BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TPHCM

KHOA CÔNG NGHỆ THÔNG TIN

Báo Cáo Cuối Kỳ

THIẾT KẾ MẠNG CHO DOANH NGHIỆP

GVHD: T.S Huỳnh Nguyên Chính

Tên	MSSV
Nguyễn Thắng Lợi	22162023

TP.HCM, tháng 05/2025

MỤC LỤC

PHẦN 1. GIỚI THIỆU

Trong bối cảnh công nghệ thông tin ngày càng đóng vai trò quan trọng và là nền tảng cốt lõi cho mọi hoạt động của doanh nghiệp, việc sở hữu một hệ thống mạng máy tính hiệu quả, ổn định và an toàn là yếu tố then chốt quyết định đến sự thành công và phát triển bền vững. Hệ thống mạng không chỉ đơn thuần là công cụ kết nối các thiết bị, mà còn là hạ tầng truyền tải thông tin, hỗ trợ các ứng dụng nghiệp vụ, và là cầu nối giữa doanh nghiệp với khách hàng và đối tác.

Báo cáo này trình bày chi tiết về quá trình khảo sát, phân tích yêu cầu và đề xuất giải pháp thiết kế hệ thống mạng cho một doanh nghiệp. Mục tiêu của đồ án là xây dựng một cơ sở hạ tầng mạng máy tính hiện đại, có khả năng đáp ứng các nhu cầu hiện tại và dễ dàng mở rộng trong tương lai. Các giải pháp được đưa ra không chỉ tập trung vào hiệu năng và tính sẵn sàng cao của hệ thống mà còn chú trọng đến các yếu tố bảo mật, khả năng quản lý linh hoạt và tối ưu hóa chi phí đầu tư.

Nội dung báo cáo sẽ bao gồm các phần chính: phân tích mục tiêu thiết kế, đánh giá yêu cầu cụ thể của doanh nghiệp, trình bày sơ đồ logic và vật lý của hệ thống mạng, quy hoạch địa chỉ IP, các kỹ thuật được triển khai, danh mục thiết bị đề xuất cùng dự toán chi phí và cuối cùng là kết luận về giải pháp.

PHẦN 2. MỤC TIÊU THIẾT KẾ

Việc xác định rõ ràng các mục tiêu thiết kế là bước quan trọng, định hướng cho toàn bộ quá trình xây dựng hệ thống mạng. Các mục tiêu này được chia thành mục tiêu của tổ chức và mục tiêu về kỹ thuật, nhằm đảm bảo hệ thống mạng không chỉ đáp ứng yêu cầu vận hành mà còn phù hợp với chiến lược phát triển lâu dài của doanh nghiệp.

2.1. Mục tiêu của tổ chức

Các mục tiêu của tổ chức mà hệ thống mạng cần hướng đến bao gồm:

- **Đảm bảo hoạt động kinh doanh liên tục:** Giảm thiểu tối đa thời gian ngừng hoạt động của hệ thống mạng, từ đó tránh ảnh hưởng đến các quy trình nghiệp vụ, giao dịch với khách hàng và đối tác.
- **Nâng cao hiệu quả làm việc:** Cung cấp một hạ tầng mạng nhanh chóng, ổn định và đáng tin cậy, giúp nhân viên dễ dàng truy cập vào các tài nguyên, ứng dụng nghiệp vụ và công cụ làm việc cộng tác.
- **Tối ưu hóa chi phí vận hành:** Xây dựng một hệ thống mạng có chi phí đầu tư ban đầu hợp lý và chi phí vận hành, bảo trì, nâng cấp trong tương lai được tối ưu hóa.
- **Tăng cường khả năng cạnh tranh:** Một hệ thống mạng hiện đại và linh hoạt sẽ giúp doanh nghiệp dễ dàng ứng dụng các công nghệ mới, cải tiến quy trình và nâng cao khả năng cạnh tranh trên thị trường.
- **Bảo vệ tài sản thông tin:** Đảm bảo an toàn cho dữ liệu và các tài sản thông tin quan trọng của doanh nghiệp trước các nguy cơ tấn công từ bên trong lẫn bên ngoài.
- **Hỗ trợ tăng trưởng và mở rộng:** Thiết kế hệ thống mạng có khả năng dễ dàng mở rộng để đáp ứng sự phát triển về quy mô nhân sự, số lượng chi nhánh, và các nhu cầu kinh doanh mới trong tương lai.
- **Nâng cao sự hài lòng của khách hàng:** Gián tiếp góp phần nâng cao chất lượng dịch vụ và sản phẩm thông qua việc vận hành hiệu quả các ứng dụng hỗ trợ khách hàng.

2.2. Mục tiêu về kỹ thuật

Để đạt được các mục tiêu của tổ chức, hệ thống mạng cần đáp ứng các yêu cầu kỹ thuật sau:

- **Tính sẵn sàng cao (High Availability):** Thiết kế hệ thống với các giải pháp dự phòng cho những thành phần quan trọng như đường truyền Internet, thiết bị mạng trung tâm (core switch, firewall, router), máy chủ dịch vụ (DHCP, DNS, Email, Web) để đảm bảo hệ thống luôn hoạt động ổn định và liên tục.
- **Hiệu năng cao (High Performance):** Đảm bảo băng thông đủ lớn, độ trễ thấp và khả năng xử lý lưu lượng truy cập cao cho các ứng dụng và dịch vụ quan trọng của doanh nghiệp, đặc biệt là các ứng dụng thời gian thực như VoIP, Video Conferencing.
- **Bảo mật mạnh mẽ (Strong Security):** Áp dụng các biện pháp và công nghệ bảo mật đa lớp, từ việc kiểm soát truy cập, phân đoạn mạng (VLANs), tường lửa (Firewall), phát hiện và ngăn chặn xâm nhập (IDS/IPS), đến mã hóa dữ liệu để bảo vệ toàn diện cho hệ thống.
- **Khả năng quản lý hiệu quả (Effective Manageability):** Xây dựng hệ thống dễ dàng quản lý, giám sát tập trung, cho phép cấu hình, theo dõi trạng thái hoạt động của thiết bị và khắc phục sự cố một cách nhanh chóng và thuận tiện.
- **Khả năng mở rộng linh hoạt (Flexible Scalability):** Thiết kế theo kiến trúc module hóa, cho phép dễ dàng nâng cấp băng thông, bổ sung thiết bị, mở rộng phạm vi phủ sóng và tích hợp các công nghệ mới khi cần thiết mà không làm ảnh hưởng lớn đến cấu trúc hiện tại.
- **Tính linh hoạt (Flexibility):** Hỗ trợ đa dạng các loại hình kết nối (có dây, không dây) và các dịch vụ mạng cần thiết (DHCP, DNS, NTP,...) để đáp ứng nhu cầu làm việc đa dạng của người dùng.
- **Tối ưu hóa lưu lượng (Traffic Optimization):** Áp dụng các kỹ thuật quản lý băng thông và Chất lượng dịch vụ (QoS) để ưu tiên cho các ứng dụng quan trọng, đảm bảo trải nghiệm người dùng tốt nhất.

PHẦN 3. PHÂN TÍCH YÊU CẦU THIẾT KẾ

Để xây dựng giải pháp thiết kế mạng tối ưu, việc đầu tiên và quan trọng nhất là hiểu rõ về quy mô, nhu cầu hoạt động và các yêu cầu cụ thể của doanh nghiệp. Phần này sẽ mô tả chi tiết về doanh nghiệp giả định, từ đó làm cơ sở cho các quyết định thiết kế tiếp theo.

3.1. Quy mô và nhu cầu của doanh nghiệp

3.1.1. Giới thiệu chung về doanh nghiệp

- **Tên doanh nghiệp:** Công ty Cổ phần Phát triển Công nghệ & Giải pháp Toàn cầu (GlobalTech Solutions Corp. - GTSC).
- **Lĩnh vực hoạt động:** GTSC là một doanh nghiệp đa ngành, tập trung vào hai lĩnh vực chính:
    - **Nghiên cứu, phát triển và sản xuất phần mềm:** Cung cấp các giải pháp phần mềm quản trị doanh nghiệp (ERP), giải pháp tài chính – ngân hàng, ứng dụng di động và các nền tảng thương mại điện tử.
    - **Dịch vụ tư vấn và triển khai hệ thống Công nghệ Thông tin (CNTT):** Bao gồm tư vấn chiến lược CNTT, thiết kế và triển khai hạ tầng mạng, trung tâm dữ liệu, giải pháp an ninh mạng và dịch vụ quản trị hệ thống.
- **Tầm nhìn & Sứ mệnh:** Trở thành tập đoàn công nghệ hàng đầu khu vực, tiên phong trong việc cung cấp các giải pháp công nghệ tiên tiến, góp phần vào sự phát triển của khách hàng và cộng đồng.
- **Văn hóa doanh nghiệp:** Đề cao sự đổi mới, sáng tạo, chuyên nghiệp và lấy khách hàng làm trung tâm.

3.1.2. Quy mô cơ sở hạ tầng và nhân sự

GTSC có một trụ sở chính hiện đại tại TP. Hồ Chí Minh và hai chi nhánh hoạt động tại các thành phố lớn nhằm phục vụ khách hàng và mở rộng thị trường.

- **A. Trụ sở chính (TP. Hồ Chí Minh):**
    - **Địa điểm:** Khu Công nghệ Phần mềm Quang Trung, TP. Hồ Chí Minh.

- **Mô tả:** Là trung tâm đầu não của GTSC, nơi tập trung ban lãnh đạo, các khối R&D, kinh doanh chiến lược và trung tâm dữ liệu chính.
- **Tổng số nhân sự dự kiến tại trụ sở chính:** Khoảng 800 - 1000 người.
- **Cấu trúc tòa nhà:**
  - **Tòa nhà 1 (Building 1 - Trung tâm Điều hành & Phát triển Giải pháp):** 5 tầng nổi và 1 tầng hầm.
    - *Tầng Hầm:* **Data Center chính** của toàn công ty, phòng máy chủ, hệ thống lưu trữ SAN, hệ thống nguồn (UPS, máy phát điện dự phòng), phòng kiểm soát an ninh.
    - *Tầng 1:* Sảnh lễ tân lớn, phòng trưng bày sản phẩm & giải pháp, phòng Hành chính – Nhân sự, phòng Quan hệ Đối ngoại.
    - *Tầng 2:* Khối Phát triển Phần mềm Doanh nghiệp (ERP, CRM).
    - *Tầng 3:* Khối Phát triển Giải pháp Tài chính – Ngân hàng và Ứng dụng Di động.
    - *Tầng 4:* Ban Lãnh đạo Tập đoàn (Chủ tịch, TGĐ, các Phó TGĐ), phòng Kế hoạch – Chiến lược, phòng Pháp chế.
    - *Tầng 5:* Phòng Tài chính – Kế toán Tập đoàn, phòng Đầu tư & Phát triển Dự án.
  - **Tòa nhà 2 (Building 2 - Trung tâm R&D Công nghệ mới & Dịch vụ Kỹ thuật):** 4 tầng. (Cách Tòa nhà 1 khoảng 200m, kết nối bằng cáp quang).
    - *Tầng 1:* Phòng Nghiên cứu & Phát triển Công nghệ mới (AI, IoT, Blockchain).
    - *Tầng 2:* Trung tâm Dịch vụ Kỹ thuật và Hỗ trợ Khách hàng (Technical Support Center).
    - *Tầng 3:* Phòng Quản lý Chất lượng Sản phẩm (QA/QC), phòng Kiểm thử Phần mềm.
    - *Tầng 4:* Phòng Đào tạo Nội bộ và Phát triển Nguồn nhân lực Công nghệ.

        - **Tòa nhà 3 (Building 3 - Khối Kinh doanh & Marketing):** 4 tầng. (Cách Tòa nhà 1 khoảng 200m, kết nối bằng cáp quang).
            - *Tầng 1:* Trung tâm Tư vấn Giải pháp và Tiếp xúc Khách hàng Doanh nghiệp.
            - *Tầng 2:* Phòng Kinh doanh Giải pháp Phần mềm.
            - *Tầng 3:* Phòng Kinh doanh Dịch vụ Hạ tầng & An ninh mạng.
            - *Tầng 4:* Phòng Marketing và Truyền thông.
- **B. Chi nhánh 1 (TP. Cần Thơ):**
    - **Địa điểm:** Trung tâm TP. Cần Thơ.
    - **Chức năng:** Trung tâm phát triển phần mềm vệ tinh, hỗ trợ về kỹ thuật và kinh doanh tại khu vực ĐBSCL.
    - **Quy mô:** 4 tầng.
    - **Số lượng nhân sự dự kiến:** Khoảng 150 - 200 người.
    - *Tầng 1:* Lễ tân, Phòng Kinh doanh khu vực Mekong, Phòng Hỗ trợ Kỹ thuật tại chỗ.
    - *Tầng 2:* Đội ngũ Phát triển Phần mềm (chi nhánh).
    - *Tầng 3:* Đội ngũ Kiểm thử và Đảm bảo Chất lượng (chi nhánh).
    - *Tầng 4:* Ban Giám đốc Chi nhánh, Phòng Hành chính – Kế toán chi nhánh.
- **C. Chi nhánh 2 (Vĩnh Long):**
    - **Địa điểm:** TP. Vĩnh Long.
    - **Chức năng:** Văn phòng đại diện, hỗ trợ kinh doanh và kỹ thuật cơ bản cho các khách hàng lân cận.
    - **Quy mô:** 1 tầng.

- **Số lượng nhân sự dự kiến:** Khoảng 30 - 50 người.
- Bao gồm khu vực làm việc chung, phòng họp nhỏ, khu vực tiếp khách và hỗ trợ kỹ thuật.

- **Dự kiến tăng trưởng:** GTSC dự kiến tăng trưởng quy mô nhân sự khoảng 15-20% mỗi năm trong vòng 3-5 năm tới và có thể mở thêm các văn phòng đại diện tại các tỉnh thành khác.

3.1.3. Nhu cầu hoạt động và ứng dụng công nghệ thông tin

Với lĩnh vực hoạt động đặc thù, GTSC có nhu cầu rất cao về một hệ thống mạng ổn định, hiệu năng cao và bảo mật:

- **Hoạt động Nghiên cứu & Phát triển (R&D):**
  - Yêu cầu truy cập nhanh đến các tài nguyên lập trình, cơ sở dữ liệu lớn, môi trường thử nghiệm (development, staging).
  - Cần băng thông lớn cho việc tải lên/tải xuống mã nguồn, các bộ thư viện lớn, máy ảo.
  - Hợp tác trực tuyến giữa các nhóm phát triển tại trụ sở chính và chi nhánh.
- **Cung cấp Dịch vụ Phần mềm và Giải pháp CNTT:**
  - Hệ thống máy chủ mạnh mẽ để vận hành các ứng dụng demo, môi trường PoC (Proof of Concept) cho khách hàng.
  - Hệ thống Email (Web + Mail server trong DMZ) tin cậy để giao tiếp với khách hàng và đối tác.
  - Website công ty (trong DMZ) để giới thiệu sản phẩm, dịch vụ, tin tức, tuyển dụng.
  - Cổng thông tin hỗ trợ khách hàng trực tuyến (có thể tích hợp trên website hoặc hệ thống riêng).
- **Quản trị Doanh nghiệp:**
  - **Hệ thống ERP:** Quản lý toàn diện các hoạt động (tài chính, nhân sự, dự án, khách hàng). Yêu cầu tính sẵn sàng 24/7, bảo mật cao.
  - **Hệ thống CRM:** Quản lý thông tin và tương tác với khách hàng.

    - **Hệ thống quản lý tài liệu và tri thức nội bộ.**
    - **Hệ thống chấm công, tính lương.**
- **Truyền thông và Hợp tác:**
    - Hệ thống Video Conferencing chất lượng cao cho các cuộc họp giữa ban lãnh đạo, các phòng ban và giữa trụ sở chính với chi nhánh.
    - Hệ thống điện thoại VoIP.
    - Công cụ chat và làm việc nhóm trực tuyến.
- **An ninh và Giám sát:**
    - Hệ thống camera giám sát (CCTV) tại tất cả các tòa nhà và khu vực quan trọng.
    - Kiểm soát ra vào điện tử.
- **Kết nối mạng:**
    - **Truy cập Internet:** Tốc độ cao, ổn định, có dự phòng từ nhiều nhà cung cấp internet cho toàn bộ nhân viên và hệ thống máy chủ.
    - **Kết nối WAN:** Ổn định, an toàn và hiệu quả giữa trụ sở chính và các chi nhánh.
    - **Mạng không dây (Wi-Fi):** Phủ sóng toàn bộ các khu vực văn phòng, phòng họp, khu vực chung cho nhân viên, đối tác và khách (Guest Wi-Fi).
    - **Mạng có dây (LAN):** Hiệu suất cao cho máy tính để bàn, máy trạm R&D, máy chủ.
- **Lưu trữ và Sao lưu Dữ liệu:**
    - Hệ thống lưu trữ tập trung (SAN - Storage Area Network) cho cơ sở dữ liệu, máy ảo, dữ liệu người dùng và mã nguồn.

- Chính sách sao lưu (backup) dữ liệu tự động, định kỳ và có kế hoạch khôi phục sau thảm họa (Disaster Recovery Plan - DRP).

- **Truy cập từ xa (Remote Access):**
  - Cung cấp giải pháp truy cập từ xa an toàn (VPN) cho những nhân viên làm việc tại nhà, đi công tác hoặc đội ngũ IT quản trị hệ thống.
- **Các dịch vụ mạng cơ bản:** DHCP, DNS, NTP, File Server, Print Server.

3.2. Xác định các yêu cầu thiết kế

Dựa trên quy mô và nhu cầu hoạt động đã phân tích của GlobalTech Solutions Corp., các yêu cầu thiết kế cụ thể cho hệ thống mạng được xác định như sau:

- **Yêu cầu về hiệu năng (Performance):**
  - **Mạng lõi (Core Network):** Băng thông chuyển mạch cực lớn (hàng Terabit/giây), hỗ trợ kết nối 40Gbps/100Gbps đến lớp Phân phối (Distribution Layer) và các thành phần quan trọng trong Data Center.
  - **Mạng Phân phối (Distribution Network):** Kết nối 10Gbps/25Gbps từ Core, và cung cấp kết nối 1Gbps/10Gbps đến lớp Truy cập (Access Layer) tại mỗi tòa nhà/khu vực.
  - **Mạng Truy cập (Access Network):** Cung cấp kết nối 1Gbps cho các máy tính người dùng, hỗ trợ PoE+ (Power over Ethernet Plus) cho điện thoại IP, Camera IP và các điểm truy cập Wi-Fi. Các máy trạm chuyên dụng (R&D) có thể yêu cầu kết nối 2.5Gbps hoặc 10Gbps.
  - **Kết nối liên tòa nhà (Inter-Building):** Sử dụng liên kết cáp quang đa sợi tốc độ cao (ví dụ: 2 x 10Gbps hoặc 2 x 40Gbps EtherChannel) giữa các tòa nhà tại trụ sở chính, đảm bảo dự phòng và cân bằng tải.
  - **Mạng Không dây (WLAN):** Hỗ trợ chuẩn Wi-Fi 6/6E (802.11ax) để đáp ứng mật độ người dùng cao, cung cấp băng thông lớn và độ trễ thấp cho các ứng dụng di động và IoT. Phân chia SSID riêng cho nhân viên, khách và các thiết bị IoT.

- **Truy cập Internet:** Tổng băng thông lớn từ hai nhà cung cấp dịch vụ (ISP) khác nhau, hỗ trợ cân bằng tải và chuyển đổi dự phòng tự động.
- **Kết nối WAN (Trụ sở - Chi nhánh):** Sử dụng giải pháp SD-WAN để tối ưu hóa việc sử dụng đường truyền, đảm bảo chất lượng dịch vụ (QoS) cho các ứng dụng quan trọng (ERP, VoIP, Video Conference) và bảo mật cao. Băng thông phải đáp ứng đủ nhu cầu của từng chi nhánh.
- **Trung tâm Dữ liệu (Data Center):** Kết nối tốc độ cao (10Gbps/25Gbps/40Gbps) cho các máy chủ ứng dụng, máy chủ cơ sở dữ liệu, và hệ thống lưu trữ SAN. Độ trễ cực thấp trong Data Center.

- **Yêu cầu về ính sẵn sàng (Availability):**
  - Thiết kế dự phòng hoàn toàn (Full Redundancy) cho các thiết bị mạng trung tâm: Core Switches (ví dụ: StackWise Virtual), Firewalls (HA Cluster), SD-WAN Gateways.
  - Dự phòng liên kết (Link Redundancy) giữa các lớp mạng và các thiết bị quan trọng.
  - Dự phòng nguồn điện (Dual Power Supply) cho tất cả các thiếtبی thiết yếu, kết hợp với hệ thống UPS tập trung và máy phát điện cho Data Center và các phòng thiết bị tại mỗi tòa nhà.
  - Dự phòng cho các dịch vụ mạng nền tảng như DHCP, DNS, Active Directory thông qua cơ chế clustering hoặc triển khai nhiều máy chủ.
  - Thời gian phục hồi sau sự cố (RTO) và điểm phục hồi mục tiêu (RPO) phải được xác định rõ ràng và ở mức thấp nhất có thể cho các hệ thống trọng yếu.
- **Yêu cầu về Bảo mật (Security):**
  - **Kiến trúc Zero Trust:** Từng bước tiếp cận mô hình bảo mật không tin cậy hoàn toàn.
  - **Phân đoạn mạng (Network Segmentation):** Sử dụng VLANs và VRF (Virtual Routing and Forwarding) để cô lập lưu lượng giữa các phòng ban, giữa mạng người dùng - mạng máy chủ - mạng DMZ - mạng khách - mạng quản trị - mạng IoT/CCTV.

- **Tường lửa Thế hệ mới (NGFW):** Tại biên mạng (kết nối ra ISP), bảo vệ DMZ, và có thể giữa các vùng mạng nội bộ quan trọng (ví dụ: giữa các tòa nhà hoặc giữa mạng người dùng và Data Center). Tính năng bao gồm IPS/IDS, Application Control, Web Filtering, Antivirus Gateway.
- **Web Application Firewall (WAF):** Bảo vệ các ứng dụng web (Website công ty, cổng thông tin khách hàng) khỏi các tấn công tầng ứng dụng. (Như trong sơ đồ logic).
- **Bảo mật Điểm cuối (Endpoint Security):** Giải pháp EDR (Endpoint Detection and Response) cho máy tính người dùng và máy chủ.
- **Quản lý Truy cập Mạng (NAC - Network Access Control):** Xác thực và ủy quyền người dùng/thiết bị trước khi cho phép truy cập vào tài nguyên mạng.
- **Bảo mật Truy cập Từ xa:** Sử dụng VPN mạnh (ví dụ: SSL VPN, IPsec VPN) với xác thực đa yếu tố (MFA).
- **Bảo mật Mạng Không dây:** Sử dụng WPA3 Enterprise, xác thực 802.1X qua RADIUS server.
- **Giám sát An ninh (Security Monitoring):** Hệ thống SIEM (Security Information and Event Management) để thu thập, phân tích log và phát hiện các mối đe dọa.
- **Cập nhật bản vá và quản lý cấu hình:** Quy trình chặt chẽ để đảm bảo an toàn cho các thiết bị và phần mềm.

- **Yêu cầu về Khả năng mở rộng (Scalability):**
  - Thiết kế theo mô hình module hóa, phân cấp rõ ràng (Core - Distribution - Access), cho phép mở rộng từng thành phần độc lập.
  - Lựa chọn thiết bị có mật độ cổng cao, khả năng nâng cấp phần cứng (CPU, RAM, module giao diện) hoặc stacking/clustering.
  - Quy hoạch địa chỉ IP linh hoạt và có khả năng mở rộng (sử dụng cả IPv4 và có kế hoạch chuyển đổi sang IPv6).
  - Hệ thống cáp cấu trúc (Structured Cabling System) được thiết kế để dễ dàng bổ sung các điểm kết nối mới hoặc nâng cấp loại cáp.

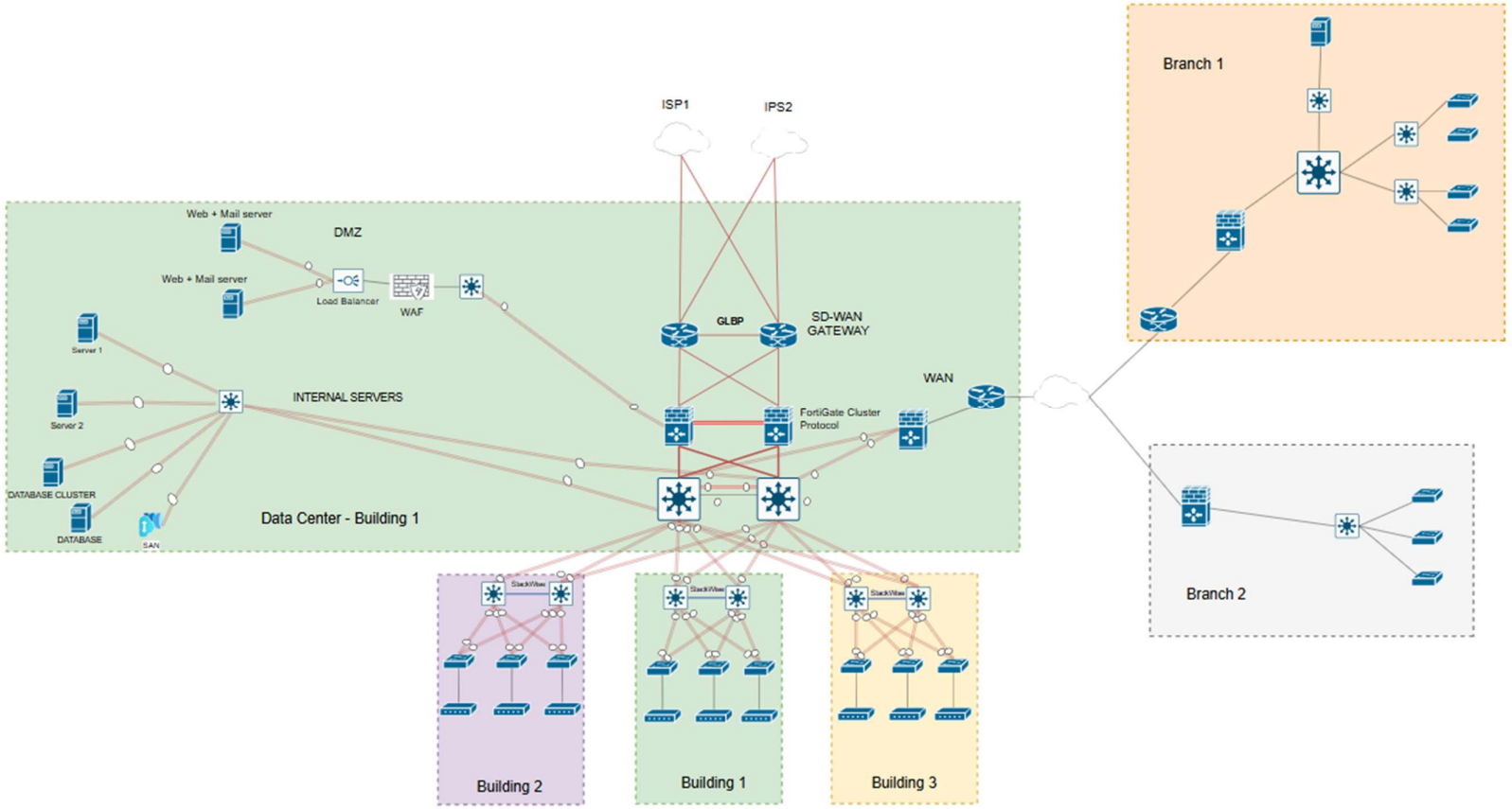
- **Yêu cầu về Quản lý (Manageability):**
    - Triển khai Hệ thống Quản lý Mạng (NMS - Network Management System) tập trung để giám sát hiệu năng, tình trạng hoạt động, cảnh báo sự cố và quản lý cấu hình của toàn bộ thiết bị mạng (Controller, Administration server như trong sơ đồ logic).
    - Sử dụng các giao thức quản lý tiêu chuẩn như SNMPv3, Syslog, NetFlow/sFlow, NTP.
    - Khả năng quản lý tập trung cho các điểm truy cập Wi-Fi (Wireless LAN Controller).
    - Tự động hóa các tác vụ quản trị lặp đi lặp lại.
    - Hệ thống tài liệu mạng chi tiết, trực quan và được cập nhật thường xuyên.
- **Yêu cầu về Chi phí (Cost-Effectiveness):**
    - Tối ưu hóa Tổng chi phí Sở hữu (TCO - Total Cost of Ownership), cân bằng giữa chi phí đầu tư ban đầu (CAPEX) và chi phí vận hành (OPEX).
    - Lựa chọn các giải pháp và thiết bị có tỷ lệ hiệu năng trên giá thành tốt, phù hợp với ngân sách của doanh nghiệp và đáp ứng được các yêu cầu kỹ thuật.
    - Ưu tiên các giải pháp tiết kiệm năng lượng.
- **Yêu cầu về Dịch vụ Mạng (Network Services):**
    - **DHCP:** Cấp phát địa chỉ IP động một cách tin cậy và có dự phòng cho các VLAN người dùng, Wi-Fi, thiết bị IoT.
    - **DNS:** Hệ thống DNS nội bộ có khả năng phân giải tên miền nhanh chóng, chính xác, có dự phòng và tích hợp với Active Directory. Forwarder ra DNS của ISP hoặc Public DNS tin cậy.
    - **NTP:** Đảm bảo đồng bộ thời gian chính xác cho tất cả thiết bị và máy chủ trong hệ thống.

- **Chất lượng Dịch vụ (QoS):** Triển khai QoS end-to-end để ưu tiên các loại lưu lượng quan trọng (VoIP, Video Conferencing, ERP, ứng dụng R&D chuyên dụng) so với các loại lưu lượng khác (truy cập web thông thường, tải file lớn không quan trọng).

PHẦN 4. SƠ ĐỒ HỆ THỐNG MẠNG

4.1. Sơ đồ luận lý (Logical Diagram)

Sơ đồ luận lý thể hiện kiến trúc tổng thể của hệ thống mạng GTSC, được thiết kế theo mô hình phân lớp hierarchial ba lớp (Core, Distribution, Access) kết hợp với các vùng chức năng chuyên biệt như Data Center, DMZ, và kết nối WAN đến các chi nhánh.



4.1.1. Kiến trúc tổng thể và các Khu vực chính

Mô hình Phân lớp:

- **Lớp Lõi (Core Layer):** Là xương sống tốc độ cao của mạng, chịu trách nhiệm chuyển mạch chính và định tuyến lưu lượng giữa các khu vực khác nhau (Data Center, các khối Distribution của tòa nhà, và biên mạng WAN/Internet). Thiết kế với hai thiết bị Core Switch Cisco Catalyst C9500 series chạy StackWise Virtual để đảm bảo tính sẵn sàng cao và băng thông lớn.
- **Lớp Phân phối (Distribution Layer):** Kết nối giữa lớp Core và lớp Access. Chịu trách nhiệm tổng hợp lưu lượng từ lớp Access, thực thi các chính sách bảo mật, định tuyến giữa các VLAN và giới hạn miền quảng bá. Mỗi tòa nhà (Building 1, 2, 3) và Data Center có các cặp Distribution Switch Cisco Catalyst C9300 series hoạt động dự phòng.
- **Lớp Truy cập (Access Layer):** Cung cấp kết nối mạng trực tiếp cho các thiết bị đầu cuối của người dùng (máy tính, điện thoại IP, máy in, camera) và các điểm truy cập không dây (APs). Sử dụng các Access Switch Cisco Catalyst C1300 series hỗ trợ PoE+ cho các thiết bị cần nguồn.

Khu vực Trung tâm Dữ liệu (Data Center - Đặt tại tầng hầm Building 1):

- **Vùng DMZ (Demilitarized Zone):**
    - **Web + Mail Server:** Cung cấp các dịch vụ công cộng như website công ty, cổng thông tin khách hàng và hệ thống email.
    - **Load Balancer (Kemp LoadMaster LM-X15 như trong danh-muc-thiet-bi.pdf):** Phân phối tải cho cụm Web/Mail server, tăng cường hiệu năng và tính sẵn sàng.
    - **WAF (Web Application Firewall):** Bảo vệ các ứng dụng web trước các cuộc tấn công tầng ứng dụng.
    - Vùng DMZ được kết nối và bảo vệ bởi cụm Firewall chính.
- **Vùng Máy chủ Nội bộ (Internal Servers):**
    - **Server 1, Server 2 (HPE ProLiant DL380 Gen11/DL360 Gen11 như trong danh-muc-thiet-bi.pdf):** Nơi đặt các máy chủ ứng dụng nghiệp vụ quan trọng (ERP, CRM), máy chủ cơ sở dữ liệu, máy chủ R&D, máy chủ quản lý file (SAN),...

- **SAN (Storage Area Network):** Hệ thống lưu trữ tập trung hiệu năng cao cho toàn bộ dữ liệu quan trọng của công ty.
- **Administration, Controller, DHCP, DNS:** Các máy chủ quản trị hệ thống, máy chủ quản lý Wi-Fi Controller, dịch vụ cấp phát IP (DHCP) và phân giải tên miền (DNS) nội bộ.
- Các máy chủ nội bộ được kết nối vào lớp Distribution của Data Center, đảm bảo tốc độ truy cập cao và được bảo vệ bởi các chính sách an ninh.

Kết nối Internet và Biên mạng (WAN Edge):

- **ISP1 & ISP2:** Hệ thống sử dụng hai đường truyền Internet từ hai nhà cung cấp dịch vụ khác nhau để đảm bảo tính sẵn sàng và cân bằng tải.
- **GLBP (Gateway Load Balancing Protocol) Routers:** Cặp router biên chạy GLBP để cung cấp default gateway ảo có khả năng dự phòng và phân tải cho các kết nối ra Internet.
- **Firewalls (FortiGate 1000F Cluster):** Hai thiết bị Firewall FortiGate 1000F chạy ở chế độ High Availability (Active-Active FGCP) là cổng kiểm soát an ninh chính, thực hiện lọc gói tin, NAT, VPN, IPS/IDS cho toàn bộ lưu lượng ra vào mạng.
- **SD-WAN Gateway:** Thiết bị chuyên dụng để quản lý và tối ưu hóa kết nối WAN đến các chi nhánh, hỗ trợ lựa chọn đường đi thông minh, đảm bảo QoS cho ứng dụng.

Kết nối Chi nhánh (Branch 1 - Cần Thơ, Branch 2 - Vĩnh Long):

- Các chi nhánh được kết nối về trụ sở chính thông qua SD-WAN Gateway, sử dụng các đường truyền WAN (ví dụ: MPLS, Internet Leased Line, FTTH) với các cơ chế dự phòng.
- Mỗi chi nhánh có hạ tầng mạng riêng bao gồm Router/SD-WAN edge device, Firewall (nếu cần thiết ở chi nhánh lớn), Switch Access và Access Points để phục vụ người dùng tại chỗ.

4.1.2. Luồng dữ liệu và Tương tác giữa các thành phần

- Lưu lượng từ người dùng tại các tòa nhà (Building 1, 2, 3) đi qua Access Switches, lên Distribution Switches (nơi thực hiện định tuyến giữa các VLAN của phòng ban), sau đó có thể đi đến Core Switches để truy cập tài nguyên trong Data Center hoặc ra Internet/WAN qua cụm Firewall và Router biên.
- Lưu lượng truy cập các dịch vụ công cộng (Web, Mail) từ Internet sẽ đi qua Router biên, Firewall, WAF, Load Balancer rồi mới đến các máy chủ trong DMZ.
- Lưu lượng giữa trụ sở chính và các chi nhánh được định tuyến và bảo mật thông qua SD-WAN Gateway và cụm Firewall chính.
- Các máy chủ trong Data Center giao tiếp với nhau qua mạng tốc độ cao của Data Center (Distribution và Core Layer của Data Center).

4.1.3. Biện luận đồ luận lý

Thiết kế luận lý này đáp ứng các yêu cầu của GTSC như sau:

- **Tính Sẵn sàng Cao:**
    - Redundancy ở mọi lớp: Core Switches (StackWise Virtual), Distribution Switches (cặp dự phòng), Firewalls (HA Cluster), Router biên (GLBP), Dual ISP, SD-WAN với nhiều đường truyền.
    - Dự phòng cho các máy chủ dịch vụ quan trọng (DHCP, DNS, Load Balancer cho Web/Mail).
- **Hiệu năng Cao:**
    - Phân lớp rõ ràng giúp tối ưu hóa luồng dữ liệu. Lớp Core tốc độ rất cao.
    - Băng thông lớn cho Data Center, kết nối liên tòa nhà và kết nối đến các server.
    - SD-WAN giúp tối ưu hiệu năng ứng dụng qua WAN. Load Balancer tối ưu hiệu năng cho server DMZ.
- **Bảo mật Mạnh mẽ:**
    - Vùng DMZ tách biệt các dịch vụ công cộng.

- Cụm Firewall mạnh mẽ ở biên và có thể giữa các vùng nội bộ. WAF bảo vệ ứng dụng web.
- Phân đoạn mạng chi tiết (VLANs) sẽ được định nghĩa ở phần quy hoạch IP, giới hạn bởi Distribution Layer và Firewall.

- **Khả năng Mở rộng:**
  - Kiến trúc phân lớp và module hóa cho phép dễ dàng thêm người dùng, thêm tòa nhà, mở rộng Data Center hoặc thêm chi nhánh.
  - SD-WAN đơn giản hóa việc kết nối và quản lý các chi nhánh mới.
- **Khả năng Quản lý:**
  - Kiến trúc rõ ràng giúp dễ dàng xác định sự cố và quản lý. Các máy chủ quản trị (Administration, Controller) được bố trí tập trung

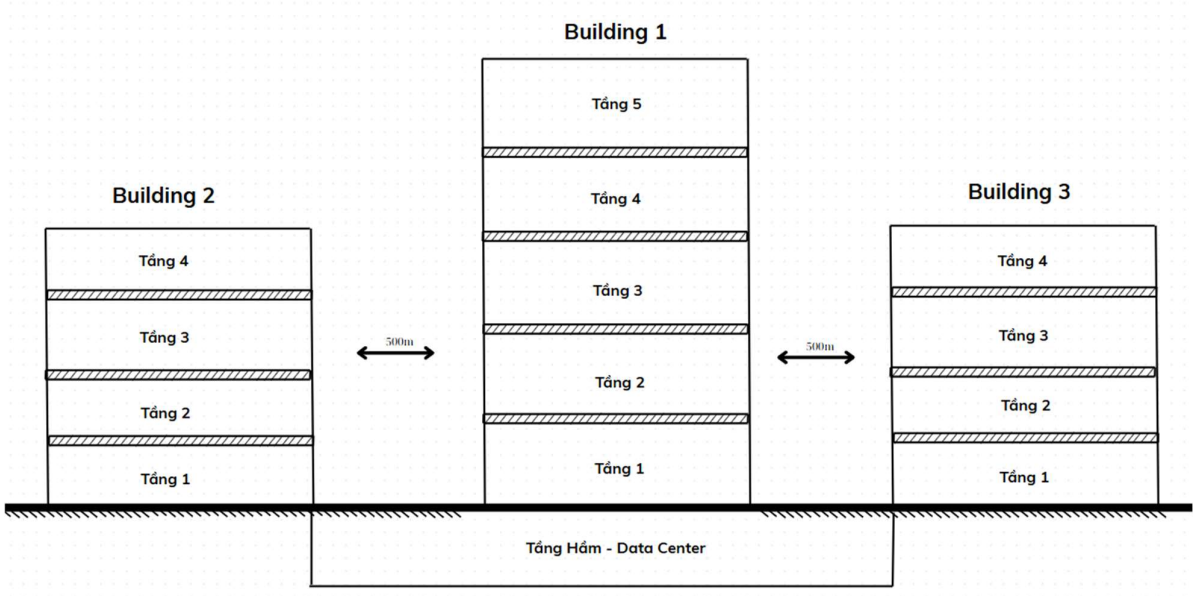
4.2. Sơ đồ vật lý (Physical Diagram)

Sơ đồ vật lý mô tả vị trí lắp đặt thực tế của các thiết bị mạng, hệ thống tủ rack, và đường đi của hệ thống cáp mạng trong khuôn viên trụ sở chính và các chi nhánh của GTSC.

4.2.1. Bố trí tổng thể tại Trụ sở chính (TP. Hồ Chí Minh)

- **Sơ đồ tổng thể campus:**
  - Thể hiện rõ vị trí của 3 tòa nhà: Building 1 (5 tầng + tầng hầm), Building 2 (4 tầng), Building 3 (4 tầng).
  - Tầng hầm của Building 1 được chỉ định là vị trí của Trung tâm Dữ liệu (Data Center) chính.
  - Khoảng cách 200m giữa Building 1 với Building 2 và Building 1 với Building 3 là yếu tố quan trọng để lựa chọn loại cáp quang kết nối liên tòa nhà (dự kiến là Single-Mode Fiber để đảm bảo băng thông và khoảng cách xa hơn trong tương lai nếu cần).

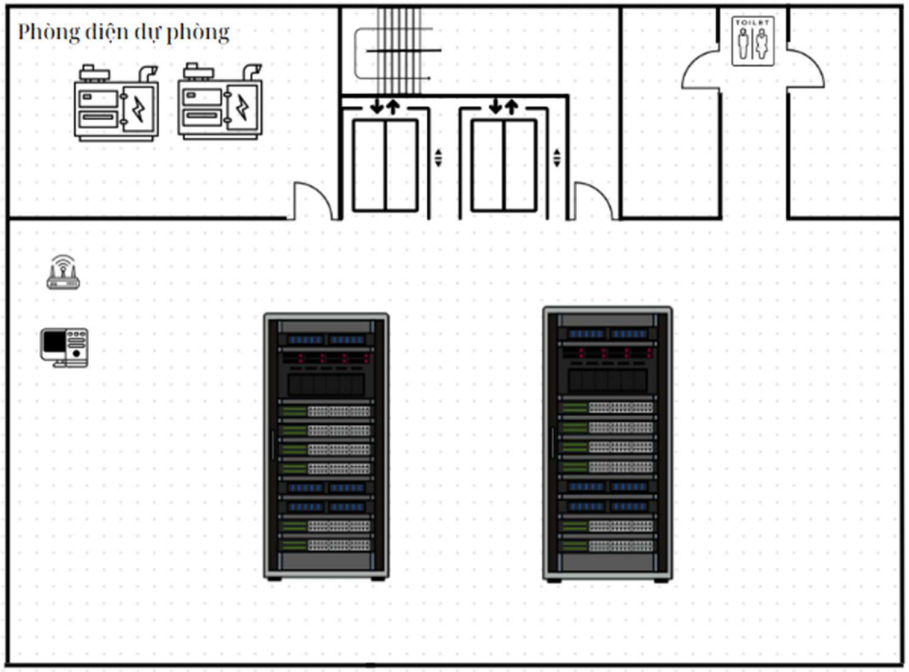
Campus trụ sở chính tại TP. HCM



4.2.2. Bố trí chi tiết Trung tâm Dữ liệu (Tầng hầm Building 1)

- **Sơ đồ Tầng hầm Building 1:**
  - Hiển thị hai dãy tủ rack chính, nơi lắp đặt các thiết bị mạng lõi (Core Switches), tường lửa (Firewalls), router biên, SD-WAN gateway, các máy chủ ứng dụng, máy chủ cơ sở dữ liệu, hệ thống lưu trữ SAN, và các thiết bị hỗ trợ khác.
  - Phòng điện dự phòng (UPS, máy phát) được bố trí gần đó, đảm bảo cung cấp nguồn liên tục cho Data Center.
  - Hệ thống làm mát, phòng cháy chữa cháy, kiểm soát ra vào vật lý được ngầm định là có để đảm bảo môi trường hoạt động tối ưu và an toàn cho thiết bị.
  - Đây là Main Distribution Frame (MDF) của toàn bộ campus.

Tầng hầm Building 1, nơi đặt Data Center



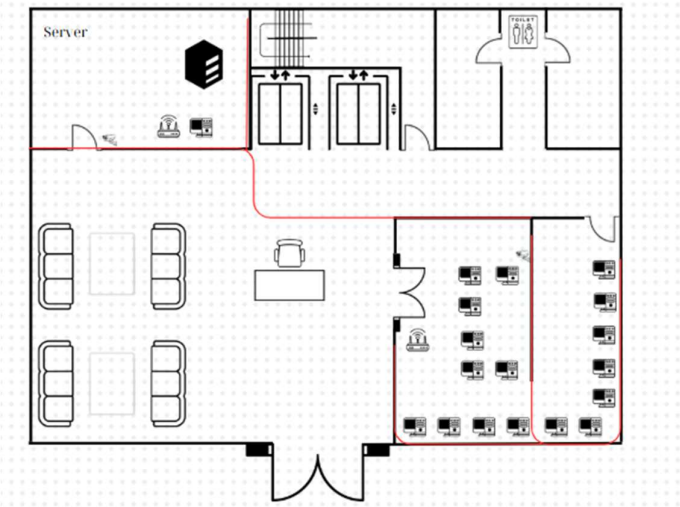
4.2.3. Bố trí chi tiết tại các tầng của Tòa nhà (Trụ sở chính)

- **Sơ đồ Tầng 1 các tòa nhà:**
  - Mỗi tòa nhà có một phòng kỹ thuật hoặc tủ rack (Intermediate Distribution Frame - IDF) tập trung tại mỗi tầng hoặc cho một khu vực lớn. Sơ đồ tầng 1 cho thấy có khu vực "Server" nhỏ, đây có thể là phòng IDF của tầng.
  - Các Access Switch và patch panel được đặt trong các IDF này.

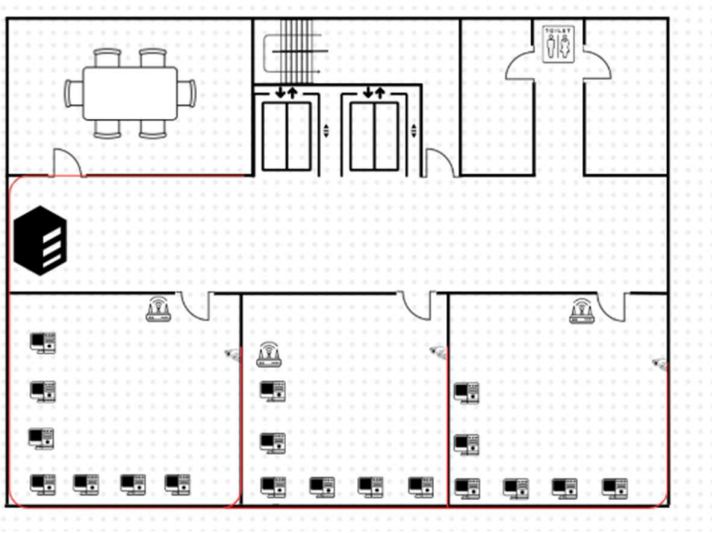
- Hệ thống cáp ngang (Horizontal Cabling) từ IDF sẽ đi đến các ổ cắm mạng (network outlets) tại bàn làm việc của nhân viên, phòng họp.
- Các điểm truy cập không dây (APs) được lắp đặt trên trần tại các vị trí chiến lược để đảm bảo vùng phủ sóng tối ưu.

- **Sơ đồ các tầng khác:**
  - Tương tự như tầng 1, mỗi tầng sẽ có ít nhất một IDF chứa Access Switches.
  - Sự phân bố thiết bị sẽ dựa trên mật độ người dùng và yêu cầu kết nối của từng phòng ban.
  - Cáp trục đứng (Vertical Cabling) kết nối các IDF ở các tầng về MDF của tòa nhà (nếu có) hoặc trực tiếp về lớp Distribution của tòa nhà đó, sau đó kết nối về Data Center (Building 1). Cáp trục đứng thường là cáp quang để đảm bảo băng thông.

Tầng 1 của các tòa building 1-2-3



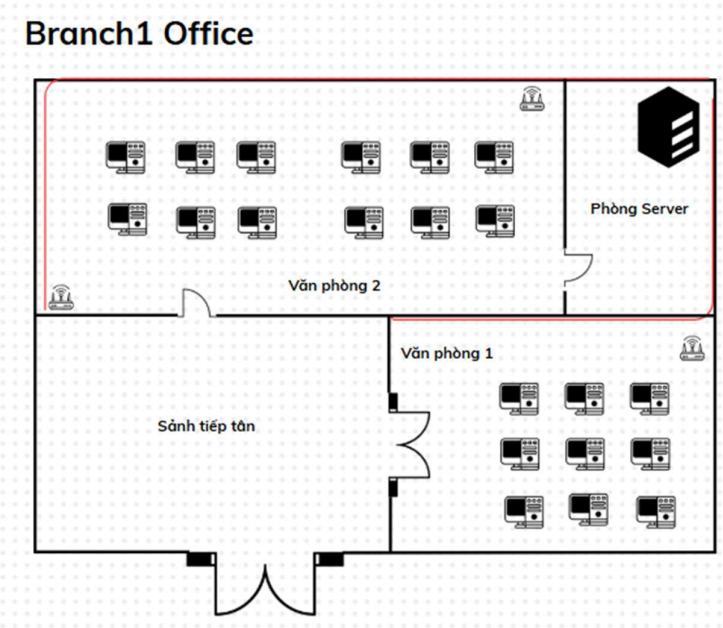
Các tầng khác trong 3 tòa nhà ở campus chính



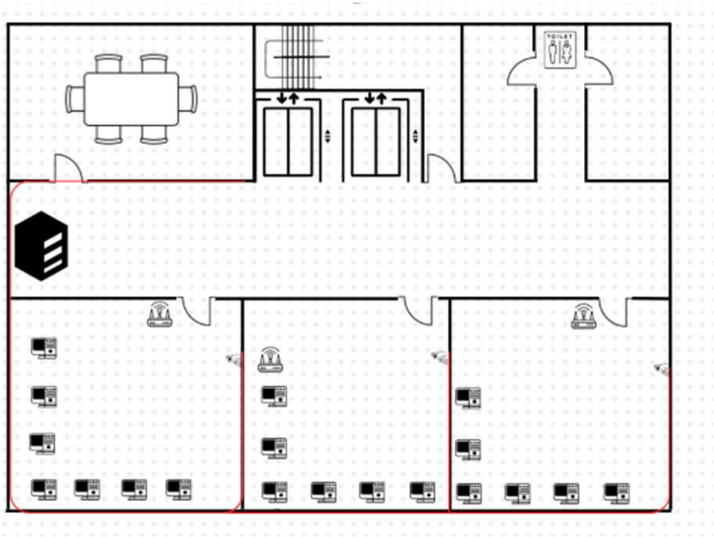
4.2.4. Bố trí chi tiết tại các Chi nhánh

- **Chi nhánh 1 (TP. Cần Thơ)**
    - Sơ đồ tầng 1 cho thấy có "Phòng Server", đây là nơi đặt các thiết bị mạng chính của chi nhánh như router/SD-WAN edge, firewall (nếu có), switch tập trung và có thể một vài máy chủ cục bộ (ví dụ: file server, print server).
    - Mỗi tầng của chi nhánh sẽ có các Access Switch và APs tương tự như ở trụ sở chính, được kết nối về phòng server trung tâm của chi nhánh.

Tầng 1 của Chi nhánh 1

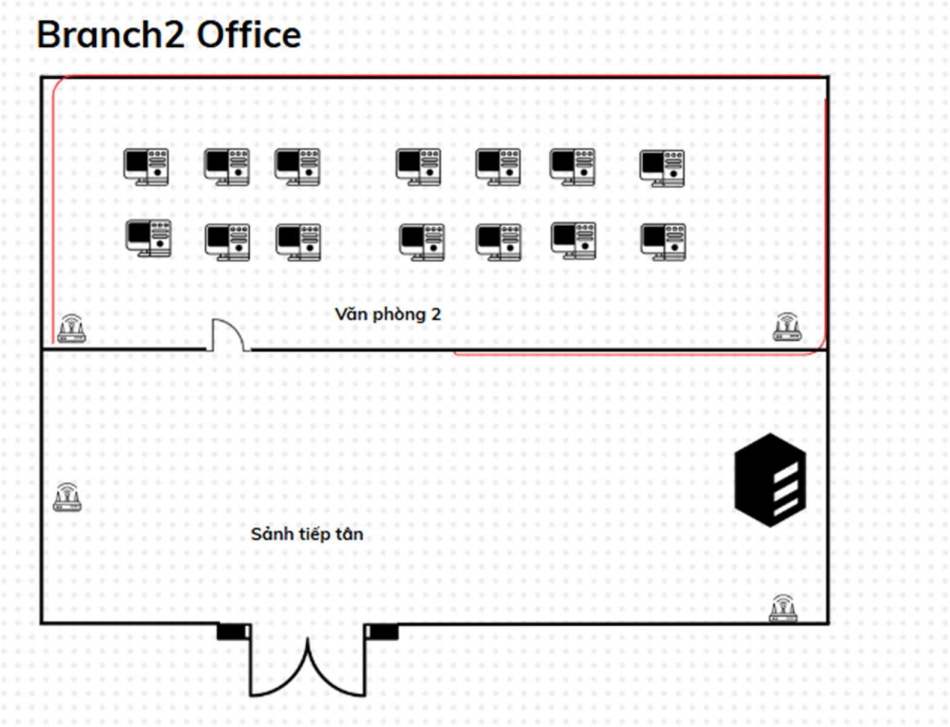


Các tầng khác tương tự ở campus chính



- **Chi nhánh 2 (Vĩnh Long):**
    - Tương tự, có một khu vực đặt thiết bị mạng ("Phòng Server" hoặc tủ rack) để quản lý kết nối cho toàn bộ văn phòng.

Branch 2: có 1 tầng duy nhất tại Vĩnh Long



4.2.5. Hệ thống Cáp mạng (Cabling Infrastructure)

- **Cáp quang liên tòa nhà (Inter-Building Backbone):** Sử dụng cáp quang Single-Mode (SMF) OS2, dự phòng nhiều đôi sợi, chạy trong ống bảo vệ ngầm hoặc treo giữa các tòa nhà để kết nối lớp Distribution của Building 2 và Building 3 về lớp Core/Distribution trong Data Center (Building 1). Tốc độ dự kiến 2x10Gbps hoặc 2x40Gbps cho mỗi tòa nhà.
- **Cáp trục đứng trong tòa nhà (Intra-Building Backbone):** Sử dụng cáp quang Multi-Mode (MMF) OM4 hoặc OM5 từ MDF/IDF chính của tòa nhà đến các IDF trên mỗi tầng.

- **Cáp ngang đến người dùng (Horizontal Cabling):** Sử dụng cáp đồng xoắn đôi Category 6A (Cat6A) UTP/FTP để hỗ trợ tốc độ 10Gbps ở khoảng cách ngắn nếu cần cho máy trạm R&D, và tối thiểu là Cat6 cho các kết nối 1Gbps thông thường.
- **Hệ thống Patch Panel, Outlet, Tủ Rack:** Lắp đặt chuyên nghiệp, dán nhãn rõ ràng theo tiêu chuẩn để dễ dàng quản lý, bảo trì và mở rộng.

4.2.6. Biện luận về Sơ đồ Vật lý

- **Hỗ trợ Sơ đồ Luận lý:** Bố trí vật lý phản ánh rõ ràng kiến trúc phân lớp và các vùng chức năng đã được thiết kế trong sơ đồ luận lý.
- **Tối ưu hóa Hiệu năng và Độ tin cậy:**
    - Data Center trung tâm giúp quản lý tập trung các tài nguyên quan trọng.
    - Phân bố các IDF hợp lý giúp giảm chiều dài cáp ngang, đảm bảo chất lượng tín hiệu.
    - Lựa chọn loại cáp phù hợp với khoảng cách và yêu cầu băng thông.
- **Đảm bảo An toàn Vật lý:** Data Center và các phòng IDF cần được bảo vệ về mặt vật lý (kiểm soát ra vào, camera, PCCC, làm mát).
- **Khả năng Bảo trì và Mở rộng:**
    - Hệ thống cáp cấu trúc tiêu chuẩn giúp dễ dàng thay thế, sửa chữa và thêm mới các điểm kết nối.
    - Các tủ rack được bố trí khoa học, có không gian cho việc lắp đặt thêm thiết bị.
- **Phù hợp Quy mô Doanh nghiệp:** Thiết kế vật lý đáp ứng được số lượng tòa nhà, số tầng và sự phân bổ nhân sự của GTSC tại trụ sở chính cũng như các chi nhánh.

PHẦN 5. QUY HOẠCH ĐỊA CHỈ IP

5.1. Nguyên tắc chung và Dải địa chỉ sử dụng

- **Dải địa chỉ IP Private:** Hệ thống mạng của GTSC sẽ sử dụng dải địa chỉ IP private theo RFC 1918. Với quy mô và nhu cầu mở rộng của GTSC, dải địa chỉ **10.0.0.0/8** (từ 10.0.0.0 đến 10.255.255.255) được lựa chọn để cung cấp không gian địa chỉ rộng lớn và linh hoạt cho tất cả các khu vực mạng tại trụ sở chính và các chi nhánh.
- **Sử dụng VLSM (Variable Length Subnet Mask):** Áp dụng VLSM để chia mạng con một cách hiệu quả, tiết kiệm địa chỉ IP và phù hợp với số lượng thiết bị dự kiến trong mỗi VLAN/subnet.
- **Dự phòng cho tăng trưởng:** Kích thước của mỗi subnet được tính toán dựa trên số lượng thiết bị hiện tại và dự kiến tăng trưởng khoảng 20% mỗi năm trong vòng 5 năm tới.
- **Tính dễ nhớ và nhất quán:** Cố gắng đặt tên VLAN ID và các octet trong địa chỉ IP một cách logic để dễ dàng nhận diện và quản lý.

5.2. Phân chia VLAN và Subnet chi tiết

Dưới đây là bảng quy hoạch chi tiết các VLAN và subnet cho trụ sở chính (TP.HCM) và các chi nhánh của GTSC:

5.2.1. Trụ sở chính (TP. Hồ Chí Minh)

Dải IP chính cho Trụ sở: 10.0.0.0/12 (từ 10.0.0.0 đến 10.15.255.255)

VLAN ID	Tên VLAN / Mục đích	Subnet IP	Network Address	Usable Host Range	Broadcast Address	Subnet Mask	Default Gateway	Số lượng host tối đa	Ghi chú
10	Quản lý Thiết bị Mạng (Management)	10.0.0.0/23	10.0.0.0	10.0.0.1 - 10.0.1.254	10.0.1.255	255.255.254.0	10.0.0.1	510	Switches, Routers, Firewalls, AP Controllers, SD-WAN, WAF, Load Balancer (management interfaces)

Data Center									
20	DC - Servers Nội bộ (Production)	10.0.2.0/23	10.0.2.0	10.0.2.1 - 10.0.3.254	10.0.3.255	255.255.254.0	10.0.2.1	510	ERP, CRM, Core DBs, AD, DNS, DHCP, File Servers, Application Servers
22	DC - Servers Nội bộ (Dev/Test/Staging)	10.0.4.0/23	10.0.4.0	10.0.4.1 - 10.0.5.254	10.0.5.255	255.255.254.0	10.0.4.1	510	Môi trường phát triển, kiểm thử
24	DC - SAN & Storage Management	10.0.6.0/26	10.0.6.0	10.0.6.1 - 10.0.6.62	10.0.6.63	255.255.255.192	10.0.6.1	62	Giao diện quản lý của hệ thống lưu trữ SAN, FC Switches
30	DC - DMZ Servers	10.0.7.0/25	10.0.7.0	10.0.7.1 - 10.0.7.126	10.0.7.127	255.255.255.128	10.0.7.1	126	Web Servers, Mail Servers, Public DNS, Load Balancer VIPs
Building 1 Users									
101	B1 - R&D Hardware	10.1.0.0/24	10.1.0.0	10.1.0.1 - 10.1.0.254	10.1.0.255	255.255.255.0	10.1.0.1	254	
102	B1 - R&D Software	10.1.1.0/24	10.1.1.0	10.1.1.1 - 10.1.1.254	10.1.1.255	255.255.255.0	10.1.1.1	254	
103	B1 - Ban Lãnh đạo & Kế hoạch	10.1.2.0/25	10.1.2.0	10.1.2.1 - 10.1.2.126	10.1.2.127	255.255.255.128	10.1.2.1	126	
104	B1 - Tài chính & Kế toán	10.1.3.0/25	10.1.3.0	10.1.3.1 - 10.1.3.126	10.1.3.127	255.255.255.128	10.1.3.1	126	
105	B1 - Hành chính, Nhân sự & Pháp chế	10.1.4.0/25	10.1.4.0	10.1.4.1 - 10.1.4.126	10.1.4.127	255.255.255.128	10.1.4.1	126	

Building 2 Users									
201	B2 - R&D Công nghệ mới	10.2.0.0/24	10.2.0.0	10.2.0.1 - 10.2.0.254	10.2.0.255	255.255.255.0	10.2.0.1	254	
202	B2 - TT Dịch vụ Kỹ thuật & Hỗ trợ KH	10.2.1.0/24	10.2.1.0	10.2.1.1 - 10.2.1.254	10.2.1.255	255.255.255.0	10.2.1.1	254	
203	B2 - QA/QC & Kiểm thử	10.2.2.0/24	10.2.2.0	10.2.2.1 - 10.2.2.254	10.2.2.255	255.255.255.0	10.2.2.1	254	
204	B2 - Đào tạo & Phát triển NNL Công nghệ	10.2.3.0/25	10.2.3.0	10.2.3.1 - 10.2.3.126	10.2.3.127	255.255.255.128	10.2.3.1	126	
Building 3 Users									
301	B3 - TT Tư vấn Giải pháp & Tiếp xúc KH	10.3.0.0/24	10.3.0.0	10.3.0.1 - 10.3.0.254	10.3.0.255	255.255.255.0	10.3.0.1	254	
302	B3 - KD Giải pháp Phần mềm	10.3.1.0/24	10.3.1.0	10.3.1.1 - 10.3.1.254	10.3.1.255	255.255.255.0	10.3.1.1	254	
303	B3 - KD Dịch vụ Hạ tầng & An ninh mạng	10.3.2.0/24	10.3.2.0	10.3.2.1 - 10.3.2.254	10.3.2.255	255.255.255.0	10.3.2.1	254	
304	B3 - Marketing & Truyền thông	10.3.3.0/25	10.3.3.0	10.3.3.1 - 10.3.3.126	10.3.3.127	255.255.255.128	10.3.3.1	126	
Dịch vụ chung Trụ sở chính									
50	VoIP HQ	10.0.8.0/22	10.0.8.0	10.0.8.1 - 10.0.11.254	10.0.11.255	255.255.252.0	10.0.8.1	1022	Điện thoại IP

60	CCTV HQ	10.0.12.0/23	10.0.12.0	10.0.12.1 - 10.0.13.254	10.0.13.255	255.255.254.0	10.0.12.1	510	Camera IP giám sát
70	Printers HQ	10.0.14.0/25	10.0.14.0	10.0.14.1 - 10.0.14.126	10.0.14.127	255.255.255.128	10.0.14.1	126	Máy in mạng
80	Wi-Fi Corporate HQ	10.0.16.0/21	10.0.16.0	10.0.16.1 - 10.0.23.254	10.0.23.255	255.255.248.0	10.0.16.1	2046	Laptop, thiết bị di động của nhân viên (kết nối Wi-Fi)
90	Wi-Fi Guest HQ	10.0.24.0/23	10.0.24.0	10.0.24.1 - 10.0.25.254	10.0.25.255	255.255.254.0	10.0.24.1	510	Khách truy cập, cô lập với mạng nội bộ
Liên kết Point-to-Point (P2P) HQ									
500-599	P2P Links HQ	10.15.250.0/24	Phân chia /30			255.255.255.252	x.x.x.1 / x.x.x.2	2/link	Kết nối giữa Core-Distribution, Core-Firewall, Firewall-Router,... Sẽ phân bổ cụ thể khi cấu hình. Ví dụ: 10.15.250.0/30, 10.15.250.4/30

5.2.2. Chi nhánh 1 (TP. Cần Thơ)

Dải IP chính cho Chi nhánh 1: 10.64.0.0/16 (từ 10.64.0.0 đến 10.64.255.255)

VLAN ID	Tên VLAN / Mục đích	Subnet IP	Default Gateway (Virtual IP)	Số lượng host tối đa	Ghi chú
6410	BR1 - Quản lý Thiết bị Mạng	10.64.0.0/24	10.64.0.1	254	
6411	BR1 - Users Floor 1 (KD, HTKT)	10.64.1.0/24	10.64.1.1	254	
6412	BR1 - Users Floor 2 (Dev Team)	10.64.2.0/24	10.64.2.1	254	
6413	BR1 - Users Floor 3 (QA Team)	10.64.3.0/24	10.64.3.1	254	
6414	BR1 - Users Floor 4 (Mgmt, Admin)	10.64.4.0/25	10.64.4.1	126	
6420	BR1 - Servers (Nếu có)	10.64.5.0/26	10.64.5.1	62	Máy chủ cục bộ (nếu cần)
6450	BR1 - VoIP Phones	10.64.8.0/24	10.64.8.1	254	
6460	BR1 - CCTV Cameras	10.64.9.0/25	10.64.9.1	126	
6480	BR1 - Wi-Fi Corporate	10.64.16.0/23	10.64.16.1	510	
6490	BR1 - Wi-Fi Guest	10.64.18.0/24	10.64.18.1	254	
6499	BR1 - P2P Links	10.64.255.0/26	x.x.x.1 / x.x.x.2	2/link	Chia /30 cho các kết nối P2P nội bộ chi nhánh

5.2.3. Chi nhánh 2 (Vĩnh Long)

Dải IP chính cho Chi nhánh 2: 10.65.0.0/16 (từ 10.65.0.0 đến 10.65.255.255)

VLAN ID	Tên VLAN / Mục đích	Subnet IP	Default Gateway (Virtual IP)	Số lượng host tối đa	Ghi chú
6510	BR2 - Quản lý Thiết bị Mạng	10.65.0.0/25	10.65.0.1	126	
6511	BR2 - Users (Văn phòng chung)	10.65.1.0/24	10.65.1.1	254	
6550	BR2 - VoIP Phones	10.65.8.0/26	10.65.8.1	62	
6560	BR2 - CCTV Cameras	10.65.9.0/27	10.65.9.1	30	
6580	BR2 - Wi-Fi Corporate	10.65.16.0/24	10.65.16.1	254	
6590	BR2 - Wi-Fi Guest	10.65.17.0/25	10.65.17.1	126	
6599	BR2 - P2P Links	10.65.255.0/27	x.x.x.1 / x.x.x.2	2/link	Chia /30 cho các kết nối P2P nội bộ chi nhánh

5.3. Default Gateway dự phòng

- Tại Trụ sở chính, các VLAN người dùng và máy chủ sẽ sử dụng địa chỉ IP ảo làm Default Gateway. Địa chỉ IP ảo này được cung cấp bởi giao thức dự phòng gateway như **GLBP (Gateway Load Balancing Protocol)**, HSRP (Hot Standby Router Protocol) hoặc VRRP (Virtual Router Redundancy Protocol) chạy trên cặp Core Switch (L3).
    - Ví dụ: Cho VLAN 101 (10.1.0.0/24), Default Gateway ảo là 10.1.0.1. Core Switch 1 có thể có IP 10.1.0.2, Core Switch 2 có IP 10.1.0.3 trên interface VLAN 101.

- Tương tự tại các chi nhánh lớn (Chi nhánh 1) nếu có thiết bị L3 distribution dự phòng. Tại chi nhánh nhỏ (Chi nhánh 2), default gateway sẽ là địa chỉ IP của router/firewall biên.

5.4. Cấp phát IP tĩnh và động (DHCP)

- **IP tĩnh:**
    - Được sử dụng cho tất cả các thiết bị mạng (Switches, Routers, Firewalls, AP Controllers, APs trong một số mô hình), máy chủ (Servers trong Data Center và DMZ), máy in mạng, thiết bị VoIP gateway, đầu ghi camera (NVR), và các thiết bị quan trọng khác.
    - Thông thường, một dải nhỏ ở đầu hoặc cuối mỗi subnet sẽ được dành riêng cho việc cấp phát IP tĩnh (ví dụ: .1 đến .20 hoặc .254 xuống .230). Default gateway luôn là địa chỉ đầu tiên hoặc cuối cùng trong dải usable.
- **IP động (DHCP):**
    - Hệ thống DHCP Server trung tâm (dự phòng) đặt tại Data Center (VLAN 20) sẽ cấp phát địa chỉ IP động cho các thiết bị người dùng cuối (máy tính, laptop), điện thoại IP, thiết bị kết nối Wi-Fi (Corporate và Guest).
    - Các L3 interface (SVI - Switched Virtual Interface) trên Core/Distribution switches sẽ được cấu hình với câu lệnh ip helper-address để chuyển tiếp các bản tin DHCP Discover từ client đến DHCP Server.
    - Phạm vi (scope) DHCP sẽ được cấu hình tương ứng cho từng VLAN, loại trừ các dải IP tĩnh đã định nghĩa. Thời gian cho thuê (lease time) sẽ được thiết lập phù hợp (ví dụ: 8 ngày cho mạng có dây, 1 ngày cho Wi-Fi Corporate, 2-4 giờ cho Wi-Fi Guest).

5.5. Kế hoạch IPv6

Mặc dù quy hoạch IPv4 là trọng tâm chính ở thời điểm hiện tại, GTSC cần có kế hoạch sẵn sàng cho việc triển khai IPv6 trong tương lai:

- **Lựa chọn Prefix IPv6:** Khi có nhu cầu, GTSC sẽ đăng ký một prefix IPv6 từ ISP (ví dụ: /48 hoặc /56).
- **Quy hoạch Subnet IPv6:** Mỗi VLAN IPv4 sẽ tương ứng với một subnet IPv6 (thường là /64).

- **Phương thức Cấp phát:** Sử dụng SLAAC (Stateless Address Autoconfiguration) kết hợp với DHCPv6 (cho DNS, domain name) hoặc chỉ DHCPv6.
- **Dual-Stack:** Trong giai đoạn chuyển tiếp, hệ thống sẽ hoạt động ở chế độ dual-stack (hỗ trợ cả IPv4 và IPv6) trên các thiết bị và máy chủ quan trọng.
- Tất cả các thiết bị mạng mới được mua sắm cần đảm bảo hỗ trợ đầy đủ IPv6.

PHẦN 6. CÁC KỸ THUẬT TRIỂN KHAI

Để hiện thực hóa một hệ thống mạng mạnh mẽ, linh hoạt và an toàn cho GTSC, việc áp dụng các kỹ thuật và công nghệ tiên tiến là điều tất yếu. Phần này sẽ trình bày chi tiết về các kỹ thuật triển khai chính, từ lớp vật lý, lớp liên kết dữ liệu, lớp mạng, đến các giải pháp bảo mật, WAN và dịch vụ mạng. Các kỹ thuật này được lựa chọn dựa trên yêu cầu về hiệu năng, tính sẵn sàng, khả năng mở rộng và bảo mật của GTSC, đồng thời tham chiếu các thiết bị đã được lựa chọn trong danh mục (Phần 7).

6.1. Kỹ thuật Hạ tầng Lớp 2 (Layer 2 Technologies)

6.1.1. Mạng LAN Ảo (VLANs) và Trunking (IEEE 802.1Q)

- **Mô tả:** VLANs được sử dụng để phân đoạn mạng một cách logic thành nhiều miền quảng bá (broadcast domain) riêng biệt trên cùng một hạ tầng vật lý. Điều này giúp tăng cường an ninh, cải thiện hiệu năng và đơn giản hóa việc quản lý mạng. Các cổng kết nối giữa các switch (ví dụ: Access-Distribution, Distribution-Core) sẽ được cấu hình ở chế độ Trunking sử dụng giao thức IEEE 802.1Q để cho phép lưu lượng của nhiều VLAN đi qua.
- **Triển khai tại GTSC:**
    - Các VLAN sẽ được tạo theo quy hoạch địa chỉ IP đã trình bày ở Phần 5, bao gồm VLAN cho từng phòng ban/khối người dùng tại mỗi tòa nhà, VLAN cho Server (Internal, DMZ), VLAN Quản lý, VLAN VoIP, VLAN CCTV, VLAN Wi-Fi (Corporate, Guest).

- Các Access Switch (Cisco Catalyst C1300 series) sẽ gán cổng cho các VLAN tương ứng. Các kết nối uplink từ Access lên Distribution (Cisco Catalyst C9300 series) và từ Distribution lên Core (Cisco Catalyst C9500 series) sẽ là các đường trunk 802.1Q.

6.1.2. Giao thức Spanning Tree (STP)

- **Mô tả:** STP (IEEE 802.1D) và các biến thể cải tiến như Rapid Spanning Tree Protocol (RSTP - IEEE 802.1w) hoặc Multiple Spanning Tree Protocol (MSTP - IEEE 802.1s) được sử dụng để ngăn chặn hiện tượng lặp vòng (loop) ở lớp 2 trong các mạng có đường kết nối dự phòng, đồng thời vẫn cho phép các liên kết dự phòng này tự động được kích hoạt khi liên kết chính gặp sự cố.
- **Triển khai tại GTSC:**
  - RSTP sẽ được kích hoạt trên tất cả các switch để đảm bảo thời gian hội tụ nhanh (vài giây) khi có thay đổi trong topo mạng.
  - Cặp Core Switch (Cisco Catalyst C9500) sẽ được cấu hình với độ ưu tiên (priority) cao nhất để trở thành Root Bridge chính và phụ cho các VLAN, đảm bảo kiến trúc loop-free ổn định.
  - Các tính năng như BPDU Guard, Root Guard sẽ được triển khai trên các cổng Access để tăng cường sự ổn định của STP.

6.1.3. Gộp Kênh (Link Aggregation - EtherChannel)

- **Mô tả:** EtherChannel (hay Port Channel) là kỹ thuật cho phép gộp nhiều cổng vật lý thành một kênh logic duy nhất, giúp tăng băng thông tổng hợp và cung cấp khả năng dự phòng liên kết. Giao thức LACP (Link Aggregation Control Protocol - IEEE 802.3ad) được sử dụng để tự động hóa việc cấu hình và duy trì các kênh EtherChannel.
- **Triển khai tại GTSC:**
  - **Core - Distribution:** Sử dụng SFP+ 10G EtherChannel (2x10Gbps) giữa mỗi Core Switch và cụm Distribution Switch của từng tòa nhà/khu vực Data Center.
  - **Distribution - Access:** Sử dụng SFP 1G/10G EtherChannel giữa Distribution Switches và các Access Switches quan trọng hoặc các Access Switch tổng hợp nhiều người dùng.

- **Kết nối Server:** Các máy chủ quan trọng (HPE ProLiant DL380/DL360 Gen11) có thể sử dụng NIC Teaming/Bonding (tương đương EtherChannel) để kết nối đến Access/Distribution switches trong Data Center với tốc độ 2x10GbE.
- **Kết nối giữa các thiết bị HA:** Ví dụ, giữa hai Firewall FortiGate trong cụm HA hoặc giữa hai Core Switch trong cấu hình StackWise Virtual.

6.1.4. Ảo hóa và Gộp Chồng Switch (Switch Stacking/Virtualization)

- **Mô tả:** Các công nghệ này cho phép nhiều switch vật lý hoạt động như một switch logic duy nhất, đơn giản hóa việc quản lý, tăng băng thông stack và loại bỏ sự cần thiết của các giao thức loop avoidance phức tạp giữa các switch trong stack.
- **Triển khai tại GTSC:**
  - **Core Layer (Cisco Catalyst C9500):** Hai thiết bị Core Switch Cisco Catalyst C9500-24Y4C-A sẽ được triển khai với công nghệ **StackWise Virtual**. Điều này cho phép hai switch hoạt động như một thực thể logic duy nhất, cung cấp một mặt phẳng điều khiển (control plane) và mặt phẳng quản lý (management plane) chung, đồng thời tăng gấp đôi băng thông hệ thống và khả năng phục hồi nhanh chóng.
  - **Distribution Layer (Cisco Catalyst C9300):** Các cặp Distribution Switch Cisco Catalyst C9300-48T-M trong mỗi tòa nhà hoặc khu vực Data Center sẽ được kết nối bằng công nghệ **StackWise-480**, tạo thành một switch logic duy nhất với băng thông stack cao (480Gbps), đơn giản hóa cấu hình và tăng cường tính sẵn sàng.

6.2. Kỹ thuật Hạ tầng Lớp 3 (Layer 3 Technologies)

6.2.1. Định tuyến giữa các VLAN (Inter-VLAN Routing)

- **Mô tả:** Do VLANs tạo ra các miền quảng bá riêng biệt, việc định tuyến là cần thiết để cho phép các thiết bị ở các VLAN khác nhau có thể giao tiếp với nhau (nếu được cho phép bởi chính sách an ninh).
- **Triển khai tại GTSC:**
  - Inter-VLAN routing sẽ được thực hiện chủ yếu trên cặp Core Switch Cisco Catalyst C9500. Mỗi VLAN sẽ có một Switched Virtual Interface (SVI) được cấu hình trên Core Switch, đóng vai trò là default gateway cho các thiết bị trong VLAN đó.

- Tại các chi nhánh lớn có Distribution Switch Layer 3, Inter-VLAN routing có thể được thực hiện tại lớp Distribution của chi nhánh.

6.2.2. Giao thức Định tuyến Nội miền (Interior Gateway Protocol - IGP)

- **Mô tả:** IGP được sử dụng để trao đổi thông tin định tuyến giữa các router và switch Layer 3 trong cùng một hệ thống tự trị (Autonomous System - AS). OSPF (Open Shortest Path First) là một IGP phổ biến dựa trên trạng thái đường link (link-state), cung cấp khả năng hội tụ nhanh và hỗ trợ các thiết kế mạng phức tạp.
- **Triển khai tại GTSC:**
  - OSPF sẽ là IGP chính được triển khai tại trụ sở chính, chạy giữa các Core Switches, Distribution Switches (nếu chúng tham gia định tuyến L3), và các router biên (nếu có).
  - Hệ thống mạng OSPF sẽ được thiết kế với một Area 0 (Backbone Area) bao gồm các Core Switches và các kết nối chính. Các tòa nhà hoặc khu vực lớn có thể được cấu hình thành các Area riêng (Stub Area, NSSA) để tối ưu hóa bảng định tuyến và giảm thiểu việc trao đổi thông tin OSPF nếu cần.
  - Router ID sẽ được cấu hình duy nhất cho mỗi thiết bị tham gia OSPF. Chi phí (cost) của các đường link sẽ được điều chỉnh để ưu tiên các đường băng thông cao.

6.2.3. Giao thức Dự phòng Gateway Đầu tiên (First Hop Redundancy Protocol - FHRP)

- **Mô tả:** FHRP cung cấp khả năng dự phòng cho default gateway của các thiết bị đầu cuối. Nếu một router gateway gặp sự cố, một router khác sẽ tự động đảm nhận vai trò đó mà không làm gián đoạn kết nối của người dùng. GLBP (Gateway Load Balancing Protocol) là một giao thức FHRP của Cisco cho phép sử dụng đồng thời nhiều gateway và cân bằng tải giữa chúng.
- **Triển khai tại GTSC:**
  - GLBP sẽ được cấu hình trên các SVI của Core Switches (Cisco Catalyst C9500) cho các VLAN người dùng và server. Một địa chỉ IP ảo duy nhất sẽ được quảng bá làm default gateway, và lưu lượng sẽ được phân phối giữa hai Core Switch, tối ưu hóa việc sử dụng tài nguyên và cung cấp dự phòng liền mạch.
  - Router biên kết nối ra ISP cũng có thể được cấu hình với GLBP nếu có nhiều hơn một router.

6.3. Kỹ thuật Bảo mật (Security Technologies)

6.3.1. Tường lửa (Firewall) và Tính năng Sẵn sàng Cao (HA)

- **Mô tả:** Tường lửa là thành phần bảo mật thiết yếu, kiểm soát luồng lưu lượng ra vào mạng và giữa các vùng mạng khác nhau dựa trên các chính sách an ninh.
- **Triển khai tại GTSC:**
    - Hai thiết bị tường lửa **FortiGate 1000F** sẽ được triển khai ở biên mạng, kết nối giữa mạng nội bộ và Internet, cũng như bảo vệ vùng DMZ.
    - Chúng sẽ được cấu hình ở chế độ **FGCP (FortiGate Cluster Protocol) Active-Active** để đảm bảo tính sẵn sàng cao và tăng cường thông lượng xử lý. Nếu một Firewall gặp sự cố, Firewall còn lại sẽ tiếp quản toàn bộ lưu lượng mà không gây gián đoạn.
    - Các chính sách (Policies) sẽ được định nghĩa chi tiết để cho phép/chặn lưu lượng dựa trên nguồn, đích, cổng, ứng dụng. Các tính năng NGFW như IPS/IDS, Application Control, Web Filtering, Antivirus Gateway sẽ được kích hoạt.

6.3.2. Web Application Firewall (WAF)

- **Mô tả:** WAF được thiết kế để bảo vệ các ứng dụng web trước các cuộc tấn công phổ biến ở tầng ứng dụng như SQL injection, Cross-Site Scripting (XSS),...
- **Triển khai tại GTSC:** Một giải pháp WAF (có thể là tính năng trên FortiGate hoặc một thiết bị WAF chuyên dụng nếu ngân sách cho phép) sẽ được đặt trước các Web Server và Mail Server trong vùng DMZ để tăng cường lớp bảo vệ. Sơ đồ logic đã thể hiện sự hiện diện của WAF.

6.3.3. Kiểm soát Truy cập Mạng (Network Access Control - NAC)

- **Mô tả:** NAC cho phép kiểm soát việc truy cập vào mạng dựa trên việc xác thực định danh người dùng và tình trạng tuân thủ chính sách bảo mật của thiết bị đầu cuối.
- **Triển khai tại GTSC:**

- Triển khai giải pháp NAC sử dụng chuẩn **IEEE 802.1X** cho cả kết nối có dây và không dây. Người dùng sẽ cần xác thực (ví dụ: qua Active Directory) trước khi được cấp quyền truy cập vào mạng.
- Các cổng trên Access Switch sẽ được cấu hình cho 802.1X.

6.3.4. Các biện pháp bảo mật lớp 2 khác

- **DHCP Snooping:** Ngăn chặn các DHCP server giả mạo.
- **Dynamic ARP Inspection (DAI):** Ngăn chặn tấn công ARP spoofing.
- **IP Source Guard:** Ngăn chặn giả mạo địa chỉ IP.
- Các kỹ thuật này sẽ được triển khai trên các Access Switch để bảo vệ người dùng.

6.3.5. Mạng Riêng Ảo (VPN)

- **Site-to-Site VPN:** Sử dụng IPsec VPN làm kênh kết nối dự phòng hoặc kết nối chính cho các chi nhánh nhỏ nếu SD-WAN gặp sự cố hoặc chưa triển khai tới đó.
- **Remote Access VPN:** Cung cấp SSL VPN hoặc IPsec VPN (với client) cho nhân viên làm việc từ xa, đảm bảo kết nối an toàn đến tài nguyên nội bộ. FortiGate 1000F hỗ trợ các loại VPN này.

6.4. Kỹ thuật Mạng Diện rộng (WAN Technologies)

6.4.1. SD-WAN (Software-Defined WAN)

- **Mô tả:** SD-WAN là một kiến trúc mạng WAN hiện đại cho phép quản lý tập trung, tự động hóa việc lựa chọn đường truyền tối ưu dựa trên ứng dụng, cải thiện hiệu năng và giảm chi phí vận hành WAN.
- **Triển khai tại GTSC:**
  - Một SD-WAN Gateway sẽ được triển khai tại trụ sở chính và các thiết bị SD-WAN edge tại mỗi chi nhánh.

- Giải pháp này sẽ cho phép GTSC sử dụng linh hoạt nhiều loại đường truyền (MPLS, Internet Leased Line, FTTH), tự động định tuyến lưu lượng ứng dụng quan trọng (ERP, VoIP) qua đường truyền tốt nhất, và đơn giản hóa việc quản lý kết nối WAN.

6.4.2. Dự phòng Đường truyền Internet (Dual ISP)

- **Mô tả:** Kết nối đến hai nhà cung cấp dịch vụ Internet (ISP) khác nhau để đảm bảo kết nối Internet liên tục ngay cả khi một trong hai đường truyền gặp sự cố.
- **Triển khai tại GTSC:** Hai đường truyền Internet từ ISP1 và ISP2 sẽ được kết nối vào cụm Firewall/Router biên. Có thể sử dụng BGP (Border Gateway Protocol) để quảng bá prefix IP của GTSC (nếu có IP public riêng) hoặc sử dụng các kỹ thuật load balancing/failover trên Firewall.

6.5. Kỹ thuật Mạng Không dây (Wireless Technologies)

6.5.1. Chuẩn Wi-Fi và Bảo mật

- **Mô tả:** Triển khai mạng không dây hiệu năng cao và an toàn.
- **Triển khai tại GTSC:**
  - Các điểm truy cập không dây (APs) **FortiAP 431F** hỗ trợ chuẩn **Wi-Fi 6 (802.11ax)** sẽ được lắp đặt tại tất cả các khu vực văn phòng.
  - Bảo mật mạng không dây sẽ sử dụng **WPA3 Enterprise** với xác thực qua **802.1X/EAP** (kết nối đến RADIUS server, thường tích hợp với Active Directory).
  - SSID riêng biệt sẽ được tạo cho mạng Wi-Fi nhân viên (Corporate Wi-Fi) và mạng Wi-Fi cho khách (Guest Wi-Fi). Mạng Guest Wi-Fi sẽ được cô lập hoàn toàn với mạng nội bộ.

6.5.2. Quản lý Wi-Fi Tập trung

- **Mô tả:** Sử dụng Wireless LAN Controller (WLC) hoặc giải pháp quản lý trên cloud để cấu hình, giám sát và quản lý tập trung tất cả các APs trong hệ thống.

- **Triển khai tại GTSC:** FortiAP 431F có thể được quản lý tập trung thông qua **FortiGate Firewall** (đóng vai trò WLC) hoặc qua **FortiAP Cloud**. Điều này giúp đơn giản hóa việc triển khai chính sách, cập nhật firmware và theo dõi hiệu suất mạng Wi-Fi.

6.6. Dịch vụ Mạng (Network Services)

6.6.1. DHCP (Dynamic Host Configuration Protocol)

- **Mô tả:** Cung cấp địa chỉ IP và các thông tin cấu hình mạng khác (default gateway, DNS server) một cách tự động cho các thiết bị client.
- **Triển khai tại GTSC:**
    - Hai máy chủ **Windows Server 2025 Standard** (HPE ProLiant DL360 Gen11) sẽ được cấu hình làm DHCP Server, hoạt động ở chế độ dự phòng (DHCP Failover - Load Balancing hoặc Hot Standby).
    - Các scope DHCP sẽ được tạo cho từng VLAN người dùng và Wi-Fi theo quy hoạch IP.
    - ip helper-address sẽ được cấu hình trên các SVI của Core/Distribution switches.

6.6.2. DNS (Domain Name System)

- **Mô tả:** Phân giải tên miền thành địa chỉ IP và ngược lại.
- **Triển khai tại GTSC:**
    - Hai máy chủ **Windows Server 2025 Standard** (cùng với DHCP Server) sẽ được cấu hình làm DNS Server nội bộ, tích hợp với Active Directory. Chúng sẽ chịu trách nhiệm phân giải tên miền nội bộ của GTSC (ví dụ: gtsc.local hoặc *.gtsc.com.vn).
    - Cấu hình Primary và Secondary DNS Server để đảm bảo tính sẵn sàng.
    - Các DNS Server nội bộ sẽ được cấu hình Forwarder đến DNS của ISP hoặc Public DNS (ví dụ: Google DNS 8.8.8.8, Cloudflare 1.1.1.1) để phân giải các tên miền Internet.

6.6.3. NTP (Network Time Protocol)

- **Mô tả:** Đồng bộ thời gian cho tất cả các thiết bị và máy chủ trong mạng.
- **Triển khai tại GTSC:** Một hoặc hai máy chủ NTP nội bộ (có thể là một vai trò trên Domain Controller) sẽ được cấu hình để đồng bộ thời gian từ một nguồn thời gian tin cậy trên Internet. Tất cả các thiết bị mạng, máy chủ và máy trạm sẽ được cấu hình để đồng bộ thời gian với NTP server nội bộ này.

6.6.4. Cân bằng tải Máy chủ (Server Load Balancing)

- **Mô tả:** Phân phối lưu lượng truy cập đến một cụm máy chủ để cải thiện hiệu năng, tính sẵn sàng và khả năng mở rộng của ứng dụng.
- **Triển khai tại GTSC:** Thiết bị **Kemp LoadMaster LM-X15** sẽ được sử dụng để cân bằng tải L4/L7 cho cụm Web Server và Mail Server trong vùng DMZ.

6.6.5. Chất lượng Dịch vụ (Quality of Service - QoS)

- **Mô tả:** QoS cho phép ưu tiên các loại lưu lượng mạng quan trọng hơn so với các loại lưu lượng khác, đảm bảo hiệu năng cho các ứng dụng nhạy cảm với độ trễ và băng thông như VoIP, Video Conferencing, ERP.
- **Triển khai tại GTSC:** Chính sách QoS sẽ được triển khai trên các thiết bị mạng từ Access, Distribution, Core đến WAN edge. Lưu lượng sẽ được phân loại (Classification), đánh dấu (Marking - DSCP), đưa vào hàng đợi (Queuing) và lập lịch (Scheduling) dựa trên độ ưu tiên đã định.

6.7. Quản lý và Giám sát Mạng (Network Management and Monitoring)

- **SNMP (Simple Network Management Protocol):** SNMPv3 (phiên bản an toàn hơn) sẽ được kích hoạt trên tất cả các thiết bị mạng để cho phép thu thập thông tin trạng thái và hiệu năng.
- **Syslog:** Tất cả các thiết bị mạng và máy chủ sẽ được cấu hình để gửi log đến một Syslog Server tập trung để lưu trữ, phân tích và phục vụ việc điều tra sự cố.

- **NMS (Network Management System):** Một giải pháp NMS (ví dụ: Cisco DNA Center cho các thiết bị Cisco, FortiManager/FortiAnalyzer cho Fortinet, hoặc một giải pháp NMS của bên thứ ba như PRTG, SolarWinds) sẽ được triển khai để cung cấp giao diện quản lý, giám sát trực quan, cảnh báo tự động và báo cáo hiệu năng cho toàn bộ hệ thống mạng.

PHẦN 7. DANH MỤC THIẾT BỊ VÀ DỰ TOÁN

STT	Loại thiết bị	Tên thiết bị & thông số chi tiết	Đơn vị tính	Số lượng	Đơn giá (VND)	Tổng (VND)
1.1	Core Switch	Cisco Catalyst C9500-24Y4C-A (24x25G SFP28, 4x100G QSFP28)	Cái	2	518.400.000	1.036.800.000
1.1.2001	Nguồn cho Core Switch	C9K-PWR-650WAC-R (650W AC Power Supply)	Cái	4	19.175.000 (ước tính ~767 USD)	76.700.000
1.1.2002	Fan Tray cho Core Switch	C9K-T1-FANTRAY	Cái	2	6.385.000 (ước tính ~255 USD)	12.770.000
1.1.2003	SSD cho Core Switch	C9K-F1-SSD-240G (Pluggable SSD 240GB)	Cái	2	88.487.000 (ước tính ~3,539 USD)	176.974.000
1.1.2004	License cho Core Switch	C9500-DNA-L-A-3Y (Cisco DNA Advantage, 3 Years for C9500)	Gói	2	224.500.000 (ước tính ~8,980 USD)	449.000.000
1.1.2005	Module quang 100G (cho Core-Firewall)	QSFP-100G-SR4-S (hoặc tương đương)	Module	4	10.000.000	40.000.000
1.1.2006	Module quang 10G (cho Core-Distribution)	SFP-10G-SR-S (hoặc tương đương)	Module	12	1.500.000	18.000.000
2.1	Distribution Switch	Cisco Catalyst C9300-48T-M (48x1G Copper, Modular Uplink)	Cái	6	120.000.000	720.000.000

2.1.2001	Nguồn cho Dist. Switch	PWR-C1-715WAC-P (715W AC Power Supply, Platinum)	Cái	12	12.000.000 (ước tính ~480 USD)	144.000.000
2.1.2002	Fan Tray cho Dist. Switch	(C9300 Fan Tray - thường đi kèm, kiểm tra lại) FAN-T1	Cái	6	2.000.000	12.000.000
2.1.2003	Module Uplink cho Dist. Switch	C9300-NM-8X (8-port 10G SFP+ Network Module)	Cái	6	63.750.000 (ước tính ~2,550 USD List)	382.500.000
2.1.2004	Cáp Stack cho Dist. Switch	STACK-T1-50CM (50cm StackWise-480 Stacking Cable)	Sợi	6	1.500.000	9.000.000
2.1.2005	License cho Dist. Switch	C9300-DNA-A-3Y (Cisco DNA Advantage, 3 Years for C9300)	Gói	6	37.000.000 (ước tính ~1,481 USD)	222.000.000
3.1	Access Switch	Cisco Catalyst C1300-48FP-4X (48x1G PoE+ 740W, 4x10G SFP+)	Cái	40	35.000.000	1.400.000.000
3.1.2001	License cho Access Switch	Network Essentials (Perpetual - thường đi kèm với dòng C1000/C1300)	Gói	40	0	0
3.1.2002	Module quang 1G (Uplink Access Switch)	GLC-SX-MMD (MMF) hoặc GLC-LH-SMD (SMF)	Module	80	3.200.000	256.000.000
4.1	Firewall	Fortinet FortiGate 1000F	Cái	2	646.625.000 (ước tính ~25,865 USD)	1.293.250.000

4.1.2001	Nguồn cho Firewall	SP-FG400F-PS (AC Power Supply for FortiGate 1000F - nếu cần mua thêm làm dự phòng, FortiGate 1000F thường có sẵn 2 nguồn)	Cái	2	5.000.000	10.000.000
4.1.2002	License & Subscription Firewall	FortiGate-1000F Hardware + 3 Year FortiCare Premium and FortiGuard Enterprise Protection (FC-10-F100F-950-02-36)	Gói	2	2.490.000.000 (ước tính ~99,600 USD)	4.980.000.000
4.1.2003	Module quang 25G (cho Firewall)	Fortinet FG-TRAN-SFP28-SR (hoặc tương đương)	Module	4	5.450.000 (ước tính ~202 EUR)	21.800.000
5.1	Access Point	Fortinet FortiAP 431F (Wi-Fi 6, Tri-radio, 4x4 MU-MIMO)	Cái	75	25.000.000 (ước tính ~1,000 USD)	1.875.000.000
5.1.2001	License quản lý AP (nếu cần cho FortiCloud)	FortiAP Cloud Management License (3 năm/AP)	License/AP	75	7.500.000 (ước tính ~300 USD)	562.500.000
6.1	Load Balancer	Kemp LoadMaster LM-X15 (8x1GbE, 4x10GbE SFP+, 15Gbps L4 Throughput)	Cái	1	398.750.000 (ước tính ~15,950 USD)	398.750.000
7.1	Máy chủ DMZ (Web/Mail)	HPE ProLiant DL360 Gen11 (Cấu hình chi tiết: 2x Intel Xeon Platinum 8468 48-core/CPU, 256GB RAM DDR5, 2x960GB NVMe U.3 RI SSD, 6x16TB SAS 7.2K LFF HDD, Broadcom	Bộ	2	450.000.000	900.000.000

		57414 2x10GbE SFP+ Adapter, 2xHPE 800W PSU, 3yr NBD Support)				
7.2	Máy chủ Internal (AD/DNS/DHCP/DB/App)	HPE ProLiant DL380 Gen11 (Cấu hình chi tiết: 1x Intel Xeon Silver 4416+ 20-core, 256GB RAM DDR5, 2x960GB NVMe U.3 RI SSD, 6x16TB SAS 7.2K LFF HDD, Broadcom 57414 2x10GbE SFP+ Adapter, 2xHPE 800W PSU, 3yr NBD Support)	Bộ	2	300.000.000	600.000.000
8.1	Windows Server 2025 Standard Core License	License cho DMZ Servers (96 cores vật lý/server)	Core Pack	48	5.000.000 (ước tính ~200USD/2-core pk)	240.000.000
8.2	Windows Server 2025 Standard Core License	License cho Internal Servers (20 cores vật lý/server)	Core Pack	10	5.000.000 (ước tính ~200USD/2-core pk)	50.000.000
8.3	Windows Server CAL	User CALs hoặc Device CALs cho Windows Server 2025	CAL	~800	1.250.000 (ước tính ~50 USD/CAL)	1.000.000.000
8.4	Phần mềm Database (nếu cần bản quyền)	Ví dụ: SQL Server Standard (nếu MariaDB không đủ)	License	4	98.625.000 (ước tính ~3,945USD/2core)	394.500.000
9.1	Firewall/SD-WAN Edge Branch 1	FortiGate 100F (bao gồm 3yr FortiCare & FortiGuard)	Cái	1	223.000.000	223.000.000

9.2	Distribution/Aggregation Switch Branch 1	Cisco Catalyst C1300-24T-4X (24x1G Copper, 4x10G SFP+)	Cái	2	35.790.000	71.580.000
9.3	Access Switch Branch 1	Cisco Catalyst C1300-24FP-4X (24x1G PoE+, 4x10G SFP+)	Cái	8	25.000.000	200.000.000
9.4	Access Point Branch 1	FortiAP 431F	Cái	15	25.000.000 (ước tính ~1,000 USD)	375.000.000
10.1	Firewall/SD-WAN Edge Branch 2	FortiGate 60F (bao gồm 3yr FortiCare & FortiGuard)	Cái	1	54.375.000	54.375.000
10.2	Access Switch Branch 2	Cisco Catalyst C1300-24FP-4X	Cái	2	25.000.000	50.000.000
10.3	Access Point Branch 2	FortiAP 231F (Wi-Fi 6, 2x2 MU-MIMO)	Cái	4	5.375.000 (ước tính ~215 USD)	21.500.000
11.1	Cáp quang MMF OM4 Duplex LC-LC	Patch cord các độ dài (1m, 2m, 3m, 5m, 10m)	Sợi	~300	~200,000	~60,000,000
11.2	Cáp quang SMF OS2 Duplex LC-LC	Patch cord các độ dài (10m, 20m, 50m, >200m cho liên tòa nhà)	Sợi	~50	~250,000	~12,500,000
11.3	Cáp mạng Cat6A (UTP/FTP)	Thùng 305m, chất lượng cao (Belden, Commscope, AMP, etc.)	Thùng	~100	~7,000,000	~700,000,000
11.4	Nhân công mạng (Modular Jack Cat6A)	Nhân công chất lượng cao	Cái	~1300	~80,000	~104,000,000

11.5	Mặt nạ (Faceplate) & Đế âm/nổi	Mặt đơn/đôi cho ổ cắm mạng	Bộ	~1300	~30,000	~39,000,000
11.6	Dây nhảy mạng (Patch Cord Cat6A)	Các độ dài (1m, 2m, 3m) từ patch panel đến switch, từ ổ cắm đến PC	Sợi	~2600	~70,000	~182,000,000
11.7	Patch Panel Cat6A	24 port hoặc 48 port, loaded hoặc unloaded	Cái	~60	~3,000,000	~180,000,000
11.8	Thanh quản lý cáp (Cable Management Panel)	1U/2U, ngang/dọc	Cái	~60	~300,000	~18,000,000
12.1	Tủ Rack 42U (cho Data Center, MDF)	Kích thước tiêu chuẩn (ví dụ: 600x1000mm hoặc 800x1000mm)	Cái	6	~25,000,000	~150,000,000
12.2	Tủ Rack 15U-20U (cho IDF tầng, chi nhánh)	Treo tường hoặc đặt sàn nhỏ	Cái	~20	~5,000,000	~100,000,000
12.3	UPS (Bộ lưu điện) Online	Công suất tổng thể cho Data Center (ví dụ: 2x30KVA redundant), UPS cho MDF/IDF các tòa nhà (ví dụ: 3-5KVA/tủ), UPS cho chi nhánh.	Hệ thống	1	500.000.000	500.000.000
12.4	Thanh nguồn PDU (Power Distribution Unit)	PDU cơ bản hoặc PDU thông minh (có đo đếm)	Cái	~30	~2,000,000	~60,000,000
13.1	Dịch vụ Đường truyền Internet (hàng năm)	Gói cước Leased Line & FTTH tốc độ cao từ 2 ISP	Gói/Năm	1.620.000.000	1.620.000.000	1.620.000.000

		cho HQ, và các gói phù hợp cho chi nhánh.				
13.2	Chi phí Nhân sự Thi công & Lắp đặt	Bao gồm kéo cáp, bấm đầu mạng, lắp đặt thiết bị vào tủ rack, dán nhãn.	Gói	364.000.000	364.000.000	364.000.000
13.3	Chi phí Nhân sự Cấu hình & Tích hợp Hệ thống	Cấu hình switch, router, firewall, server, storage, Wi-Fi, security, SD-WAN, các dịch vụ mạng.	Gói	700.000.000	700.000.000	700.000.000
13.4	Chi phí Quản lý Dự án	Nhân sự quản lý dự án từ phía nhà thầu hoặc thuê ngoài.	Gói	(Tính sau, 7.5% của Tổng Mục 1-13.3)	(Tính sau)	(Tính sau, 7.5% của Tổng Mục 1-13.3)
13.5	Chi phí Đào tạo Quản trị Hệ thống	Đào tạo cho đội ngũ IT của GTSC về cách vận hành, quản trị và khắc phục sự cố cơ bản.	Gói	100.000.000	100.000.000	100.000.000
13.6	Chi phí Tư vấn Thiết kế (nếu thuê ngoài)	Chi phí cho đơn vị tư vấn thực hiện khảo sát, phân tích, thiết kế chi tiết.	Gói	100.000.000	100.000.000	100.000.000
13.7	Chi phí Phát sinh Dự phòng	Khoản dự phòng cho các hạng mục phát sinh không lường trước.	Gói	(Tính sau, 7.5% của Tổng Mục 1-13.6)	(Tính sau)	(Tính sau, 7.5% của Tổng Mục 1-13.6)
Tổng Cộng Dự Toán		**~21.000.000.000 VNĐ**				

PHẦN 8. KẾT LUẬN

Báo cáo này đã trình bày một cách chi tiết giải pháp thiết kế hệ thống mạng toàn diện cho Công ty Cổ phần Phát triển Công nghệ & Giải pháp Toàn cầu (GlobalTech Solutions Corp. - GTSC). Mục tiêu trọng tâm của bản thiết kế là xây dựng một cơ sở hạ tầng mạng hiện đại, đáp ứng đầy đủ các yêu cầu khắt khe về hiệu năng, tính sẵn sàng, độ bảo mật, khả năng quản lý và tiềm năng mở rộng, qua đó hỗ trợ hiệu quả cho các hoạt động nghiên cứu, phát triển phần mềm, cung cấp dịch vụ công nghệ thông tin và chiến lược tăng trưởng dài hạn của GTSC.

Giải pháp đề xuất được xây dựng trên mô hình phân lớp Core – Distribution – Access, sử dụng các thiết bị chuyển mạch Cisco Catalyst hiệu năng cao (C9500 cho lớp Core, C9300 cho lớp Distribution và C1300 cho lớp Access) với các cơ chế dự phòng tiên tiến như StackWise Virtual và Stacking. Hệ thống tường lửa FortiGate 1000F được triển khai theo cụm HA (High Availability) kết hợp với các giải pháp bảo mật chuyên sâu như DMZ, WAF, NAC và phân đoạn mạng VLAN chi tiết, tạo nên một vành đai an ninh vững chắc bảo vệ tài sản thông tin của doanh nghiệp. Kết nối WAN giữa trụ sở chính và các chi nhánh được tối ưu hóa bằng công nghệ SD-WAN, đảm bảo tính linh hoạt, hiệu quả và khả năng phục hồi cao. Mạng không dây Wi-Fi 6 sử dụng các điểm truy cập FortiAP 431F cung cấp kết nối tốc độ cao và ổn định cho người dùng di động. Bên cạnh đó, hạ tầng máy chủ HPE ProLiant Gen11 mạnh mẽ và các dịch vụ mạng thiết yếu như DHCP, DNS, NTP, cân bằng tải được thiết kế với tính dự phòng cao. Với thiết kế này, GTSC sẽ sở hữu một hệ thống mạng:

- **Hoạt động ổn định và liên tục:** Giảm thiểu thời gian chết, đảm bảo các quy trình nghiệp vụ và R&D không bị gián đoạn.
- **Hiệu suất vượt trội:** Đáp ứng nhu cầu băng thông lớn cho các ứng dụng chuyên sâu, truyền tải dữ liệu nhanh chóng.
- **An toàn và bảo mật:** Bảo vệ hiệu quả trước các mối đe dọa từ bên trong lẫn bên ngoài.
- **Linh hoạt và dễ mở rộng:** Sẵn sàng thích ứng với sự tăng trưởng về quy mô nhân sự, mở rộng chi nhánh và tích hợp các công nghệ mới trong tương lai.
- **Dễ dàng quản lý và vận hành:** Thông qua các công cụ quản lý tập trung và kiến trúc mạng rõ ràng.

Để triển khai thành công giải pháp đã đề xuất, GTSC cần thực hiện các bước tiếp theo bao gồm:

1. **Khảo sát chi tiết mặt bằng:** Thực hiện khảo sát kỹ lưỡng tại tất cả các địa điểm để xác định chính xác vị trí lắp đặt thiết bị, đường đi của hệ thống cáp và các yếu tố môi trường khác.
2. **Hoàn thiện kế hoạch triển khai chi tiết:** Xây dựng một lộ trình triển khai cụ thể với các giai đoạn, hạng mục công việc, thời gian thực hiện và nguồn lực phân bổ rõ ràng.
3. **Lựa chọn nhà thầu và nhà cung cấp:** Tổ chức đấu thầu hoặc lựa chọn các đối tác cung cấp thiết bị và dịch vụ triển khai uy tín, có năng lực và kinh nghiệm phù hợp với quy mô dự án.
4. **Triển khai theo giai đoạn:** Cân nhắc việc triển khai hệ thống theo từng giai đoạn (phased implementation) để giảm thiểu ảnh hưởng đến hoạt động hiện tại của công ty và dễ dàng quản lý rủi ro.
5. **Đào tạo và chuyển giao công nghệ:** Tổ chức các khóa đào tạo chuyên sâu cho đội ngũ IT của GTSC để có thể tự chủ vận hành, quản trị và bảo trì hệ thống mới một cách hiệu quả.
6. **Kiểm thử và nghiệm thu:** Thực hiện quy trình kiểm thử toàn diện sau khi lắp đặt và cấu hình, đảm bảo hệ thống hoạt động đúng theo các tiêu chí thiết kế trước khi nghiệm thu và đưa vào sử dụng chính thức.
7. **Xây dựng quy trình vận hành và bảo trì:** Thiết lập các quy trình chuẩn cho việc giám sát, bảo trì định kỳ, cập nhật bản vá và ứng phó sự cố sau khi hệ thống đi vào hoạt động.

Giải pháp thiết kế mạng được trình bày trong báo cáo này là một nền tảng vững chắc, không chỉ đáp ứng các nhu cầu trước mắt mà còn tạo đà cho sự phát triển công nghệ và đổi mới sáng tạo của GlobalTech Solutions Corp. trong tương lai.