BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP. HCM
KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO ĐỒ ÁN CUỐI KỲ

MÔN HỌC: THIẾT KẾ MẠNG

GVHD: Huỳnh Nguyên Chính

MÃ HP: CNDE430780

SINH VIÊN THỰC HIỆN

HỌ VÀ TÊN	MSSV
Nguyễn Minh Tâm	22162039

MỤC LỤC

I. KHẢO SÁT VÀ PHÂN TÍCH HIỆN TRẠNG 1
1. Tổng quan công ty THACO: 1
2. Phân tích yêu cầu 1
3. Phân tích hiện trạng 2
II. SƠ ĐỒ THIẾT KẾ MẠNG VÀ TRIỂN KHAI THIẾT KẾ 5
1.1 Mô hình mạng: 5
1.1.1 Mô hình mạng phân lớp: 5
1.1.2 Mô hình mạng Spine-Leaf cho Data Center: 5
1.2 Sơ đồ thiết kế 7
2.1 Phân chia VLAN và hoạch định IP 12
2.2 Phân bố phòng ban và thiết bị 13
3. Lựa chọn thiết bị 18
III. TRIỂN KHAI DỊCH VỤ, DỰ PHÒNG VÀ BẢO MẬT THIẾT BỊ 30
1.1 Dịch vụ mạng nội bộ 30
1.2 Dịch vụ mạng công cộng 31
1.3 Tính sẵn sàng và dự phòng của hệ thống 32
1.4 Các yếu tố bảo mật tích hợp 35
1.5 Phân tích chi phí và tối ưu ngân sách 39
Kết luận 48

I. KHẢO SÁT VÀ PHÂN TÍCH HIỆN TRẠNG

1. Tổng quan công ty THACO:

Công ty THACO chuyên về sản xuất linh kiện, phụ tùng ô tô có chi nhánh chính ở quận 7 gồm hai tòa nhà: Tòa A1 (3 tầng, 7 văn phòng, tầng 1 có 3 phòng ban, tầng 2 có 4 phòng ban và tầng 3 chứa các server, thiết bị mạng quan trọng), Tòa A2 (1 tầng với 3 phòng ban). Chi nhánh thứ 2 ở quận 9 là một tòa nhà B có 2 tầng với 7 phòng ban (với tầng 1 có 3 phòng ban và tầng 2 có 4 phòng ban).

2. Phân tích yêu cầu

- Với tổng 17 văn phòng, mỗi văn phòng có 20-30 máy trạm.
- Mỗi chi nhánh có 2 máy chủ: một máy chủ Domain Controller nội bộ và một máy chủ cung cấp dịch vụ Web/Email công khai. Đảm bảo bảo mật giữa các khu vực khác nhau trong mạng, bao gồm các dịch vụ công cộng (Web, Email Server) và các dịch vụ nội bộ (DNS, DHCP, VPN).
- Hệ thống cung cấp dịch vụ Web/Email cho ~2000 lượt người dùng/ngày. Nhu cầu sử dụng thiết bị mạng và lưu trữ dữ liệu ở mức trung bình lớn, có khu vực lưu trữ dữ liệu khách hàng và sản phẩm.
- Đảm bảo tính sẵn sàng cao, giảm thiểu tối đa thời gian gián đoạn dịch vụ. Luôn sẵn sàng để phục vụ việc hoạt động của công ty.
- Tối ưu chi phí đầu tư hạ tầng mà vẫn đảm bảo hiệu suất cao.
- Cung cấp khả năng mở rộng bảo trì và nâng cấp dễ dàng khi cần thiết.
- Bảo mật qua tường lửa, mã hóa và phân quyền
- Kết nối tốc độ cao, ổn định: Hỗ trợ băng thông Gigabit đến máy trạm, sẵn sàng cho nâng cấp 10 Gigabit với triển khai cáp cấu trúc Cat6A toàn tòa nhà, sơ đồ đi dây hợp lý, đảm bảo tối ưu số lượng và độ dài cáp.
- Hiệu năng và dự phòng: Thiết kế có tính sẵn sàng cao, dự phòng thiết bị và đường truyền (redundancy), hỗ trợ failover khi xảy ra sự cố.
- Ngân sách: Tối ưu chi phí, tổng đầu tư dự kiến trong khoảng 8 tỷ VNĐ, đạt hiệu quả cao nhất trong phạm vi ngân sách.

3. Phân tích hiện trạng

Số lượng phòng ban: 17

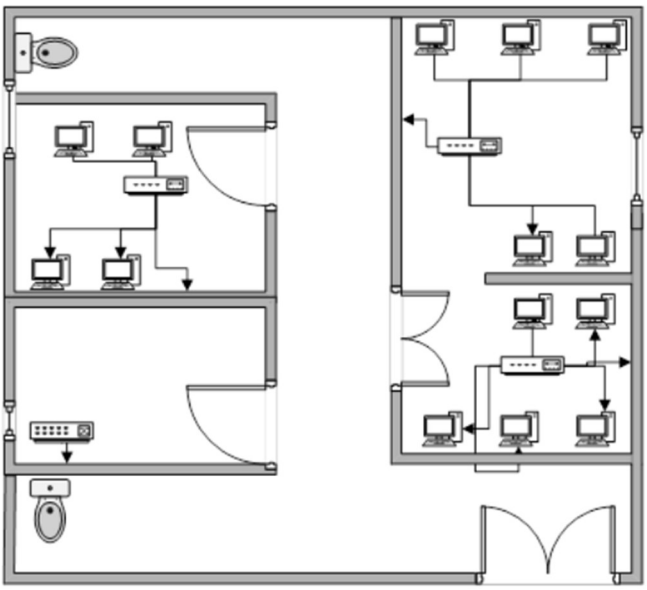
Các phòng ban bao gồm: Phòng kế toán, phòng nhân sự, phòng kinh doanh, phòng marketing, phòng hành chính, phòng pháp chế, phòng kỹ thuật, phòng sản xuất, phòng chăm sóc khách hàng, phòng nghiên cứu và phát triển, phòng dự án, phòng IT Admin (quản trị thiết bị mạng)

Máy chủ và dịch vụ cần thiết:

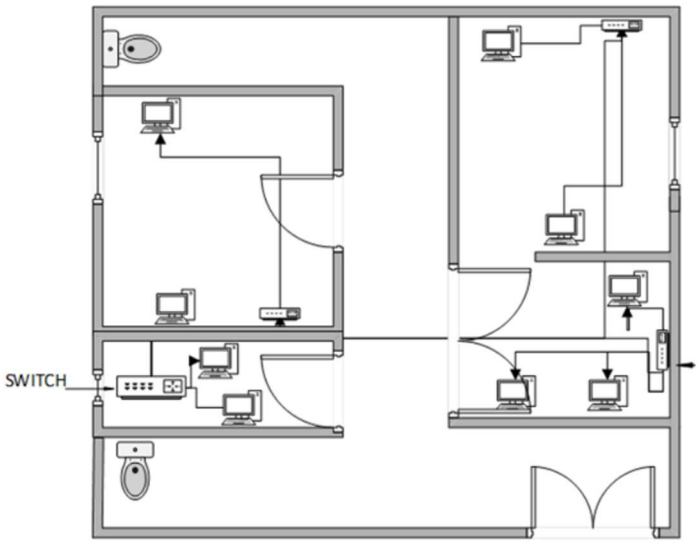
- Web Server: Đặt tại trụ sở chính, cung cấp dịch vụ web cho công ty.
- Email Server: Đặt tại trụ sở chính, cung cấp dịch vụ email cho công ty.
- File Server: Đặt tại trụ sở chính, phục vụ chia sẻ tài liệu cho nhân viên.
- Database Server: Đặt tại trụ sở chính, cung cấp cơ sở dữ liệu cho các ứng dụng.
- VPN: Cho phép nhân viên làm việc từ xa.
- DNS, DHCP: Các dịch vụ nội bộ tại trụ sở chính.
- Firewall: Đảm bảo bảo mật giữa các thiết bị.

Sơ đồ toà nhà

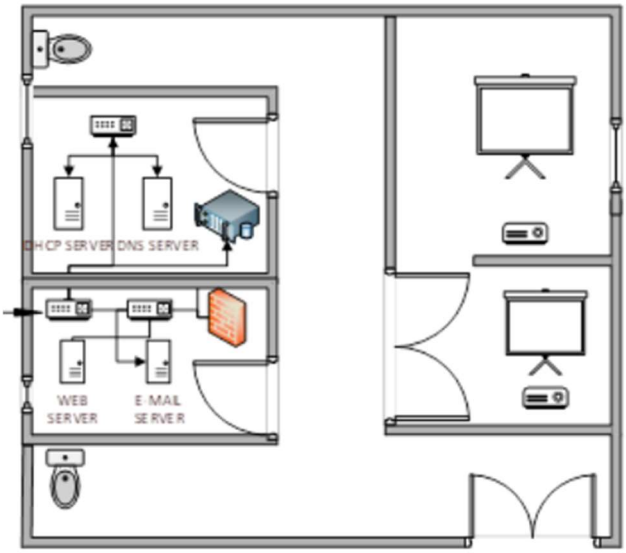
- Tòa A1: (Toà chính, gồm 3 tầng, 7 văn phòng, tầng 1 có 3 văn phòng, tầng 2 có 4 văn phòng, tầng 3 chứa các thiết bị mạng (các Server, Core Switch, Firewall, Router)
    - Tầng 1



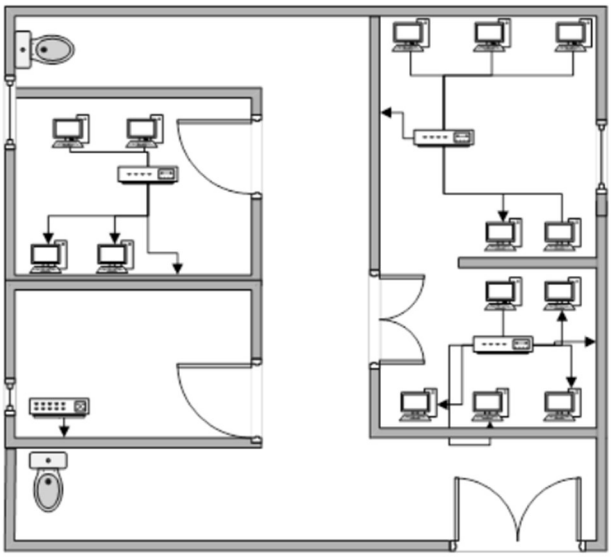
- Tầng 2



- Tầng 3

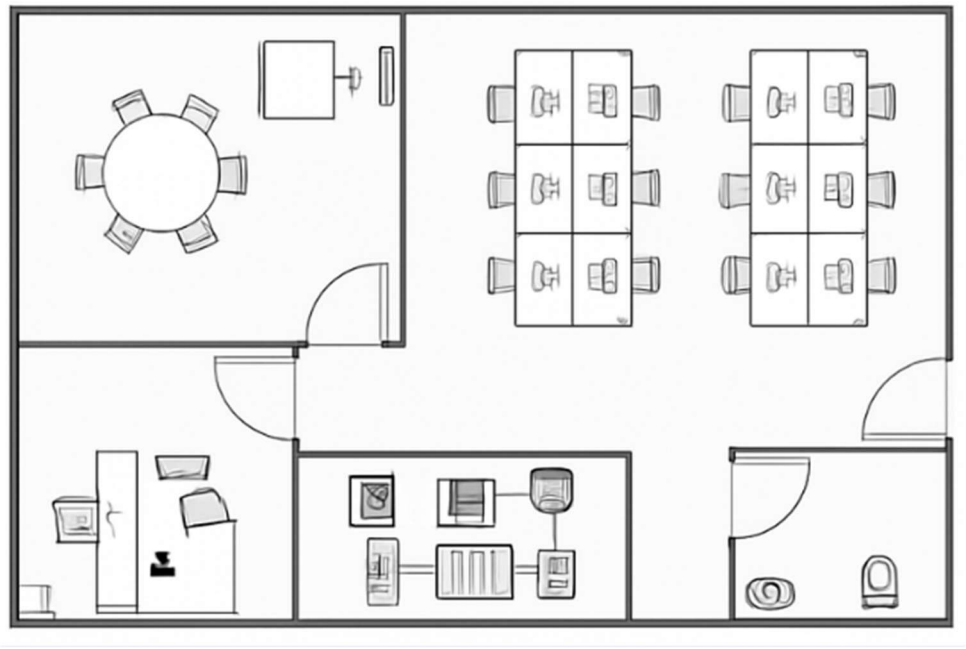


- Tòa A2: (Gồm 1 tầng, 3 phòng ban)

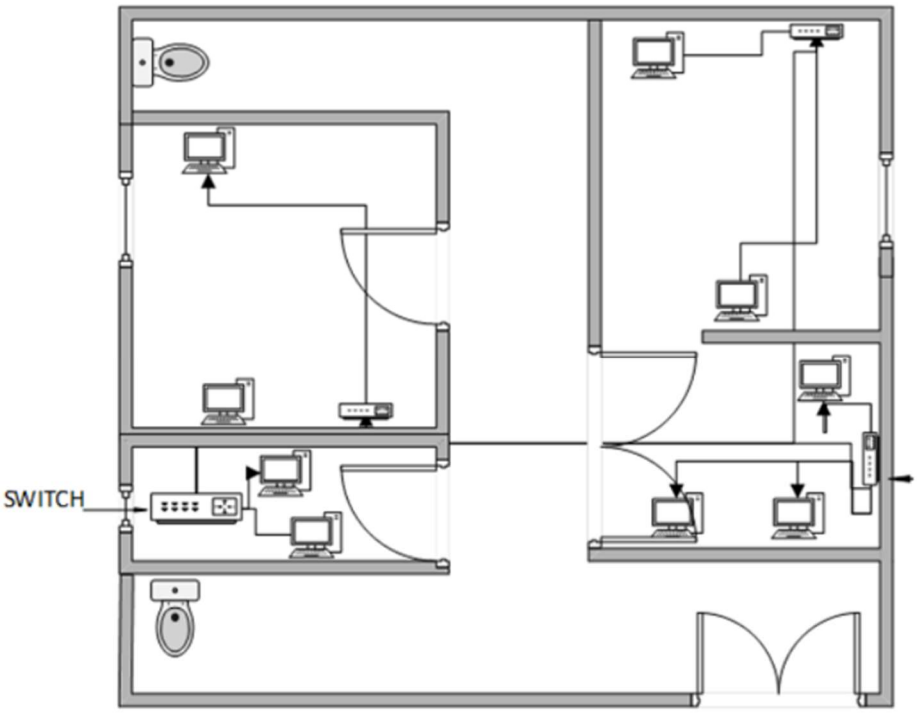


- Tòa B: (Gồm 2 tầng, tầng 1 có 3 phòng ban, 1 phòng chứa DHCP và DNS server tầng 2 có 4 phòng ban)

  - Tầng 1



  - Tầng 2



II. SƠ ĐỒ THIẾT KẾ MẠNG VÀ TRIỂN KHAI THIẾT KẾ

1.1 Mô hình mạng:

1.1.1 Mô hình mạng phân lớp:

Mô hình phân lớp cho phép chúng ta thiết kế các đường mạng mà sử dụng những chức năng chuyên môn kết hợp với một tổ chức có thứ bậc. Việc thiết kế mạng đơn giản là nhiệm vụ đòi hỏi phải xây dựng một mạng mà nó thỏa mãn nhu cầu hiện tại và có thể phát triển tiếp theo nhu cầu ở tương lai. Mô hình phân cấp sử dụng các lớp để đơn giản nhiệm vụ kết nối mạng, mỗi lớp có thể chỉ tập trung vào một chức năng cụ thể, cho phép chúng ta lựa chọn các tính năng và các hệ thống thích hợp cho mỗi lớp phù hợp để xây dựng một mạng lưới doanh nghiệp.

Các lợi ích của doanh nghiệp khi sử dụng mô hình phân lớp:

- Có khả năng mở rộng.
- Dễ dàng triển khai.
- Khắc phục lỗi.
- Quản lý dễ dàng.

1.1.2 Mô hình mạng Spine-Leaf cho Data Center:

Hệ thống mạng áp dụng kiến trúc spine-leaf hai tầng tại mỗi chi nhánh. Mô hình này gồm spine switches (lớp lõi trung tâm) và leaf switches (lớp access/aggregation), giúp giảm độ trễ, tăng băng thông east-west (máy chủ – máy chủ) và dễ mở rộng. Cụ thể:

- **Leaf switches:** Mỗi leaf switch kết nối trực tiếp đến một nhóm switch cấp văn phòng (mỗi switch leaf cấp địa phương cho 1-2 văn phòng hoặc 1 tầng) và các máy chủ tại chi nhánh.
    - Chi nhánh Quận 7 gồm ~9 leaf (7 leaf cho tòa 1, 3 leaf cho tòa 2),
    - Chi nhánh Quận 9 gồm ~6 leaf. Mỗi leaf có 48 cổng Gigabit (có PoE+), kết nối máy trạm, AP và uplink đến spine.

- **Spine switches:** Cấp spine gồm ít nhất 2 switch vật lý để dự phòng, mỗi switch spine có mật độ cổng cao (tích hợp cổng 10G/25G) để uplink tới các leaf và lên mạng lưới lõi. Mỗi leaf liên kết đến tất cả các spine (full-mesh giữa leaf và spine). Đảm bảo mọi kết nối server-đến-server chỉ qua 2 switch (leaf → spine → leaf), giảm độ trễ và ngăn chặn điểm nghẽn "cổ chai". Spine switches giữ vai trò định tuyến (Layer 3) giữa các VLAN và chịu tải chính, giúp hệ thống dễ nâng cấp bằng cách thêm switch mà không ảnh hưởng.
- **Kết nối hai chi nhánh:** Giữa hai chi nhánh cần kết nối WAN (VPN IPsec trên internet) để đồng bộ AD và chia sẻ dịch vụ nếu cần. Mỗi chi nhánh trang bị một router/firewall ở biên, kết nối internet và tạo VPN tới chi nhánh kia (có thể cấu hình sẵn sàng là HA pair, VRRP).
- **Dịch vụ máy chủ:** Hai máy chủ quan trọng ở mỗi chi nhánh (Domain Controller và Web/Email) được đặt trong trung tâm dữ liệu nội bộ (nằm ở tòa chính). Domain Controller đồng bộ giữa hai chi nhánh đảm bảo dịch vụ xác thực luôn sẵn sàng. *Khuyến nghị* có ít nhất 2 DC (một mỗi chi nhánh) để nếu một DC ngừng, DC kia vẫn hoạt động bình thường. Máy chủ Web/Email (chạy dịch vụ công khai) có thể là cụm vật lý hoặc ảo hóa để HA (VD: hai VM chạy cân bằng tải hoặc dự phòng cho nhau). Hai server này nối mạng đến leaf cấp cao nhất ở chi nhánh, có thể đặt trong VLAN DMZ hoặc mạng nội bộ tuỳ nhu cầu bảo mật.

Kiến trúc spine-leaf giải quyết các yêu cầu: độ sẵn sàng cao nhờ đường truyền dự phòng (multiple spine/leaf, router HA), khả năng mở rộng dễ dàng bằng cách thêm leaf mới cho văn phòng hoặc spine mới cho tải lớn. Mỗi payload (dữ liệu) chỉ đi qua đúng 2 switch như trên, giảm độ trễ và nghẽn mạng. Theo Cisco và HPE, mô hình này thay thế mô hình ba tầng truyền thống bằng một kiến trúc hai tầng đơn giản, bỏ qua STP phức tạp và hỗ trợ scale-out linh hoạt.

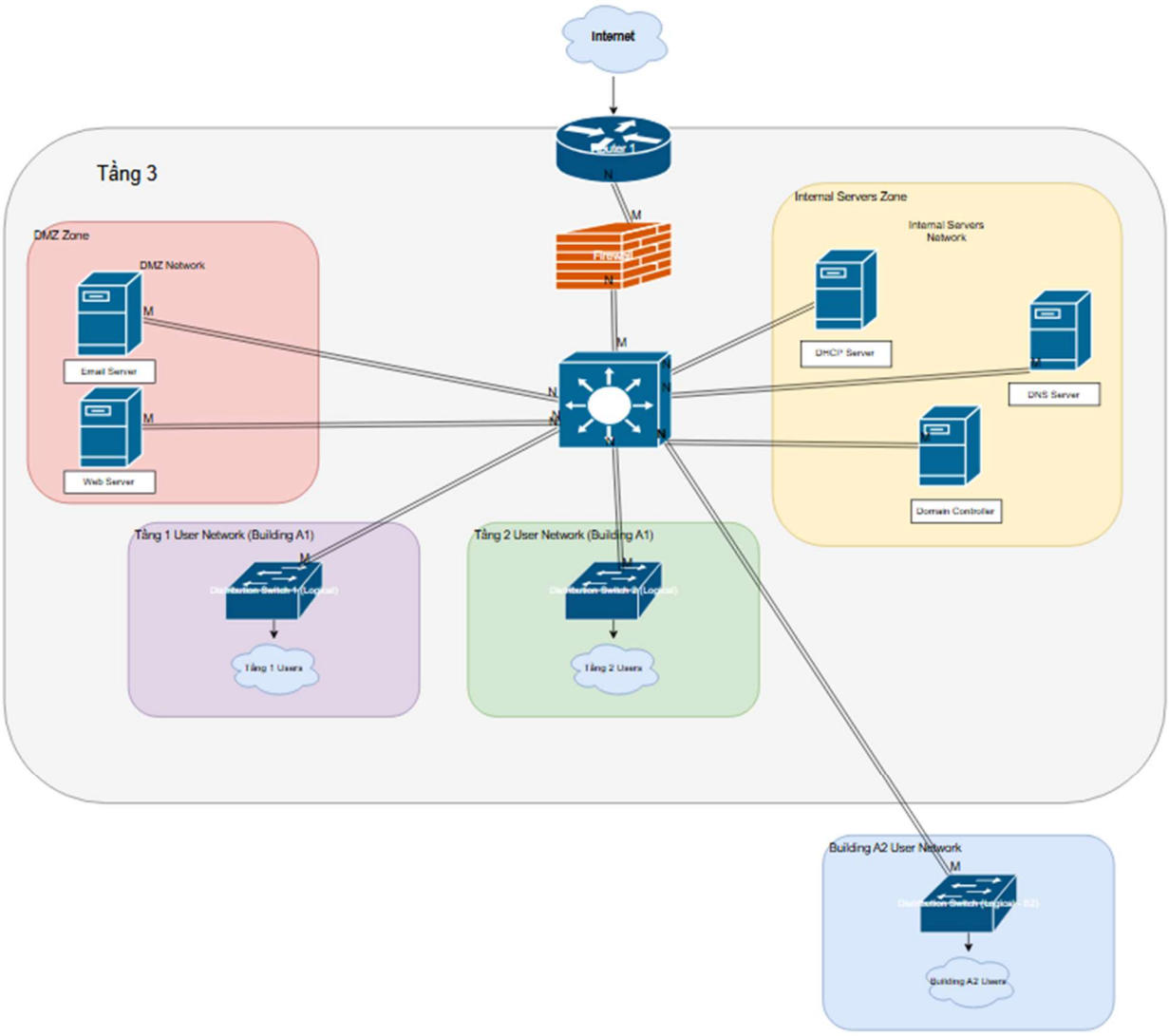
Các lợi ích khi sử dụng mô hình Spine-Leaf:

- Tối ưu East-West Traffic.
- Khả năng mở rộng cao.
- Tính dự phòng và hiệu suất cao.
- Hỗ trợ công nghệ hiện đại.
- Đơn giản hóa quản lý.

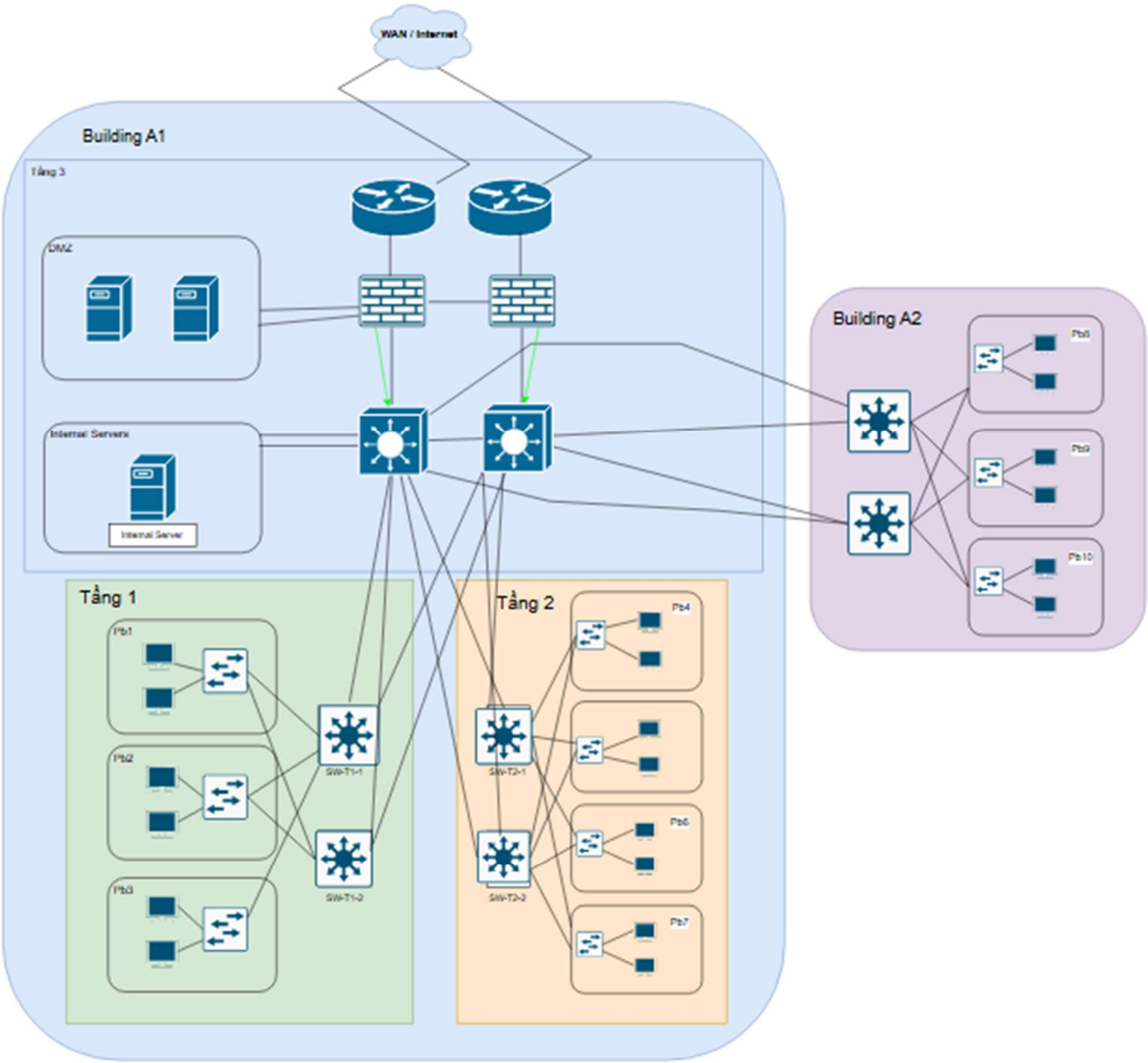
1.2 Sơ đồ thiết kế

Trụ sở chính ở quận 7, TP.HCM

- *Sơ đồ luân lý*

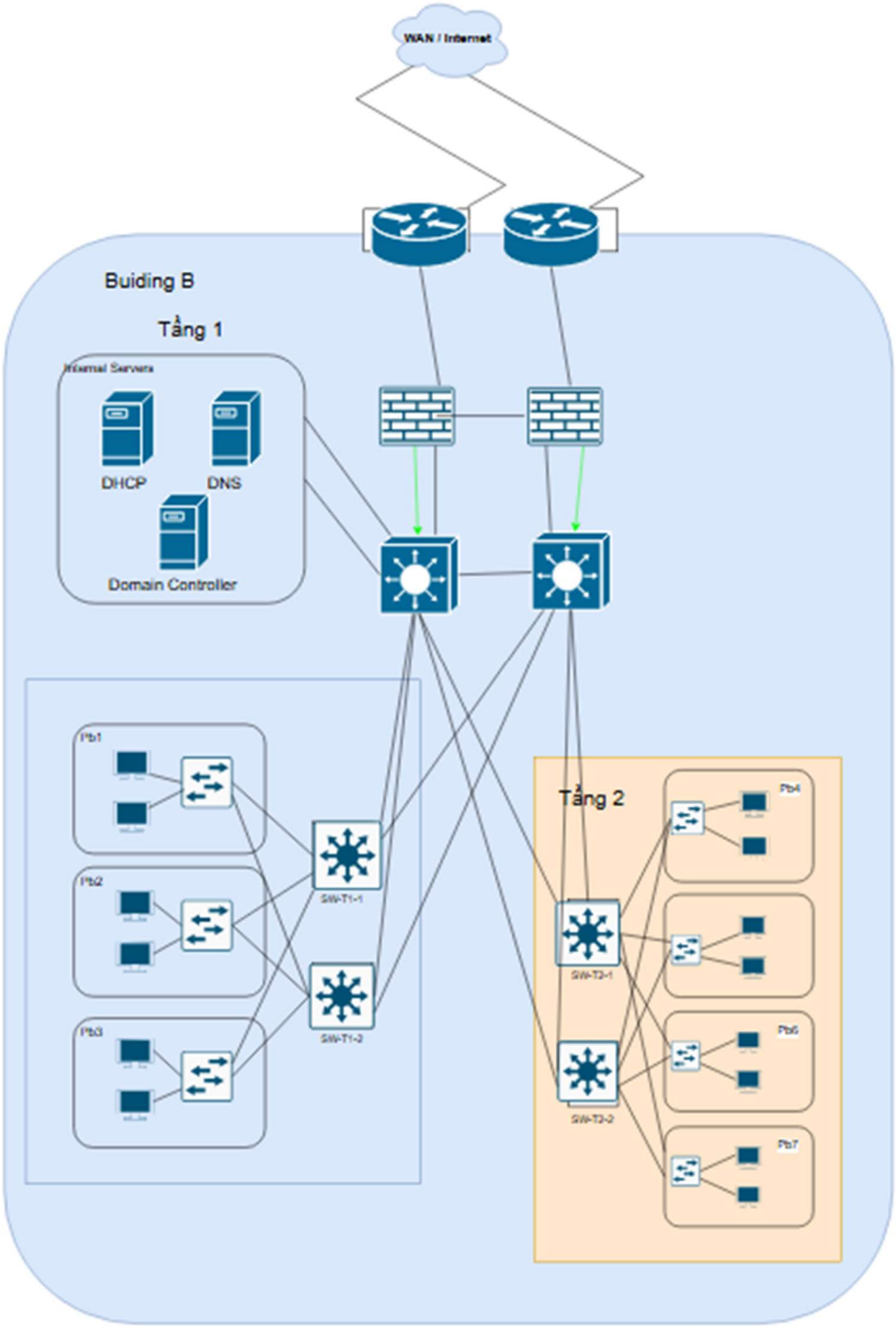


- *Sơ đồ vật lý*

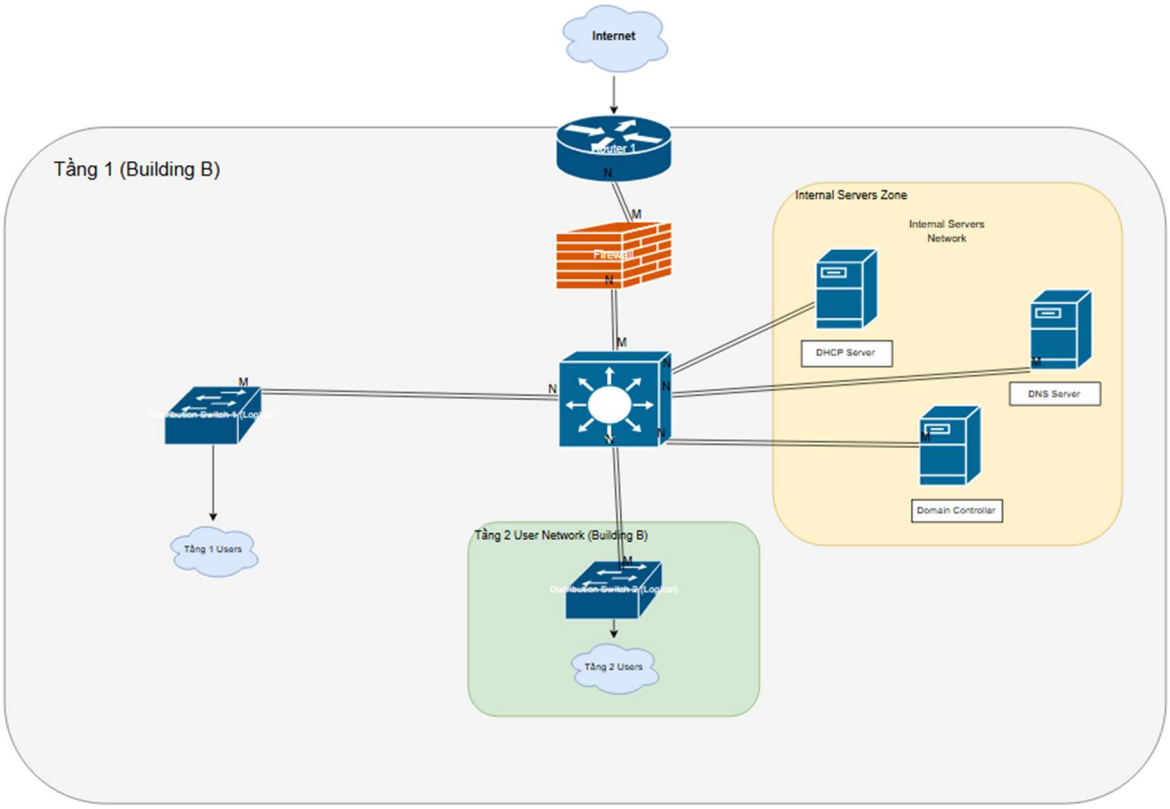

WAN / Internet
Building A1
Tầng 3
DMZ
Internal Servers
Internal Server
Tầng 1
Pb1
Pb2
Pb3
SW-T1-1
SW-T1-2
Tầng 2
Pb4
Pb6
Pb7
SW-T2-1
SW-T2-2
Building A2
Pb8
Pb9
Pb10

Chi nhánh ở quận 9, TP.HCM

- *Sơ đồ vật lý*



- *Sơ đồ luân lý*



Sơ đồ mạng logic đề xuất cho doanh nghiệp THACO. Sơ đồ trên minh họa kiến trúc mạng phân lớp với core switch đặt tại trung tâm (Data Center), kết nối đến các switch phân phối/cấp truy cập ở từng tòa nhà và phòng ban. Mạng gồm các VLAN nội bộ cho 17 phòng ban (mỗi phòng ban một VLAN riêng), VLAN cho server nội bộ và VLAN cho DMZ (vùng máy chủ web/email công bố ra ngoài). Tại biên mạng, một thiết bị Firewall chuyên dụng kết nối giữa mạng nội bộ (Inside) và mạng ngoài Internet (Outside), đồng thời tạo vùng DMZ chứa các máy chủ web/email. Firewall đóng vai trò cổng an ninh, thực thi chính sách và cung cấp các chức năng như IPS, VPN... Phía trước firewall là Router gateway kết nối đến ISP (nhà cung cấp Internet). Core switch tại trung tâm định tuyến liên VLAN trong mạng nội bộ và kết nối lên firewall (router-on-a-stick hoặc thông qua liên kết trunk).

Tại mỗi tòa nhà đều có một phòng kỹ thuật (telecom closet) đặt thiết bị chuyển mạch truy cập và patch panel để kết nối người dùng gần đó. Các tòa nhà được liên kết với nhau qua đường trục cáp quang multimode 10 Gigabit về phòng Data Center trung tâm (tòa nhà chính), nơi đặt core switch, firewall, router và server quan trọng. Kiến trúc phân lớp đảm bảo phạm vi broadcast được chia nhỏ theo VLAN, tăng hiệu năng và dễ quản lý, đồng thời tạo điểm tập trung để thực hiện các biện pháp bảo mật và dự phòng.

Triển khai sơ đồ mạng thành 3 khu vực chính là Outside, DMZ, Inside:

Outside: là khu vực từ Firewall triển khai nối dây ra hai nhóm Border Router với mỗi nhóm là 2 router vật lý, đây là khu vực lưu lượng mạng đi từ ngoài Internet/Wan vào nội bộ và ngược lại

DMZ: Đặt các public server như web server, mail server. Các máy chủ này phải được bảo vệ bằng firewall để ngăn chặn truy cập trái phép từ mạng bên ngoài vào mạng nội bộ (Inside).

Inside: Khu vực Firewall triển khai nối dây với mô hình phân lớp (Core-Distribution-Access) mạng nội bộ của công ty. Chỉ dành cho các thiết bị và người dùng trong công ty, có thể truy cập vào các tài nguyên chung của công ty (file server, DNS, DHCP, email).

Outside: là khu vực từ Firewall triển khai nối dây ra hai nhóm Border Router với mỗi nhóm là 2 router vật lý, đây là khu vực lưu lượng mạng đi từ ngoài Internet/Wan vào nội bộ và ngược lại

Inside: là khu vực Firewall triển khai nối dây với mô hình phân lớp (Core-Distribution-Access) mạng nội bộ của công ty.

2.1 Phân chia VLAN và hoạch định IP

Trụ sở chính ở Quận 7:

2 Tòa nhà (tòa nhà A1, A2): A1 có 3 tầng và A2 có 1 tầng

10 phòng ban tương ứng với 10 VLAN (1-10), bao gồm:

- VLAN 1: Phòng Kế toán
- VLAN 2: Phòng Marketing
- VLAN 3: Phòng IT Admin (quản trị thiết bị mạng)
- VLAN 4: Phòng Nghiên cứu & Phát triển (R&D)
- VLAN 5: Phòng Hành chính, pháp chế
- VLAN 6: Phòng Kỹ thuật
- VLAN 7: Phòng Chăm sóc khách hàng
- VLAN 8: Phòng Sản xuất
- VLAN 9: Phòng Kinh Doanh
- VLAN 10: Phòng Dự án

VLAN quản lý dành phòng ban quản trị thiết bị mạng.

- VLAN 100: Management VLAN (cho thiết bị mạng và phòng IT Admin)

VLAN dành cho các thiết camera và máy in v.v:

- VLAN 110: camera và máy in.

VLAN cho DMZ:

- VLAN 220: DMZ (dịch vụ công cộng như web server, email server).

VLAN cho Data Center:

- VLAN 221: Server ứng dụng.
- VLAN 222: Server cơ sở dữ liệu.
- VLAN 223: Server backup.

Chi nhánh Quận 9:

Toà nhà B có 2 tầng (tầng 1 gồm 3 phòng ban và tầng 2 gồm 4 phòng ban)

7 phòng ban tương ứng với 7 vlan (201-207)

- VLAN 201: Phòng Chăm sóc khách hàng
- VLAN 202: Phòng Nhân sự
- VLAN 203: Phòng Kinh doanh, Marketing
- VLAN 204: Phòng Kỹ thuật
- VLAN 205: Phòng Hành chính
- VLAN 206: Phòng IT Admin (quản trị thiết bị mạng)
- VLAN 207: Phòng Sản xuất

VLAN cho camera và máy in:

- VLAN 220: Camera và máy in

VLAN quản lý:

- VLAN 300: Management VLAN

VLAN cho Server:

- VLAN 240: Server DHCP/DNS

2.2 Phân bố phòng ban và thiết bị

Trụ sở chính Quận 7:

Tòa nhà A1 và A2: dành cho các phòng ban.

Tầng 3 của tòa nhà A1: Dành cho các thiết bị mạng quan trọng (firewall, border router, core switch, distribution switch, access switch, Data Center, Public Server) và phòng ban IT Admin.

Tòa nhà A1:

- Tầng 1: Phòng Kế toán (VLAN 1); Phòng Hành chính, pháp chế (VLAN 5); Phòng Chăm sóc khách hàng(VLAN 7).

- Tầng 2: Phòng IT Admin (*quản trị thiết bị mạng cho tầng 3*)(VLAN 3); Phòng Nghiên cứu & Phát triển (R&D)(VLAN 4); Phòng Marketing (VLAN 2)
- Tầng 3: Data center, Distribution Switch, Public Server và thiết bị giám sát (VLAN 100) và các thiết bị mạng
    - Access Switches: Mỗi tầng có một Access Switch kết nối các thiết bị đầu cuối (máy tính, camera, máy in) và gán port vào VLAN tương ứng.
    - Distribution Switch: Mỗi tòa có một Distribution Switch Kết nối đến từng Access Switch của từng tầng.

Tòa nhà A2:

Phòng Sản xuất (VLAN 8); Phòng Kinh Doanh (VLAN 9); Phòng Dự án (VLAN 10)

Kết nối giữa các tòa nhà:

- Các Access Switches trong Building A1 và A2 kết nối đến Distribution Switches trong cùng tòa.
- Distribution Switches từ Building kết nối về Core Switch qua liên kết tốc độ cao (fiber optic).
- Core Switch trong Building kết nối tới Firewall, Border Router, và ra Internet.

Chi nhánh Quận 9:

Tầng 1: dành cho phòng IT Admin và Server, phòng ban chăm sóc khách hàng, hành chính.

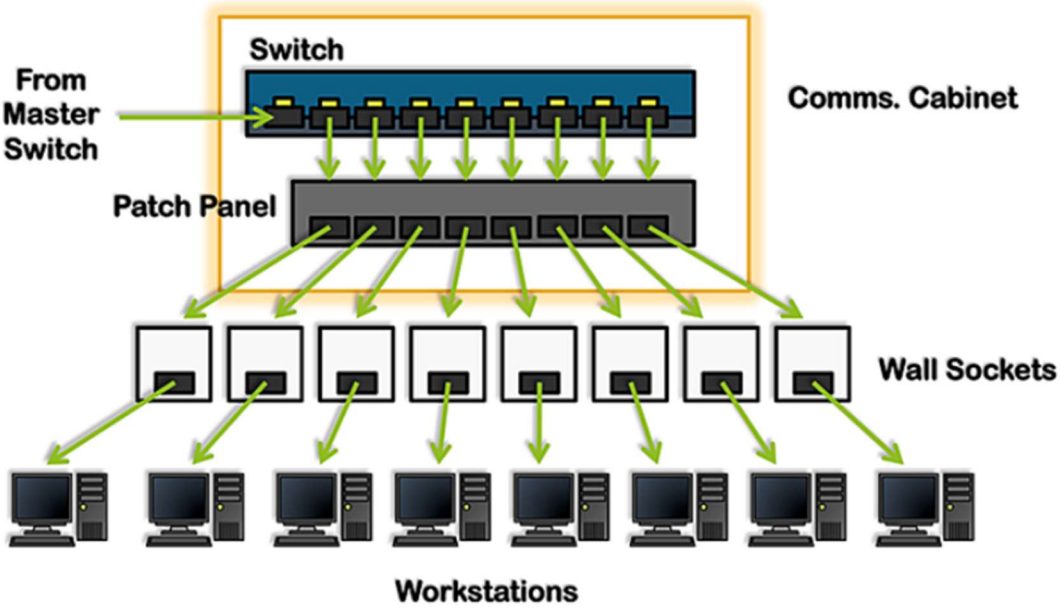
Tầng 2: các phòng ban còn lại.

Cụ thể

- Tầng 1: Phòng Chăm sóc khách hàng(VLAN 201); Phòng Hành chính (VLAN 205); Phòng IT Admin (quản trị thiết bị mạng) (VLAN 206) và các Server (DHCP,DNS,Domain Controller)
- Tầng 2 Phòng Nhân sự (VLAN 202); Phòng Phòng Kinh doanh, Marketing (VLAN 203); Phòng Kỹ thuật (VLAN 204); Phòng Sản xuất (VLAN 207)
- Access Switches: Mỗi tầng có một Access Switch.

- Distribution Switch: Mỗi Tòa có 1 Distribution Switch kết nối đến từng Access Switch của từng tầng.

Hạ tầng cáp và sơ đồ đi dây (cáp cấu trúc Cat6A)



Mô phỏng hệ thống cáp cấu trúc kết nối máy trạm tới tủ mạng (patch panel -> switch).

Hệ thống mạng sử dụng cấu trúc cáp đồng Cat6A theo chuẩn Structured Cabling để đảm bảo hiệu năng và tính ổn định. Tại mỗi bàn làm việc của người dùng sẽ có một ổ cắm mạng (wall socket) kết nối bằng cáp Cat6A về patch panel trong tủ mạng gần nhất. Từ patch panel, các cổng được nối sang switch thông qua các dây nhảy mạng ngắn. Mô hình sao tập trung này đảm bảo mỗi kết nối máy trạm đều chạy độc lập về tủ mạng, dễ dàng quản lý, bảo trì và thay đổi cấu hình khi cần thiết.

Cụ thể, trong mỗi tòa nhà của doanh nghiệp

- Các ổ cắm mạng được lắp tại vị trí người dùng (văn phòng các phòng ban, phòng họp, etc.). Mỗi ổ cắm kéo một sợi cáp Cat6A về phòng thiết bị của tòa nhà.

- Tại phòng thiết bị (telecom closet): tất cả cáp từ các ổ cắm tập kết vào patch panel (bảng đấu dây) gắn trên tủ rack. Mỗi port trên patch panel tương ứng một ổ cắm ngoài thực địa, có nhãn đánh số để tiện xác định.
- Switch truy cập (access switch) trong tủ rack sẽ kết nối tới patch panel bằng dây nhảy ngắn. Nhờ đó, thiết bị người dùng được thông suốt với switch qua patch panel. (Hình minh họa nguyên lý: các máy trạm -> ổ cắm tường -> patch panel -> switch).
- Liên kết giữa các tòa nhà: sử dụng cáp quang đa mốt OM4 (hoặc đơn mốt) kết nối từ switch tòa nhà về core switch tại Data Center trung tâm. Cáp quang đảm bảo đường truyền backbone tốc độ cao 10Gbps và khoảng cách xa hàng trăm mét giữa các tòa nhà. Mỗi tòa nhà dự kiến có ít nhất 2 sợi quang (1 chính + 1 dự phòng) nối về core.

Việc sử dụng cáp Cat6A cho toàn bộ kết nối đồng đảm bảo hệ thống sẵn sàng cho nhu cầu tốc độ 10 Gigabit trong tương lai. Theo tiêu chuẩn, Cat6A hỗ trợ truyền dẫn 10Gbps ở khoảng cách tối đa 100 mét vượt trội so với Cat6 (chỉ ~55m cho 10Gb). Ngoài ra, Cat6A có băng thông 500MHz, chống nhiễu tốt hơn, phù hợp cho môi trường văn phòng đông thiết bị. Tất cả các đường dây tuân thủ cấu trúc ngôi sao: từ tủ tập trung tỏa ra các vị trí, giúp dễ dàng quản lý và mở rộng.

Tính toán số lượng và độ dài cáp Cat6A

Dựa trên sơ đồ mặt bằng và phân bố 17 phòng ban trong 3 tòa nhà, ta ước tính nhu cầu cáp mạng như sau:

- **Số lượng nút mạng người dùng:** ~100 người dùng tương ứng 100 điểm nút (ổ cắm) cần kết nối. Thực tế triển khai, nên dự phòng thêm ~20% cổng cho thiết bị mở rộng, nâng tổng số cổng lên khoảng **200 cổng mạng** Cat6A (bao gồm cả người dùng hiện tại, máy in mạng, camera IP, điện thoại IP tương lai, v.v.).

- **Mỗi phòng ban** (~8-10 người): Trung bình mỗi phòng có 10 cổng (bao gồm PC, máy in, dự phòng). 17 phòng ban ≈ 200 cổng như tính ở trên. Các cổng này sẽ được phân bổ vào patch panel tại các tòa nhà:
    - Tòa nhà A1 (Data Center + 7 phòng): ~100 cổng.
    - Tòa nhà A2 (3 phòng): ~30 cổng.
    - Tòa nhà B (7 phòng): ~70 cổng.
- **Số lượng cáp Cat6A:** Mỗi cổng tương ứng một sợi cáp từ ổ cắm về patch panel. Do đó cần khoảng **200 sợi cáp Cat6A horizontal**. Cáp Cat6A 4 đôi, tiêu chuẩn UTP (hoặc FTP nếu môi trường nhiễu cao), lõi đồng 23 AWG.
- **Độ dài cáp trung bình:** Theo số liệu đo đạc được, các tòa nhà có diện tích mặt bằng cho 4 phòng ban, khoảng cách tối đa từ tủ mạng đến người dùng xa nhất ~70m. Khoảng cách trung bình mỗi kết nối ước tính ~40–50m. Tính trung bình 50m mỗi sợi để bù dư cho đường đi dây thực tế và đấu nối.
- **Tổng chiều dài cáp Cat6A:** 200 sợi * 50m/sợi = **~10000 mét** cáp Cat6A. (Khoảng 10 km cáp). Trong đó tòa nhà A1 ~5000m, A2 ~1500m, B ~3500m.
- **Dây nhảy (patch cord):** Mỗi kết nối cần 2 đoạn patch cord (1 nối PC/thiết bị đến ổ cắm, 1 nối patch panel sang switch). Patch cord thường dài ~3m. Với 200 cổng, cần ~400 dây nhảy, tổng chiều dài ~1200m.
- **Cáp quang backbone:** Kết nối liên tòa nhà: dự kiến 2 tuyến quang chính về core. Cặp sợi quang đa mốt OM4 chạy từ tòa nhà A2 về tòa nhà A. Chiều dài tùy khoảng cách giữa các tòa (giả sử 100m mỗi tuyến). Tổng cáp quang ~100m (2 sợi *50m).

Lưu ý: Các con số trên là ước tính. Khi triển khai thực tế cần khảo sát chi tiết mặt bằng để đo đạc chính xác độ dài từng tuyến cáp, thêm cáp dự phòng cho tương lai, và tuân thủ khoảng cách tối đa 90m cho cáp ngang cố định + 10m patch cord (theo chuẩn TIA-568).

Việc chuẩn bị đủ cáp và bố trí hợp lý sẽ giúp quá trình thi công diễn ra thuận lợi, đảm bảo mỹ quan (có máng cáp, ống luồn dây) và hiệu suất tín hiệu tốt nhất.

3. Lựa chọn thiết bị

1. Spine Switch (Core Layer): Catalyst 9500-24Q

Giá tham khảo: 234.312.000 VND

Số lượng: 4-6 (Hai spine chạy dự phòng (active/active)).

Thông số chính:

Switching Capacity: 1.92 Tbps.

Forwarding Rate: 1,440 Mpps.

Cổng: 24 cổng 40G QSFP+ (có thể chia thành 4x10G SFP+ mỗi cổng).

StackWise Virtual: Hỗ trợ ghép 2 switch (băng thông 480 Gbps).

Layer 3 Features:

- OSPF, BGP, IS-IS, VXLAN, VRF.
- 64,000 IPv4 routes.

Bảo mật: ACL, 802.1X, MACsec, ETA (Encrypted Traffic Analytics).

Nguồn: Dual PSU, 950W AC.

Quản lý: Cisco DNA Center, NetFlow, SD-Access.

Ứng dụng:

- Core Layer: Kết nối giữa Firewall (Firepower 4125) và Spine Switch (Catalyst 9500-40X), định tuyến lưu lượng north-south (Internet/WAN đến data center).
- Tích hợp cloud: Định tuyến lưu lượng đến AWS/Azure qua Border Router.

- Quản lý tập trung: Giám sát toàn bộ hệ thống qua Cisco DNA Center.
- Hỗ trợ stack wise tăng HA cho hệ thống.

Lisence:

- Network Advantage (NA): C9500-NW-A (Perpetual)
- Cisco DNA License (Term-based, tối thiểu 3 năm):
- HSECK9 License (Tùy chọn): C9500-HSECK9.

2. Distribution Switch: Juniper EX4300-24T

Giá tham khảo: 50,000,000 VND

Số lượng: 12 (dự phòng 2) cho cả 2 chi nhánh

Thông số chính:

- 24-port 10/100/1000BaseT (Includes 1 PSU JPSU-350-AC-AFO; 40GE QSFP+)
- Hiệu suất Dung lượng chuyển đổi (kích thước gói 64 byte): 448 Gbps

Chức năng:

- MAC limiting (per port and per VLAN)
- Allowed MAC addresses configurable per port
- Dynamic ARP inspection (DAI)
- IP source guard
- Local proxy ARP
- Static ARP support

- DHCP snooping
- Captive portal
- Persistent MAC address configurations
- Distributed denial of service (DDoS) protection (CPU control path flooding protection)

Lisence:

Network Advantage (NA): C9300-NW-A (Perpetual)

Cisco DNA License (Term-based, tối thiểu 3 năm):

HSECK9 License (Tùy chọn): C9300-HSECK9.

3. Leaf switches (Access Layer): Cisco Catalyst 9200L-48P-4X

Giá tham khảo: 124.388.400 VND

Số lượng: 19 (dự phòng 2) cho cả 2 chi nhánh

Thông số chính:

- Cổng: 24 cổng Gigabit Ethernet (1G) (740W max) và 4 cổng Gigabit SFP uplinks
- PoE: Cung cấp Power over Ethernet (PoE) cho các thiết bị đầu cuối như điện thoại IP và camera giám sát.
- Dual PSU (Power Supply Units)

- Băng thông: 176 Gbps
- Chế độ bảo mật: Hỗ trợ 802.1X, DHCP Snooping, ARP Inspection.
- Cung cấp: Tương tự như các thiết bị khác, SmartNet bảo vệ phần cứng và phần mềm cho một năm.

Ứng dụng:

- Access Layer: Kết nối thiết bị đầu cuối (PC, camera, VoIP) tại chi nhánh.
- PoE+: Cấp nguồn cho thiết bị không cần nguồn riêng.
- Bảo mật: Áp dụng 802.1X để xác thực người dùng/thiết bị.

Lisence: Network Advantage (NA): C9200-NW-A-48 (Perpetual)

Cisco Smart Net Total Care (SNTC) cho các dịch vụ bảo trì và hỗ trợ phần mềm

4. Server: Dell PowerEdge R750

Giá tham khảo: 92.438.640 VND

Số lượng: 3 (2 server ảo hoá các dịch vụ nội bộ và 1 dự phòng) cho cả 2 chi nhánh

*Do sử dụng Dell PowerEdge R750 nên hoàn toàn có thể sử dụng công nghệ ảo hóa để chạy tất cả các dịch vụ cần thiết trên cho chi nhánh trên MỘT máy chủ vật lý.

Thông số chính:

CPU:

- 2x Intel Xeon Gold 6330 (28 cores, 2.0-3.1 GHz).

- Hỗ trợ Intel VT-x (ảo hóa phần cứng).

RAM:

- 512GB DDR4 (16 khe DIMM, mở rộng lên 4TB).

Storage:

- 8x 1.92TB NVMe SSD (RAID 5).
- 4x 10TB HDD (RAID 6).
- Hỗ trợ hot-swap.

Networking:

- 2x 10G SFP+ NIC (Broadcom).
- Hỗ trợ NIC Teaming.

Form Factor: 2U rack server.

Nguồn: Dual PSU (1100W, 80 PLUS Platinum).

Quản lý: iDRAC9 Enterprise (quản lý từ xa).

Hỗ trợ ảo hóa: VMware vSphere, Microsoft Hyper-V.

Ứng dụng:

- Chạy ứng dụng nội bộ: ERP (SAP, Oracle), tài chính, trên server tại data center.
- Ảo hóa: Chạy 50-100 VMs (VMware vSphere hoặc Microsoft Hyper-V) để tối ưu tài nguyên.
- Lưu trữ dữ liệu: Dữ liệu nhạy cảm (khách hàng, tài chính), sao lưu lên cloud (AWS S3, Azure Blob Storage).
- Tích hợp cloud: Đồng bộ dữ liệu với AWS/Azure qua API.

Lisence:

- Firepower Threat Defense (FTD) Base License
- IPS, Malware Protection, VPN (Site-to-Site, Remote Access)

- Advanced Malware Protection (AMP)
- URL Filtering
- Smart Licensing

5. Router: Juniper MX204-HWBASE-AC-FS

Giá tham khảo: ~ 173.000.000 VND

Số lượng: 3 (2 chính, 1 dự phòng) cho cả 2 chi nhánh

Thông số chính:

Vật lý:

- 4 cổng QSFP28.
- 8 cổng SPF+.
- 400 Gbps capacity.
- Đi kèm 2 bộ nguồn.

Phần mềm:

- Các giao thức định tuyến tiêu chuẩn (OSPF, IS-IS, BGP, RIP). Các tính năng MPLS cơ bản. Các tính năng VPN lớp 2 và lớp 3 cơ bản. Các tính năng chuyển mạch Ethernet. Các tính năng bảo mật cơ bản (firewall filters).
- Chạy hệ điều hành Junos – bảo mật cao, hỗ trợ nhiều chính sách routing phức tạp.
- Thiết kế dạng rack 1U, 2 nguồn AC dự phòng, phù hợp Data Center.
- Có thể hoạt động HA (High Availability) khi kết hợp 2 thiết bị chạy song song.

Networking:

- BGP, OSPF, IS-IS, MPLS, SD-WAN.
- Kết nối tốc độ cao (10G/100G),

- Routing mạnh (hỗ trợ nhiều protocol),
- Phù hợp triển khai đa tầng, nhiều tòa nhà, VLAN, DMZ.

6. Firewall: Juniper SRX320

Giá tham khảo: 30.800.000 VND (kèm VAT)

Số lượng: 3 (2 chính, 1 dự phòng) cho cả 2 chi nhánh

Thông số chính:

Vật lý:

- Số cổng Ethernet: 8 cổng 10/100/1000BASE-T (6 LAN + 2 WAN RJ-45)
- Số cổng SFP/SFP+: 2 cổng 1GbE (SFP)
- Số khe cắm mô-đun mở rộng: Không có khe cắm PIM

Phần mềm: Juniper SRX320 Base License

- Thông lượng Firewall: Lên đến 1 Gbps
- Thông lượng IPSec VPN: Lên đến 300 Mbps
- Số kết nối đồng thời: Lên đến 64.000 kết nối
- Các tính năng bảo mật: Firewall, IPSec VPN, NAT, Application Security, SSL VPN, AppSecure, IDP (theo license tùy chọn)

7. Aruba AP-515 (Aruba HPE)

Thông số chính:

- Chuẩn Wi-Fi 6 (802.11ax) 4×4 MU-MIMO
- Tốc độ tối đa:
    - 5 GHz: 4,8 Gbps
    - 2,4 GHz: 574 Mbps
- Công suất phát (Max TX): 4×4 @ 5 GHz, 2×2 @ 2,4 GHz
- Số lượng client hỗ trợ tối đa: 1 024 thiết bị

Cổng:

- 1× 2,5 GbE RJ-45 (uplink PoE+)
- 1× 1 GbE RJ-45 (data only hoặc quản lý)
- 1× Micro USB console (CLI)

PoE & Nguồn:

- Hỗ trợ PoE: 802.3at (PoE+) – công suất cấp tối đa 30 W
- Có thể dùng adaptor AC rời (12 VDC, 3 A)

Tính năng không dây & bảo mật:

- WPA3, WPA2-Enterprise, Enhanced Open
- BSS Coloring, OFDMA, Target Wake Time
- ClientMatch™: tự động cân bằng tải giữa AP
- AirSlice™: đảm bảo chất lượng dịch vụ cho voice/video
- IDS/IPS tích hợp trên radio phụ

License:

- Aruba Central Subscription (Base + Advanced)
- Aruba Instant (perpetual license cho controller-less)
- Smart Rate License (tùy chọn)

Ứng dụng:

- Môi trường office văn phòng mật độ cao
- Lớp học, hội trường, không gian công cộng
- Kết nối IoT (cảm biến, camera, thiết bị y tế)
- Triển khai Flex-Campus, Secure Edge

8. HPE LCD8500 1U US Rackmount Console Kit

Giá tham khảo: 22.000.000 VND

Số lượng: 1

Thông số chính:

Loại màn hình: LCD

Kích thước màn hình (đường chéo): Màn hình kỹ thuật số 18.51 inch

Cổng hiển thị có sẵn: Có

Độ phân giải (tối đa): 1600 x 1200 @ Tốc độ làm mới 60 Hz

Kích thước Rack: 1U (bao gồm màn hình và bàn phím)

Thiết bị trỏ (Pointing device): Bàn di chuột ba nút với bốn (4) phím cuộn

Tốc độ làm mới được hỗ trợ: 60 đến 75 Hz Tương thích với dịch vụ định vị vị trí: Có

Bảo hành: Bảo hành giới hạn ba năm chỉ cho linh kiện

Mô tả sản phẩm: Bộ Console Rackmount 1U LCD8500 kết hợp màn hình WXGA+ 18.5 inch đầy đủ và bàn phím với bàn di chuột trong định dạng 1U, có đủ không gian để gắn KVM switch của HPE phía sau nó. Thanh ray không cần dụng cụ giúp việc lắp đặt dễ dàng.

9. Tủ Rack chính: 42U Data Cabinet

Giá tham khảo: 12 000 000 – 48 000 000 VND

Số lượng: 2

Thông số chính:

- Kích thước: 42U (1.98 m) × 600–800 mm × 800–1 200 mm
- Khung: Thép tĩnh điện, cửa lưới thông gió
- Thông gió: Lỗ trước/sau & khe bên
- Chịu tải: 1 000 kg Lắp đặt: rack 19″, dễ dàng tháo lắp
- Tính năng: quản lý cáp tích hợp, quạt làm mát, ổ khóa bảo mật

10. Tủ Rack phụ: 15U Wall-mount Cabinet

Giá tham khảo: 2 400 000 – 12 000 000 VND

Số lượng: 3

Thông số chính:

Kích thước: 15U (0.75 m) × 600–800 mm × 400–800 mm

Khung: Thép sơn tĩnh điện

Cửa: Kính hoặc thép + lưới tản nhiệt Chịu tải: 300–500 kg

Lắp đặt: treo tường hoặc đặt sàn, rack 19″

Quản lý cáp: khung tích hợp, gọn gàng Quạt làm mát & khóa bảo mật tùy chọn

III. TRIỂN KHAI DỊCH VỤ, DỰ PHÒNG VÀ BẢO MẬT THIẾT BỊ

1.1 Dịch vụ mạng nội bộ

Domain name System (DNS): Cài đặt DNS nội bộ trên Windows Server tích hợp với Active Directory để phân giải tên miền trong mạng. Sử dụng tên miền nội bộ cho AD, và tạo các bản ghi A/AAAA tương ứng cho máy chủ, server và thiết bị. Đặt ít nhất hai máy chủ DNS tại các site khác nhau để dự phòng (DNS chuyển đổi tương ứng với các DC AD). Cấu hình DNS nội bộ tham chiếu đến DNS của ISP hoặc dịch vụ DNS công cộng khi cần để truy cập Internet.

DHCP: Cấu hình dịch vụ DHCP trên Windows Server (hoặc trên thiết bị mạng chuyên dụng) để cấp phát động địa chỉ IP cho máy trạm và thiết bị trong từng VLAN. Thiết lập nhiều scope DHCP phù hợp với từng subnet/VLAN. Thiết lập các ngoại lệ cho các thiết bị cố định (server, máy in, IP phone) bằng cách cấp phát tĩnh qua địa chỉ MAC hoặc réservatiou. Cho phép DHCP cập nhật bản ghi DNS tự động (DDNS) để đồng bộ địa chỉ IP và tên host. Có thể dùng tính năng DHCP Failover hoặc phân bổ DHCP riêng cho từng site để đảm bảo hoạt động liên tục khi một server bị lỗi.

Active Directory (AD): Triển khai dịch vụ AD Domain Services trên ít nhất hai Domain Controller (DC) ở trụ sở chính, với vai trò Global Catalog và DNS tích hợp. Cấu hình Sites and Services nếu có nhiều site để tối ưu hóa lưu lượng đồng bộ. Sử dụng Group Policy để quản lý tập trung chính sách bảo mật, cấu hình máy trạm và triển khai phần mềm. Đảm bảo đồng bộ hóa AD giữa các DC để dự phòng dữ liệu người dùng và nhóm.

File Server: Cài đặt máy chủ file (Windows File Server hoặc NAS) đặt tại trung tâm dữ liệu, chia sẻ thư mục dùng chung cho nhân viên. Có thể sử dụng dịch vụ DFS (Distributed File System) để đồng bộ dữ liệu giữa các site hoặc phân phối tải. Thiết lập phân quyền thư mục dựa trên nhóm AD. Định kỳ sao lưu dữ liệu máy chủ sang ổ lưu trữ khác (tape/đám mây) để đảm bảo an toàn dữ liệu.

1.2 Dịch vụ mạng công cộng

Web Hosting

Hạ tầng: Web server (IIS/Apache/Nginx) đặt trong DMZ, kết nối qua Load Balancer (HAProxy/Nginx) sử dụng NAT/Reverse Proxy trên firewall.

Tính năng:

SSL/TLS với chứng chỉ Let's Encrypt hoặc CA thương mại.

Tự động gia hạn SSL.

Giảm tải (caching), WAF (mod_security) để chống DDoS, XSS, SQLi.

Email Server

Hạ tầng: Exchange Server hoặc Postfix/Dovecot cluster trong DMZ.

Chức năng:

SMTP, IMAP/POP3, ActiveSync.

Anti-spam (SpamAssassin), Anti-virus (ClamAV/Trend Micro).

Backup mailbox định kỳ.

Dự phòng: Database Availability Group (Exchange DAG) hoặc MTA cluster.

VPN Gateway

Kiến trúc: SSL VPN + IPSec VPN trên firewall FortiGate hoặc Cisco ASA.

Chức năng:

Remote-Access VPN cho nhân viên: xác thực AD + MFA (OTP).

Site-to-Site VPN kết nối chi nhánh, kết hợp BGP/OSPF nếu cần.

Tính dự phòng: HA Active-Passive / Active-Active trên firewall.

Load Balancing & CDN

Load Balancer: Dùng F5, HAProxy hoặc Azure/AWS ELB cho web/email.

CDN: Tích hợp Cloudflare/Akamai để giảm độ trễ, chống DDoS lớp 7.

Public DNS & Mail Exchange

Public DNS: Quản lý bản ghi A/AAAA, MX, TXT (SPF, DKIM) với Cloudflare hoặc Amazon Route 53 để tăng tính sẵn sàng.

MX Backup: Thiết lập MX backup trên dịch vụ thứ cấp (Mailbackup.vn) phòng khi mail server chính lỗi.

1.3 Tính sẵn sàng và dự phòng của hệ thống

Thiết kế mạng doanh nghiệp Titans đặc biệt chú trọng đến **tính sẵn sàng (availability)** nhằm tránh gián đoạn công việc khi xảy ra sự cố. Các cơ chế dự phòng được tích hợp ở nhiều lớp như sau:

- **Dự phòng đường truyền (Link Redundancy):** Giữa core switch và mỗi access switch triển khai **EtherChannel (port-channel)** gom nhóm 2 cáp uplink thành một kết nối logic (). Ví dụ: mỗi tòa nhà B, C kéo 2 sợi cáp quang 10G về 2 core switch (mỗi core 1 sợi) tạo thành EtherChannel 20 Gbps. Nếu một sợi bị đứt, sợi còn lại vẫn duy trì kết nối (dung lượng giảm còn 10G nhưng không mất liên lạc). Tương tự, các liên kết từ core xuống server chính, firewall cũng có thể cấu hình LACP (nếu thiết bị hỗ trợ) để tăng băng thông và dự phòng.
- **Dự phòng thiết bị ở lớp Core/Distribution:** Sử dụng **2 core switches Cisco 9300** chạy chế độ **Stackwise** (hoặc **VRRP** nếu chạy độc lập) để tạo thành một cụm chuyển mạch dự phòng nóng. Khi stack, hai switch hoạt động như một thiết bị logic: nếu một chiếc hỏng, chiếc kia tiếp quản toàn bộ vai trò mà mạng không gián đoạn. Cơ chế **Stackwise** của Cisco cho phép thông lượng xếp chồng lên tới 480 Gbps, rất phù hợp xây dựng core switch dư công suất. Thêm vào đó, việc cấu hình gateway ảo qua VRRP/HSRP giữa 2 core đảm bảo default gateway của các VLAN luôn sẵn sàng. Ví dụ, core#1 và core#2 cùng quảng bá địa chỉ gateway; nếu core#1 ngưng, core#2 sẽ tiếp quản địa chỉ IP gateway ngay lập tức, các user không bị mất kết nối mạng.

- **Dự phòng thiết bị Firewall/Router:** Tường lửa FortiGate 100F hỗ trợ chế độ **HA (High Availability)** active-passive. Có thể đầu tư 2 chiếc FortiGate chạy HA để nếu một chiếc lỗi, chiếc còn lại tiếp tục xử lý luồng dữ liệu (thời gian failover vài giây). Điều này đặc biệt quan trọng cho kết nối Internet liên tục (VPN, dịch vụ online). Tương tự, router Cisco ISR có thể cấu hình **HSRP** nếu dùng 2 chiếc router và 2 đường truyền ISP song song – khi router chính hoặc line chính gặp sự cố, router phụ sẽ tự động trở thành gateway ra Internet (). Trong phạm vi ngân sách, doanh nghiệp T có thể trước mắt dùng 1 firewall + 1 router, nhưng thiết kế đã tính đến khả năng mở rộng lên cấu hình dự phòng khi cần (dự phòng cold-standby: chuẩn bị sẵn thiết bị thay thế).
- **Nguồn và điều hòa dự phòng:** Core switch Cisco 9300 có **2 nguồn cấp điện (dual power supply)**, nếu một nguồn hoặc một UPS hỏng, nguồn còn lại vẫn giữ cho thiết bị chạy. Tương tự, các thiết bị khác như firewall, server dùng UPS để chống mất điện lưới. Phòng đặt thiết bị có điều hòa làm mát 24/7; nếu một máy lạnh hỏng đã có máy lạnh phụ đảm bảo nhiệt độ trong giới hạn an toàn cho thiết bị (18-25°C).
- **Giao thức chống vòng lặp và hội tụ mạng nhanh:** Triển khai **Spanning Tree Protocol (STP)** ở lớp switching (RSTP hoặc MSTP) để ngăn chặn loop khi có nhiều đường dự phòng. STP đảm bảo chỉ một đường chính hoạt động, đường còn lại ở trạng thái chờ. Nếu đường chính đứt, STP sẽ **hội tụ** chuyển sang đường chờ trong <1 giây (với RSTP). Ngoài ra, cổng người dùng cấu hình **STP PortFast + BPDU Guard** để tránh ảnh hưởng quá trình hội tụ khi user cắm nhầm thiết bị sinh loop.
- **Failover các dịch vụ mạng:** Các dịch vụ như DHCP, DNS nội bộ có thể cấu hình dự phòng trên 2 máy chủ (primary/secondary). Ví dụ 2 DHCP server chia dải 50/50 hoặc dùng tính năng DHCP failover, để nếu một server ngừng thì server kia vẫn cấp IP cho thiết bị trong VLAN (). Email server có thể đặt backup MX offsite để không mất mail khi server chính offline. VPN cũng có thể cấu hình trên cả hai firewall HA để user không bị mất kết nối VPN.

- **Giám sát và bảo trì:** Triển khai hệ thống **giám sát mạng (NMS)** để theo dõi tình trạng thiết bị (CPU, RAM, lưu lượng, UP/DOWN) và đường truyền. Các công cụ như PRTG, SolarWinds hoặc chính FortiGate, Cisco DNA Center giúp phát hiện sớm sự cố (đứt cáp, mất nguồn…) để có phương án xử lý kịp thời. Đồng thời ký hợp đồng hỗ trợ kỹ thuật với hãng (Cisco SmartNet, Fortinet Support) để được thay thế phần cứng nhanh nếu thiết bị lỗi (4 giờ hoặc next-business-day tùy gói).

Với các biện pháp trên, hệ thống đạt **độ sẵn sàng cao**. Ví dụ, ngay cả khi một core switch hỏng đột ngột, mạng nội bộ vẫn hoạt động bình thường trên switch còn lại; hoặc nếu một tuyến cáp quang backbone bị đứt, lưu lượng tự động chuyển sang tuyến dự phòng. Thiết kế loại bỏ các **điểm đơn lẻ dễ hỏng (single point of failure)** tại các nút quan trọng. Mục tiêu uptime có thể đạt 99.99% (chỉ ngừng hoạt động vài phút mỗi năm) nếu kết hợp cả dự phòng thiết bị lẫn quy trình vận hành, backup cấu hình đầy đủ.

- **Công nghệ dự phòng:**

StackWise/StackWise Virtual: Sử dụng tính năng StackWise (hoặc StackWise Virtual trên Catalyst 9000) để ghép nối hai switch vật lý thành một switch logic duy nhất. Khi đó, hai thiết bị chia sẻ cấu hình và trạng thái chuyển mạch Công nghệ này kết hợp SSO (Stateful Switch Over) và NSF (Non-Stop Forwarding) giúp chuyển đổi chế độ chủ/dự phòng mà không mất gói dữ liệu, nâng cao tính liên tục dịch vụ.

EtherChannel/Multi-Chassis LAG**:** Sử dụng EtherChannel (MLAG) để gom nhiều cổng uplink giữa các switch thành một liên kết ảo. EtherChannel vừa tăng gấp đôi (hoặc nhiều hơn) băng thông, vừa cho dự phòng khi một liên kết vật lý gặp lỗi. Ví dụ, kết nối giữa switch access và distribution có thể dùng kênh EtherChannel 2-4 cổng gigabit, nhằm cân bằng tải và duy trì kết nối nếu cáp hỏng. Ngoài ra, EtherChannel cũng được dùng cho liên kết StackWise Virtual để duy trì kênh song song giữa hai switch thành phần.

VRRP/HSRP: Trên thiết bị router, cấu hình giao thức dự phòng gateway như VRRP hoặc Cisco HSRP. VRRP cho phép nhóm các router/virtual-router chia sẻ một địa chỉ IP gateway ảo duy nhất. Khi router chính (master) gặp sự cố, một router dự phòng sẽ tự động

đảm nhận địa chỉ ảo và tiếp tục chuyển tiếp lưu lượng, đảm bảo liên lạc cho các máy chủ và máy trạm không bị gián đoạn. Quy trình tương tự áp dụng cho HSRP (chọn gateway ảo giữa các router Cisco).

1.4 Các yếu tố bảo mật tích hợp

An ninh mạng là thành phần không thể thiếu trong thiết kế. Giải pháp đề xuất đã tích hợp nhiều lớp bảo mật hợp lý, đảm bảo an toàn cho hệ thống mà vẫn tối ưu chi phí:

- **Phân vùng mạng bằng VLAN và subnet:** Mỗi phòng ban được cô lập thành một VLAN riêng () (ví dụ: VLAN10-Tài chính, VLAN11-Nhân sự,...). Điều này giới hạn broadcast trong từng VLAN, và cho phép áp dụng chính sách kiểm soát truy cập giữa các VLAN. Các máy chủ nội bộ đặt trong VLAN riêng (Internal Server VLAN) chỉ phục vụ nội bộ (); các máy chủ public (web, email) đặt VLAN DMZ tách biệt (). VLAN Wi-Fi khách cũng được tạo riêng để tách khỏi VLAN nhân viên. Mỗi VLAN sẽ được định địa chỉ IP khác nhau (VD: Phòng A: 192.168.10.0/24, Phòng B: 192.168.11.0/24, …), nhờ đó firewall định danh được lưu lượng theo nguồn gốc để kiểm soát.
- **Kiểm soát truy cập nội bộ (ACL):** Trên core switch, cấu hình các **Access Control List (ACL)** hạn chế lưu lượng không cần thiết giữa các VLAN. Ví dụ: chặn hoàn toàn truy cập từ VLAN nhân viên thường vào VLAN server nội bộ ngoại trừ các cổng/dịch vụ cần thiết; chặn VLAN khách truy cập VLAN nội bộ; chỉ cho phép VLAN IT quản trị thiết bị mạng. ACL ở lớp 3 giúp giảm nguy cơ lan truyền sự cố hoặc truy cập trái phép nếu một segment bị xâm nhập.

- **Tường lửa bảo vệ chu vi (Perimeter Firewall):** làm lá chắn giữa mạng **Inside**, **DMZ** và **Outside (Internet)**. Tường lửa sẽ có các chính sách:
    - Chỉ cho phép lưu lượng hợp lệ từ trong ra ngoài (ví dụ HTTP, HTTPS, VPN) và chặn hết các kết nối bất thường.
    - Chặn truy cập trực tiếp từ ngoài Internet vào VLAN nội bộ; chỉ mở cổng cần thiết đến DMZ (ví dụ HTTP(S) đến Web Server, SMTP đến Mail Server).
    - Bật chức năng **IPS** (Intrusion Prevention) để phát hiện và ngăn chặn tấn công vào server DMZ hoặc từ Internet lọt vào LAN. IPS cập nhật thường xuyên giúp bảo vệ trước các cuộc tấn công mới.
    - **Web Filtering & Anti-malware:** Lọc web ngăn người dùng truy cập các trang web độc hại, đồng thời quét virus/trojan trên luồng lưu thông nếu khả thi. FortiGate có sẵn cơ chế này, có thể áp dụng cho VLAN người dùng để tăng cường bảo mật.
    - **NAT/PAT:** Firewall thực hiện chuyển đổi địa chỉ (NAT) cho toàn bộ máy trong mạng khi ra Internet, ẩn cấu trúc IP nội bộ. Đồng thời cấu hình DNAT cho các dịch vụ public (Web/Email) trỏ vào IP public của firewall rồi vào server DMZ.
    - Nhật ký (log) lưu lại các kết nối, cảnh báo an ninh để đội quản trị theo dõi.
- **Hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS):** Như trên, tính năng IPS tích hợp trong FortiGate được kích hoạt cho luồng vào từ Internet. Nếu ngân sách cho phép và yêu cầu cao, có thể triển khai thêm một thiết bị **IDS/IPS độc lập** (như Cisco FirePOWER hoặc Snort sensor) đặt song song để giám sát lưu lượng ngang. Tuy nhiên, với mạng 2000 user, IPS trên firewall đã khá hiệu quả và tối ưu.

- **VPN (Mạng riêng ảo):** FortiGate hỗ trợ cả **SSL VPN** và **IPsec VPN**. Triển khai VPN sẽ cho phép:
    - **Truy cập từ xa an toàn:** Nhân viên đi công tác có thể kết nối vào mạng công ty qua SSL VPN (đăng nhập bằng tài khoản AD và token OTP). Lưu lượng VPN được mã hóa SSL qua Internet và firewall sẽ giới hạn chỉ truy cập các hệ thống cần thiết.
    - **Kết nối chi nhánh:** Nếu doanh nghiệp T có chi nhánh khác, có thể dựng kênh IPsec VPN site-to-site giữa các firewall FortiGate để nối mạng hai bên an toàn.
    - VPN cũng giúp quản trị viên có thể truy cập cấu hình thiết bị từ xa (qua VPN vào mạng nội bộ thay vì mở cổng quản trị trên Internet rất nguy hiểm).
- **Bảo mật tầng 2:** Trên switch Cisco, kích hoạt các biện pháp bảo mật như **DHCP Snooping** (chống giả mạo DHCP server), **Dynamic ARP Inspection** (chống ARP spoofing) trong các VLAN người dùng. Cấu hình **Port Security** trên cổng access khóa số lượng MAC tối đa, tránh tình trạng cắm switch lạ gây mở rộng VLAN trái phép. Các cổng quan trọng cấu hình 802.1X + MAC authentication để chỉ cho phép thiết bị đã xác thực mới truy cập mạng (nếu doanh nghiệp triển khai hệ thống quản lý truy cập mạng như Cisco ISE, có thể thêm sau).
- **Phân quyền truy cập tài nguyên:** Đây là lớp bảo mật ở tầng hệ thống. Các server nội bộ (AD, File) thiết lập chính sách phân quyền theo nhóm AD, đảm bảo chỉ nhân viên thuộc phòng ban mới truy cập được dữ liệu tương ứng. Các máy trạm cài đủ antivirus endpoint, được cập nhật bản vá Windows định kỳ (WSUS server nội bộ hỗ trợ). Những biện pháp này kết hợp với bảo mật mạng thành bức tường nhiều lớp.

- **Giám sát và phản ứng sự cố bảo mật:** Bật logging trên firewall, switch về syslog server tập trung. Xây dựng quy trình giám sát nhật ký để phát hiện bất thường (ví dụ một máy trong LAN quét cổng hàng loạt -> có thể máy đó nhiễm virus nội bộ). Khi phát hiện, đội IT sẽ cách ly VLAN hoặc chặn trên switch port tương ứng. Doanh nghiệp có thể đầu tư một hệ thống SIEM nhỏ (Security Information and Event Management) nếu cần phân tích log tự động, nhưng với 2000 user thì chưa bắt buộc.

Nhìn chung, các yếu tố bảo mật được thiết kế theo mô hình phòng thủ nhiều lớp: từ lớp mạng vật lý (VLAN, ACL) đến lớp ứng dụng (tường lửa, IPS, web filter) và cả lớp thiết bị người dùng (antivirus, phân quyền). Sự kết hợp hợp lý này đảm bảo nếu một lớp bị xuyên thủng thì còn lớp khác bảo vệ. Đồng thời, giải pháp được tối ưu để không vượt ngân sách: tận dụng tối đa khả năng của firewall FortiGate thay vì mua thêm thiết bị rời; dùng tính năng sẵn có trên switch Cisco thay vì hệ thống NAC phức tạp. Mức độ bảo mật này là phù hợp với quy mô doanh nghiệp T, vừa đảm bảo an toàn, vừa không quá phức tạp gây khó vận hành.

1.5 Phân tích chi phí và tối ưu ngân sách

Thiết bị	Số lượng	Đơn giá Phần cứng (VNĐ)	Thành tiền Phần cứng (VNĐ)	Ước tính License/Thiết bị (VNĐ)	Tổng chi phí License (VNĐ)	Tổng cộng (Phần cứng + License) (VNĐ)
Spine Switch (Core Layer)						
Catalyst 9500-24Q	4	234,312,000	937,248,000	30,000,000 - 70,000,000	120,000,000 - 280,000,000	1,057,248,000 - 1,217,248,000
Distribution Switch						
Juniper EX4300-24T	12	50,000,000	600,000,000	5,000,000 - 15,000,000	60,000,000 - 180,000,000	660,000,000 - 780,000,000
Leaf Switch (Access Layer)						
Cisco Catalyst 9200L-48P-4X	19	124,388,400	2,363,379,600	10,000,000 - 25,000,000	190,000,000 - 475,000,000	2,553,379,600 - 2,838,379,600
Server						
Dell PowerEdge R750	3	92,438,640	277,315,920	20,000,000 - 50,000,000	60,000,000 - 150,000,000	337,315,920 - 427,315,920
Router						
Juniper MX204-HWBASE-AC-FS	3	173,000,000	519,000,000	20,000,000 - 60,000,000	60,000,000 - 180,000,000	579,000,000 - 699,000,000
Firewall						
Juniper SRX320 (kèm VAT)	3	30,800,000	92,400,000	10,000,000 - 30,000,000	30,000,000 - 90,000,000	122,400,000 - 182,400,000

Wi-Fi Access Point						
Aruba AP-515 (Aruba HPE)	15	17,500,000 (Ước tính)	262,500,000 (Ước tính)	1,500,000 - 3,000,000 (cho Central)	22,500,000 - 45,000,000	285,000,000 - 307,500,000
Hạ tầng tủ Rack và UPS						
Tủ Rack chính 42U Data Cabinet	2	30,000,000 (TB)	60,000,000	0	0	60,000,000
Tủ Rack phụ 15U Wall-mount Cabinet	3	7,000,000 (TB)	21,000,000	0	0	21,000,000
HPE LCD8500 1U Console Kit	1	22,000,000	22,000,000	0	0	22,000,000
UPS APC Smart-UPS 3000VA	3	33,750,000	101,250,000	0	0	101,250,000
Hạ tầng cáp mạng						
Cáp mạng Cat6A UTP (~10,000m)	1 lô	75,000,000	75,000,000	0	0	75,000,000
Cáp quang OM4 backbone (~100m)	1 lô	8,750,000	8,750,000	0	0	8,750,000
Patch Panel Cat6A, Dây nhảy, Module	1 lô	50,000,000	50,000,000	0	0	50,000,000
Tổng cộng ước tính (Phần cứng + License cơ bản)			**~5,389,843,520**		**~542,500,000 - ~1,400,000,000**	**~5,932,343,520 - ~6,789,843,520 VNĐ**

Phân tích chi phí chi tiết và tối ưu ngân sách:

1. **Chi phí thiết bị phần cứng chính:**
    - **Spine Switch (Core Layer) - Catalyst 9500-24Q:** Với số lượng 4-6 chiếc (giả định 2 spine cho mỗi chi nhánh nếu có 2 chi nhánh, hoặc 2 spine cho Data Center chính và 1-2 spine cho mỗi chi nhánh), tổng chi phí dao động từ **937 triệu đến 1,4 tỷ VNĐ**. Đây là dòng switch core mạnh mẽ, đảm bảo hiệu năng và khả năng mở rộng. Việc lựa chọn 4 hay 6 chiếc phụ thuộc vào cấu trúc dự phòng mong muốn cho từng site.
    - **Distribution Switch - Juniper EX4300-24T:** 12 chiếc với tổng chi phí **600 triệu VNĐ**. Số lượng này đủ để triển khai dự phòng (2 chiếc/tầng hoặc khu vực) cho cả trụ sở chính và một chi nhánh lớn (hoặc hai chi nhánh nhỏ hơn).
    - **Leaf Switch (Access Layer) - Cisco Catalyst 9200L-48P-4X:** 19 chiếc, tổng chi phí khoảng **2,36 tỷ VNĐ**. Đây là lựa chọn cung cấp đủ cổng PoE+ cho các thiết bị đầu cuối và uplink tốc độ cao. Số lượng này đảm bảo phủ sóng cho khoảng 200-300 người dùng/thiết bị đầu cuối.
    - **Server - Dell PowerEdge R750:** 3 chiếc, tổng chi phí khoảng **277 triệu VNĐ**. Với khả năng ảo hóa, 2 server có thể chạy các dịch vụ nội bộ và DMZ, server còn lại đóng vai trò dự phòng hoặc phục vụ các tác vụ chuyên biệt. Số lượng này phù hợp cho việc triển khai các dịch vụ cơ bản cho cả trụ sở và 1-2 chi nhánh (nếu dịch vụ chi nhánh được ảo hóa trên server này).
    - **Router - Juniper MX204:** 3 chiếc, tổng chi phí **519 triệu VNĐ**. Cung cấp kết nối WAN mạnh mẽ và dự phòng cho cả trụ sở và chi nhánh.
    - **Firewall - Juniper SRX320:** 3 chiếc, tổng chi phí **92,4 triệu VNĐ**. Đủ cho việc bảo vệ biên mạng cho trụ sở và chi nhánh với các tính năng cơ bản.

2. **Hạ tầng tủ Rack và UPS:**
    - Chi phí tủ rack và console kit ước tính khoảng **53 triệu đến 154 triệu VNĐ**.
    - Chi phí UPS cần được tính toán cụ thể dựa trên tổng công suất tiêu thụ của tất cả thiết bị trong từng tủ rack để đảm bảo thời gian hoạt động mong muốn khi mất điện.
3. **Hạ tầng cáp mạng:**
    - Chi phí cáp Cat6A, cáp quang và phụ kiện đấu nối ước tính khoảng **133,75 triệu VNĐ**. Quan trọng cho hiệu suất và độ ổn định của mạng.
4. **Chi phí phần mềm và dịch vụ:**
    - **Bản quyền phần mềm:** Windows Server, có thể là SQL Server, các license cho phần mềm ảo hóa (nếu không dùng bản miễn phí), license cho các tính năng nâng cao của Firewall/Switch (ví dụ: Cisco DNA, Juniper Security Services). Tạm tính **~200 - 500 triệu VNĐ** tùy thuộc vào số lượng và loại license.
    - **Dịch vụ cài đặt, cấu hình:** Nếu thuê đối tác triển khai, chi phí có thể dao động từ **150 - 300 triệu VNĐ** tùy thuộc vào độ phức tạp và quy mô.
    - **Đào tạo vận hành, tài liệu, quản lý dự án:** Khoảng **50 - 100 triệu VNĐ**.
    - **License cho Access Point (nếu dùng giải pháp quản lý tập trung):** Ví dụ Aruba Central.
5. **Nhân công thi công mạng:**
    - Chi phí này phụ thuộc vào số lượng điểm mạng, độ phức tạp của việc đi dây. Ước tính khoảng **100 - 200 triệu VNĐ**.

Phân tích chi tiết license và tối ưu:

1. **License cho Switch (Cisco & Juniper):**
    - **Cisco Catalyst 9500/9200L:**
        - **Network Advantage (Perpetual):** Thường đã bao gồm các tính năng Layer 2/Layer 3 cơ bản đến nâng cao (OSPF, BGP cơ bản, VRF-lite, PIM, StackWise Virtual trên 9500). Chi phí này thường đã nằm trong giá phần cứng ban đầu hoặc là một phần nhỏ.
        - **Cisco DNA Advantage (Subscription - 3, 5, 7 năm):** Cung cấp các tính năng tự động hóa, phân tích, bảo mật nâng cao thông qua Cisco DNA Center. Đây là khoản chi phí đáng kể (có thể từ 15-30% giá trị phần cứng mỗi năm). **Tối ưu:** Nếu không có nhu cầu sử dụng DNA Center ngay lập tức hoặc các tính năng quá nâng cao, có thể bắt đầu với Network Advantage và cân nhắc DNA sau. Chi phí ước tính: **10-70 triệu/switch/3 năm** tùy dòng.
        - **HSECK9 (Tùy chọn):** License cho các tính năng mã hóa mạnh, thường cần cho các quy định đặc thù.
        - **SmartNet Total Care (SNTC - Subscription):** Dịch vụ hỗ trợ kỹ thuật và thay thế phần cứng từ Cisco. Rất quan trọng cho các thiết bị Core/Distribution. Chi phí khoảng 8-15% giá trị phần cứng/năm.
    - **Juniper EX4300/MX204:**
        - **Junos OS (Base):** Đã bao gồm các tính năng routing, switching cơ bản.
        - **Advanced Feature Licenses (AFL) hoặc Subscription cho dịch vụ:** Cần cho các tính năng như MPLS, VXLAN nâng cao, các dịch vụ bảo mật trên MX series. Chi phí: **5-60 triệu/thiết bị/năm hoặc vĩnh viễn** tùy tính năng.

- **Juniper Care (Support):** Tương tự SNTC của Cisco, cung cấp hỗ trợ kỹ thuật và thay thế phần cứng.

2. **License cho Server (Dell PowerEdge R750):**
    - **Windows Server Standard/Datacenter:**
        - Standard: Cho phép 2 máy ảo (OSEs/Hyper-V containers).
        - Datacenter: Cho phép số lượng máy ảo không giới hạn.
        - License theo số core vật lý của CPU (tối thiểu 16 core/server, 8 core/CPU). Với Xeon Gold 6330 (28 cores), bạn sẽ cần license cho 28 core/CPU, tổng 56 core/server.
        - Chi phí: Windows Server Standard khoảng **15-25 triệu/16 core**. Datacenter khoảng **80-120 triệu/16 core**.
        - **Tối ưu:** Nếu số lượng VM trên mỗi server ít (ví dụ < 10-12 VMs), bản Standard có thể kinh tế hơn. Nếu nhiều VM, Datacenter là lựa chọn tốt.
    - **Client Access Licenses (CALs):** Cần User CALs hoặc Device CALs cho mỗi người dùng/thiết bị truy cập Windows Server. Chi phí: **~800,000 - 1,200,000 VNĐ/User CAL**. Với ~100-150 user, đây là một khoản đáng kể.
    - **VMware vSphere (Nếu dùng):**
        - Essentials Kit (cho 3 server, tối đa 2 CPU/server): ~15-20 triệu.
        - Standard/Enterprise Plus: Chi phí cao hơn nhiều, tính theo CPU socket.
        - **Tối ưu:** Hyper-V của Microsoft (đi kèm Windows Server) là giải pháp ảo hóa miễn phí và mạnh mẽ, có thể không cần VMware nếu không có yêu cầu đặc thù.

- **iDRAC9 Enterprise License:** Cho phép quản lý từ xa nâng cao. Thường nên có. Chi phí: **~2-5 triệu/server**.

3. **License cho Firewall (Juniper SRX320):**
    - **SRX320 Base License:** Đã bao gồm các tính năng firewall cơ bản, NAT, VPN cơ bản.
    - **Juniper Security Services (JSB/JSE - Subscription 1, 3, 5 năm):** Cung cấp IPS, Application Security (AppSecure), Antivirus, Web Filtering, Anti-Spam. Rất quan trọng để tăng cường bảo mật.
    - Chi phí: Gói JSB/JSE cho SRX320 có thể từ **10-30 triệu/thiết bị/năm**.
    - **Tối ưu:** Mua gói subscription dài hạn (3-5 năm) thường có giá tốt hơn. Đánh giá kỹ các tính năng cần thiết trong gói.
4. **License cho Wi-Fi Access Point (Aruba AP-515):**
    - **Aruba Instant OS (Controller-less):** Thường là miễn phí, cho phép AP hoạt động độc lập hoặc tạo cluster ảo mà không cần controller vật lý.
    - **Aruba Central (Cloud Management - Subscription):** Cung cấp quản lý tập trung, giám sát, cấu hình từ cloud. Rất tiện lợi cho hệ thống nhiều AP.
    - Chi phí: Aruba Central subscription khoảng **1.5 - 3 triệu/AP/năm**.
    - **Tối ưu:** Nếu số lượng AP ít và quản lý phân tán chấp nhận được, có thể không cần Aruba Central ban đầu. Tuy nhiên, với số lượng 15 AP trở lên, Central rất được khuyến nghị.

Tổng cộng ước tính (bao gồm cả license và các chi phí khác):

- Phần cứng + License (ước tính mức trung bình): **~6.3 tỷ VNĐ**
- Chi phí phần mềm khác (SQL, Exchange nếu có, phần mềm backup...): **50 - 200 triệu VNĐ**
- Dịch vụ cài đặt, cấu hình: **150 - 300 triệu VNĐ**
- Đào tạo, tài liệu, quản lý dự án: **50 - 100 triệu VNĐ**
- Dự phòng (10-15%): **~600 - 900 triệu VNĐ**

Tổng cộng dự kiến toàn bộ dự án: ~7.2 tỷ - 8.0 tỷ VNĐ (Con số này có thể cao hơn hoặc thấp hơn tùy thuộc vào lựa chọn cuối cùng và đàm phán giá).

Tối ưu ngân sách:

Mục tiêu là đưa tổng chi phí dưới mức ngân sách dự kiến (8tỷ VNĐ)

- **Lựa chọn thiết bị phù hợp với nhu cầu thực tế:**
    - **Spine Switch:** Cân nhắc kỹ số lượng Spine. Nếu chỉ có 1 chi nhánh chính, có thể ban đầu chỉ cần 2 Spine Switch cho Data Center trung tâm, sau đó mở rộng khi cần.
    - **Firewall:** Juniper SRX320 là lựa chọn tiết kiệm. Nếu yêu cầu tính năng UTM cao cấp hơn và ngân sách cho phép, có thể xem xét FortiGate hoặc Palo Alto Networks ở phân khúc tương đương, nhưng chi phí license có thể cao hơn. Tận dụng tối đa các tính năng sẵn có trên SRX320 trước khi mua thêm license.
    - **Server:** Tối ưu hóa ảo hóa để giảm số lượng server vật lý. Đánh giá kỹ liệu 3 server R750 đã đủ cho tất cả các workload dự kiến hay chưa, hay có thể bắt đầu với 2 server và nâng cấp sau.

- **Tối ưu hóa License:**
    - Sử dụng các phiên bản phần mềm phù hợp với nhu cầu, tránh mua các license cao cấp không cần thiết.
    - Cân nhắc các giải pháp mã nguồn mở cho một số dịch vụ (ví dụ: Zabbix/PRTG free cho giám sát, pfSense/OPNsense cho một số vai trò firewall đơn giản nếu phù hợp). Tuy nhiên, cần cân nhắc về hỗ trợ và chuyên môn quản trị.
- **Đàm phán giá với nhà cung cấp:** Mua số lượng lớn thiết bị từ một hoặc một vài nhà cung cấp uy tín để có được mức chiết khấu tốt (thường từ 5-15% hoặc hơn).
- **Phân kỳ đầu tư:**
    - Triển khai các hạng mục cốt lõi trước (Core, Distribution, kết nối WAN, Firewall cơ bản, các server thiết yếu).
    - Các tính năng nâng cao, dự phòng đầy đủ cho tất cả các site, hoặc mở rộng số lượng AP có thể được thực hiện trong các giai đoạn sau khi hệ thống đã đi vào hoạt động ổn định và có thêm ngân sách.
    - Ví dụ, ban đầu có thể chỉ trang bị 1 router/firewall cho mỗi site, sau đó nâng cấp lên HA pair.
- **Lựa chọn Access Point:** Aruba AP-515 là dòng tốt. Tuy nhiên, nếu cần tối ưu chi phí Wi-Fi, có thể xem xét các dòng AP khác của Aruba hoặc các hãng khác (Ubiquiti UniFi, TP-Link Omada) có chi phí thấp hơn nhưng vẫn đáp ứng nhu cầu cơ bản, đặc biệt nếu không yêu cầu các tính năng quản lý quá phức tạp.
- **Tự thực hiện một số phần việc (nếu có đội ngũ IT đủ năng lực):** Ví dụ, việc cấu hình cơ bản, giám sát thi công có thể giúp giảm chi phí thuê ngoài.

Kết luận

Báo cáo đã trình bày thiết kế mạng LAN chi tiết cho doanh nghiệp THACO gồm 17 phòng ban và ~2000 người dùng. Giải pháp đề xuất sử dụng kiến trúc mạng phân lớp với thiết bị từ các hãng uy tín, kết hợp hạ tầng cáp Cat6A hiện đại. Thiết kế đảm bảo hiệu năng cao, khả năng mở rộng, đồng thời tích hợp các cơ chế dự phòng và bảo mật nhiều lớp để mạng hoạt động ổn định, an toàn.

Các tính toán về số lượng cáp, lựa chọn thiết bị và chi phí cho thấy phương án nằm trong phạm vi ngân sách 6 tỷ VNĐ và tối ưu hiệu quả đầu tư. Với hệ thống này, doanh nghiệp T có thể yên tâm về một nền tảng hạ tầng mạng vững chắc phục vụ cho hoạt động hiện tại và mở rộng trong tương lai gần.

Kiến nghị: Doanh nghiệp nên tiến hành triển khai theo từng giai đoạn (mua sắm thiết bị, thi công cáp, cấu hình và kiểm thử) với sự giám sát của đội ngũ kỹ thuật. Đồng thời xây dựng các quy trình vận hành, backup cấu hình định kỳ và đào tạo nhân sự quản trị mạng để khai thác hệ thống một cách hiệu quả, lâu dài.