**A white rectangular frame with black border

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

🙞🕮🙜



**BÁO CÁO**

**MÔN HỌC: THIẾT KẾ MẠNG**

**GVHD: Huỳnh Nguyên Chính**

**MÃ HP: CNDE430780**

**SINH VIÊN THỰC HIỆN:**

|  |  |
| --- | --- |
| **HỌ VÀ TÊN** | **MSSV** |
| **Lê Trường Khoa** | **22162017** |

**Mục Lục**

[Chương 1: Giới thiệu 4](#_Toc197516768)

[1.1. Bối cảnh Dự án 4](#_Toc197516769)

[1.2. Mục tiêu Thiết kế 4](#_Toc197516770)

[1.3. Phạm vi Tài liệu 4](#_Toc197516771)

[1.4. Đối tượng Sử dụng 4](#_Toc197516772)

[Chương 2: Yêu cầu Thiết kế 4](#_Toc197516773)

[2.1. Yêu cầu Nghiệp vụ 4](#_Toc197516774)

[2.2. Yêu cầu Kỹ thuật 4](#_Toc197516775)

[Chương 3: Thiết kế Logic 7](#_Toc197516776)

[3.1. Kiến trúc Mạng Tổng thể và Vai trò của Ảo hóa 7](#_Toc197516777)

[3.2. Quy hoạch Chức năng Tòa nhà, Tầng và Kế hoạch IP/VLAN Chi tiết 8](#_Toc197516778)

[3.3. Thiết kế Định tuyến (Routing) 16](#_Toc197516779)

[3.4. Thiết kế Tính sẵn sàng cao (High Availability - HA) 16](#_Toc197516780)

[3.5. Thiết kế Bảo mật Logic 17](#_Toc197516781)

[3.6. Dịch vụ Mạng (DHCP, DNS, NTP) 17](#_Toc197516782)

[3.7. Ước tính Lưu lượng và Băng thông (Traffic Estimation & Bandwidth Analysis) - Cập nhật 18](#_Toc197516783)

[3.8. Thiết kế Chất lượng Dịch vụ (Quality of Service - QoS) 19](#_Toc197516784)

[Chương 4: Thiết kế Vật lý 21](#_Toc197516785)

[4.0. Vai trò của Trung tâm Dữ liệu (Data Center - DC) 21](#_Toc197516786)

[4.1. Lựa chọn Thiết bị - Cập nhật 21](#_Toc197516787)

[4.2. Sơ đồ Kết nối Vật lý - Cập nhật 21](#_Toc197516788)

[4.3. Bố trí Thiết bị và Hạ tầng Vật lý 21](#_Toc197516789)

[Bảng 4.1: Mô tả Đường truyền và Kết nối Cáp (Cabling Description) 22](#_Toc197516790)

[Chương 5: Danh mục Vật tư Đề xuất (Bill of Materials - BoM) - Cập nhật 26](#_Toc197516791)

[Chương 5 Phụ lục: Đặc tả Kỹ thuật Chính và Lý do Lựa chọn Thiết bị - Cập nhật 31](#_Toc197516792)

[A. Thiết bị Mạng (Network Hardware) - Cập nhật 31](#_Toc197516793)

[B. Thiết bị Không dây (Wireless Hardware) 32](#_Toc197516794)

[C. Máy chủ & Lưu trữ (Server & Storage Hardware) 32](#_Toc197516795)

[D. Quản lý & Giám sát (Management & Monitoring) 33](#_Toc197516796)

[E. Thành phần Ảo hóa Khác (Other Virtualized Components) 34](#_Toc197516797)

[Chương 6: Ước tính Chi phí Dự án (Project Cost Estimation) - Cập nhật 35](#_Toc197516798)

[Chương 7: Kết luận - Cập nhật 40](#_Toc197516799)

[7.1. Tóm tắt Thiết kế 40](#_Toc197516800)

[7.2. Đáp ứng Yêu cầu 40](#_Toc197516801)

[7.3. Hướng Phát triển Tương lai 40](#_Toc197516802)

## ****Chương 1: Giới thiệu****

### **1.1. Bối cảnh dự án**

Công ty TechNova Solutions, một công ty công nghệ đang phát triển nhanh chóng, chuẩn bị chuyển đến trụ sở mới gồm 3 tòa nhà (B1, B2, B3). Hạ tầng mạng hiện tại không còn đáp ứng đủ nhu cầu về hiệu năng, độ tin cậy và bảo mật cho quy mô hoạt động **khoảng 800 nhân viên hoạt động đồng thời** và định hướng phát triển tương lai của công ty. Dự án này nhằm thiết kế và triển khai một hạ tầng mạng LAN mới, hiện đại, linh hoạt và có khả năng mở rộng cho toàn bộ trụ sở mới, với cơ cấu tổ chức và chức năng rõ ràng cho từng tòa nhà, tầng lầu.

### **1.2. Mục tiêu Thiết kế**

Tài liệu này trình bày chi tiết giải pháp thiết kế hạ tầng mạng LAN cho trụ sở mới của TechNova Solutions, nhằm đạt được các mục tiêu chính sau **cho quy mô ~800 người dùng đồng thời**:

* **Hiệu năng cao (High Performance):** Cung cấp băng thông đủ lớn và độ trễ thấp, **khai thác tối đa hiệu năng chuyển mạch của phần cứng**, cho các ứng dụng nghiệp vụ, truyền dữ liệu lớn, hội nghị truyền hình và các dịch vụ đám mây, **đặc biệt là băng thông Internet và VPN.**
* **Độ sẵn sàng cao (High Availability):** Đảm bảo hoạt động liên tục thông qua **dự phòng đa lớp** (thiết bị, đường truyền, dịch vụ), **tận dụng các cơ chế HA tiên tiến như StackWise Virtual, FGCP, VMware HA** để giảm thiểu thời gian chết (downtime).
* **Bảo mật mạnh mẽ (Robust Security):** Bảo vệ tài nguyên và dữ liệu thông qua **phân đoạn mạng đa lớp (VLAN, VRF-lite, TrustSec), kiểm soát truy cập chặt chẽ (NAC 802.1X), tường lửa thế hệ mới (NGFW) hiệu năng cao, và bảo mật chuyên sâu cho môi trường ảo hóa.**
* **Khả năng quản lý và Tự động hóa (Manageability & Automation):** Dễ dàng cấu hình, giám sát, bảo trì và khắc phục sự cố thông qua **quản lý tập trung (DNA Center, vCenter), đồng thời xây dựng nền tảng sẵn sàng cho tự động hóa mạng.**
* **Khả năng mở rộng (Scalability):** Thiết kế module hóa, có khả năng đáp ứng sự tăng trưởng về người dùng, thiết bị, ứng dụng và**lưu lượng băng thông** mà không cần thay đổi kiến trúc cốt lõi.
* **Hỗ trợ Di động và Cộng tác (Mobility & Collaboration Support):** Cung cấp kết nối không dây Wi-Fi 6 ổn định, hiệu năng cao và các dịch vụ mạng cần thiết**, đảm bảo chất lượng dịch vụ (QoS) cho thoại và video.**
* **Tối ưu Chi phí và Hiệu quả (Cost-Effectiveness & Efficiency):** Lựa chọn giải pháp cân bằng giữa hiệu năng, tính năng và chi phí**. Ứng dụng triệt để ảo hóa (Server & NFV) để tối ưu hóa tài nguyên phần cứng, điện năng và không gian.**

### **1.3. Phạm vi Tài liệu**

Tài liệu này bao gồm các nội dung chính sau:

* Phân tích yêu cầu nghiệp vụ và kỹ thuật.
* Thiết kế logic mạng (sơ đồ, địa chỉ IP, VLAN, định tuyến, bảo mật, vai trò ảo hóa, quy hoạch chức năng tòa nhà/tầng).
* Thiết kế vật lý mạng (vai trò DC, lựa chọn thiết bị, sơ đồ kết nối, bố trí, nền tảng ảo hóa).
* Danh mục vật tư đề xuất chi tiết (BoM).
* Đặc tả kỹ thuật chính và lý do lựa chọn thiết bị (bao gồm cấu hình RAM/ROM/Storage cụ thể được đề xuất, yêu cầu tài nguyên cho các thành phần ảo hóa, mã hiệu module quang).
* Ước tính lưu lượng băng thông cơ bản.
* Thiết kế Chất lượng Dịch vụ (QoS).
* Ước tính chi phí dự án chi tiết.
* Kết luận và hướng phát triển tương lai.

Tài liệu này không bao gồm:

* Thiết kế chi tiết hệ thống điện, làm mát, phòng cháy chữa cháy cho phòng máy chủ.
* Cấu hình chi tiết từng thiết bị (sẽ có trong tài liệu cấu hình riêng).
* Thiết kế chi tiết hệ thống Tổng đài IP (PBX) hoặc Hội nghị truyền hình (Video Conferencing).
* Phân tích tải công việc chi tiết để xác thực cấu hình máy chủ/lưu trữ và tài nguyên VM cụ thể.
* Chính sách bảo mật chi tiết (sẽ có trong tài liệu chính sách riêng).

### **1.4. Đối tượng Sử dụng**

* Ban Lãnh đạo Công ty TechNova Solutions.
* Bộ phận IT của TechNova Solutions.
* Đơn vị tư vấn, triển khai hệ thống mạng.
* Các bên liên quan khác.

## ****Chương 2: Yêu cầu Thiết kế****

### **2.1. Yêu cầu Nghiệp vụ**

* **Số lượng người dùng:** **~800 nhân viên hoạt động đồng thời** (bao gồm cả tại văn phòng và từ xa nếu có).
* **Số lượng thiết bị:** Ước tính 1600+ thiết bị có dây và không dây (PC, Laptop, IP Phone, Mobile, IoT...).
* **Ứng dụng chính:**
  + Ứng dụng văn phòng (Email, Office Suite).
  + Hệ thống ERP, CRM nội bộ.
  + Phần mềm phát triển (IDE, Git - GitLab nội bộ).
  + Máy chủ ảo hóa (VMware) cho môi trường Dev, Test, Production.
  + Hệ thống cơ sở dữ liệu (SQL Server, PostgreSQL).
  + Truy cập Internet tốc độ cao.
  + Hội nghị truyền hình (Webex, Zoom, Teams).
  + Chia sẻ file dung lượng lớn (NAS).
  + Truy cập từ xa an toàn cho nhân viên (VPN).
* **Yêu cầu về hiệu năng ứng dụng:** Đảm bảo độ trễ thấp và băng thông đủ cho các ứng dụng nhạy cảm (VoIP, Video Conference, truy cập DB).
* **Yêu cầu về bảo mật:** Phân tách mạng Khách và mạng Nội bộ, kiểm soát truy cập chặt chẽ vào tài nguyên máy chủ và dữ liệu nhạy cảm, bảo vệ chống lại mã độc và tấn công mạng.
* **Yêu cầu về làm việc từ xa:** Hỗ trợ kết nối VPN ổn định và an toàn cho **số lượng lớn người dùng đồng thời (ví dụ: 300-500+).**
* **Yêu cầu về mạng Khách (Guest Wi-Fi):** Cung cấp truy cập Internet cơ bản, tách biệt hoàn toàn với mạng nội bộ.

### **2.2. Yêu cầu Kỹ thuật**

#### **2.2.1. Hiệu năng và Băng thông**

* Kết nối người dùng có dây: Tối thiểu 1 Gbps, **sẵn sàng cho Multi-Gigabit.**
* Kết nối không dây: Wi-Fi 6 (802.11ax), **đảm bảo mật độ và thông lượng cao.**
* Kết nối máy chủ & Lưu trữ: **Tối thiểu 25 Gbps, ưu tiên 40/100G cho các kết nối chính.**
* Kết nối Backbone: **Tối thiểu 2x100 Gbps (Core-DC Dist), 2x25 Gbps (Core-Bldg Dist).**
* **Kết nối Internet (WAN): Tối thiểu 2 đường truyền WAN từ 2 nhà cung cấp khác nhau, mỗi đường 10 Gbps (Tổng 20 Gbps), hỗ trợ Load Balancing và Failover.**
* **Chất lượng Dịch vụ (QoS):** Ưu tiên lưu lượng nhạy cảm độ trễ (Voice, Video) và ứng dụng nghiệp vụ quan trọng.

#### **2.2.2. Độ sẵn sàng (Availability)**

* Dự phòng N+1 hoặc Active/Active cho tất cả các thành phần mạng quan trọng (Router, Firewall, Core, Distribution, WLC, DNS, DHCP, vLB...).
* **Tận dụng tối đa StackWise Virtual và Stacking.**
* **HA cho Firewall (FGCP):** Chuyển đổi trạng thái nhanh chóng, đồng bộ session.
* **HA cho Máy chủ ảo (VMware HA/DRS).**
* **Dự phòng đường truyền:** MEC/LACP trên tất cả các liên kết chính, **bao gồm cả 2 đường WAN.**
* **Dự phòng nguồn:** Dual PSU, UPS N+1.

#### **2.2.3. Bảo mật (Security)**

* **Phân đoạn sâu:** VLAN**, VRF-lite, Security Group Tags (SGTs) thông qua Cisco TrustSec/ISE.**
* **Firewall NGFW: Hiệu năng cao**, kiểm soát dựa trên ứng dụng (App-ID), người dùng (User-ID), **giải mã SSL/TLS,** IPS, Antivirus, Web Filtering, Sandboxing. **Thông lượng VPN cao.**
* **NAC 802.1X:** Xác thực mạnh, phân VLAN động, kiểm tra tuân thủ (Posture).
* **Bảo mật Wi-Fi:** WPA3-Enterprise, Rogue AP Detection.
* **Bảo mật môi trường ảo hóa:** Kiểm soát traffic East-West.
* **Bảo mật lớp 2 nâng cao:** Port Security, DHCP Snooping, DAI, IPSG, Storm Control.
* **Quản lý truy cập quản trị:** TACACS+, SSHv2, HTTPS, RBAC.

#### **2.2.4. Địa chỉ IP và Dịch vụ Mạng**

* Sử dụng địa chỉ IP Private (RFC 1918). Lên kế hoạch địa chỉ IP chi tiết cho từng VLAN, đảm bảo đủ không gian cho hiện tại và tương lai.
* Dịch vụ DHCP: Cấp phát IP động cho người dùng cuối, IP Phone, thiết bị Wi-Fi. Cần có cơ chế dự phòng DHCP (DHCP Failover hoặc Standby). **(Triển khai trên VM có HA).**
* Dịch vụ DNS: Cung cấp phân giải tên miền nội bộ và bên ngoài. Cần có máy chủ DNS nội bộ dự phòng. **(Triển khai trên VM có HA).**
* Dịch vụ NTP: Đồng bộ thời gian cho tất cả thiết bị mạng và máy chủ. **(Triển khai trên VM hoặc thiết bị mạng tin cậy).**

#### **2.2.5. Quản lý và Giám sát**

* **Quản lý hợp nhất:** Cisco DNA Center cho hạ tầng mạng vật lý/không dây, VMware vCenter cho hạ tầng ảo hóa. **Tìm kiếm khả năng tích hợp giữa hai nền tảng.**
* **Giám sát sâu:** SNMPv3, NetFlow/sFlow/IPFIX, Syslog, **giám sát hiệu năng ứng dụng (Application Performance Monitoring - APM) nếu có.**
* **Sẵn sàng cho Tự động hóa:** Thiết bị hỗ trợ API (NETCONF/RESTCONF), tích hợp với các công cụ tự động hóa (Ansible, Python).

#### **2.2.6. Hạ tầng Vật lý**

* Data Center (DC): Tại B1, là trung tâm xử lý chính, cần đảm bảo các tiêu chuẩn về nguồn điện, làm mát, chống cháy, an ninh vật lý. **Nơi đặt các Máy chủ Vật lý (VM Hosts) và Hệ thống Lưu trữ Tập trung (SAN/NAS).**
* Phòng Kỹ thuật (Telecommunication Room - TC): Mỗi tầng/khu vực cần có phòng TC để đặt Access Switch và đấu nối cáp.
* Hệ thống Cáp cấu trúc (Structured Cabling): Sử dụng cáp đồng Cat6A cho kết nối người dùng và AP. Sử dụng cáp quang (OM4 MMF hoặc OS2 SMF) cho kết nối backbone và giữa các tòa nhà. Đảm bảo tiêu chuẩn lắp đặt và đánh dấu.

## ****Chương 3: Thiết kế Logic****

### **3.1. Kiến trúc Mạng Tổng thể và Vai trò của Ảo hóa**

Kiến trúc mạng được đề xuất theo mô hình phân lớp (Hierarchical Network Design) gồm 3 lớp chính: Core, Distribution, và Access. Mô hình này mang lại sự ổn định, khả năng mở rộng và dễ dàng quản lý.

* **Lớp Core (Core Layer):** Là lớp xương sống tốc độ cao của mạng, chịu trách nhiệm chuyển mạch gói tin nhanh chóng giữa các khu vực khác nhau (giữa các Distribution Block). Lớp này yêu cầu độ tin cậy và hiệu năng cao nhất. Thiết bị Core sẽ được đặt tại Data Center (B1).
* **Lớp Distribution (Distribution Layer):** Là điểm tập trung kết nối từ lớp Access trong một khu vực hoặc tòa nhà. Lớp này thực hiện các chức năng như tổng hợp kết nối Access, định tuyến giữa các VLAN, áp dụng chính sách (ACLs, QoS), và là ranh giới giữa các miền broadcast. Mỗi tòa nhà (B1, B2, B3) và Data Center sẽ có một cặp Distribution Switch dự phòng.
* **Lớp Access (Access Layer):** Là lớp cung cấp kết nối trực tiếp đến các thiết bị người dùng cuối (PC, Laptop, IP Phone, AP, Printer...). Lớp này thực hiện các chức năng như cấp nguồn PoE, phân loại QoS, bảo mật cổng (Port Security), và phân VLAN cho người dùng. Access Switch sẽ được đặt tại các phòng TC ở mỗi tầng.
* **Sơ đồ Logic Tổng thể (Dạng Text - Chi tiết dự phòng):**

**Vai trò của Ảo hóa trong Kiến trúc (Chi tiết hơn):**

Kiến trúc này **tích hợp sâu và xuyên suốt** công nghệ ảo hóa để tối đa hóa hiệu quả, linh hoạt và tiết kiệm chi phí:

* **Hợp nhất Máy chủ (Server Consolidation):** Như đã mô tả, giảm thiểu phần cứng vật lý thông qua việc chạy hàng loạt VM trên các VM Host mạnh mẽ.
* **Ảo hóa Chức năng Mạng (NFV):**
  + **Các chức năng chính:** WLC (C9800-CL), NMS (DNA Center), SIEM (FortiAnalyzer), AAA (ISE), **vLB** được triển khai dưới dạng VM.
  + **Tiềm năng mở rộng NFV:** Xem xét triển khai **Tường lửa ảo hóa (vFW - vd: FortiGate-VM, Cisco Secure Firewall Virtual)**bên trong Data Center để thực hiện**micro-segmentation**, kiểm soát luồng traffic East-West giữa các VM/ứng dụng với chính sách chi tiết hơn mà không cần định tuyến traffic ra Firewall vật lý.
* **Linh hoạt và Khả năng Mở rộng:** Dễ dàng điều chỉnh tài nguyên (CPU, RAM, Disk) cho các VM hoặc thêm VM Host mới khi cần mở rộng mà không cần can thiệp vật lý phức tạp.
* **Quản lý Hợp nhất:** Sử dụng vCenter để quản lý hạ tầng ảo hóa (hosts, VMs, storage) và DNA Center để quản lý hạ tầng mạng vật lý/không dây**. Việc tích hợp (ví dụ: DNA Center biết về VM từ vCenter) giúp có cái nhìn toàn diện.**

**Sự phối hợp của các thành phần trong môi trường ảo hóa:**

* **VM Hosts (vd: Dell PowerEdge R750):** Cung cấp tài nguyên CPU và RAM cho các máy ảo.
* **Hypervisor (vd: VMware ESXi):** Phần mềm quản lý và tạo máy ảo trên VM Hosts.
* **SAN Storage (vd: Dell PowerStore):** Cung cấp lưu trữ dạng block hiệu năng cao (qua iSCSI) cho ổ đĩa ảo của các VM quan trọng (VMDK).
* **NAS Storage (vd: Synology HD6500/QNAP):** Cung cấp lưu trữ dạng file dung lượng lớn (qua SMB/NFS) cho dữ liệu người dùng, chia sẻ chung và đặc biệt là **làm đích lưu trữ backup cho các máy ảo và dữ liệu khác.**
* **DC Distribution Switches (vd: C9500-24Y4C):** Cung cấp kết nối mạng tốc độ cao và dự phòng (25Gbps+) cho VM Hosts, SAN, NAS, đảm bảo băng thông cho lưu lượng VM, lưu trữ và vMotion.
* **Virtual Load Balancers (VMs):** Chạy trên VM Hosts, nhận và phân phối lưu lượng đến các VM ứng dụng backend, tăng hiệu năng và độ sẵn sàng.

### **3.2. Quy hoạch Chức năng Tòa nhà, Tầng và Kế hoạch IP/VLAN Chi tiết**

**A. Quy hoạch Chức năng Tòa nhà và Phân bổ Tầng (Đã xác nhận):**

* **Tòa nhà B1 (Trụ sở chính & R&D):**
  + **Tầng Hầm (B1):** Data Center chính (DC).
  + **Tầng 1 (F1):** Lễ tân, Phòng họp lớn, Ban Lãnh đạo, Hành chính Nhân sự (HR & Admin).
  + **Tầng 2 (F2):** Bộ phận Nghiên cứu & Phát triển (R&D) - Phần cứng & Embedded.
  + **Tầng 3 (F3):** Bộ phận Nghiên cứu & Phát triển (R&D) - Phần mềm Lõi & AI.
* **Tòa nhà B2 (Phát triển Phần mềm):**
  + **Tầng 1 (F1):** Nhóm Phát triển Ứng dụng A (DevTeam A), Nhóm Kiểm thử A (QATeam A).
  + **Tầng 2 (F2):** Nhóm Phát triển Ứng dụng B (DevTeam B), Nhóm Kiểm thử B (QATeam B).
  + **Tầng 3 (F3):** Nhóm DevOps, Nhóm Phát triển Mobile.
* **Tòa nhà B3 (Kinh doanh & Hỗ trợ):**
  + **Tầng 1 (F1):** Bộ phận Kinh doanh (Sales), Bộ phận Marketing.
  + **Tầng 2 (F2):** Bộ phận Hỗ trợ Kỹ thuật (Support), Trung tâm Đào tạo (Training Center).
  + **Tầng 3 (F3):** Phòng họp, Khu vực làm việc linh hoạt (Hot Desking).

**B. Kế hoạch Phân đoạn Mạng (VLAN) và Địa chỉ IP Chi tiết:**

Bảng dưới đây mô tả chi tiết kế hoạch VLAN và địa chỉ IP, gắn liền với chức năng của từng tòa nhà/tầng/phòng ban đã quy hoạch ở trên.

| **VLAN ID** | **Tên VLAN** | **Dải IP** | **Subnet Mask** | **Gateway (Core/Dist)** | **Mục đích / Vị trí** | **Ghi chú** |
| --- | --- | --- | --- | --- | --- | --- |
| **Hạ tầng & Quản lý** |  |  |  |  |  |  |
| 10 | Management | 10.1.10.0/24 | 255.255.255.0 | 10.1.10.1 | Quản lý thiết bị mạng (Switch, Router, FW, AP, iDRAC...) | Truy cập hạn chế |
| 99 | Native\_VLAN | N/A | N/A | N/A | VLAN Native (Không dùng cho user traffic) | Chỉ dùng cho control plane nếu cần |
| 999 | Blackhole | 10.255.255.0/24 | 255.255.255.0 | N/A | VLAN không sử dụng, dùng cho Port Security |  |
| **Data Center (DC - B1)** |  |  |  |  |  |  |
| 20 | DC\_Servers\_General | 10.1.20.0/23 | 255.255.254.0 | 10.1.20.1 | Máy chủ ảo hóa chung (AD, DNS, DHCP, GitLab, Web...) |  |
| 30 | DC\_DMZ | 10.1.30.0/24 | 255.255.255.0 | 10.1.30.1 (FW) | Máy chủ public (Web, Mail Relay...) | Kiểm soát bởi Firewall |
| 40 | DC\_Databases | 10.1.40.0/24 | 255.255.255.0 | 10.1.40.1 | Máy chủ cơ sở dữ liệu (SQL, PostgreSQL VMs) | ACLs chặt chẽ |
| 50 | DC\_Backup | 10.1.50.0/24 | 255.255.255.0 | 10.1.50.1 | Lưu lượng Backup (Server <-> NAS/Tape) | Có thể không cần định tuyến |
| 60 | DC\_Storage\_iSCSI | 10.1.60.0/24 | 255.255.255.0 | N/A | Lưu lượng iSCSI (Server <-> SAN) | Không định tuyến, Jumbo Frames |
| **Dịch vụ Chung** |  |  |  |  |  |  |
| 70 | Voice | 10.1.70.0/24 | 255.255.255.0 | 10.1.70.1 | Điện thoại IP (IP Phones) | QoS ưu tiên cao |
| 80 | IoT | 10.1.80.0/24 | 255.255.255.0 | 10.1.80.1 | Thiết bị IoT (Camera, Sensor...) | Phân đoạn, kiểm soát chặt chẽ bởi Firewall/ACL |
| **Tòa nhà B1 (HQ & R&D)** |  |  |  |  |  |  |
| 101 | B1\_F1\_AdminHR\_Wired | 10.10.1.0/24 | 255.255.255.0 | 10.10.1.1 | Nhân viên Admin/HR có dây (Tầng 1) |  |
| 111 | B1\_F1\_AdminHR\_Wireless | 10.11.1.0/24 | 255.255.255.0 | 10.11.1.1 | Nhân viên Admin/HR không dây (Tầng 1) | SSID Nội bộ |
| 102 | B1\_F2\_RnD\_HW\_Wired | 10.10.2.0/24 | 255.255.255.0 | 10.10.2.1 | Nhân viên R&D Phần cứng có dây (Tầng 2) |  |
| 112 | B1\_F2\_RnD\_HW\_Wireless | 10.11.2.0/24 | 255.255.255.0 | 10.11.2.1 | Nhân viên R&D Phần cứng không dây (Tầng 2) | SSID Nội bộ |
| 103 | B1\_F3\_RnD\_SW\_Wired | 10.10.3.0/24 | 255.255.255.0 | 10.10.3.1 | Nhân viên R&D Phần mềm có dây (Tầng 3) |  |
| 113 | B1\_F3\_RnD\_SW\_Wireless | 10.11.3.0/24 | 255.255.255.0 | 10.11.3.1 | Nhân viên R&D Phần mềm không dây (Tầng 3) | SSID Nội bộ |
| **Tòa nhà B2 (Dev)** |  |  |  |  |  |  |
| 201 | B2\_F1\_DevQA\_A\_Wired | 10.20.1.0/24 | 255.255.255.0 | 10.20.1.1 | Nhân viên Dev/QA Team A có dây (Tầng 1) |  |
| 211 | B2\_F1\_DevQA\_A\_Wireless | 10.21.1.0/24 | 255.255.255.0 | 10.21.1.1 | Nhân viên Dev/QA Team A không dây (Tầng 1) | SSID Nội bộ |
| 202 | B2\_F2\_DevQA\_B\_Wired | 10.20.2.0/24 | 255.255.255.0 | 10.20.2.1 | Nhân viên Dev/QA Team B có dây (Tầng 2) |  |
| 212 | B2\_F2\_DevQA\_B\_Wireless | 10.21.2.0/24 | 255.255.255.0 | 10.21.2.1 | Nhân viên Dev/QA Team B không dây (Tầng 2) | SSID Nội bộ |
| 203 | B2\_F3\_DevOpsMobile\_Wired | 10.20.3.0/24 | 255.255.255.0 | 10.20.3.1 | Nhân viên DevOps/Mobile có dây (Tầng 3) |  |
| 213 | B2\_F3\_DevOpsMobile\_Wireless | 10.21.3.0/24 | 255.255.255.0 | 10.21.3.1 | Nhân viên DevOps/Mobile không dây (Tầng 3) | SSID Nội bộ |
| **Tòa nhà B3 (Kinh doanh & Hỗ trợ)** |  |  |  |  |  |  |
| 301 | B3\_F1\_SalesMkt\_Wired | 10.30.1.0/24 | 255.255.255.0 | 10.30.1.1 | Nhân viên Sales/Marketing có dây (Tầng 1) |  |
| 311 | B3\_F1\_SalesMkt\_Wireless | 10.31.1.0/24 | 255.255.255.0 | 10.31.1.1 | Nhân viên Sales/Marketing không dây (Tầng 1) | SSID Nội bộ |
| 302 | B3\_F2\_SupportTrain\_Wired | 10.30.2.0/24 | 255.255.255.0 | 10.30.2.1 | Nhân viên Support/Training có dây (Tầng 2) |  |
| 312 | B3\_F2\_SupportTrain\_Wireless | 10.31.2.0/24 | 255.255.255.0 | 10.31.2.1 | Nhân viên Support/Training không dây (Tầng 2) | SSID Nội bộ |
| 303 | B3\_F3\_HotDesk\_Wired | 10.30.3.0/24 | 255.255.255.0 | 10.30.3.1 | Khu vực làm việc linh hoạt có dây (Tầng 3) |  |
| 313 | B3\_F3\_HotDesk\_Wireless | 10.31.3.0/24 | 255.255.255.0 | 10.31.3.1 | Khu vực làm việc linh hoạt không dây (Tầng 3) | SSID Nội bộ |
| **Mạng Khách** |  |  |  |  |  |  |
| 900 | Guest\_Wireless | 10.99.0.0/22 | 255.255.252.0 | 10.99.0.1 (FW) | Mạng Khách không dây (Toàn bộ trụ sở) | Cách ly hoàn toàn, kiểm soát bởi Firewall |

**Giải thích và Lưu ý:**

* **Phân chia theo Chức năng/Vị trí:** Các VLAN người dùng (101-313) được phân chia rõ ràng theo Tòa nhà (B1/B2/B3), Tầng (F1/F2/F3), Phòng ban/Chức năng (Admin, R&D, Dev, Sales...), và loại kết nối (Wired/Wireless). Điều này giúp quản lý và áp dụng chính sách bảo mật/QoS dễ dàng hơn.
* **Dải IP:** Sử dụng các octet thứ hai và thứ ba để mã hóa thông tin Tòa nhà và Tầng/VLAN ID, tạo sự nhất quán. /24 được sử dụng cho hầu hết các VLAN người dùng, cung cấp 254 địa chỉ/VLAN. VLAN Servers dùng /23 để có nhiều IP hơn. VLAN Guest dùng /22 để chứa số lượng lớn thiết bị khách tiềm năng.
* **Gateway:** Gateway mặc định cho mỗi VLAN người dùng/server được đặt trên cặp Distribution Switch của tòa nhà đó (hoặc DC Distribution cho VLAN DC), sử dụng HSRP/VRRP. Gateway cho DMZ và Guest được đặt trên Firewall.
* **VLAN Hạ tầng:** VLAN 10 (Management), 50 (Backup), 60 (Storage\_iSCSI), 70 (Voice), 80 (IoT) được dùng chung cho toàn bộ trụ sở.
* **Cân nhắc VRF-lite/SGTs:** Như đã đề cập ở mục 3.2, VRF-lite hoặc SGTs (TrustSec) có thể được áp dụng chồng lên cấu trúc VLAN này để tăng cường phân đoạn nếu cần. Ví dụ, toàn bộ môi trường R&D (VLAN 102, 112, 103, 113) có thể được đặt trong một VRF riêng hoặc gán cùng một SGT.

### **3.3. Thiết kế Định tuyến (Routing)**

* **Định tuyến Nội bộ (Internal Routing):**
  + Sử dụng giao thức định tuyến động EIGRP (hoặc OSPF) trong toàn bộ mạng nội bộ (Core, Distribution). EIGRP được ưu tiên nếu môi trường chủ yếu là Cisco.
  + Lớp Core đóng vai trò trung tâm định tuyến.
  + Lớp Distribution sẽ là Gateway mặc định (Default Gateway) cho các VLAN người dùng tại mỗi tòa nhà/khu vực. Giao thức First Hop Redundancy Protocol (FHRP) như HSRP (hoặc VRRP) sẽ được sử dụng giữa cặp Distribution Switch để cung cấp gateway dự phòng.
  + **Tối ưu EIGRP/OSPF:** Sử dụng các kỹ thuật như summarization (tại Distribution) để giảm kích thước bảng định tuyến, tinh chỉnh timer để tăng tốc độ hội tụ (cẩn trọng).
* **Định tuyến Ra Ngoài (External Routing):**
  + **Gateway Router (Catalyst 8500)** sẽ chạy BGP với các ISP để trao đổi thông tin định tuyến Internet.
  + Sử dụng định tuyến tĩnh hoặc redistribution từ EIGRP/OSPF vào BGP (và ngược lại) trên Gateway Router và Firewall để kiểm soát luồng traffic ra/vào Internet.
  + Firewall sẽ là gateway mặc định cho các máy chủ trong DMZ và có thể là gateway cho một số VLAN nội bộ cần kiểm soát chặt chẽ khi ra Internet.
  + **BGP:** Cấu hình các thuộc tính BGP (AS-Path Prepending, Local Preference, MED) để điều khiển luồng traffic ra/vào qua các ISP.

### **3.4. Thiết kế Tính sẵn sàng cao (High Availability - HA)**

* **Gateway Router (HSRP/VRRP):** Cặp Catalyst 8500 chạy HSRP/VRRP cung cấp gateway ảo dự phòng, chuyển đổi nhanh khi một router lỗi.
* **Firewall (FGCP):** Cặp FortiGate 1801F chạy FGCP Active/Passive (mặc định) hoặc Active/Active. Đồng bộ session state giúp duy trì kết nối khi failover. Liên kết HA chuyên dụng (HA link).
* **Core/DC Dist (StackWise Virtual - SVL):** Hai switch vật lý hoạt động như một switch logic duy nhất với **một control plane chung**. Sử dụng liên kết SVL tốc độ cao. Cho phép kết nối MEC từ các thiết bị khác đến cả hai switch vật lý, **tăng gấp đôi băng thông hiệu dụng và loại bỏ hoàn toàn Spanning Tree giữa cặp switch.** Failover cực nhanh.
* **Building Dist/Access (Stacking - StackWise-1T/320):** Nhiều switch vật lý hoạt động như một switch logic với**một control plane chung**. Đơn giản hóa quản lý (một IP quản lý). Cho phép kết nối MEC uplink/downlink. Tăng khả năng phục hồi trong stack.
* **WLAN Controllers (HA SSO):** Hai VM C9800-CL đồng bộ cấu hình và trạng thái AP/client. Khi WLC active lỗi, WLC standby tiếp quản ngay lập tức mà không làm rớt kết nối client (seamless roaming).
* **VMware HA/DRS:**
  + **HA:** Giám sát VM và ESXi host. Nếu host lỗi, tự động khởi động lại các VM bị ảnh hưởng trên các host còn lại trong cluster.
  + **DRS (Distributed Resource Scheduler):** Tự động cân bằng tải tài nguyên (CPU, RAM) cho các VM trên các host trong cluster thông qua vMotion, đảm bảo hiệu năng và tránh quá tải cục bộ. Có thể tự động di chuyển VM khỏi host cần bảo trì.
* **Dịch vụ Ảo hóa (AD, DNS, DHCP...):** Triển khai nhiều instance VM cho mỗi dịch vụ, đặt trên các host vật lý khác nhau, sử dụng cơ chế HA sẵn có của ứng dụng (vd: AD Replication, DHCP Failover).
* **Lưu trữ (SAN/NAS):** Dual Controller Active/Active hoặc Active/Passive. MPIO (Multi-Path I/O) trên server để cung cấp đường dẫn dự phòng đến storage. RAID để bảo vệ dữ liệu ở cấp độ ổ đĩa.
* **Kết nối Vật lý:** Sử dụng Link Aggregation (LACP/MEC) cho tất cả các kết nối quan trọng (Inter-switch links, Server links, Storage links, **Router-FW-Core links, WAN links**) để tăng băng thông và dự phòng liên kết.
* **Spanning Tree Protocol (STP):** Sử dụng Rapid PVST+ hoặc MSTP. Cấu hình các tính năng bảo vệ như BPDU Guard, Root Guard trên cổng Access. Với việc sử dụng Stacking/SVL rộng rãi, vai trò của STP chủ yếu là dự phòng và ngăn chặn loop do lỗi cấu hình.

### **3.5. Thiết kế Bảo mật Logic**

* **Phân đoạn Mạng:** VLAN là cơ bản. **Sử dụng SGTs (TrustSec) kết hợp ISE** để phân đoạn động dựa trên ngữ cảnh (gắn với vai trò từ AD/Phòng ban), linh hoạt hơn IP/VLAN ACLs. Xem xét **VRF-lite** cho các yêu cầu tách biệt định tuyến cao (vd: tách R&D khỏi các bộ phận khác).
* **Firewall NGFW Policies (FortiGate 1801F):**
  + **Kiểm soát Ứng dụng (App-ID):** Cho phép/chặn các ứng dụng cụ thể (vd: Facebook, YouTube, BitTorrent) bất kể cổng dịch vụ.
  + **Kiểm soát Người dùng (User-ID):** Tích hợp AD để áp dụng chính sách theo người dùng/nhóm người dùng (vd: Nhóm Sales được dùng CRM, Nhóm Dev được dùng GitLab).
  + **IPS:** Kích hoạt các signature phù hợp để phát hiện và ngăn chặn các cuộc tấn công đã biết (tận dụng hiệu năng cao của FG-1801F).
  + **Antivirus/Sandboxing:** Quét file download/upload để phát hiện mã độc. Gửi file nghi ngờ lên sandbox để phân tích hành vi.
  + **Web Filtering:** Chặn truy cập các trang web độc hại hoặc không phù hợp theo category.
  + **SSL Decryption:** Giải mã traffic HTTPS để kiểm tra nội dung bên trong (cần quản lý certificate cẩn thận, tận dụng hiệu năng xử lý SSL của FG-1801F).
  + **VPN Policies:** Cấu hình chính sách chi tiết cho người dùng VPN (SSL-VPN, IPsec) để kiểm soát truy cập tài nguyên nội bộ.
* **NAC (Cisco ISE):**
  + **802.1X:** Xác thực tập trung (EAP-TLS/PEAP), cấp quyền truy cập động (VLAN, dACL, SGT) dựa trên thông tin người dùng/nhóm từ AD.
  + **Posture Assessment:** Kiểm tra trạng thái bảo mật của client (antivirus, patch...) trước khi cho vào mạng đầy đủ.
  + **Guest Access:** Cổng thông tin tùy chỉnh, tài khoản tạm thời cho VLAN 900.
  + **BYOD Onboarding:** Quy trình đăng ký và cấp quyền cho thiết bị cá nhân.
* **Bảo mật Lớp 2:** Kích hoạt đầy đủ Port Security, DHCP Snooping, DAI, IPSG, Storm Control trên các cổng Access.
* **Bảo mật Quản trị:** TACACS+ với command authorization (phân quyền lệnh theo user quản trị), SSHv2, HTTPS, RBAC.

### **3.6. Dịch vụ Mạng (DHCP, DNS, NTP)**

* **DHCP:**
  + Máy chủ DHCP (Windows Server hoặc Linux **dưới dạng VM có HA**) sẽ quản lý các scope cho từng VLAN (101-113, 201-213, 301-313, 70, 80, 900...).
  + Cấu hình DHCP Failover giữa 2 máy chủ DHCP VM.
  + Cấu hình DHCP Relay Agent (IP Helper-Address) trên các gateway L3 (Distribution Switch, Firewall cho Guest).
* **DNS:**
  + Sử dụng máy chủ DNS nội bộ (Windows Server AD Integrated **dưới dạng VM có HA)** để phân giải tên miền nội bộ (\*.technova.local) và làm forwarder cho các truy vấn tên miền Internet.
  + Cấu hình ít nhất 2 máy chủ DNS nội bộ dự phòng.
  + Client DHCP sẽ được cấp địa chỉ DNS nội bộ này.
* **NTP:**
  + Sử dụng một nguồn NTP đáng tin cậy (có thể là một thiết bị mạng như Core Switch/Router hoặc một máy chủ riêng **dưới dạng VM)** làm NTP Master cho mạng nội bộ.
  + Cấu hình tất cả các thiết bị mạng, máy chủ, firewall đồng bộ thời gian với NTP Master này.

### **3.7. Ước tính Lưu lượng và Băng thông (Traffic Estimation & Bandwidth Analysis) - Cập nhật**

**A. Giả định Cơ bản:**

* **Người dùng đồng thời hoạt động: ~800**
* **Băng thông Internet trung bình/người dùng: ~10 Mbps** (Do nhu cầu cao hơn với cloud/video...)
* **Băng thông Nội bộ trung bình/người dùng:** 10-15 Mbps
* **Lưu lượng Voice/Video:** Ước tính 20-30% người dùng đồng thời (~160-240 luồng)
* **Lưu lượng Server-Storage (iSCSI):** Vẫn có thể rất lớn và bursty.
* **Lưu lượng Backup:** Vẫn chủ yếu vào ban đêm.
* **Hệ số đỉnh (Peak Factor):** 2.5 - 3

**B. Ước tính Lưu lượng tại các Điểm Chính (Cập nhật với ~800 users):**

1. **Access Switch Uplink (1 Tầng ~ 80-100 users trung bình):**
   * Người dùng đồng thời: ~60-70
   * Internet: 70 users \* 10 Mbps = 700 Mbps
   * Nội bộ: 70 users \* 15 Mbps = 1050 Mbps
   * Voice/Video: ~20 luồng \* 3 Mbps = ~60 Mbps
   * Tổng trung bình: ~1.8 Gbps
   * **Lưu lượng đỉnh (x2.5): ~ 4.5 Gbps**
   * **Thiết kế:** 2 x 10 Gbps MEC Uplink => **20 Gbps**
2. **Building Distribution Uplink (1 Tòa nhà ~ 250-300 users):**
   * Người dùng đồng thời: ~200
   * Tổng trung bình từ 3 tầng: ~1.8 Gbps \* 3 = ~5.4 Gbps
   * **Lưu lượng đỉnh (x2.5): ~ 13.5 Gbps**
   * **Thiết kế:** 2 x 25 Gbps MEC Uplink => **50 Gbps.**
3. **Core Switch (Tổng hợp từ 3 tòa nhà):**
   * Tổng lưu lượng đỉnh từ người dùng: ~13.5 Gbps \* 3 = ~40.5 Gbps
   * Thêm lưu lượng Server-Server, Server-Internet... (Ước tính thêm 10-20 Gbps đỉnh)
   * **Tổng lưu lượng đỉnh qua Core (Ước tính): ~ 50-60 Gbps**
   * **Thiết kế Core:** Khả năng chuyển mạch Tbps. Kết nối DC Dist 200G. Kết nối Bldg Dist 50G/tòa nhà.
4. **DC Distribution Switch:**
   * Nhận traffic từ Core (~50-60 Gbps đỉnh).
   * Lưu lượng Server <-> Storage (iSCSI): Vẫn có thể đạt hàng chục Gbps.
   * **Thiết kế:** Kết nối Core 200G. Kết nối Server/Storage 25G+.
5. **Firewall <-> Core Link:**
   * Lưu lượng Internet đỉnh: ~800 users \* 10 Mbps \* 2.5 = **~20 Gbps**
   * Thêm traffic DMZ, VPN... (Ước tính 2-5 Gbps đỉnh)
   * **Tổng lưu lượng đỉnh qua Firewall (Ước tính): ~ 22-25 Gbps**
   * **Thiết kế:** 2 x 25 Gbps MEC => **50 Gbps**. => **Đủ headroom.**
6. **Internet Gateway:**
   * **Tổng lưu lượng đỉnh ra Internet: ~20 Gbps (như trên).**
   * **Thiết kế: 2 x 10 Gbps WAN => Tổng 20 Gbps. => Vừa đủ đáp ứng đỉnh ước tính.**Cần theo dõi sát sao và có thể cần nâng cấp thêm trong tương lai nếu nhu cầu tăng.

**C. Kết luận Phân tích Băng thông:**

* Hệ thống Backbone nội bộ (Core, Distribution, Access Uplink) vẫn có **đủ băng thông** cho ~800 người dùng.
* Kết nối trong Data Center (Server, Storage) với 25G **vẫn phù hợp** nhưng cần theo dõi.
* **Việc nâng cấp WAN lên 2x10Gbps (20Gbps) là rất quan trọng và vừa đủ đáp ứng nhu cầu đỉnh ước tính.**
* **Việc nâng cấp Firewall lên dòng FG-1801F (NGFW 30Gbps, TP 25Gbps) đảm bảo khả năng xử lý cho băng thông WAN mới và lượng kết nối lớn.**

### **3.8. Thiết kế Chất lượng Dịch vụ (Quality of Service - QoS)**

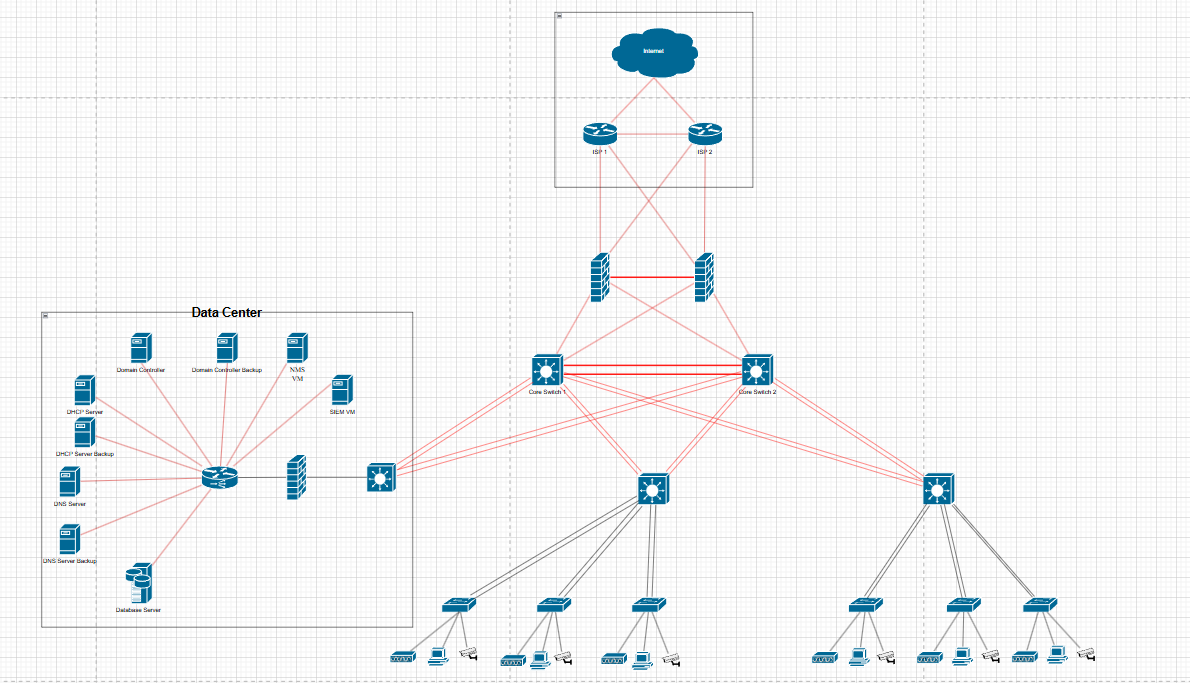
Chiến lược QoS end-to-end được áp dụng để đảm bảo hiệu năng cho các ứng dụng quan trọng:

* **Phân loại và Đánh dấu (Classification & Marking):**
  + **Tại Access Switch (Cổng vào):** Phân loại traffic dựa trên ứng dụng (NBAR2), VLAN (VLAN 70 cho Voice), hoặc chính sách từ ISE (SGT). Đánh dấu gói tin bằng DSCP (Differentiated Services Code Point) theo các lớp ưu tiên:
    - EF (Expedited Forwarding - DSCP 46): Voice (RTP)
    - AF41/AF42 (Assured Forwarding - DSCP 34/36): Video Conference
    - AF31/AF32 (DSCP 26/28): Ứng dụng nghiệp vụ quan trọng (ERP, CRM, DB Access)
    - AF21 (DSCP 18): Các ứng dụng nghiệp vụ khác
    - CS0/BE (Best Effort - DSCP 0): Các traffic còn lại (Web, Email...)
  + **Tại VM Host (vSwitch):** Có thể thực hiện đánh dấu DSCP tương tự cho traffic từ VM.
* **Hàng đợi và Lập lịch (Queuing & Scheduling):**
  + **Tại Distribution và Core Switch (Cổng ra):** Cấu hình các hàng đợi dựa trên giá trị DSCP. Sử dụng cơ chế hàng đợi ưu tiên (Priority Queuing - PQ) cho Voice (EF) để đảm bảo độ trễ thấp nhất. Sử dụng cơ chế hàng đợi công bằng theo trọng số (Weighted Fair Queuing - WFQ hoặc Weighted Round Robin - WRR) cho các lớp AF và BE để phân chia băng thông còn lại một cách hợp lý, tránh tình trạng "đói" băng thông.
  + **Kiểm soát Tắc nghẽn (Congestion Avoidance):** Sử dụng Weighted Random Early Detection (WRED) để loại bỏ gói tin một cách có chọn lọc khi hàng đợi bắt đầu đầy, ưu tiên loại bỏ các gói tin có độ ưu tiên thấp hơn trước.
* **Kiểm soát Băng thông (Policing & Shaping):**
  + **Policing (Tại cổng vào):** Có thể áp dụng để giới hạn băng thông tối đa cho một số loại traffic không mong muốn hoặc cho mạng Guest (VLAN 900).
  + **Shaping (Tại cổng ra WAN - Gateway Router):** Định hình lưu lượng ra từng ISP để phù hợp với tốc độ cam kết (10 Gbps/đường), tránh bị ISP loại bỏ gói tin.

**Tin cậy DSCP:** Cấu hình các thiết bị mạng nội bộ tin cậy (trust) giá trị DSCP đã được đánh dấu tại biên mạng (Access Switch hoặc VM Host).

## ****Chương 4: Thiết kế Vật lý****

## ****Sơ đồ tổng quan:****



### **4.0. Vai trò của Trung tâm Dữ liệu (Data Center - DC)**

Data Center (DC) đặt tại Tòa nhà B1 (Tầng Hầm) là trái tim của hạ tầng mạng và CNTT của TechNova. Vai trò chính của DC bao gồm:

* **Điểm Tập trung Mạng Lõi (Core Network Hub):** Chứa các thiết bị Core Switch, là nơi hội tụ của tất cả các kết nối backbone từ các tòa nhà và các khu vực khác.
* **Trung tâm Kết nối Internet và Bảo mật:** Chứa **các Gateway Router (Catalyst 8500)** và cụm **Firewall hiệu năng cao (FortiGate 1801F),** kiểm soát toàn bộ luồng traffic ra/vào Internet và giữa các vùng mạng.
* **Nơi chứa Hạ tầng Tính toán & Lưu trữ:** DC là nơi đặt **các Máy chủ vật lý mạnh mẽ (VM Hosts)** chạy hàng loạt máy ảo cung cấp dịch vụ cho toàn công ty (AD, DNS, DHCP, GitLab, CI/CD, NMS, SIEM, WLC, **Virtual Load Balancer...),** cùng với các hệ thống lưu trữ tập trung hiệu năng **cao (SAN - Dell PowerStore** cho block storage/VM disk) và dung lượng lớn **(NAS - Synology HD6500** hoặc tương đương cho file storage/backup).
* **Trung tâm Quản lý và Giám sát:** Thường là nơi đặt các máy chủ quản lý mạng (NMS), máy chủ giám sát (SIEM), máy chủ AAA.

DC cần được thiết kế đảm bảo các tiêu chuẩn cao về nguồn điện dự phòng (UPS, máy phát), hệ thống làm mát chính xác, phòng cháy chữa cháy tự động, kiểm soát truy cập vật lý nghiêm ngặt và hệ thống cáp cấu trúc chuyên nghiệp.

### **4.1. Lựa chọn Thiết bị - Cập nhật**

Việc lựa chọn thiết bị được cập nhật để đáp ứng yêu cầu ~800 người dùng và băng thông WAN 20Gbps:

* **Gateway Router:**Nâng cấp từ ISR4431 **lên Cisco Catalyst 8500-12X**.
* **Firewall:** Nâng cấp từ FortiGate FG-601F lên**FortiGate FG-1801F.**
* Các thiết bị Core, Distribution, Access, Wireless, Server, Storage giữ nguyên như v1.3.

### **4.2. Sơ đồ Kết nối Vật lý - Cập nhật**

Các kết nối vật lý chính được cập nhật (tham khảo thêm Bảng 4.1):

* **ISP <-> Gateway Router (C8500-12X):** Cáp quang SMF, **10 Gbps/link.**
* **Gateway Router (C8500-12X) <-> Firewall (FG-1801F):** Cáp quang MMF (OM4) hoặc DAC**, 2 x 25 Gbps MEC.**
* **Firewall (FG-1801F) <-> Core Switch (C9500):** Cáp quang MMF (OM4**), 2 x 25 Gbps MEC.**
* **Core Switch <-> DC Distribution Switch:** Cáp quang MMF (OM4), 2 x 100 Gbps MEC.
* **Core Switch <-> Building Distribution Switch:**Cáp quang MMF (OM4) cho B1, SMF (OS2) cho B2/B3, 2 x 25 Gbps MEC.
* **Distribution Switch <-> Access Switch:** Cáp quang MMF (OM4), 2 x 10 Gbps MEC.
* **Access Switch <-> End Devices:** Cáp đồng Cat6A.
* **Switch Stacking/SVL:** Sử dụng cáp stacking chuyên dụng.
* **DC Dist <-> VM Hosts/SAN/NAS:** Kết nối dự phòng 25Gbps+.

### **4.3. Bố trí Thiết bị và Hạ tầng Vật lý**

* **Data Center (DC - Tòa nhà B1, Tầng Hầm):**
  + Đặt các tủ rack tiêu chuẩn 42U.
  + Lắp đặt: Cặp **Gateway Router (C8500)**, Cặp **Firewall (FG-1801F),** Cặp Core Switch, Cặp DC Distribution Switch, **VM Hosts (vd: 4 x Dell R750), SAN (vd: 1 x Dell PowerStore), NAS (vd: 1 x Synology HD6500)**, Máy chủ quản lý (NMS, SIEM nếu là vật lý), Patch Panel quang/đồng, Hệ thống UPS tập trung.
  + Đảm bảo luồng khí lạnh/nóng, quản lý cáp gọn gàng.
* **Phòng Kỹ thuật Tòa nhà (Building TC):**
  + **B1 TC (Tầng 1):** Phục vụ Tòa nhà B1 (HQ & R&D). Chứa cặp Distribution Switch B1 (C9300X-24Y-A), Patch Panel chính B1, UPS cục bộ.
  + **B2 TC (Tầng 1):** Phục vụ Tòa nhà B2 (Dev). Chứa cặp Distribution Switch B2 (C9300X-24Y-A), Patch Panel chính B2, UPS cục bộ.
  + **B3 TC (Tầng 1):** Phục vụ Tòa nhà B3 (Kinh doanh & Hỗ trợ). Chứa cặp Distribution Switch B3 (C9300X-24Y-A), Patch Panel chính B3, UPS cục bộ.
* **Phòng Kỹ thuật Tầng (Floor TC):**
  + **B1 F1 TC:** Phục vụ Tầng 1 (Lễ tân, Lãnh đạo, Admin/HR). Chứa Access Stack B1-F1 (C9300L-48P-4X), Patch Panel đồng, UPS.
  + **B1 F2 TC:** Phục vụ Tầng 2 (R&D HW). Chứa Access Stack B1-F2 (C9300L-48P-4X), Patch Panel đồng, UPS.
  + **B1 F3 TC:** Phục vụ Tầng 3 (R&D SW). Chứa Access Stack B1-F3 (C9300L-48P-4X), Patch Panel đồng, UPS.
  + **B2 F1 TC:** Phục vụ Tầng 1 (DevTeam A, QATeam A). Chứa Access Stack B2-F1 (C9300L-48P-4X), Patch Panel đồng, UPS.
  + **B2 F2 TC:** Phục vụ Tầng 2 (DevTeam B, QATeam B). Chứa Access Stack B2-F2 (C9300L-48P-4X), Patch Panel đồng, UPS.
  + **B2 F3 TC:** Phục vụ Tầng 3 (DevOps, Mobile). Chứa Access Stack B2-F3 (C9300L-48P-4X), Patch Panel đồng, UPS.
  + **B3 F1 TC:** Phục vụ Tầng 1 (Sales, Marketing). Chứa Access Stack B3-F1 (C9300L-48P-4X), Patch Panel đồng, UPS.
  + **B3 F2 TC:** Phục vụ Tầng 2 (Support, Training). Chứa Access Stack B3-F2 (C9300L-48P-4X), Patch Panel đồng, UPS.
  + **B3 F3 TC:** Phục vụ Tầng 3 (Họp, Hot Desking). Chứa Access Stack B3-F3 (C9300L-48P-4X), Patch Panel đồng, UPS.
* **Hệ thống Cáp:**
  + Cáp trục quang (Backbone): Đi cáp quang MMF/SMF dự phòng giữa DC và các Building TC, giữa Building TC và các Floor TC.
  + Cáp ngang đồng (Horizontal): Đi cáp đồng Cat6A từ Patch Panel tại Floor TC đến các ổ cắm mạng (outlet) tại khu vực làm việc của người dùng. Mỗi vị trí làm việc có ít nhất 2 ổ cắm mạng.
  + Cáp cho AP: Đi cáp đồng Cat6A từ Access Switch đến vị trí lắp đặt AP trên trần.
  + Đánh dấu (Labeling): Tất cả cáp, ổ cắm, patch panel phải được đánh dấu rõ ràng theo tiêu chuẩn.
  + Kiểm tra (Testing): Tất cả các kết nối cáp quang và đồng phải được kiểm tra bằng thiết bị chuyên dụng sau khi lắp đặt.

### **Bảng 4.1: Mô tả Đường truyền và Kết nối Cáp (Cabling Description)**

Bảng này mô tả chi tiết loại cáp, tốc độ, và phương thức kết nối cho các liên kết chính trong hạ tầng mạng được thiết kế.

| **Điểm kết nối (Từ -> Đến)** | **Loại Cáp (Đề xuất)** | **Tốc độ / Chuẩn (Dự kiến)** | **Module Quang (Nếu có)** | **Phương thức Kết nối** | **Ghi chú** |
| --- | --- | --- | --- | --- | --- |
| **ISP -> Gateway Router (C8500)** | **Cáp quang Single-mode (OS2)** | **10 Gbps** | **SFP-10G-LR-S** | **Point-to-Point (2 đường)** | **WAN Links** |
| **Gateway Router (C8500) <-> FW (FG1801F)** | **Cáp quang MMF (OM4) / DAC** | **2 x 25 Gbps** | SFP-25G-SR-S | **MEC (Cross-connected)** | **Kết nối Router-Firewall** |
| **Firewall (FG1801F) <-> Core (C9500)** | **Cáp quang MMF (OM4)** | **2 x 25 Gbps** | SFP-25G-SR-S | **MEC** | **Kết nối Firewall-Core** |
| Core Switch <-> DC Distribution Switch | Cáp quang MMF (OM4) | 2 x 100 Gbps | QSFP-100G-SR4-S | MEC |  |
| Core Switch <-> B1 Distribution Switch | Cáp quang MMF (OM4) | 2 x 25 Gbps | SFP-25G-SR-S | MEC |  |
| Core Switch <-> B2/B3 Dist. Switch | Cáp quang SMF (OS2) | 2 x 25 Gbps | SFP-10/25G-LR-S | MEC |  |
| DC Distribution Switch <-> VM Host | Cáp quang MMF (OM4) / DAC | 2 x 25 Gbps | SFP-25G-SR-S | LACP/MEC | Hoặc DAC nếu cùng rack |
| DC Distribution Switch <-> SAN Storage | Cáp quang MMF (OM4) | 4 x 25 Gbps | SFP-25G-SR-S | MPIO/LACP |  |
| DC Distribution Switch <-> NAS Storage | Cáp quang MMF (OM4) | 2 x 25 Gbps | SFP-25G-SR-S | LACP |  |
| Building Dist. Switch <-> Access Stack | Cáp quang MMF (OM4) | 2 x 10 Gbps | SFP-10G-SR-S | MEC |  |
| Access Switch Port -> User PC/Laptop | Cáp đồng Cat6A (U/FTP hoặc F/UTP) | 1 Gbps | N/A | Point-to-Point |  |
| Access Switch Port -> IP Phone | Cáp đồng Cat6A (U/FTP hoặc F/UTP) | 1 Gbps (PoE+) | N/A | Point-to-Point | PC có thể nối tiếp qua Phone |
| Access Switch Port -> Access Point | Cáp đồng Cat6A (U/FTP hoặc F/UTP) | 1 Gbps (PoE+) | N/A | Point-to-Point | Đảm bảo Cat6A cho băng thông AP tương lai |
| Switch <-> Switch (Stacking Core/DC) | Cáp StackWise Virtual Link | (Tốc độ rất cao) | N/A | SVL (StackWise Virtual Link) | Cáp chuyên dụng (CAB-SS-VSS-3M) |
| Switch <-> Switch (Stacking Bldg Dist) | Cáp StackWise-1T | 1 Tbps | N/A | StackWise-1T | Cáp chuyên dụng (STACK-T3-1M) |
| Switch <-> Switch (Stacking Access) | Cáp StackWise-320 | 320 Gbps | N/A | StackWise-320 (Ring) | Cáp chuyên dụng + Module (C9300L-STACK-KIT) |
| Management Port -> Mgmt Switch/VLAN | Cáp đồng Cat6A (hoặc Cat6) | 1 Gbps | GLC-T (Nếu là SFP) | Point-to-Point | Kết nối quản trị Out-of-Band hoặc In-Band vào VLAN 10 |
| Console Port -> Console Server | Cáp Console Rollover (RJ45) | Serial (9600/115200 bps) | N/A | Point-to-Point | Sử dụng adapter USB nếu cần |

**Ghi chú chung:**

* **MEC (Multi-chassis EtherChannel):** Giao thức gộp băng thông và dự phòng liên kết đến hai thiết bị vật lý khác nhau hoạt động như một thể logic (vd: cặp Core chạy StackWise Virtual, cặp Firewall chạy FGCP).
* **LACP (Link Aggregation Control Protocol):** Giao thức chuẩn để gộp băng thông giữa hai thiết bị.
* **MMF (Multi-mode Fiber):** Cáp quang đa mode, thường dùng cho khoảng cách ngắn hơn (trong DC, trong tòa nhà). OM4 hỗ trợ tốc độ cao hơn OM3.
* **SMF (Single-mode Fiber):** Cáp quang đơn mode, dùng cho khoảng cách xa (giữa các tòa nhà, kết nối WAN).
* **SR (Short Reach):** Module quang cho khoảng cách ngắn (thường dùng với MMF).
* **LR (Long Reach):** Module quang cho khoảng cách xa (thường dùng với SMF).
* **DAC (Direct Attach Copper):** Cáp đồng gắn trực tiếp, giải pháp chi phí thấp cho kết nối tốc độ cao trong cùng tủ rack hoặc giữa các rack liền kề.
* **Cat6A:** Chuẩn cáp đồng hỗ trợ 10Gbps ở khoảng cách lên đến 100m, đảm bảo cho tương lai. U/FTP hoặc F/UTP giúp chống nhiễu tốt hơn UTP.
* Tất cả cáp quang và đồng cần được bấm đầu/thi công và kiểm tra theo đúng tiêu chuẩn.
* Hệ thống cáp cần được đánh dấu (labeling) rõ ràng ở cả hai đầu.

## ****Chương 5: Danh mục Vật tư Đề xuất (Bill of Materials - BoM) - Cập nhật****

**Bảng A: Phần cứng Mạng (Network Hardware)**

| **Hạng mục** | **Mã hiệu Đề xuất** | **SL** | **ĐV** |
| --- | --- | --- | --- |
| **Gateway Router** | **Cisco Catalyst C8500-12X** | **2** | **Chiếc** |
| **Firewall** | **FortiGate FG-1801F (Fortinet)** | **2** | **Chiếc** |
| Core Switch | C9500-40X-A | 2 | Chiếc |
| DC Distribution Switch | C9500-24Y4C-A | 2 | Chiếc |
| Bldg Distribution Sw | C9300X-24Y-A | 6 | Chiếc |
| Access Switch (PoE+) | C9300L-48P-4X-E | 18 | Chiếc |
| Module Uplink Core | C9500-NM-8X | 2 | Module |
| Module Uplink Bldg Dst | C9300X-NM-8Y | 6 | Module |
| Module Stacking Acc | C9300L-STACK-KIT | 18 | Kit |
| Cáp Stacking Core/DC | CAB-SS-VSS-3M | 2 | Sợi |
| Cáp Stacking Bldg Dst | STACK-T3-1M | 6 | Sợi |
| Transceiver 100G SR4 | QSFP-100G-SR4-S | 8 | Chiếc |
| Transceiver 25G SR | SFP-25G-SR-S | **72** | **Chiếc** |
| Transceiver 25G LR | SFP-10/25G-LR-S | 8 | Chiếc |
| Transceiver 10G SR | SFP-10G-SR-S | 80 | Chiếc |
| **Transceiver 10G LR** | **SFP-10G-LR-S** | **4** | **Chiếc** |
| Transceiver 1G SX | GLC-SX-MMD | 20 | Chiếc |
| Transceiver 1G T | GLC-T | 40 | Chiếc |

**Bảng B: Phần cứng Không dây (Wireless Hardware)**

| **Hạng mục** | **Mã hiệu Đề xuất (Cisco)** | **SL** | **ĐV** | **Ghi chú** |
| --- | --- | --- | --- | --- |
| Access Point (Indoor) | C9120AXI-E | 45 | Chiếc |  |
| Wireless LAN Controller | C9800-CL-K9 | 2 | Lic | (Cloud WLC License) |

**Bảng C: Phần cứng Máy chủ & Lưu trữ (Server & Storage Hardware)**

| **Hạng mục** | **Mã hiệu/Cấu hình (Đề xuất)** | **SL** | **ĐV** | **Ghi chú** |
| --- | --- | --- | --- | --- |
| VM Host Server | Dell PowerEdge R750 | 4 | Chiếc |  |
| SAN Storage | Dell PowerStore 3000T | 1 | Hệ thống |  |
| NAS Storage | Synology HD6500 | 1 | Hệ thống |  |

**Bảng D: Quản lý & Giám sát (Management & Monitoring)**

| **Hạng mục** | **Mã hiệu Đề xuất** | **SL** | **ĐV** | **Ghi chú** |
| --- | --- | --- | --- | --- |
| NMS Software License | Cisco DNA Center Virtual Appliance L | 1 | Lic | (DNAC-VA-L License, 3 năm) |
| SIEM/Log Collector | FortiAnalyzer-VM | 1 | Lic | (FAZ-VM-GB5 License, 3 năm) |
| AAA Server License | Cisco ISE Virtual Appliance L | 2 | Lic | (ISE-VM-L License, HA Pair, 3 năm Base+Plus) |

**Bảng E: Hạ tầng Vật lý & Cáp (Physical Infrastructure & Cabling)**

| **Hạng mục** | **Mô tả/Tiêu chuẩn** | **SL** | **ĐV** | **Ghi chú** |
| --- | --- | --- | --- | --- |
| Tủ Rack 42U (DC) | Tiêu chuẩn 19-inch, sâu 1000-1200mm, cửa lưới | 6 | Chiếc | Bao gồm PDU, Cable Management |
| Tủ Rack (TC) | 12U-24U treo tường hoặc đứng | 12 | Chiếc | Tùy theo số lượng switch và patch panel tại TC |
| UPS (DC) | UPS Online Double Conversion, công suất phù hợp | 2 | Hệ thống | Dự phòng N+1, thời gian lưu điện 30 phút+ |
| UPS (TC) | UPS Line-Interactive/Online, 1500-3000VA | 12 | Chiếc | Cho Switch tại TC |
| Thanh nguồn PDU (Rack) | PDU Basic/Metered/Switched, số lượng ổ cắm phù hợp | 12 | Chiếc |  |
| Patch Panel Quang LC | 24/48 port, MMF/SMF | 20 | Chiếc |  |
| Patch Panel Đồng Cat6A | 24/48 port, UTP/FTP Shielded | 50 | Chiếc |  |
| Dây nhảy Quang LC-LC | OM4 MMF / OS2 SMF, Duplex, độ dài khác nhau | 200 | Sợi |  |
| Dây nhảy Đồng Cat6A | UTP/FTP Shielded, độ dài khác nhau | 1000 | Sợi |  |
| Cáp đồng Cat6A | Cuộn 305m, U/FTP hoặc F/UTP Shielded, LSZH | 100 | Cuộn | Ước tính số lượng |
| Cáp quang MMF OM4 | 12/24 sợi, Indoor/Outdoor, LSZH | 3000 | Mét | Ước tính cho Backbone trong tòa nhà/DC |
| Cáp quang SMF OS2 | 12/24 sợi, Indoor/Outdoor, LSZH | 2000 | Mét | Ước tính cho Backbone liên tòa nhà |
| Ổ cắm mạng Cat6A | Modular Jack Keystone Cat6A, mặt nạ, đế âm/nổi | 800 | Bộ |  |
| Hộp phối quang (ODF) | Treo tường/Trong rack, adapter, khay hàn | 20 | Bộ |  |
| Vật tư phụ | Dây hàn quang, ống co nhiệt, dây rút, nhãn dán... | 1 | Gói |  |

**Bảng F: Phần mềm & Giấy phép (Software & Licenses) - Cập nhật**

| **Hạng mục** | **Đơn vị Tính** | **SL** | **Ghi chú (Cần xác nhận chi tiết license với vendor)** |
| --- | --- | --- | --- |
| **Cisco DNA SW (Routers)** | **Lic/Router/3năm** | **2** | **DNA Advantage/Premier cho C8500** |
| Cisco DNA SW (Switches) | Lic/Switch/3năm | 28 | DNA Advantage (Core/Dist), Essentials (Access) |
| Cisco DNA SW (APs) | Lic/AP/3năm | 15 | DNA Essentials/Advantage for APs |
| Cisco DNA SW (Controller) | Lic/Controller/3năm | 1 | License bổ sung cho C9800-CL (nếu cần) |
| **FW Security Bundle** | **Lic/Firewall/3năm** | **2** | **FortiGuard UTP Bundle cho FG-1801F** |
| Virtualization OS | Lic/Socket | 8 | vd: VMware vSphere Enterprise Plus (8 sockets, 3yr) |
| Server Guest OS | Lic/2-core pack | 50 | vd: Windows Server Standard/Datacenter (ước tính cores) |
| Backup Software License | Lic/VM/Năm | 30 | vd: Veeam Backup & Replication (30 VMs, 3yr) |
| Database License | Lic/Core (2pk) | 5 | vd: SQL Server Standard (10 cores, 3yr) |
| Virtual Load Balancer | Lic/VM/Năm | 2 | vd: F5 BIG-IP VE or similar (HA Pair, 3yr) |

**Bảng G: Hỗ trợ & Dịch vụ (Support & Services)**

| **Hạng mục** | **Mô tả** | **SL** | **ĐV** | **Ghi chú** |
| --- | --- | --- | --- | --- |
| Hỗ trợ Kỹ thuật (Hardware) | Cisco SmartNet (8x5xNBD/24x7x4), FortiCare, Dell ProSupport | 1 | Gói/3năm | Cho tất cả phần cứng quan trọng |
| Hỗ trợ Kỹ thuật (Software) | Hỗ trợ cho VMware, Windows Server, Veeam... | 1 | Gói/3năm |  |
| Dịch vụ Tư vấn & Thiết kế | Phân tích yêu cầu, Thiết kế chi tiết, Lập BoM | 1 | Gói |  |
| Dịch vụ Triển khai & Cấu hình | Lắp đặt, Cấu hình thiết bị, Tích hợp hệ thống | 1 | Gói | Bao gồm cấu hình ảo hóa, storage, security... |
| Dịch vụ Quản lý Dự án | Điều phối, Giám sát tiến độ, Báo cáo | 1 | Gói |  |
| Dịch vụ Đào tạo & Chuyển giao | Đào tạo quản trị, Vận hành hệ thống | 1 | Gói |  |
| Dịch vụ Kiểm tra & Nghiệm thu | Kiểm tra chức năng, Hiệu năng, Bảo mật, Bàn giao | 1 | Gói |  |

## ****Chương 5 Phụ lục: Đặc tả Kỹ thuật Chính và Lý do Lựa chọn Thiết bị - Cập nhật****

### **A. Thiết bị Mạng (Network Hardware) - Cập nhật**

#### **1. Core Switch: Cisco Catalyst 9500 Series (C9500-40X)**

* **Vai trò:** Trung tâm chuyển mạch tốc độ cao, định tuyến liên VLAN, kết nối các Distribution Block.
* **Đặc tả chính:** 40 port 1/10G SFP+, hỗ trợ module uplink C9500-NM-8X (8x10G), khả năng chuyển mạch lên đến 1.6 Tbps, hỗ trợ StackWise Virtual, tính năng Layer 3 đầy đủ (EIGRP, OSPF, BGP, PIM), QoS, Security (MACsec, TrustSec).
* **Lý do Lựa chọn:** Hiệu năng cao, độ tin cậy (StackWise Virtual loại bỏ STP/FHRP tại Core), tính năng phong phú, phù hợp vai trò Core trong mạng doanh nghiệp lớn.

#### **2. DC Distribution Switch: Cisco Catalyst 9500 Series (C9500-24Y4C)**

* **Vai trò:** Tập trung kết nối từ VM Hosts, SAN, NAS trong DC, kết nối lên Core, định tuyến VLAN DC.
* **Đặc tả chính:** 24 port 1/10/25G SFP28 + 4 port 40/100G QSFP28, khả năng chuyển mạch lên đến 3.2 Tbps, hỗ trợ StackWise Virtual, tính năng L3, QoS, Security. Mật độ cổng 25G/100G cao.
* **Lý do Lựa chọn:** Mật độ cổng 25G/100G cao phù hợp DC, hiệu năng mạnh, HA với StackWise Virtual, tích hợp tốt với Core C9500.

#### **3. Building Distribution Switch: Cisco Catalyst 9300X Series (C9300X-24Y)**

* **Vai trò:** Tập trung kết nối từ Access Switches trong tòa nhà, kết nối lên Core, định tuyến VLAN tòa nhà, áp dụng chính sách ACL/QoS.
* **Đặc tả chính:** 24 port 1/10/25G SFP28, hỗ trợ module uplink C9300X-NM-8Y (8x25G), hỗ trợ Stacking (StackWise-1T - 1Tbps), hiệu năng cao, tính năng L3, QoS, Security (TrustSec).
* **Lý do Lựa chọn:** Hiệu năng cao, mật độ cổng 10/25G, khả năng Stacking mạnh mẽ, tính năng đầy đủ cho lớp Distribution.

#### **4. Access Switch: Cisco Catalyst 9300L Series (C9300L-48P-4X)**

* **Vai trò:** Cung cấp kết nối có dây cho người dùng cuối, AP, IP Phone, cấp nguồn PoE+, bảo mật cổng.
* **Đặc tả chính:** 48 port 1G UTP PoE+ (IEEE 802.3at, 30W/port, tổng budget 740W), 4 port 10G SFP+ uplink (dùng SFP-10G-SR-S), hỗ trợ Stacking (StackWise-320 - 320Gbps) với module C9300L-STACK-KIT, tính năng Layer 2 phong phú, QoS, Security (802.1X, DHCP Snooping, DAI, IPSG, TrustSec).
* **Lý do Lựa chọn:** Mật độ cổng cao, PoE+ đầy đủ, uplink 10G, khả năng Stacking tốt, tính năng bảo mật mạnh mẽ, chi phí hợp lý cho lớp Access.

#### **5. Firewall: FortiGate FG-1801F (Nâng cấp)**

* **Vai trò:** Bảo vệ biên mạng hiệu năng cao, kiểm soát truy cập giữa các zone, VPN Gateway cho số lượng lớn user, IPS, Web Filtering, App Control cho băng thông WAN 20Gbps.
* **Đặc tả chính:** Thông lượng Firewall ~198 Gbps, IPS ~30 Gbps, NGFW ~30 Gbps, Threat Protection ~25 Gbps, SSL-VPN ~20 Gbps. Nhiều cổng giao tiếp tốc độ cao (GE, 10G SFP+, 25G SFP28, 40/100G QSFP28). Hỗ trợ HA (Active/Passive, Active/Active). Có ổ SSD onboard (1TB) cho logging/WAN Opt.
* **Lý do Lựa chọn:** **Hiệu năng vượt trội** so với FG-601F, đáp ứng tốt băng thông WAN 20Gbps và lượng kết nối/VPN của ~800 người dùng. Cung cấp các cổng tốc độ cao phù hợp với Core switch và Router mới.

#### **6. Gateway Router: Cisco Catalyst 8500-12X (Nâng cấp)**

* **Vai trò:** Kết nối đến ISP tốc độ cao (10G), chạy BGP, định tuyến traffic Internet, hỗ trợ SD-WAN (nếu cần).
* **Đặc tả chính:** Nền tảng Aggregation Services Router hiệu năng cao. Model C8500-12X có 12 cổng 1/10G SFP+. Thông lượng IPsec/Service cao. Hỗ trợ đầy đủ các tính năng định tuyến (BGP), QoS, Security, HA (HSRP/VRRP). Chạy IOS-XE tương thích DNA Center.
* **Lý do Lựa chọn:** **Hiệu năng cao hơn nhiều** so với ISR4431, hỗ trợ cổng 10G native để kết nối trực tiếp đường WAN 10Gbps. Phù hợp vai trò biên mạng tốc độ cao.

### **B. Thiết bị Không dây (Wireless Hardware)**

#### **1. Access Point: Cisco Catalyst 9120AX Series (C9120AXI)**

* **Vai trò:** Cung cấp kết nối Wi-Fi 6 cho người dùng cuối.
* **Đặc tả chính:** Chuẩn 802.11ax (Wi-Fi 6), 4x4 MU-MIMO trên cả 2.4GHz và 5GHz, OFDMA, TWT, BSS Coloring, hỗ trợ WPA3, tích hợp antenna trong (Internal - I), cổng uplink 2.5G mGig, yêu cầu PoE+ (802.3at).
* **Lý do Lựa chọn:** Chuẩn Wi-Fi 6 mới nhất cho hiệu năng và dung lượng cao, tính năng bảo mật WPA3, tích hợp tốt trong hệ sinh thái Cisco.

#### **2. Wireless LAN Controller: Cisco Catalyst 9800-CL (Cloud)**

* **Vai trò:** Quản lý tập trung các AP, cấu hình SSID, chính sách bảo mật, roaming, HA.
* **Đặc tả chính:** WLC ảo hóa chạy trên nền tảng VM (VMware ESXi), hỗ trợ lên đến 6000 AP và 64000 client (tùy license và tài nguyên VM), kiến trúc IOS-XE ổn định, hỗ trợ HA SSO, tính năng phong phú (RF Management, Security, Guest Access, Application Visibility).
* **Lý do Lựa chọn:** Linh hoạt (triển khai VM), tiết kiệm chi phí phần cứng, khả năng mở rộng tốt, HA mạnh mẽ, tính năng tương đương WLC vật lý.

### **C. Máy chủ & Lưu trữ (Server & Storage Hardware)**

#### **1. VM Host Server: Dell PowerEdge R750 (Cấu hình đề xuất)**

* **Vai trò:** **Nền tảng ảo hóa chính, chạy hàng chục máy ảo (VMs) để hợp nhất nhiều dịch vụ (AD, DNS, DHCP, WLC, NMS, SIEM, vLB, File Server, App Server, DB Server...). Giúp tiết kiệm chi phí phần cứng, điện năng, không gian.**
* **Cấu hình Đề xuất:**
  + CPU: 2 x Intel Xeon Gold 6330 (28 Cores/56 Threads mỗi CPU, tổng 56 Cores/112 Threads).
  + RAM: 768 GB DDR4 ECC RDIMM (24 x 32GB).
  + Storage (Boot): 2 x 960GB SSD BOSS (Boot Optimized Storage Solution) RAID 1 (cho Hypervisor OS).
  + Network: 2 x Dual-Port 25GbE SFP28 Adapter (SFP-25G-SR-S).
  + Quản lý: iDRAC9 Enterprise. Dual Hot-plug PSU 1100W.
* **Lý do Lựa chọn:** Hiệu năng CPU/RAM cực cao cho ảo hóa, khả năng mở rộng tốt, network 25G tốc độ cao, quản lý từ xa mạnh mẽ (iDRAC), độ tin cậy cao.

#### **2. SAN Storage: Dell PowerStore 3000T (Cấu hình đề xuất)**

* **Vai trò: Cung cấp lưu trữ block hiệu năng cực cao (All-NVMe) qua iSCSI cho các VM Hosts. Là nơi chứa các ổ đĩa ảo (VMDK) của các VM quan trọng, đòi hỏi IOPS và độ trễ thấp (databases, ứng dụng...). Tối ưu cho môi trường ảo hóa.**
* **Cấu hình Đề xuất:**
  + Model: PowerStore 3000T Base Enclosure (2U).
  + Loại ổ: All NVMe SSD. Số lượng ổ: 18 x 3.84TB NVMe SSD.
  + Dung lượng thô: ~69 TB. Dung lượng sử dụng hiệu quả (Ước tính sau RAID & Data Reduction): ~45-100+ TB (tùy tỷ lệ nén/dedupe).
  + Kết nối: Dual Controller Active-Active, mỗi controller có 4 x 25GbE SFP28 ports (dùng SFP-25G-SR-S) hỗ trợ iSCSI/NVMe-oF.
  + **Data Services:** Deduplication & Compression (inline, luôn bật, đảm bảo hiệu quả), Thin Provisioning, Snapshots, Replication (Async/Sync).
* **Lý do Lựa chọn:** Hiệu năng NVMe vượt trội, kiến trúc container-based linh hoạt, tối ưu dữ liệu hiệu quả, HA mạnh mẽ, tích hợp tốt với VMware (VAAI, VASA).

#### **3. NAS Storage: Synology HD6500 (Cấu hình đề xuất)**

* **Vai trò:** **Cung cấp lưu trữ file dung lượng lớn qua SMB/NFS. Dùng cho chia sẻ file người dùng, lưu trữ dữ liệu dự án, và đặc biệt quan trọng là làm đích lưu trữ backup cho các máy ảo và dữ liệu trên SAN/Server. Chi phí trên mỗi TB thấp hơn SAN.**
* **Cấu hình Đề xuất:**
  + Model: Synology HD6500 (4U, 60-bay SAS/SATA HDD/SSD).
  + Loại ổ cứng: 24 x 18TB Synology HAT5300 SAS HDD (Có thể mở rộng).
  + Dung lượng thô: ~432 TB. Dung lượng sử dụng (Ước tính RAID 6): ~396 TB.
  + RAM: 128 GB ECC DDR4 (Nâng cấp).
  + SSD Cache: 2 x 1.92TB Synology SAT5200 SATA SSD (RAID 1 Read/Write Cache).
  + Kết nối: 2 x 10GbE RJ45 onboard + 1 x Dual-Port 25GbE SFP28 Adapter (E25G21-F2, dùng SFP-25G-SR-S).
* **Lý do Lựa chọn:** Dung lượng cực lớn, chi phí hợp lý cho lưu trữ file/backup, hệ điều hành DSM mạnh mẽ và nhiều tính năng (Snapshot Replication, Active Backup for Business...), hỗ trợ network 10G/25G, khả năng mở rộng cao.

### **D. Quản lý & Giám sát (Management & Monitoring)**

#### **1. NMS: Cisco DNA Center Virtual Appliance**

* **Vai trò:** Quản lý tập trung thiết bị mạng Cisco, tự động hóa cấu hình, giám sát hiệu năng, bảo mật, đảm bảo chất lượng dịch vụ.
* **Đặc tả chính:** Triển khai dạng VM (Large profile đề xuất), cung cấp giao diện đồ họa, tính năng Assurance (phân tích mạng, health score), Automation (PnP, SWIM), SD-Access (nếu cần), tích hợp ISE/vCenter.
* **Lý do Lựa chọn:** Giải pháp quản lý toàn diện cho hạ tầng Cisco, giúp đơn giản hóa vận hành và tăng hiệu quả.

#### **2. SIEM: FortiAnalyzer-VM**

* **Vai trò:** Thu thập, phân tích và lưu trữ log tập trung từ FortiGate Firewall và các thiết bị khác, cung cấp báo cáo bảo mật, phát hiện mối đe dọa.
* **Đặc tả chính:** Triển khai dạng VM (GB/day license tùy nhu cầu, vd: 5GB/day), khả năng thu thập log cao, phân tích và tạo báo cáo chi tiết, tích hợp FortiGuard IOC, tự động hóa phản ứng (Automation Stitches).
* **Lý do Lựa chọn:** Tích hợp chặt chẽ với FortiGate, cung cấp cái nhìn sâu sắc về tình hình bảo mật, hỗ trợ tuân thủ.

#### **3. AAA Server: Cisco ISE Virtual Appliance**

* **Vai trò:** Cung cấp dịch vụ AAA (Authentication, Authorization, Accounting) cho quản trị thiết bị (TACACS+) và kiểm soát truy cập mạng (RADIUS, 802.1X). Trung tâm của giải pháp TrustSec/SGT.
* **Đặc tả chính:** Triển khai dạng VM (Large profile đề xuất cho HA), hỗ trợ nhiều giao thức AAA, tích hợp AD, phân quyền chi tiết, tính năng Posture Assessment, Guest Access, BYOD, pxGrid (chia sẻ ngữ cảnh bảo mật).
* **Lý do Lựa chọn:** Giải pháp NAC/AAA mạnh mẽ và toàn diện của Cisco, tích hợp tốt với hạ tầng mạng Cisco, nền tảng cho Zero Trust Network Access.

### **E. Thành phần Ảo hóa Khác (Other Virtualized Components)**

#### **1. Virtual Load Balancer (vLB) VM (License)**

* **Vai trò: Phân phối lưu lượng truy cập đến các nhóm máy chủ ảo (VM backend) để tăng hiệu năng và độ sẵn sàng cho ứng dụng (vd: GitLab, Web Servers, App Servers). Triển khai dưới dạng VM giúp tiết kiệm chi phí so với mua thiết bị phần cứng chuyên dụng.**
* **Ví dụ Giải pháp:** F5 BIG-IP VE, Nginx Plus, HAProxy...
* **Cấu hình VM Đề xuất (Ví dụ - Cần sizing theo vendor và tải):**
  + vCPU: 4-8 cores / VM.
  + RAM: 8-16 GB / VM.
  + Disk: 100-200 GB / VM.
  + Network: Nhiều vNICs kết nối các VLAN cần thiết (vd: VLAN 20 frontend, VLAN 20 backend).
* **HA:** Triển khai 2 VM chạy Active/Standby hoặc Active/Active.
* **Lý do Lựa chọn:** Linh hoạt, tiết kiệm chi phí phần cứng, dễ dàng quản lý trong môi trường ảo hóa.

## ****Chương 6: Ước tính Chi phí Dự án (Project Cost Estimation) - Cập nhật****

(Lưu ý: Đơn vị: VNĐ. Giá chỉ là tham khảo, chi phí Router/Firewall mới cao hơn đáng kể, cần lấy báo giá chính thức)

**Bảng A: Chi phí Phần cứng Mạng (Network Hardware) - Cập nhật**

| **Hạng mục** | **SL** | **Đơn giá Ước tính** | **Thành tiền Ước tính** | **Ghi chú (Thông số chính)** |
| --- | --- | --- | --- | --- |
| **Gateway Router** | **2** | **1,200,000,000** | **2,400,000,000** | **Cisco C8500-12X** |
| **Firewall** | **2** | **1,500,000,000** | **3,000,000,000** | **FortiGate FG-1801F** |
| Core Switch | 2 | 600,000,000 | 1,200,000,000 | CiscoC950040X,40x10G, SVL, L3 |
| DC Distribution Switch | 2 | 550,000,000 | 1,100,000,000 | Cisco C9500-24Y4C, 24x25G+4x100G, SVL, L3 |
| Bldg Distribution Sw | 6 | 300,000,000 | 1,800,000,000 | Cisco C9300X-24Y, 24x25G, Stack-1T, L3 |
| Access Switch (PoE+) | 18 | 80,000,000 | 1,440,000,000 | Cisco C9300L-48P, 48p PoE+ 740W, 4x10G, Stack |
| Modules (Core/Dist) | 8 | 30,000,000 | 240,000,000 | C9500-NM-8X / C9300X-NM-8Y Module |
| Transceivers Tổng | LS | 920,000,000 | 920,000,000 | QSFP28, SFP28 SR/LR, SFP+ SR/LR, SFP SX/T |
| **Tổng cộng (A)** |  |  | **12,100,000,000** | (Tổng A tăng mạnh) |

**Bảng B: Chi phí Phần cứng Không dây (Wireless Hardware)**

| **Hạng mục** | **SL** | **Đơn giá Ước tính** | **Thành tiền Ước tính** | **Ghi chú (Thông số chính)** |
| --- | --- | --- | --- | --- |
| Access Point (Indoor) | 45 | 5,000,000 | 225,000,000 | Cisco C9120AXI, Wi-Fi 6, 4x4 MU-MIMO |
| Wireless LAN Controller | 2 | 35,000,000 | 70,000,000 | Cisco C9800-CL License (HA Pair) |
| **Tổng cộng (B)** |  |  | **295,000,000** |  |

**Bảng C: Chi phí Phần cứng Máy chủ & Lưu trữ (Server & Storage Hardware)**

| **Hạng mục** | **SL** | **Đơn giá Ước tính** | **Thành tiền Ước tính** | **Ghi chú (Thông số chính)** |
| --- | --- | --- | --- | --- |
| VM Host Server | 4 | 550,000,000 | 2,200,000,000 | Dell R750, 2x28 Core, 768GB RAM, 2x25G NIC |
| SAN Storage | 1 | 1,800,000,000 | 1,800,000,000 | Dell PowerStore 3000T, All-NVMe, ~45TB, 25G iSCSI |
| NAS Storage | 1 | 980,000,000 | 980,000,000 | Synology HD6500, 60-bay, ~360TB HDD, 25G NIC |
| **Tổng cộng (C)** |  |  | **4,980,000,000** |  |

**Bảng D: Chi phí Quản lý & Giám sát (Management & Monitoring)**

| **Hạng mục** | **SL** | **Đơn giá Ước tính** | **Thành tiền Ước tính** | **Ghi chú (Thông số chính)** |
| --- | --- | --- | --- | --- |
| NMS Software License | 1 | 150,000,000 | 150,000,000 | Cisco DNAC-VA-L (3yr), Quản lý hạ tầng Cisco |
| SIEM/Log Collector | 1 | 60,000,000 | 60,000,000 | FortiAnalyzer-VM (3yr), Phân tích log FortiGate |
| AAA Server License | 2 | 37,500,000 | 75,000,000 | Cisco ISE-VM-L (3yr HA), NAC/TACACS+ |
| **Tổng cộng (D)** |  |  | **285,000,000** |  |

**Bảng E: Chi phí Hạ tầng Vật lý & Cáp (Physical Infrastructure & Cabling)**

| **Hạng mục** | **SL** | **Đơn giá Ước tính** | **Thành tiền Ước tính** | **Ghi chú (Thông số chính)** |
| --- | --- | --- | --- | --- |
| Tủ Rack 42U (DC) | 6 | 25,000,000 | 150,000,000 | 19", 1000-1200mm depth, PDU, Cable Mgmt |
| Tủ Rack (TC) | 12 | 8,000,000 | 96,000,000 | 12U-24U Wall-mount/Floor-standing |
| UPS (DC) | 2 | 300,000,000 | 600,000,000 | Online Double Conversion, N+1, ~30min runtime |
| UPS (TC) | 12 | 10,000,000 | 120,000,000 | Line-Interactive/Online, 1.5-3kVA |
| Patch Panels & PDU | LS | 80,000,000 | 80,000,000 | LC Fiber Panels, Cat6A Copper Panels, Rack PDUs |
| Hệ thống Cáp (Đồng) | 800 | 1,000,000 | 800,000,000 | Cat6A U/FTP or F/UTP, Outlets, Patch Cords, Labor |
| Hệ thống Cáp (Quang) | LS | 350,000,000 | 350,000,000 | OM4 MMF, OS2 SMF Backbone, ODF, Patch Cords, Labor |
| Vật tư phụ & Lắp đặt | LS | 59,000,000 | 59,000,000 | Trays, Ties, Labels, Consumables, Installation Labor |
| **Tổng cộng (E)** |  |  | **2,255,000,000** |  |

**Bảng F: Chi phí Phần mềm & Giấy phép (Software & Licenses) - Cập nhật**

| **Hạng mục** | **Đơn vị Tính** | **SL** | **Đơn giá Tham khảo** | **Thành tiền Tham khảo** | **Ghi chú** |
| --- | --- | --- | --- | --- | --- |
| **Cisco DNA SW (Routers)** | **Lic/Router/3năm** | **2** | **100,000,000** | **200,000,000** | **DNA Advantage/Premier cho C8500** |
| Cisco DNA SW (Switches) | Lic/Switch/3năm | 28 | 9,000,000 | 252,000,000 | DNA Advantage (Core/Dist), Essentials (Access) |
| Cisco DNA SW (APs) | Lic/AP/3năm | 15 | 4,500,000 | 67,500,000 | DNA Essentials/Advantage for APs |
| Cisco DNA SW (Controller) | Lic/Controller/3năm | 1 | 15,000,000 | 15,000,000 | Additional license for C9800-CL (if needed) |
| **FW Security Bundle** | **Lic/Firewall/3năm** | **2** | **(Cần báo giá)** | **1,000,000,000** | **FortiGuard UTP Bundle cho FG-1801F (Ước tính rất cao)** |
| Virtualization OS | Lic/Socket | 8 | 50,000,000 | 400,000,000 | VMware vSphere Enterprise Plus (8 sockets, 3yr) |
| Server Guest OS | Lic/2-core pack | 50 | 3,000,000 | 150,000,000 | Windows Server Standard/Datacenter (ước tính cores) |
| Backup Software License | Lic/VM/Năm | 30 | 3,000,000 | 270,000,000 | Veeam Backup & Replication (30 VMs, 3yr) |
| Database License | Lic/Core (2pk) | 5 | 50,000,000 | 250,000,000 | SQL Server Standard (10 cores, 3yr) |
| Virtual Load Balancer | Lic/VM/Năm | 2 | 40,000,000 | 240,000,000 | F5 BIG-IP VE or similar (HA Pair, 3yr) |
| **Tổng cộng (F)** |  |  |  | **2,844,500,000** | (Tổng F tăng mạnh) |

**Bảng G: Chi phí Hỗ trợ & Dịch vụ (Support & Services)**

| **Hạng mục** | **Thành tiền Ước tính** | **Ghi chú (Thông số chính)** |
| --- | --- | --- |
| Hỗ trợ Kỹ thuật (HW+SW) 3 năm | 1,500,000,000 | SmartNet, FortiCare, ProSupport, VMware Support... |
| Dịch vụ Tư vấn & Thiết kế | 250,000,000 | Requirement Analysis, Detailed Design, BoM Validation |
| Dịch vụ Triển khai & Cấu hình | 2,000,000,000 | Installation, Configuration, Integration, Migration |
| Dịch vụ Quản lý Dự án | 300,000,000 | Project Planning, Coordination, Reporting |
| Dịch vụ Đào tạo & Chuyển giao | 150,000,000 | Admin Training, Operational Handover |
| Dịch vụ Kiểm tra & Nghiệm thu | 194,000,000 | Testing (Functional, Performance, Security), Acceptance |
| **Tổng cộng (G)** | **4,394,000,000** |  |

**Bảng H: Tổng Chi phí Ước tính Dự án (Cập nhật)**

| **Hạng mục Chi phí** | **Thành tiền Ước tính (VNĐ)** |
| --- | --- |
| A. Phần cứng Mạng (Network Hardware) | **12,100,000,000** |
| B. Phần cứng Không dây (Wireless Hardware) | 295,000,000 |
| C. Phần cứng Máy chủ & Lưu trữ (Server & Storage) | 4,980,000,000 |
| D. Quản lý & Giám sát (Management & Monitoring) | 285,000,000 |
| E. Hạ tầng Vật lý & Cáp (Physical Infra & Cabling) | 2,255,000,000 |
| F. Phần mềm & Giấy phép (Software & Licenses) | **2,844,500,000** |
| G. Hỗ trợ & Dịch vụ (Support & Services) | 4,394,000,000 |
| **TỔNG CỘNG TẠM TÍNH (Chưa VAT, Chưa Dự phòng)** | **27,153,500,000** |

**Ngân sách Dự kiến (Tham khảo - Cập nhật):**

* **Tổng cộng tạm tính:** 27,153,500,000 VNĐ
* **Thuế VAT (ước tính 10%):** 2,715,350,000 VNĐ
* **Chi phí Dự phòng (ước tính 10% trên tổng tạm tính):** 2,715,350,000 VNĐ
* **TỔNG NGÂN SÁCH DỰ KIẾN (Ước tính):** \*\*~ 32,584,200,000 VNĐ\*\*

**Khoảng 32.58 tỷ VNĐ là ngân sách dự kiến mới sau khi nâng cấp Router, Firewall và các license liên quan để hỗ trợ ~800 người dùng đồng thời.**

## ****Chương 7: Kết luận - Cập nhật****

### **7.1. Tóm tắt Thiết kế**

Tài liệu này đã trình bày một giải pháp thiết kế hạ tầng mạng LAN **tiên tiến, chi tiết và toàn diện** cho trụ sở mới của TechNova Solutions, **được nâng cấp để hỗ trợ hiệu quả khoảng 800 người dùng hoạt động đồng thời**. Kiến trúc phân lớp kết hợp với việc ứng dụng sâu các công nghệ như StackWise Virtual, Wi-Fi 6, **NGFW hiệu năng cao (FortiGate 1801F)**, **Router biên mạnh mẽ (Catalyst 8500)**, NAC 802.1X, TrustSec, và QoS end-to-end đảm bảo hiệu năng, độ sẵn sàng và bảo mật cao. **Băng thông WAN được nâng cấp lên 2x10Gbps**. Ảo hóa vẫn được tích hợp xuyên suốt, tối ưu hóa việc sử dụng tài nguyên và chi phí. **Các thiết bị đề xuất được tin là đang được hỗ trợ tích cực, tuy nhiên cần xác nhận lại với nhà cung cấp trước khi mua hàng.**

### **7.2. Đáp ứng Yêu cầu**

Thiết kế **đã được nâng cấp** đáp ứng đầy đủ các yêu cầu nghiệp vụ và kỹ thuật cho **quy mô ~800 người dùng đồng thời**, khai thác hiệu quả các tính năng nâng cao của thiết bị được chọn. Kế hoạch IP/VLAN chi tiết theo phòng ban/tầng lầu cung cấp nền tảng vững chắc cho quản lý và bảo mật. **Việc nâng cấp WAN và Firewall giải quyết các điểm nghẽn chính**, đảm bảo hiệu năng truy cập Internet và VPN. Chiến lược ảo hóa và NFV giúp tối ưu đáng kể chi phí đầu tư và vận hành.

### **7.3. Hướng Phát triển Tương lai**

* **Nâng cấp Băng thông:** Dễ dàng nâng cấp tốc độ các liên kết backbone nội bộ lên 40/100G hoặc cao hơn khi cần. Nâng cấp Access lên Multi-Gigabit (2.5/5/10G) nếu có yêu cầu. Nâng cấp WAN lên cao hơn 20Gbps nếu nhu cầu tăng.
* **Software-Defined Access (SD-Access):** Kiến trúc sẵn sàng cho việc triển khai SD-Access của Cisco để tăng cường tự động hóa, bảo mật và phân đoạn vi mô (micro-segmentation).
* **Cloud Integration:** Tích hợp sâu hơn với các dịch vụ đám mây (IaaS, PaaS, SaaS) thông qua kết nối WAN tốc độ cao và bảo mật. Xem xét SD-WAN (Catalyst 8500 hỗ trợ tốt) nếu có nhiều chi nhánh hoặc nhu cầu tối ưu cloud access.
* **IoT Security:** Triển khai các giải pháp bảo mật chuyên dụng cho IoT khi số lượng thiết bị tăng lên.
* **Zero Trust Architecture:** Từng bước áp dụng các nguyên tắc của kiến trúc Zero Trust để tăng cường bảo mật.
* **Tự động hóa sâu hơn:** Sử dụng DNA Center APIs, Ansible/Python để tự động hóa các tác vụ cấu hình, kiểm tra tuân thủ, và khắc phục sự cố.
* **Micro-segmentation:** Triển khai vFW hoặc sử dụng TrustSec/SGACLs một cách triệt để để kiểm soát traffic East-West chi tiết hơn.