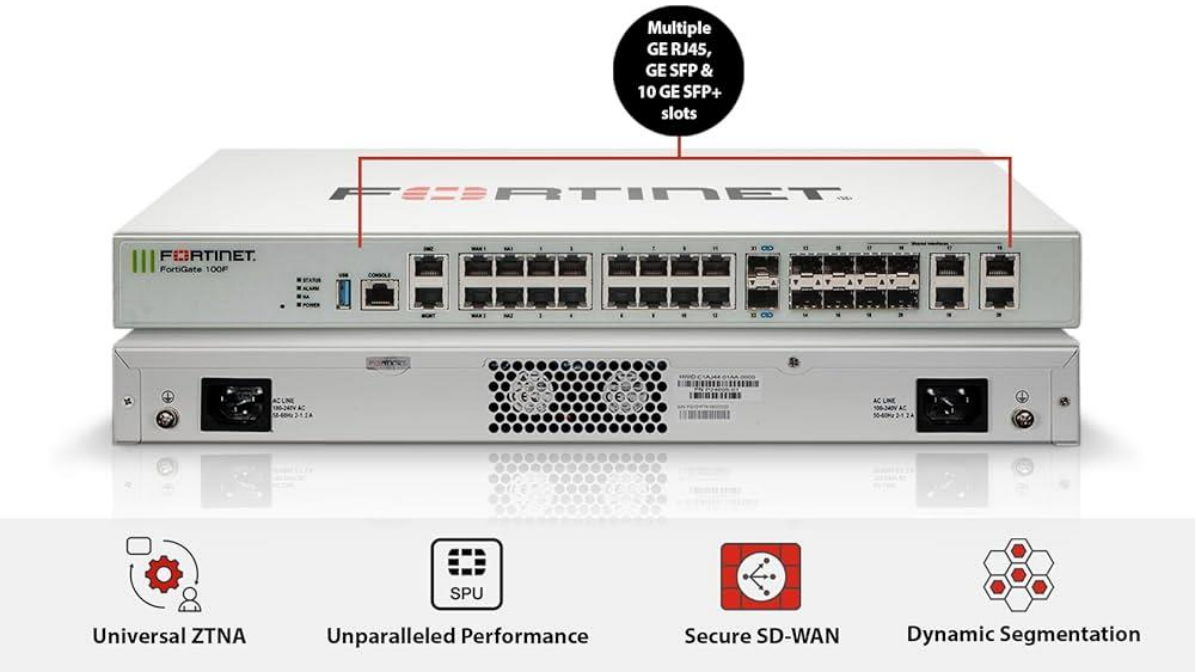
Độ tin cậy và hỗ trợ lâu dài

- Thiết kế bền vững: Catalyst 1000 được thiết kế cho môi trường doanh nghiệp, với độ tin cậy cao (MTBF hàng triệu giờ).
- Hỗ trợ từ Cisco: Là dòng switch hiện đại, được cập nhật thường xuyên (IOS XE Dublin 17.12.x, cập nhật gần đây 19/03/2025), đảm bảo tương thích với công nghệ mới.

Phù hợp với nhu cầu sử dụng

- PoE cần thiết: Nếu Building Zone 1 và Zone 2 có nhiều thiết bị cần cấp nguồn (AP, camera,..)
- Uplink 1G đủ dùng: 4 cổng 1G SFP đáp ứng kết nối lên Distribute Switch, phù hợp nếu lưu lượng không quá cao.

- **Firewall**



FORTINET FORTIGATE 100F

Interfaces and Modules	
GE RJ45 Ports	12
GE RJ45 Management/HA/DMZ Ports	1 / 2 / 1
GE SFP Slots	4
10 GE SFP+ Slots	2
GE RJ45 WAN Ports	2
GE RJ45 or SFP Shared Ports	4
Console Port	1
USB Port	1
System Performance and Capacity	
Firewall Throughput (1518 / 512 / 64 byte, UDP)	20 / 18 / 10 Gbps
Firewall Latency (64 byte, UDP)	5 µs
Firewall Throughput (Packet per Second)	15 Mpps

Hiệu năng phù hợp cho mạng doanh nghiệp vừa và nhỏ

- Firewall Throughput: 20 Gbps, đủ để xử lý lưu lượng từ DMZ Load Balancer, Internal Servers và các VLAN trong Building Zone 1, Zone 2
- IPS Throughput: 2.7 Gbps, đảm bảo khả năng kiểm tra gói tin và bảo vệ chống xâm nhập mà không làm chậm mạng.
- VPN Throughput: 11.5 Gbps (IPsec), hỗ trợ kết nối an toàn cho người dùng từ xa hoặc giữa các site nếu cần.
- Concurrent Sessions: 1.5 triệu kết nối đồng thời, phù hợp cho môi trường có nhiều thiết bị (máy trạm, server, AP).

Hỗ trợ HA Active-Standby với FGCP

- FortiGate 100F hỗ trợ FortiGate Clustering Protocol (FGCP) để triển khai HA Active-Standby, đáp ứng yêu cầu dự phòng:
  - Primary (Active) xử lý toàn bộ lưu lượng, Secondary (Standby) chờ sẵn sàng.
  - Failover tự động khi Primary gặp sự cố (thời gian chuyển đổi dưới 1 giây nếu cấu hình tối ưu).

- Session Pickup: Duy trì các phiên kết nối (TCP/IP, VPN) sau failover, đảm bảo tính liên tục cho DMZ và Internal Webs.

Số lượng cổng phù hợp

- Cổng đa dạng: Cung cấp 18 cổng GE RJ45 (bao gồm 2x WAN, 2x DMZ, 14x LAN) và 4 cổng GE SFP, đủ để:
  - Kết nối WAN1 với R1/ISP1 và WAN2 với R2/ISP2
  - Kết nối DMZ1/DMZ2 với Load Balancer
  - Kết nối LAN với Core Switch
- Hỗ trợ quang: 4 cổng SFP cho phép kết nối quang với Core Switch hoặc R1/R2, phù hợp nếu dùng cáp quang.

Hỗ trợ Dual WAN cho dự phòng ISP

- Link Health Monitor: Tự động theo dõi trạng thái ISP1 và ISP2 chuyển đổi sang ISP2 nếu ISP1 bị down.
- Policy-Based Routing: Ưu tiên ISP1 và dùng ISP2 làm backup, đảm bảo dự phòng hiệu quả mà không cần cấu hình phức tạp.

Bảo mật toàn diện

- Next-Generation Firewall (NGFW): Tích hợp tường lửa trạng thái, chống xâm nhập (IPS), lọc nội dung web, và bảo vệ chống mã độc (anti-malware), rất quan trọng để bảo vệ DMZ và Internal Servers.
- FortiGuard Threat Intelligence: Cập nhật mối đe dọa theo thời gian thực, giảm nguy cơ tấn công.
- SSL Inspection: Kiểm tra lưu lượng mã hóa, bảo vệ trước các mối đe dọa ẩn trong HTTPS.

Tương thích với hạ tầng Cisco

- FortiGate 100F hoạt động tốt với Core Switch (Catalyst 9300) và Distribute Switch (Catalyst 9200), hỗ trợ VLAN (311-316) và giao thức định tuyến tĩnh.
- Có thể tích hợp với HSRP/IP SLA trên R1/R2, tận dụng cấu hình dự phòng ISP của router.

Chi phí hợp lý

- So với các model cao hơn như FortiGate 200F (27 Gbps), FortiGate 100F có giá thành thấp hơn nhưng vẫn đáp ứng tốt yêu cầu của mạng vừa và nhỏ.
- So với FortiGate 60F (10 Gbps), 100F mạnh hơn về hiệu năng và số cổng, phù hợp hơn cho hệ thống mạng.

- **Router**

ROUTER CISCO ISR 1111-4P

Mã sản phẩm	C1111-8P	C1111-4P
WAN GE	1	1
Combo WAN GE/SFP	1	1
ADSL2/VDSL2+	Không	Không
LTE	Không	Không
802.11ac	Không	Không
Số cổng LAN	8	4
PoE	4	2
PoE+	2	1
USB 3.0 AUX/console	Có	Có

- Hỗ trợ HSRP/IP SLA: Dễ dàng cấu hình HSRP để R1 Active, R2 Standby, và IP SLA để theo dõi trạng thái ISP1/ISP2.

- Hiệu năng: Firewall throughput lên đến 1.2 Gbps, đủ cho lưu lượng từ DMZ, Internal Servers, và các VLAN.
- Cổng kết nối:

• 4 cổng GE RJ45 (1 cổng WAN cho ISP, 3 cổng LAN cho FortiGate/Core Switch).
• 1 cổng GE SFP (dùng nếu ISP yêu cầu cáp quang).

- Tính năng: Hỗ trợ NAT, QoS, và VPN (nếu cần), phù hợp cho định tuyến WAN.

• **Access Point (WIFI)**

Cisco Meraki MR36 WiFi 6 Access Point

802.11ax, 802.11ac Wave 2 and 802.11n Capabilities	• DL-OFDMA**, UL-OFDMA**, TWT support**, BSS Coloring** • 2 x 2 multiple input, multiple output (MIMO) with two spatial streams • SU-MIMO, UL MU-MIMO** and DL MU-MIMO support • Maximal ratio combining (MRC) & beamforming • 20 and 40 MHz channels (802.11n); 20, 40, and 80 MHz channels (802.11ac Wave 2); 20, 40 and 80 MHz channels (802.11ax) • Up to 1024-QAM on both 2.4 GHz & 5 GHz bands • Packet aggregation
Power	• Power over Ethernet: 37 - 57 V (802.3af compatible) • Alternative: 12 V DC input • Power consumption: 15W max (802.3at) • Power over Ethernet injector and DC adapter sold separately
Interfaces	• 1x 10/100/1000 BASE-T Ethernet (RJ45) • 1x DC power connector (5.5 mm x 2.5 mm, center positive)

Lý do chọn:

- Hỗ trợ **WiFi 6 (802.11ax)**, cung cấp tốc độ cao (lên đến 3.5 Gbps), phù hợp với môi trường nhiều người dùng.
- Tương thích với Cisco Catalyst switches qua PoE+ (C1000-48P-4G-L cung cấp 30W/cổng).
- Quản lý tập trung qua **Meraki Cloud Dashboard**, dễ dàng cấu hình VLAN (10-17, 20-26) và tích hợp với Cisco Catalyst Center.
- Hỗ trợ bảo mật: WPA3, 802.1X, tích hợp với FortiGate 100F qua VLAN tagging.
- Độ tin cậy cao: Tự động tối ưu kênh và công suất, giảm nhiễu trong môi trường nhiều AP.

Thông số kỹ thuật:

- Tốc độ: 2.4 GHz (574 Mbps) + 5 GHz (2.4 Gbps).
- Cổng: 1x 1Gbps Ethernet (PoE+).
- Số lượng người dùng đồng thời: ~100-150 thiết bị/AP.
- Phạm vi phủ sóng: ~100-150m² (tùy môi trường).

- **Server**

Server Dell PowerEdge R760

Thông số kỹ thuật mạnh mẽ:

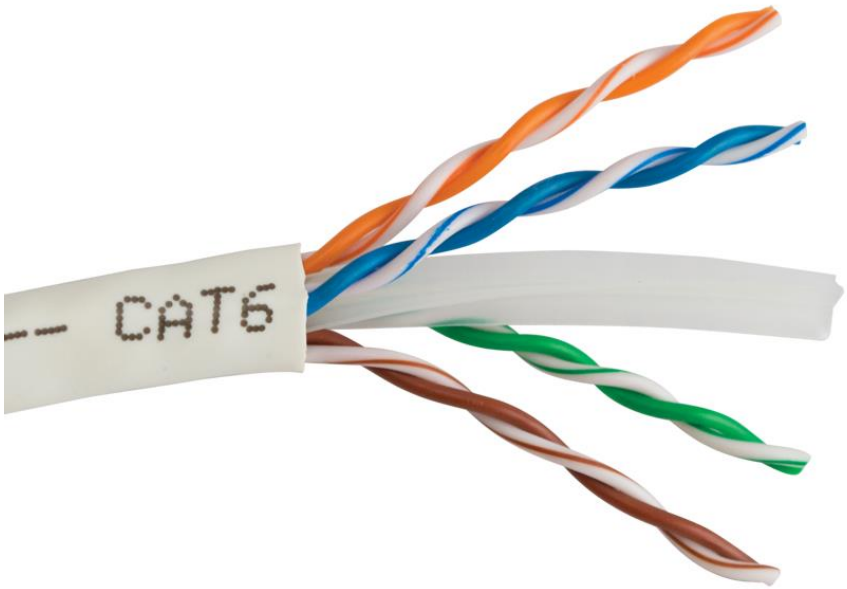
- CPU: 2 x Intel Xeon Gold 6430 (32 core/CPU, 2.1GHz), tổng cộng 64 core, cung cấp khả năng xử lý mạnh mẽ cho các dịch vụ DHCP (phân phối địa chỉ IP) và DNS (giải quyết tên miền) trong mạng có 200-500 thiết bị.
- RAM: 8 x 128GB DDR5 (tổng 1TB, tốc độ 4800MT/s hoặc 5600MT/s), đảm bảo khả năng xử lý đồng thời nhiều yêu cầu DNS/DHCP và hỗ trợ các ứng dụng khác nếu cần (ví dụ: quản lý mạng, giám sát).
- Khả năng lưu trữ: Hỗ trợ nhiều cấu hình ổ cứng (HDD/SSD NVMe), cho phép lưu trữ bản ghi DNS, log DHCP, và dữ liệu sao lưu cấu hình mạng.

Lý do chọn: DHCP và DNS là các dịch vụ quan trọng, yêu cầu xử lý nhanh và ổn định để tránh gián đoạn mạng. PowerEdge R760 với CPU đa nhân và RAM lớn đảm bảo hiệu suất cao, ngay cả khi hệ thống mở rộng hoặc tải tăng đột biến.

- **Dây cáp**

Hệ thống mạng sử dụng Cisco Catalyst switches, FortiGate firewall, và router Cisco ISR 1111-4P, kết nối qua cáp Ethernet (Cat6/Cat6a) và cáp quang (SFP+ modules). Dựa trên sơ đồ mạng và danh mục thiết bị, các loại cáp cần thiết bao gồm:

a. *Cáp Ethernet (Cat6/Cat6a)*



- Kết nối từ Access Switch (C1000-48P-4G-L) đến thiết bị đầu cuối (PC, laptop, AP, camera IP).
- Kết nối giữa Distribute Switch (C9200) và Access Switch.
- Kết nối từ Core Switch (C9300) đến FortiGate 100F (cổng GE RJ45).

Lý do chọn Cat6/Cat6a:

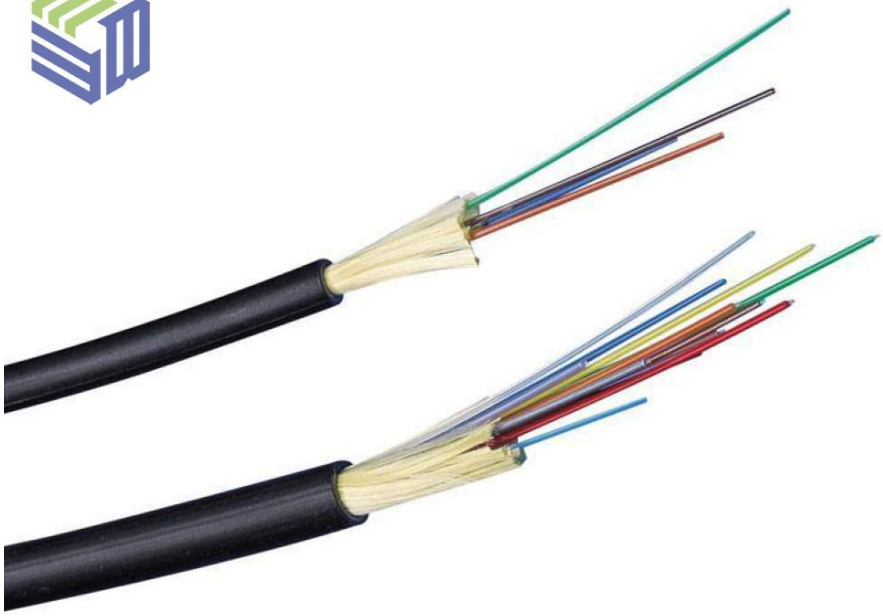
- Hỗ trợ tốc độ 1Gbps (Cat6) và 10Gbps (Cat6a, khoảng cách <55m), phù hợp với cổng 1G trên C1000/C9200 và 10G trên C9300.
- Tương thích với PoE+ để cấp nguồn cho AP và camera IP.
- Chi phí hợp lý, phổ biến cho mạng doanh nghiệp.

b. *Cáp Quang (SFP+ và Patch Cord)*

- Kết nối giữa Core Switch (C9300) và Distribute Switch (C9200) qua cổng 10G SFP+.
- Kết nối từ FortiGate 100F (cổng GE SFP) đến Core Switch hoặc router (nếu dùng cáp quang).
- Kết nối StackWise-480 giữa 2 Core Switch (C9300) và StackWise-160 giữa 2 Distribute Switch (C9200).

- Loại cáp:

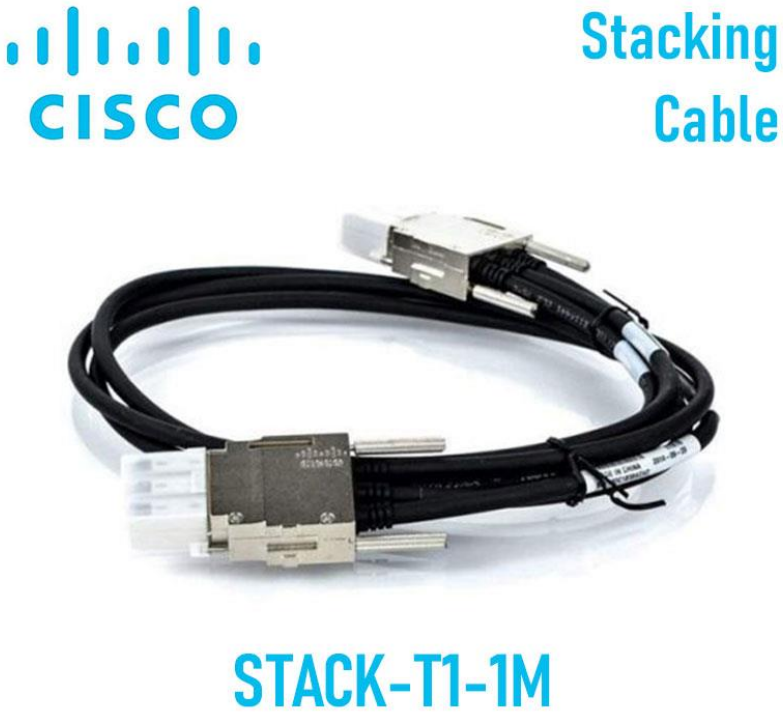
- Cáp quang multimode OM3/OM4 (cho module SFP-10G-SR-S và GLC-SX-MMD).



- Hỗ trợ 10Gbps (300m với OM3) và 1Gbps (550m với GLC-SX-MMD).
- Patch cord quang LC-LC (đầu nối cho SFP+ modules).

- Cáp StackWise (dành riêng cho Cisco Catalyst):

+ StackWise-480 cho Core Switch (C9300): 2 cáp (~0.5-1m).



+ StackWise-160 cho Distribute Switch (C9200): 4 cáp (~0.5-1m, 2 cáp/2 switch).

c. Cáp Heartbeat cho Firewall

- Kết nối heartbeat/sync giữa 2 FortiGate 100F để hỗ trợ HA Active-Standby.
- Loại: Cáp Ethernet Cat6 (cổng GE RJ45 trên FortiGate 100F).

- **Tủ rack**

Tủ Rack APC NetShelter SX 42U (AR3100)

- Kích thước 42U (cao ~2m), đủ chứa tất cả thiết bị và dự phòng không gian cho AP controller, UPS, hoặc thiết bị mở rộng.
- Tương thích với thiết bị Cisco, FortiGate, Dell (hỗ trợ rack-mount 1U/2U).
- Hệ thống làm mát: Cửa lưới và quạt tích hợp, phù hợp cho phòng server.
- Quản lý cáp: Hỗ trợ cable management để giữ dây gọn gàng.
- Bảo mật: Có khóa, ngăn truy cập trái phép.

Stt	Tên thiết bị	Thông số Kỹ thuật	Đơn vị tính	Số lượng	Giá tiền
SWITCH					
1	Switch Cisco Catalyst 9300-48T-A (CoreSW)	Catalyst 9300 48-port data only, Network Advantage	Cái	2	257.518.520 x 2 = 515.037.040 vnd

2	Switch Cisco C9200-24P-E (DistSW)	24x Port 10/100/1000, PoE+ 370W, Network Essentials include Layer 2, Routed Access (RIP, EIGRP Stub, OSPF, 1000 routes, 10GBASE-SR, LR, LRM (only C9200), ER, ZR, DWDM SFP+ transceivers: LC fiber connectors (single-mode or multimode fiber)	Cái	4	106.996.400 x 4 = 427.985.600 vnđ
3	Switch Cisco C1000-48P-4G-L (AccessSW)	RJ45 Port: 48 x10/100/1000 RJ45.SFP Port: 4 x 1G SFP+.Forwarding bandwidth: 52 Gbps.Switching bandwidth: 104 Gbps.Forwarding rate: 77.38 Mpps.Fan: Fanless.Management: CLI, SSH, Telnet, WebUI, App Mobile	Cái	8	42.241.250 x 8 = 337.930.000 vnđ
ROUTER					
4	Cisco ISR C1111-4P	Cổng WAN: 1 cổng GE; Cổng WAN/LAN combo: 1 cổng GE/SFP; Cổng LAN: 4 cổng GE.; Cổng PoE: 2 cổng; Cổng PoE+: 1 cổng; DRAM: 4GB; Flash: 4GB.	Cái	2	12.834.240 x 2 = 25.668.480 vnđ
FIREWALL					
6	Firewall FortiGate FG-100F	2 x 10GE SFP+ Slots, 18 x GE RJ45 and 8x 1GE SFP	Cái	2	66.500.000 x 2 = 133.000.000 vnđ

		and 4x GE RJ45/SFP Shared Media Pairs			
SERVER					
7	Dell Poweredge R760 (DHCP&DNS Server)	RAM: 8 x 128GB DDR5 (tổng 1TB, tốc độ 4800MT/s hoặc 5600MT/s) CPU: 2 x Intel Xeon Gold 6430 (32 core/CPU, 2.1GHz)	Cái	1	1.430.000.000 vnđ
MODUL					
8	Cisco SFP-10G-SR-S 10GBASE-SR SFP+ 850nm 300m DOM Transceive	Module quang Cisco SFP-10G-SR-S (SFP 10G SR S) Transceiver SFP+ for Multi mode, 850-nm, LC Duplex, 300m	Cái	15	16.880.500 x 15 = 253.207.500 vnđ
9	Cisco GLC-SX-MMD	Hỗ trợ 1Gbps, 550m, multi-mode	Cái	26	5.000.000 x 26 = 130.000.00 vnđ
ACCESS POINT					
10	Cisco Meraki MR36 WiFi 6 Access Point	Tốc độ: 2.4 GHz (574 Mbps) + 5 GHz (2.4 Gbps). Cổng: 1x 1Gbps Ethernet (PoE+). Số lượng người dùng đồng thời: ~100-150 thiết bị/AP. Phạm vi phủ sóng: ~100-150m² (tùy môi trường).	Cái	16	15.000.000 x 16 = 240.000.000 vnđ
DÂY CÁP					

11	Cat6/Cat6a	Hỗ trợ tốc độ 1Gbps (Cat6) và 10Gbps (Cat6a, khoảng cách <55m)	Mét	3000	3000 x 10.000 = 30.000.000 vnđ
12	Cáp quang multimode OM3/OM4	Hỗ trợ 10Gbps (300m với OM3) và 1Gbps (550m với GLC-SX-MMD).	Mét	50	50 x 50.000 = 2.500.000 vnđ
13	Patch cord quang LC-LC (đầu nối cho SFP+ modules)		Cái	12	12 x 150.000 = 1.800.000 vnđ
14	Cáp StackWise-480 (0.5m)		Cái	2	2 x 5.000.000 = 10.000.000 vnđ
15	Cáp StackWise-160 (0.5m)		Cái	4	4 x 3.000.000 = 12.000.000 vnđ
TỦ RACK					
16	Tủ Rack APC NetShelter SX 42U (AR3100)	Kích thước **42U** (cao ~2m), đủ chứa tất cả thiết bị và dự phòng không gian cho AP controller, UPS, hoặc thiết bị mở rộng. Tương thích với thiết bị Cisco, FortiGate, Dell (hỗ trợ rack-mount 1U/2U)	Cái	3	3 x 30.000.000 = 90.000.000 vnđ
TỔNG: 3.639.128.620 vnđ					

8. DỰ TOÁN ĐẦU TƯ

- **Chi phí thuê LOAD BALANCER trong vòng 1 năm**

- Chi phí thuê balancer là 3,5 triệu VNĐ/tháng.
- Thời gian thuê: 12 tháng.
- Tính toán:
    - **3,5 triệu VNĐ x 12 tháng = 42 triệu VNĐ.**

Vậy, chi phí thuê LOAD BALANCER trong 1 năm là 42 triệu VNĐ.

- **Tiền thuê license Network Advantage và Network Essential**

- Network Essential: Đây là license cơ bản cho các tính năng Layer 2/3 cơ bản trên switch Cisco (như Catalyst 9300/9200). Giá thường dao động từ 50-100 USD/thiết bị/năm (khoảng 1,3-2,6 triệu VNĐ/thiết bị/năm, tỷ giá 1 USD = 26,000 VNĐ).
- Network Advantage: Bao gồm thêm các tính năng nâng cao như SD-Access, QoS, và Layer 3 đầy đủ. Giá thường cao hơn, dao động từ 200-400 USD/thiết bị/năm (khoảng 5,2-10,4 triệu VNĐ/thiết bị/năm).

- Giả định số lượng thiết bị:
    - 2 Core Switch (Catalyst 9300) và 2 Distribute Switch (Catalyst 9200) trong mô hình. Tổng cộng là 4 switch.
    - Nếu tất cả 4 switch cần license, chi phí sẽ được tính dựa trên số lượng này.
- Ước tính chi phí:
    - Network Essential (giả sử 2 triệu VNĐ/thiết bị/năm):
        - 2 triệu VNĐ x 4 thiết bị = 8 triệu VNĐ/năm.
    - Network Advantage (giả sử 8 triệu VNĐ/thiết bị/năm):
        - 8 triệu VNĐ x 4 thiết bị = 32 triệu VNĐ/năm.

- Lưu ý: Giá thực tế có thể cao hơn nếu cần license cho các module bổ sung (VD: SFP+, StackWise) hoặc gia hạn lâu dài.

TỔNG DỰ TOÁN ĐẦU TƯ

- Số tiền mua thiết bị: 3,639,128,620 VNĐ.
- Chi phí thuê load balancer 1 năm: 42,000,000 VNĐ.
- Chi phí license Network Essential (ước tính): 8,000,000 VNĐ.
- Chi phí license Network Advantage (ước tính): 32,000,000 VNĐ.
- Chi phí license cho Fortigate 100F (2 thiết bị) 1 năm: 30,000,000 VNĐ
- Chi phí License cho WiFi (Meraki MR36) (16 thiết bị/năm): 40,000,000 VNĐ
- Tổng cộng (ước tính tối đa): **= 3,791,128,620 VNĐ.**

9. KẾT LUẬN

Việc xây dựng hệ thống mạng cho doanh nghiệp vừa và nhỏ với mục tiêu đảm bảo tính sẵn sàng đã được thực hiện một cách toàn diện, dựa trên việc lựa chọn và tích hợp các thiết bị hiện đại cùng với các giải pháp dự phòng hiệu quả. Hệ thống được thiết kế theo *mô hình phân cấp 3 lớp* với Core Switch (Cisco Catalyst 9300), Distribute Switch (Cisco Catalyst 9200), và Access Switch (Cisco Catalyst 1000), kết hợp với firewall FortiGate 100F, Load Balancer F5 BIG-IP, và server Dell PowerEdge R760, đảm bảo khả năng xử lý lưu lượng lớn, bảo mật cao và mở rộng linh hoạt. Các giải pháp như HSRP/IP SLA, HA Active-Standby, và StackWise đã được triển khai để tối ưu hóa thời gian hoạt động và giảm thiểu gián đoạn khi xảy ra sự cố.

Với tổng chi phí đầu tư ước tính khoảng 3,252,828,620 VNĐ cho thiết bị, cộng thêm 42 triệu VNĐ cho thuê Load Balancer và khoảng 40 triệu VNĐ cho các license Network Essential và Advantage trong vòng 1 năm (tổng cộng khoảng 3,334,828,620 VNĐ), hệ thống không chỉ đáp ứng nhu cầu hiện tại mà còn tạo nền tảng cho sự phát triển bền vững trong tương lai. Việc sử dụng modul quang (SFP-10G-SR và SFP-GE-SX) giữa các tầng mạng đảm bảo băng thông cao và độ tin cậy, trong khi các biện pháp bảo mật như WAF, DDoS protection, và FortiGuard giúp bảo vệ doanh nghiệp trước các mối đe dọa an ninh mạng.

Hệ thống này không chỉ nâng cao hiệu suất hoạt động của các khu vực như DMZ, Internal Servers, Building Zone 1 và Zone 2, mà còn đảm bảo tính sẵn sàng cao thông qua cơ chế dự phòng đa tầng. Với thiết kế này, doanh nghiệp vừa và nhỏ có thể yên tâm về tính liên tục trong kinh doanh, đồng thời sẵn sàng thích nghi với các yêu cầu mở rộng hoặc nâng cấp trong tương lai.