**TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI**

**THÀNH PHỐ HỒ CHÍ MINH**

**VIỆN CÔNG NGHỆ THÔNG TIN VÀ ĐIỆN, ĐIỆN TỬ**

****

**BÁO CÁO ĐỀ TÀI**

**THIẾT KẾ VÀ MÔ PHỎNG MẠNG SD-WAN CHO TRƯỜNG HỌC**

**Môn: Mạng máy tính nâng cao**

**Mã lớp học phần: 010112304402**

**Sinh viên thực hiện**

|  |  |
| --- | --- |
| **Họ tên sinh viên** | **Mã số sinh viên** |
| 1. **Vũ Hoàng Yến** | **072305008527** |
| 1. **Lê Thiên Trứ** | **083305003459** |
| 1. **Huỳnh Võ Huyền Trân** | **091305001510** |
| 1. **Võ Hồng Phúc** | **077205008111** |
| 1. **Đặng Duy Khánh** | **052205011731** |

**Thành phố Hồ Chí Minh, tháng 11 năm 2025**

**TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI**

**THÀNH PHỐ HỒ CHÍ MINH**

**VIỆN CÔNG NGHỆ THÔNG TIN VÀ ĐIỆN, ĐIỆN TỬ**

****

**BÁO CÁO ĐỀ TÀI**

**THIẾT KẾ VÀ MÔ PHỎNG MẠNG SD-WAN CHO TRƯỜNG HỌC**

**Môn: Mạng máy tính nâng cao**

**Mã lớp học phần: 010112304402**

**NGƯỜI HƯỚNG DẪN KHOA HỌC: GV. PHAN THỊ HỒNG NHUNG**

**Sinh viên thực hiện**

|  |  |
| --- | --- |
| **Họ tên sinh viên** | **Mã số sinh viên** |
| 1. **Vũ Hoàng Yến** | **072305008527** |
| 1. **Lê Thiên Trứ** | **083305003459** |
| 1. **Huỳnh Võ Huyền Trân** | **091305001510** |
| 1. **Võ Hồng Phúc** | **077205008111** |
| 1. **Đặng Duy Khánh** | **052205011731** |

**Thành phố Hồ Chí Minh, tháng 11 năm 2025**

# LỜI CAM ĐOAN

Chúng tôi xin cam đoan đây là công trình nghiên cứu của riêng chúng tôi. Các số liệu, kết quả nêu trong báo cáo là trung thực và chưa từng được công bố trong bất kỳ công trình nào khác. Mọi sự giúp đỡ cho việc thực hiện báo cáo này đã được cảm ơn và các thông tin trích dẫn trong báo cáo đã được chỉ rõ nguồn gốc.

Chúng tôi xin chịu trách nhiệm về đề tài nghiên cứu của nhóm mình.

Hồ Chí Minh, ngày 14 tháng 11 năm 2025

Đại diện nhóm E

Vũ Hoàng Yến

# LỜI CẢM ƠN

Để hoàn thành báo cáo này, chúng tôi đã nhận được sự giúp đỡ và hỗ trợ quý báu từ nhiều cá nhân và tổ chức. Chúng tôi xin bày tỏ lòng biết ơn sâu sắc tới:

* GV. Phan Thị Hồng Nhung, người hướng dẫn khoa học, đã tận tình chỉ bảo và định hướng cho chúng tôi trong suốt quá trình thực hiện báo cáo.
* Ban lãnh đạo và các thầy cô giáo Khoa Công nghệ thông tin, Trường Đại học Giao thông vận tải TP.HCM đã trang bị cho chúng tôi nền tảng kiến thức vững chắc để thực hiện nghiên cứu này.
* Gia đình, bạn bè đã luôn động viên và hỗ trợ tôi trong suốt quá trình học tập và nghiên cứu.

Mặc dù đã có nhiều cố gắng, song báo cáo không tránh khỏi những thiếu sót. Chúng tôi rất mong nhận được ý kiến đóng góp của quý thầy cô và các bạn đọc để báo cáo được hoàn thiện hơn.

Xin trân trọng cảm ơn!

Hồ Chí Minh, ngày 14 tháng 11 năm 2025

Đại diện nhóm E

Vũ Hoàng Yến

# MỤC LỤC

[LỜI CAM ĐOAN 3](#_Toc214678803)

[LỜI CẢM ƠN 4](#_Toc214678804)

[MỤC LỤC 5](#_Toc214678805)

[BẢNG PHÂN CÔNG NHIỆM VỤ 7](#_Toc214678806)

[DANH MỤC BẢNG BIỂU 8](#_Toc214678807)

[DANH MỤC HÌNH VẼ 9](#_Toc214678808)

[DANH MỤC TỪ VIẾT TẮT 12](#_Toc214678809)

[CHƯƠNG 1 GIỚI THIỆU TỔNG QUAN 13](#_Toc214678810)

[1.1 Giới thiệu đề tài và lý do chọn đề tài 13](#_Toc214678811)

[1.2 Mục tiêu và phạm vi của đề tài 13](#_Toc214678812)

[1.3 Công cụ và thiết bị mô phỏng sử dụng (EVE-NG, Cisco IOSv, Cloud) 13](#_Toc214678813)

[CHƯƠNG 2 THU THẬP VÀ PHÂN TÍCH YÊU CẦU 14](#_Toc214678814)

[2.1 Khảo sát hiện trạng hệ thống mạng trường học 14](#_Toc214678815)

[2.2 Phân tích yêu cầu thiết kế hệ thống SD-WAN 16](#_Toc214678816)

[2.3 Đề xuất mô hình kết nối giữa các chi nhánh và trung tâm 17](#_Toc214678817)

[2.4 Xác định dịch vụ và chính sách mạng cần triển khai (VLAN, DHCP, NAT, OSPF) 17](#_Toc214678818)

[CHƯƠNG 3 THIẾT KẾ GIẢI PHÁP 18](#_Toc214678819)

[3.1 Thiết kế sơ đồ mạng ở mức logic (SD-WAN Overlay) 18](#_Toc214678820)

[3.2 Thiết kế sơ đồ mạng ở mức vật lý (Underlay) 18](#_Toc214678821)

[*3.2.1 Quy hoạch kết nối giữa các Router Edge, Server và Cloud* 18](#_Toc214678822)

[*3.2.2 Quy hoạch địa chỉ IP cho toàn hệ thống* 18](#_Toc214678823)

[*3.2.3 Quy hoạch địa chỉ IP cho toàn hệ thống* 18](#_Toc214678824)

[*3.2.4 Thuyết minh thiết bị phần cứng và mô phỏng trên EVE-NG* 22](#_Toc214678825)

[*3.2.5 Dự kiến chi phí triển khai (mô phỏng và thực tế)* 23](#_Toc214678826)

[*3.2.6 Chính sách định tuyến và kiểm soát truy cập* 23](#_Toc214678827)

[*3.2.7 Chính sách bảo mật, phân tách mạng người dùng* 23](#_Toc214678828)

[*3.2.8 Sơ đồ mạng vật lý tổng thể trên EVE-NG* 24](#_Toc214678829)

[CHƯƠNG 4 TRIỂN KHAI VÀ CẤU HÌNH 27](#_Toc214678830)

[4.1 Cấu hình mạng LAN Chi nhánh 1 27](#_Toc214678831)

[*4.1.1 Cấu hình Multilayer Switch (MLS\_CN1)* 27](#_Toc214678832)

[*4.1.2 Cấu hình các Switch Access và VLAN* 29](#_Toc214678833)

[*4.1.3 Các thiết bị cuối* 37](#_Toc214678834)

[4.2 Cấu hình mạng LAN Chi nhánh 2 38](#_Toc214678835)

[*4.2.1 Cấu hình Multilayer Switch (MLS\_CN2)* 38](#_Toc214678836)

[*4.2.2 Cấu hình các Switch Access* 40](#_Toc214678837)

[*4.2.3 Các thiết bị cuối* 44](#_Toc214678838)

[4.3 Cấu hình hệ thống kết nối WAN và SD-WAN Control Plane 45](#_Toc214678839)

[*4.3.1 Router\_CN1 (SD-WAN Edge chính)* 45](#_Toc214678840)

[*4.3.2 Router\_CN2 (Chi nhánh phụ)* 50](#_Toc214678841)

[*4.3.3 Router\_ISP* 55](#_Toc214678842)

[*4.3.4 Router\_MPLS* 57](#_Toc214678843)

[CHƯƠNG 5 KIỂM THỬ MẠNG 59](#_Toc214678844)

[5.1 Kiểm thử kết nối nội bộ tại các chi nhánh 59](#_Toc214678845)

[5.2 Kiểm thử kết nối giữa hai chi nhánh 59](#_Toc214678846)

[5.3 Kiểm thử kết nối liên chi nhánh qua MPLS và Internet 60](#_Toc214678847)

[5.4 Kiểm thử cân bằng tải và chuyển mạch khi mất kết nối WAN 60](#_Toc214678848)

[5.5 Kiểm tra NAT và truy cập Internet từ mạng LAN 61](#_Toc214678849)

[CHƯƠNG 6 BẢO TRÌ VÀ ĐÁNH GIÁ HỆ THỐNG 62](#_Toc214678850)

[6.1 Bảo trì phần cứng 62](#_Toc214678851)

[6.2 Bảo trì phần mềm và sao lưu cấu hình 62](#_Toc214678852)

[6.3 Đánh giá ưu điểm – hạn chế của mô hình SD-WAN trường học 62](#_Toc214678853)

[6.4 Đề xuất cải tiến và hướng phát triển mở rộng 63](#_Toc214678854)

[TÀI LIỆU THAM KHẢO 64](#_Toc214678855)

# BẢNG PHÂN CÔNG NHIỆM VỤ

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Nhiệm vụ | Tiến độ | Sinh viên thực hiện |
| 1 | Thiết kế logic  Báo cáo | Hoàn thành | Vũ Hoàng Yến |
| 2 | Thiết kế logic Báo cáo | Hoàn thành | Lê Thiên Trứ |
| 3 | Thiết kế logic  Power Point | Hoàn thành | Huỳnh Võ Huyền Trân |
| 4 | Thiết kế vật lý  Powerpoint | Hoàn thành | Võ Hồng Phúc |
| 5 | Thiết kế vật lý  Báo cáo | Hoàn thành | Đặng Duy Khánh |

# DANH MỤC BẢNG BIỂU

[Bảng 3. 1 Quy hoạch mạng WAN (Underlay & SD-WAN Control Plane) 23](#_Toc214066061)

[Bảng 3. 2 Chi nhánh 1 (Trụ sở chính) - Dải: 172.16.0.0/23 24](#_Toc214066062)

[Bảng 3. 3 Chi nhánh 2 (Cơ sở mới) - Dải: 172.16.2.0/24 24](#_Toc214066063)

[Bảng 3. 4 Địa chỉ IP kết nối Internet thật (Cloud NAT) 25](#_Toc214066064)

[Bảng 3. 5 Tổng hợp địa chỉ IP cấu hình Tunnel 25](#_Toc214066065)

[Bảng 3. 6 Tunnel 1 (Đường MPLS) 26](#_Toc214066066)

[Bảng 3. 7 Tunnel 2 (Đường ISP) 26](#_Toc214066067)

[Bảng 3. 8 Bảng chi phí 27](#_Toc214066068)

# DANH MỤC HÌNH VẼ

[Hình 3. 1 Sơ đồ mạng ở mức logic 16](#_Toc214668682)

[Hình 3. 2 Tầng 1\_Nhánh 1 22](#_Toc214668683)

[Hình 3. 3 Tầng 2\_Nhánh 1 23](#_Toc214668684)

[Hình 3. 4 Tầng 3\_Nhánh 1 23](#_Toc214668685)

[Hình 3. 5 Tầng 1\_Nhánh 2 24](#_Toc214668686)

[Hình 3. 6 Tầng 2\_Nhánh 2 24](#_Toc214668687)

[Hình 4. 1 Cấu hình VLAN (Layer 2) 27](#_Toc214678953)

[Hình 4. 2 Cấu hình Trunk Uplink (Router CN1) 27](#_Toc214678954)

[Hình 4. 3 Cấu hình Access Port 27](#_Toc214678955)

[Hình 4. 4 Cấu hình Access Port 28](#_Toc214678956)

[Hình 4. 5 Cấu hình Access Port 28](#_Toc214678957)

[Hình 4. 6 Cấu hình Access Port 28](#_Toc214678958)

[Hình 4. 7 STP Root Primary 28](#_Toc214678959)

[Hình 4. 8 Switch Phòng Ban Giám Hiệu 29](#_Toc214678960)

[Hình 4. 9 Switch Phòng Ban Giám Hiệu 30](#_Toc214678961)

[Hình 4. 10 Switch Phòng Quản Trị Mạng 30](#_Toc214678962)

[Hình 4. 11 Switch Phòng Hành Chính 31](#_Toc214678963)

[Hình 4. 12 Switch Thư Viện 1 32](#_Toc214678964)

[Hình 4. 13 Switch Phòng Máy Tính 1 33](#_Toc214678965)

[Hình 4. 14 Switch Phòng Máy Chủ 34](#_Toc214678966)

[Hình 4. 15 Switch Phòng Dạy Học 35](#_Toc214678967)

[Hình 4. 16 Cấu hình Server VLAN 35](#_Toc214678968)

[Hình 4. 17 Cấu hình Server VLAN 36](#_Toc214678969)

[Hình 4. 18 Cấu hình Server VLAN 37](#_Toc214678970)

[Hình 4. 19 PC phòng Ban Giám Hiệu 37](#_Toc214678971)

[Hình 4. 20 PC phòng Quản Trị Mạng 37](#_Toc214678972)

[Hình 4. 21 PC phòng Hành Chính 37](#_Toc214678973)

[Hình 4. 22 PC phòng Thư Viện 1 37](#_Toc214678974)

[Hình 4. 23 PC phòng Máy Tính 1 37](#_Toc214678975)

[Hình 4. 24 PC phòng Máy Chủ 38](#_Toc214678976)

[Hình 4. 25 PC phòng Dạy Học 1 38](#_Toc214678977)

[Hình 4. 26 Cấu Hình VLAN (Layer 2) 38](#_Toc214678978)

[Hình 4. 27 Cấu HÌnh Trunk Uplink (Router\_CN1) 38](#_Toc214678979)

[Hình 4. 28 Cấu Hình Access Port 39](#_Toc214678980)

[Hình 4. 29 STP Root Primary 39](#_Toc214678981)

[Hình 4. 30 Cấu Hình Switch Access CN2 40](#_Toc214678982)

[Hình 4. 31 Cấu Hình Switch Access CN2 41](#_Toc214678983)

[Hình 4. 32 Cấu Hình Switch Access CN2 42](#_Toc214678984)

[Hình 4. 33 Cấu Hình Switch Access CN2 43](#_Toc214678985)

[Hình 4. 34 Cấu Hình Switch Access CN2 44](#_Toc214678986)

[Hình 4. 35 PC Văn Phòng 44](#_Toc214678987)

[Hình 4. 36 PC phòng Thư Viện 2 44](#_Toc214678988)

[Hình 4. 37 PC phòng Máy Tính 2 44](#_Toc214678989)

[Hình 4. 38 PC phòng Máy Tính 3 44](#_Toc214678990)

[Hình 4. 39 PC phòng Dạy Học 2 45](#_Toc214678991)

[Hình 4. 40 Underlay Interfaces 45](#_Toc214678992)

[Hình 4. 41 Tunnel 1: MPLS (Primary Link) 46](#_Toc214678993)

[Hình 4. 42 Tunnel 2: ISP (Backup Link) 46](#_Toc214678994)

[Hình 4. 43 Routing & Failover 46](#_Toc214678995)

[Hình 4. 44 Gán Vai trò NAT trên Interfaces 46](#_Toc214678996)

[Hình 4. 45 Định nghĩa Trafic (ACLs) 47](#_Toc214678997)

[Hình 4. 46 Cấu hình Route-Map và Áp dụng (NAT-Exempt + Overload) 47](#_Toc214678998)

[Hình 4. 47 Tạo ACL phân loại traffic theo VLAN/subnet 47](#_Toc214678999)

[Hình 4. 48 IP SLA & Track (Staff failover) 47](#_Toc214679000)

[Hình 4. 49 IP SLA & Track (Staff failover) 48](#_Toc214679001)

[Hình 4. 50 Route-map PBR cho Staff + Student; Áp dụng PBR lên interface LAN 48](#_Toc214679002)

[Hình 4. 51 ACL / Security (DMVPN & IPSec) 48](#_Toc214679003)

[Hình 4. 52 Show ip policy 48](#_Toc214679004)

[Hình 4. 53 Show track 49](#_Toc214679005)

[Hình 4. 54 Show ip nhrp 49](#_Toc214679006)

[Hình 4. 55 Show dmvpn 49](#_Toc214679007)

[Hình 4. 56 Underlay Interfaces 50](#_Toc214679008)

[Hình 4. 57 DMVPN – Tunnel 50](#_Toc214679009)

[Hình 4. 58 DMVPN – Tunnel 51](#_Toc214679010)

[Hình 4. 59 Routing & Failover 51](#_Toc214679011)

[Hình 4. 60 NAT 51](#_Toc214679012)

[Hình 4. 61 NAT 51](#_Toc214679013)

[Hình 4. 62 NAT 51](#_Toc214679014)

[Hình 4. 63 NAT 51](#_Toc214679015)

[Hình 4. 64 NAT 52](#_Toc214679016)

[Hình 4. 65 ACL / SECURITY – GRE, NHRP, IPSec 52](#_Toc214679017)

[Hình 4. 66 Tạo ACL phân loại traffic theo VLAN/subnet 52](#_Toc214679018)

[Hình 4. 67 IP SLA & Track (Staff failover) 52](#_Toc214679019)

[Hình 4. 68 IP SLA & Track (Staff failover) 52](#_Toc214679020)

[Hình 4. 69 Route-map PBR cho Staff + Student 53](#_Toc214679021)

[Hình 4. 70 Áp dụng PBR lên interface LAN 53](#_Toc214679022)

[Hình 4. 71 Show ip policy 53](#_Toc214679023)

[Hình 4. 72 Show track 53](#_Toc214679024)

[Hình 4. 73 Show ip nhrp 53](#_Toc214679025)

[Hình 4. 74 Show dmvpn 54](#_Toc214679026)

[Hình 4. 75 Cấu Hình Underlay (Fa0/0 – Fa1/0 – Fa2/0) + Xóa NAT 55](#_Toc214679027)

[Hình 4. 76 Tạo DMVPN Hub (Tunnel2 – 10.10.2.254/24) 56](#_Toc214679028)

[Hình 4. 77 Định Tuyến (Routing) 56](#_Toc214679029)

[Hình 4. 78 Underlay (MPLS cloud to branches) 57](#_Toc214679030)

[Hình 4. 79 DMVPN Hub – Tunnel1 (MPLS) + NHRP (Hub) 57](#_Toc214679031)

[Hình 4. 80 DMVPN Hub – Tunnel1 (MPLS) + NHRP (Hub) 57](#_Toc214679032)

[Hình 4. 81 Routing (OSPF dưới layer MPLS) 57](#_Toc214679033)

[Hình 4. 82 Kiểm Tra 58](#_Toc214679034)

[Hình 5. 1 Kết quả ping từ VLAN STAFF đến VLAN STUDENT ở chi nhánh 1 60](#_Toc214687669)

[Hình 5. 2 Kết quả ping từ VLAN STAFF đến VLAN STUDENT ở chi nhánh 2 60](#_Toc214687670)

[Hình 5. 3 Show ip ospf neighbor ở Router\_CN1 61](#_Toc214687671)

[Hình 5. 4 Show ip ospf neighbor ở Router\_CN1 61](#_Toc214687672)

[Hình 5. 5 Show route-map PBR\_POLICY ở Router\_CN1 61](#_Toc214687673)

[Hình 5. 6 Show track 1 và Show track 2 ở Router\_CN1 62](#_Toc214687674)

# DANH MỤC TỪ VIẾT TẮT

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Thuật ngữ** | **Diễn giải** | **Ý nghĩa** |
| 1 | ACL | Access Control List | Danh sách kiểm soát truy cập |
| 2 | LAN | Local Area Network | Mạng cục bộ |
| 3 | RIP | Routing Information Protocol | Giao thức thông tin định tuyến |
| 4 | VLAN | Virtual Local Area Network | Mạng LAN ảo |
| 5 | WAN | Wide Area Network | Mạng diện rộng |
| 6 | DHCP | Dynamic Host Configuration Protocol | Giao thức Cấu hình Host Động |
| 7 | EVE-NG | Emulated Virtual Environment - Next Generation | Môi trường Ảo Hóa Thế hệ Mới |
| 8 | IPsec | Internet Protocol Security | Bộ Giao thức Bảo mật Internet |
| 9 | ISP | Internet Service Provider | Nhà Cung cấp Dịch vụ Internet |
| 10 | MLS | MultiLayer Switch | Bộ Chuyển mạch Đa lớp |
| 11 | MPLS | MultiProtocol Label Switching | Chuyển mạch Nhãn Đa giao thức |
| 12 | OSPF | Open Shortest Path First | Giao thức Định tuyến Mở Đường đi Ngắn nhất |
| 13 | PBR | Policy-Based Routing | Định tuyến Dựa trên Chính sách |
| 14 | SD-WAN | Software-Defined Wide Area Network | Mạng Diện rộng Được Xác định bằng Phần mềm |
| 15 | SVI | Switched Virtual Interface | Giao diện Chuyển mạch Ảo |

# CHƯƠNG 1 GIỚI THIỆU TỔNG QUAN

## 1.1 Giới thiệu đề tài và lý do chọn đề tài

Trong bối cảnh hệ thống giáo dục ngày càng phát triển, việc kết nối an toàn, hiệu quả và linh hoạt giữa các cơ sở (Chi nhánh) là một yêu cầu bức thiết. Mạng truyền thống (WAN) thường phức tạp, tốn kém chi phí và thiếu linh hoạt trong việc quản lý lưu lượng.

Đề tài "Thiết Kế và Mô Phỏng Mạng SD-WAN cho Trường Học" nhằm mục đích ứng dụng công nghệ SD-WAN (Software-Defined Wide Area Network) để xây dựng một giải pháp mạng tiên tiến, giúp tự động hóa việc chọn đường truyền, tăng cường bảo mật và tối ưu hóa trải nghiệm người dùng (ví dụ: ưu tiên lưu lượng học tập) cho một mô hình trường học có nhiều chi nhánh.

## 1.2 Mục tiêu và phạm vi của đề tài

- Thiết kế & Triển khai WAN: Xây dựng mô hình mạng SD-WAN (giả lập theo kiểu Cisco Viptela) kết nối 2 chi nhánh (CN1 - Main Campus và CN2 - Branch Campus) trên nền tảng ảo hóa EVE-NG.

- Tích hợp Mạng LAN: Thiết lập đầy đủ môi trường mạng nội bộ (LAN) tại mỗi chi nhánh, bao gồm: VLAN, Định tuyến liên VLAN (SVI), DHCP cho các thiết bị cuối.

- Triển khai Underlay & Overlay: Cấu hình OSPF (Underlay Network) để đảm bảo kết nối vật lý. Xây dựng 2 đường hầm IPsec VPN (Overlay Network) qua 2 đường WAN độc lập (MPLS và ISP/Internet) để tạo kênh bảo mật giữa CN1 và CN2.

- Áp dụng Chính sách: Cấu hình Policy-Based Routing (PBR) để minh họa tính năng thông minh của SD-WAN, phân luồng lưu lượng: Staff (VLAN 20) ưu tiên đường MPLS và Student (VLAN 30) sử dụng đường ISP.

- Kiểm thử: Xác minh hoạt động của các dịch vụ LAN (DHCP, DNS), kết nối giữa các VLAN, và tính năng SD-WAN (chọn đường và dự phòng (failover)).

## 1.3 Công cụ và thiết bị mô phỏng sử dụng (EVE-NG, Cisco IOSv, Cloud)

- EVE-NG: Nền tảng mô phỏng toàn bộ hệ thống mạng (Cung cấp môi trường để chạy và kết nối các máy ảo thiết bị mạng (Router, Switch) một cách chân thực, mô phỏng cả mạng LAN/WAN vật lý và mạng Overlay SD-WAN).

- Cisco IOSv (IOS Virtual): Thiết bị Định tuyến (Router Edge) và Router WAN (MPLS/ISP) (Được sử dụng cho các Router như Router\_CN1, Router\_CN2, Router\_ISP, Router\_MPLS. Hỗ trợ đầy đủ các lệnh cấu hình phức tạp của SD-WAN như OSPF, IPsec VPN Tunnel và Policy-Based Routing (PBR)).

- Cisco IOSvL2 (IOS Virtual Layer 2): Switch L3 Core (MLS\_CN1, MLS\_CN2) và Switch Access (Thực hiện các chức năng mạng Layer 2 (VLAN, Trunk) và Layer 3 (Inter-VLAN Routing/SVI, DHCP Relay) tại các chi nhánh).

- VPCS: Thiết bị đầu cuối (PC, Server) (Mô phỏng các máy tính trong các VLAN khác nhau (Staff, Student) để kiểm tra kết nối, nhận IP (DHCP) và thử nghiệm các chính sách phân luồng (PBR)).

- Cloud (Cloud0 - NAT): Cổng kết nối Internet (Cho phép các Router mô phỏng kết nối ra môi trường Internet thực tế hoặc giả lập (ví dụ: cấp DHCP/NAT cho Router\_ISP)).

# CHƯƠNG 2 THU THẬP VÀ PHÂN TÍCH YÊU CẦU

## 2.1 Khảo sát hiện trạng hệ thống mạng trường học

Thiết kế hệ thống mạng cho một trường học đáp ứng các nhu cầu như trao đổi, quản lý, lưu trữ thông tin để phục vụ cho trường học. Trường bao gồm hai chi nhánh có khoảng cách địa lý với nhau, trong đó chi nhánh 1 là cơ sở chính, chi nhánh 2 là cơ sở phụ của trường học.

Mô tả cơ bản về cấu trúc và kết nối trường học:

* Kiến trúc: Hệ thống sử dụng kiến trúc mạng phân lớp, với các Switch Access (L2) tại mỗi phòng, Switch L3 Core (MLS) tại mỗi chi nhánh, và kết nối WAN thông qua Router Edge.
* Dịch vụ Trung tâm: Phòng Máy Chủ và Server cung cấp các dịch vụ mạng tập trung (DHCP/DNS) được đặt tại Chi nhánh 1.
* Kết nối WAN: Cả hai chi nhánh được kết nối qua hai đường truyền WAN độc lập (MPLS và ISP) để triển khai SD-WAN Logic.
* Chi nhánh 1 (Cơ sở chính): gồm 3 tầng
* Tầng 1:
* Phòng Ban Giám Hiệu: là nơi quản lý và điều hành các hoạt động về giáo dục.
* Phòng Quản Trị Mạng: là nơi làm việc liên quan đến toàn bộ hệ thống mạng.
* Phòng Hành Chính: là nơi xử lý các công việc liên quan về hành chính.
* Tầng 2:
* Phòng Thư Viện 1: là nơi nghiên cứu và tra cứu tài liệu dành cho học sinh và giáo viên.
* Phòng Máy Tính 1: là nơi học sinh học thực hành bộ môn liên quan đến máy tính.
* Phòng Máy Chủ: là nơi có máy chủ cung cấp các dịch vụ mạng phục vụ cho toàn trường.
* Tầng 3:
* Phòng Dạy Học 1: là nơi học tập và giảng dạy trực tiếp của giáo viên và học sinh.
* Chi nhánh 2 (Cơ sở phụ): gồm 2 tầng
* Tầng 1:
* Văn Phòng: nơi làm việc của ban lãnh đạo và nhân viên hành chính.
* Phòng Thư Viện 2: là nơi nghiên cứu và tra cứu tài liệu dành cho học sinh và giáo viên.
* Phòng Máy Tính 2: là nơi học sinh học thực hành bộ môn liên quan đến máy tính.
* Phòng Máy Tính 3: là nơi học sinh học thực hành bộ môn liên quan đến máy tính.
* Tầng 2:
* Phòng Dạy Học 2: là nơi học tập và giảng dạy trực tiếp của giáo viên và học sinh.

Mô tả về yêu cầu thiết kế mạng từng phòng trong trường học:

* Chi nhánh 1 (Cơ sở chính):
* Tầng 1:
* Phòng Ban Giám Hiệu: 5 host.
* Phòng Quản Trị Mạng: 5 host.
* Phòng Hành Chính: 5 host.
* Tầng 2:
* Phòng Thư Viện 1: 10 host.
* Phòng Máy Tính 1: 50 host.
* Phòng Máy Chủ: 5 host.
* Tầng 3:
* Phòng Dạy Học 1: 20 host.
* Chi nhánh 2 (Cơ sở phụ): gồm 2 tầng
* Tầng 1:
* Văn Phòng:
* Phòng Thư Viện 2: 5 host.
* Phòng Máy Tính 2: 30 host.
* Phòng Máy Tính 3: 30 host.
* Tầng 2:
* Phòng Dạy Học 2: 20 host.

Yêu cầu công việc:

* Bảo mật & ổn định: Mạng CN1 phải có tính bảo mật cao, ổn định. Mạng CN2 sử dụng ổn định.
* Khả năng giao tiếp: Giao tiếp nội bộ (Inter-VLAN) và giao tiếp giữa 2 cơ sở (Site-to-Site) phải diễn ra thuận lợi. Có thể giao tiếp trao đổi thông tin giữa 2 cơ sở với nhau.
* Kiểm soát và mở rộng: Kiểm soát được lượng truy cập (ACL) và đảm bảo hệ thống mạng có thể được mở rộng trong tương lai (dự phòng khoảng 5 năm). Kiểm soát được lượng truy cập trong hệ thống mạng.

## 2.2 Phân tích yêu cầu thiết kế hệ thống SD-WAN

Sau khi khảo sát và thu thập các yêu cầu cần thiết về thiết kế mạng cho trường học, có thể đưa ra được những phân tích chi tiết như sau:

- Để việc giao tiếp nội bộ của từng cơ sở được diễn ra thì cần phải cấu hình các Switch trong các phòng sau đó gán VLAN cho từng phòng ban. Các VLAN giống nhau có thể giao tiếp được với nhau. Nếu khác VLAN thì phải thực hiện định tuyến liên VLAN.

- Việc trao đổi được thông tin giữa 2 cơ sở với nhau cần phải cấu hình giao thức định tuyến RIP trên 2 Router ở 2 cơ sở để việc giao tiếp có thể diễn ra thuận lợi mà không bị gián đoạn.

- Có thể cấu hình ACL ở Multilayer Switch để kiểm soát được lưu lượng truy cập trong hệ thống mạng.

## 2.3 Đề xuất mô hình kết nối giữa các chi nhánh và trung tâm

Mô hình được đề xuất là kiến trúc SD-WAN Overlay sử dụng DMVPN Dual-Hub (hay Dual-Overlay) trên nền EVE-NG. Theo đó, Router Edge (CN1 và CN2) kết nối trực tiếp đến hai nhà cung cấp dịch vụ giả lập (MPLS và ISP), đồng thời Router\_MPLS và Router\_ISP đóng vai trò là hai Router HUB riêng biệt cho từng lớp phủ (Overlay) tương ứng.

## 2.4 Xác định dịch vụ và chính sách mạng cần triển khai (VLAN, DHCP, NAT, OSPF)

- VLAN: 9 VLAN (CN1) và 5 VLAN (CN2) được sử dụng để phân vùng mạng dựa trên chức năng (ADMIN, STAFF, STUDENT, SERVER).

- DHCP: Cấu hình DHCP Relay (ip helper-address) trên các SVI của MLS để tất cả các VLAN đều nhận IP từ Server tập trung ở CN1.

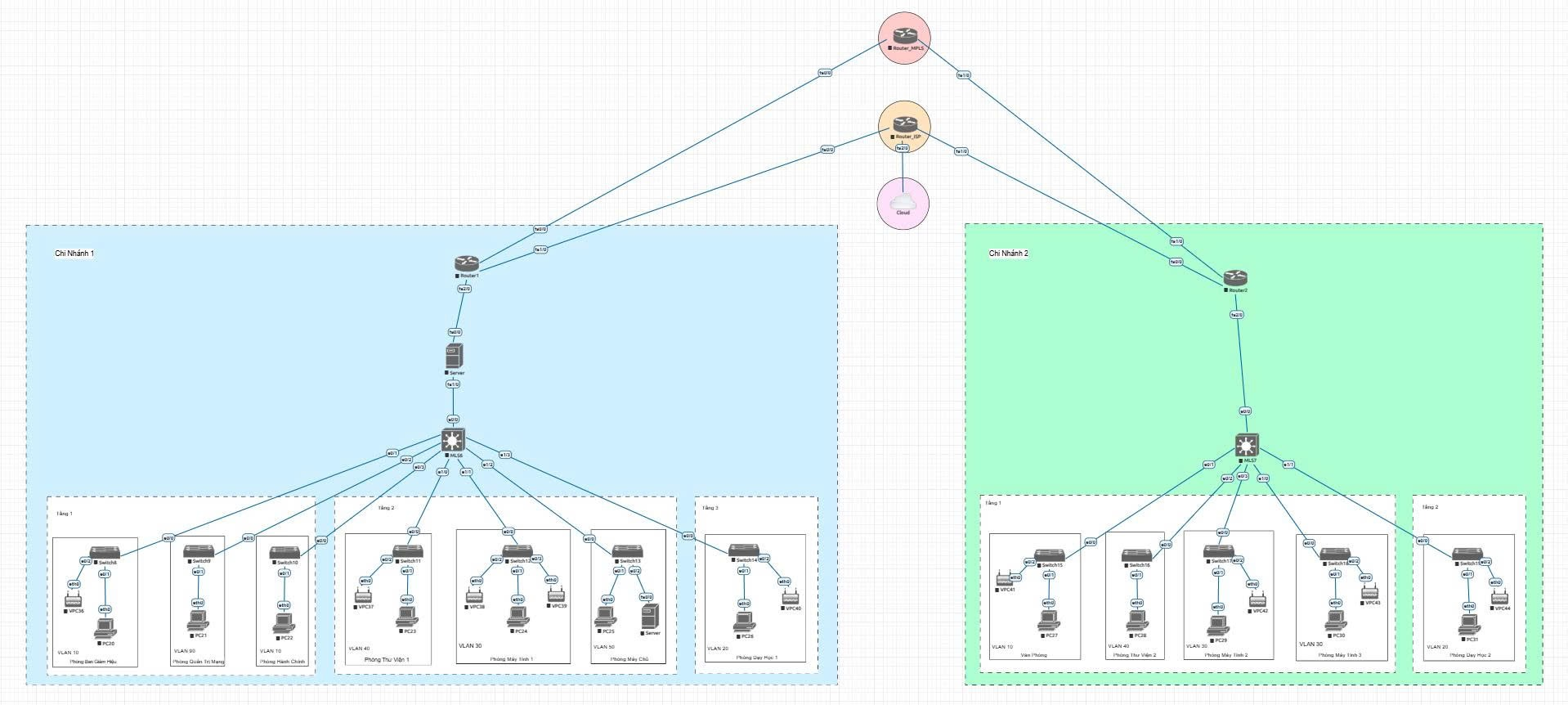
- OSPF (Underlay): Bắt buộc chạy OSPF Area 0 giữa các Router WAN/Edge để tự động học tuyến đường WAN.

- NAT: Cấu hình PAT (NAT Overload) trên Router Edge CN1/CN2 ra cổng WAN ISP.

# CHƯƠNG 3 THIẾT KẾ GIẢI PHÁP

## 3.1 Thiết kế sơ đồ mạng ở mức logic (SD-WAN Overlay)

Để mô phỏng được một thiết kế mạng WAN cho trường học thì phần mềm EVE-NG là một lựa chọn phù hợp.



**Hình 3. 1 Sơ đồ mạng ở mức logic**

## 3.2 Thiết kế sơ đồ mạng ở mức vật lý (Underlay)

### *3.2.1 Quy hoạch kết nối giữa các Router Edge, Server và Cloud*

Kết nối Layer 3 giữa MLS và Router Edge (Downlink) sử dụng dải IP WAN nhỏ (ví dụ: 172.16.255.20/30). Các Router Edge kết nối trực tiếp đến các Router WAN (MPLS và ISP) sử dụng các subnet /30 khác nhau trong dải 172.16.255.0/24.

### *3.2.2 Quy hoạch địa chỉ IP cho toàn hệ thống*

Quy hoạch sử dụng dải 172.16.0.0/22 cho LAN và 172.16.255.0/24 cho WAN, đảm bảo hơn 1000 địa chỉ khả dụng, đáp ứng yêu cầu mở rộng trong 5 năm.

### *3.2.3 Quy hoạch địa chỉ IP cho toàn hệ thống*

Trong mô hình thiết kế mạng cho trường học, địa chỉ IP cho toàn hệ thống được quy hoạch như sau:

* Mạng WAN/Control sử dụng dải 172.16.255.0/24 và các subnet /30 để kết nối các Router Edge (R0/R1), ISP, MPLS và Server Controller.

**Bảng 3. 1 Quy hoạch mạng WAN (Underlay & SD-WAN Control Plane)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Thiết bị** | **Interface** | **Vai trò** | **Subnet** | **Địa chỉ IP (Cụ thể)** |
| Router\_CN1 | Fa0/0 nối Router\_MPLS | WAN 1 (MPLS) | 172.16.255.4/30 | 172.16.255.5 |
| Router\_MPLS | Fa0/0 nối Router\_CN1 | WAN 1 (MPLS) | 172.16.255.4/30 | 172.16.255.6 |
| Router\_CN1 | Fa1/0 nối Router\_ISP | WAN 2 (Internet) | 172.16.255.8/30 | 172.16.255.9 |
| Router\_ISP | Fa0/0 nối Router\_CN1 | WAN 2 (Internet) | 172.16.255.8/30 | 172.16.255.10 |
| Router\_ISP | Fa1/0 nối Router\_CN2 | WAN 2 (Internet) | 172.16.255.12/30 | 172.16.255.13 |
| Router\_CN2 | Fa0/0 nối với Router\_ISP | WAN 2 (Internet) | 172.16.255.12/30 | 172.16.255.14 |
| Router\_CN2 | Fa1/0 nối với Router\_MPLS | WAN 1 (MPLS) | 172.16.255.16/30 | 172.16.255.17 |
| Router\_MPLS | Fa0/1 nối với Router\_CN2 | WAN 1 (MPLS) | 172.16.255.16/30 | 172.16.255.18 |
| Router\_CN1 | Fa2/0 nối với Server | Controller Link | 172.16.255.0/30 | 172.16.255.1 |

* Quy hoạch mạng LAN nội bộ (Inter-VLAN Routing): Mạng LAN sử dụng dải địa chỉ 172.16.0.0/22 cho toàn trường.

**Bảng 3. 2 Chi nhánh 1 (Trụ sở chính) - Dải: 172.16.0.0/23**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VLAN ID** | **Tên VLAN** | **Dải Địa chỉ IP** | **Subnet Mask** | **Default Gateway (Router Tầng/SVI)** |
| 20 | STAFF | 172.16.0.0/25 | 255.255.255.128 | 172.16.0.1 |
| 30 | STUDENT | 172.16.0.128/25 | 255.255.255.128 | 172.16.0.129 |
| 70 | GUEST | 172.16.1.0/26 | 255.255.255.192 | 172.16.1.1 |
| 60 | WIRELESS\_IOT | 172.16.1.64/27 | 255.255.255.224 | 172.16.1.65 |
| 40 | LIBRARY | 172.16.1.96/28 | 255.255.255.240 | 172.16.1.97 |
| 10 | ADMIN | 172.16.1.128/27 | 255.255.255.224 | 172.16.1.129 |
| 50 | SERVERS | 172.16.1.160/28 | 255.255.255.240 | 172.16.1.161 |
| 80 | PRINTERS | 172.16.1.176/28 | 255.255.255.240 | 172.16.1.177 |
| 90 | MANAGEMENT | 172.16.1.192/28 | 255.255.255.240 | 172.16.1.193 |

**Bảng 3. 3 Chi nhánh 2 (Cơ sở mới) - Dải: 172.16.2.0/24**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VLAN ID** | **Tên VLAN** | **Dải Địa chỉ IP** | **Subnet Mask** | **Default Gateway (Router Tầng/SVI)** |
| 30 | STUDENT | 172.16.2.0/25 | 255.255.255.128 | 172.16.2.1 |
| 20 | STAFF | 172.16.2.128/26 | 255.255.255.192 | 172.16.2.129 |
| 10 | ADMIN | 172.16.2.192/28 | 255.255.255.240 | 172.16.2.193 |
| 40 | LIBRARY | 172.16.2.208/28 | 255.255.255.240 | 172.16.2.209 |
| 60 | WIRELESS\_IOT | 172.16.2.224/27 | 255.255.255.224 | 172.16.2.225 |

* Địa chỉ IP kết nối Internet thật (Cloud NAT): Để kết nối Router\_ISP ra Internet thật, cần thêm Cloud (NAT) với dải IP giả định sau:

**Bảng 3. 4 Địa chỉ IP kết nối Internet thật (Cloud NAT)**

|  |  |  |  |
| --- | --- | --- | --- |
| Thiết bị | Interface | Địa chỉ IP | Next Hop |
| Router\_ISP | Fa2/0 | 192.168.255.254 | Nối với Cloud NAT |
| Cloud (NAT) | N/A | 192.168.255.1 | Gateway ra Internet thật |

* Tổng hợp địa chỉ IP cấu hình Tunnel: Có 4 địa chỉ IP chính được sử dụng để làm IP ảo (Overlay) cho hai đường hầm VPN giữa CN1 và CN2.

**Bảng 3. 5 Tổng hợp địa chỉ IP cấu hình Tunnel**

|  |  |  |  |
| --- | --- | --- | --- |
| **Địa chỉ IP** | **Router** | **Giao diện Tunnel** | **Vai trò (Overlay Network)** |
| 10.10.1.1 | Router\_CN1 | Tunnel 1 (MPLS) | IP nguồn cho lưu lượng qua đường MPLS. |
| 10.10.1.2 | Router\_CN2 | Tunnel 1 (MPLS) | IP đích/phản hồi cho lưu lượng qua đường MPLS. |
| 10.10.2.1 | Router\_CN1 | Tunnel 2 (ISP) | IP nguồn cho lưu lượng qua đường ISP. |
| 10.10.2.2 | Router\_CN2 | Tunnel 2 (ISP) | IP đích/phản hồi cho lưu lượng qua đường ISP. |

* Mỗi Tunnel sử dụng một cặp IP Overlay (IP ảo để định tuyến giữa 10.10.x.x) và một cặp IP Underlay (IP WAN thực tế).
  + Tunnel 1 (Đường MPLS): Đường hầm này sử dụng liên kết MPLS (đường ưu tiên) làm đường vật lý.

**Bảng 3. 6 Tunnel 1 (Đường MPLS)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Vai trò IP** | **Giá trị IP** | **Router Sở hữu** | **Giao diện Vật lý Liên quan** |
| Overlay IP | 10.10.1.1 | Router\_CN1 | interface tunnel 1 |
| Overlay IP | 10.10.1.2 | Router\_CN2 | interface tunnel 1 |
| Underlay Source | Router\_CN1: 172.16.255.5 (Fa0/0) | Router\_CN1 | tunnel source fa0/0 |
| Underlay Destination | Router\_CN2: 172.16.255.17 | Router\_CN1 | tunnel destination 172.16.255.17 |

* + Tunnel 2 (Đường ISP): Đường hầm này sử dụng liên kết ISP (đường thông thường) làm đường vật lý.

**Bảng 3. 7 Tunnel 2 (Đường ISP)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Vai trò IP** | **Giá trị IP** | **Router Sở hữu** | **Giao diện Vật lý Liên quan** |
| Overlay IP | 10.10.2.1 | Router\_CN1 | interface tunnel 2 |
| Overlay IP | 10.10.2.2 | Router\_CN2 | interface tunnel 2 |
| Underlay Source | Router\_CN1: 172.16.255.9 (Fa1/0) | Router\_CN1 | tunnel source fa1/0 |
| Underlay Destination | Router\_CN2: 172.16.255.14 | Router\_CN1 | tunnel destination 172.16.255.14 |

### *3.2.4 Thuyết minh thiết bị phần cứng và mô phỏng trên EVE-NG*

Các thiết bị Cisco IOSv được sử dụng để mô phỏng Router Edge/WAN, cung cấp môi trường lý tưởng để thực hiện các giao thức định tuyến và bảo mật phức tạp. Các MLS chạy IOSvL2 để thực hiện chức năng Inter-VLAN Routing hiệu suất cao tại Layer 3.

### *3.2.5 Dự kiến chi phí triển khai (mô phỏng và thực tế)*

Sau khi tham khảo tại các website [1] [2] bán thiết bị thì các thiết bị cần dùng cho mô hình thiết kế mạng cho trường học có chi phí như sau:

**Bảng 3. 8 Bảng chi phí**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Thiết bị** | **Model** | **Số lượng** | **Đơn giá (VNĐ)** | **Thành tiền (VNĐ)** |
| Router | CISCO2901/K9 | 2 | 18,000,000 | 36,000,000 |
| Multilayer Switch | WS-C3560V2-48TS-S | 2 | 9,200,000 | 18,400,000 |
| Switch L2 | WS-C2960+24TC-S | 12 | 6,700,000 | 80,400,000 |
| Access Point | AIR-CAP1702I-H-K9 | 9 | 6,200,000 | 55,800,000 |
| Máy in | Canon LBP 6030 | 2 | 2,500,000 | 5,000,000 |
| PC | PCAP Office | 200 | 4,000,000 | 800,000,000 |
| **Tổng cộng** |  |  |  | **995,600,000** |

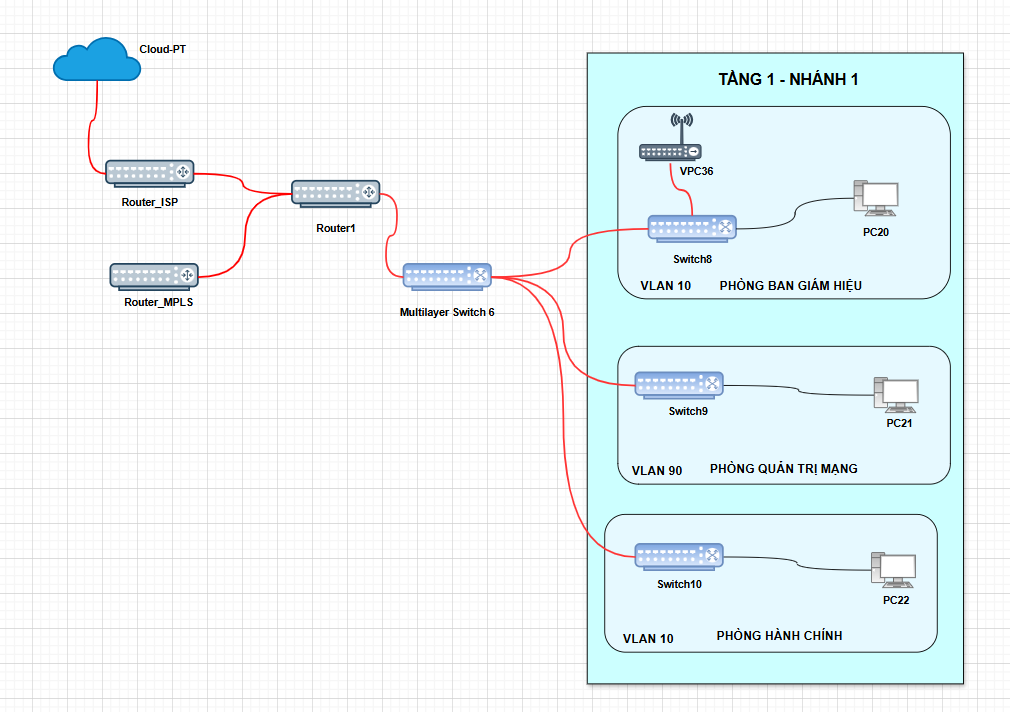
### *3.2.6 Chính sách định tuyến và kiểm soát truy cập*

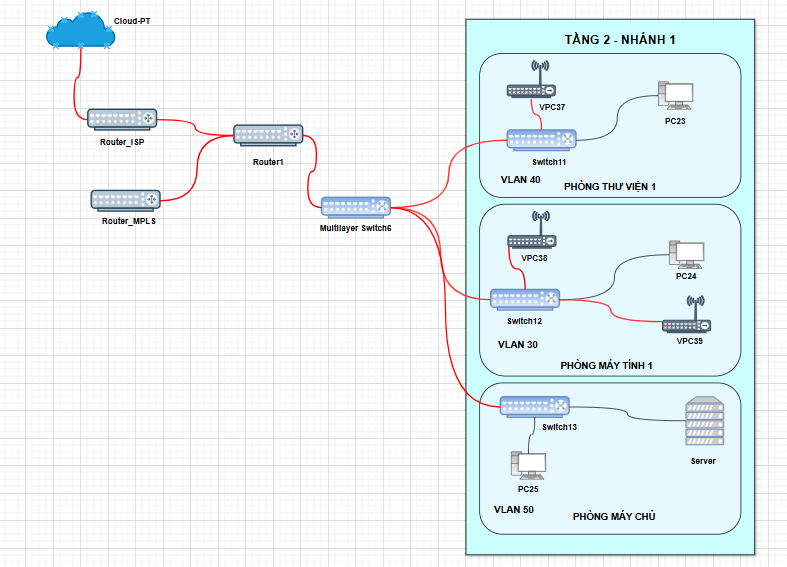
* Chính sách định tuyến:
* Underlay: OSPF duy trì bảng định tuyến WAN. nhau vẫn có thể giao tiếp được với nhau.
* SD-WAN Logic: PBR được sử dụng để phân luồng lưu lượng VLAN 20 (Staff) bắt buộc qua đường MPLS (Tunnel 1) và VLAN 30 (Student) bắt buộc qua đường ISP (Tunnel 2).
* Kiểm soát truy cập:
* Cấu hình ACL trên các Multilayer Switch giúp kiểm soát được lượng truy cập giữa các VLAN trong nội bộ của chi nhánh. Việc cấu hình này nhằm mục đích ngăn chặn các truy cập không được cho phép.

### *3.2.7 Chính sách bảo mật, phân tách mạng người dùng*

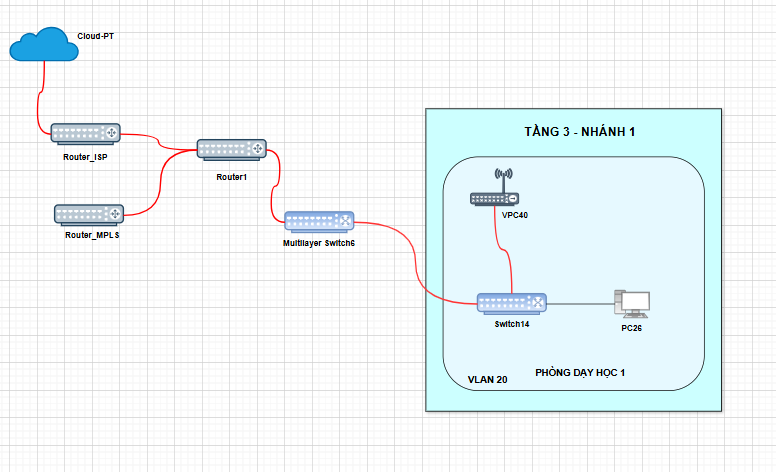
* Phân tách: Sử dụng 9 VLAN để phân chia ranh giới quản trị.
* Bảo mật: Triển khai ACL mở rộng trên MLS\_CN1 để kiểm soát chi tiết lưu lượng giữa các VLAN (ví dụ: chặn truy cập của VLAN STUDENT tới VLAN ADMIN/MANAGEMENT/PRINTER).

### *3.2.8 Sơ đồ mạng vật lý tổng thể trên EVE-NG*

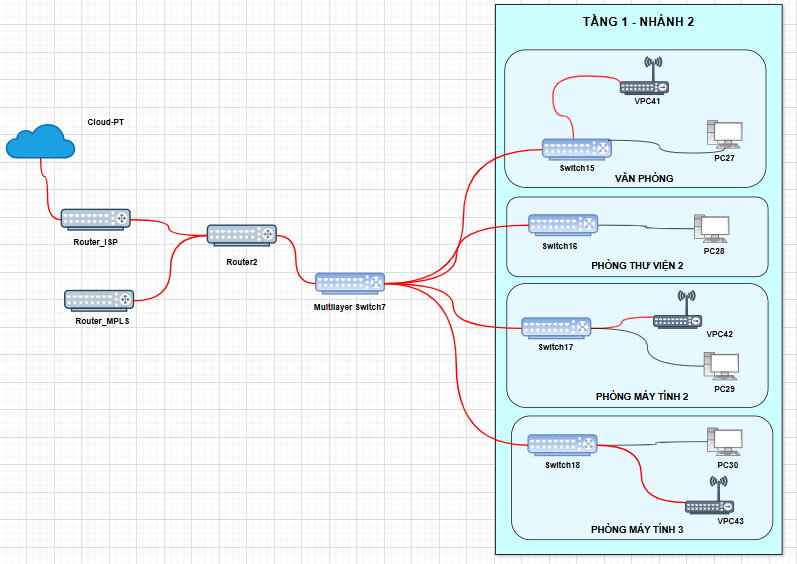
**Hình 3. 2 Tầng 1\_Nhánh 1**



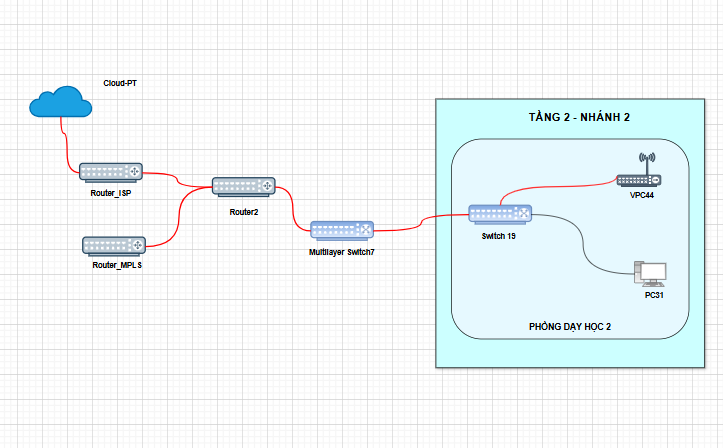
**Hình 3. 3 Tầng 2\_Nhánh 1**



**Hình 3. 4 Tầng 3\_Nhánh 1**



**Hình 3. 5 Tầng 1\_Nhánh 2**



**Hình 3. 6 Tầng 2\_Nhánh 2**

# CHƯƠNG 4 TRIỂN KHAI VÀ CẤU HÌNH

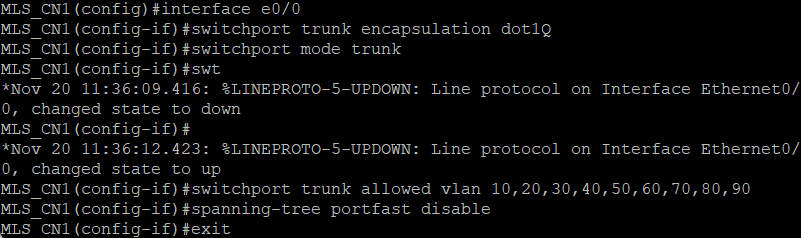
## 4.1 Cấu hình mạng LAN Chi nhánh 1

### *4.1.1 Cấu hình Multilayer Switch (MLS\_CN1)*

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, thiết kế

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 1 Cấu hình VLAN (Layer 2)**



**Hình 4. 2 Cấu hình Trunk Uplink (Router CN1)**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 3 Cấu hình Access Port**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 4 Cấu hình Access Port**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 5 Cấu hình Access Port**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 6 Cấu hình Access Port**



**Hình 4. 7 STP Root Primary**

### *4.1.2 Cấu hình các Switch Access và VLAN*

Ảnh có chứa văn bản, ảnh chụp màn hình

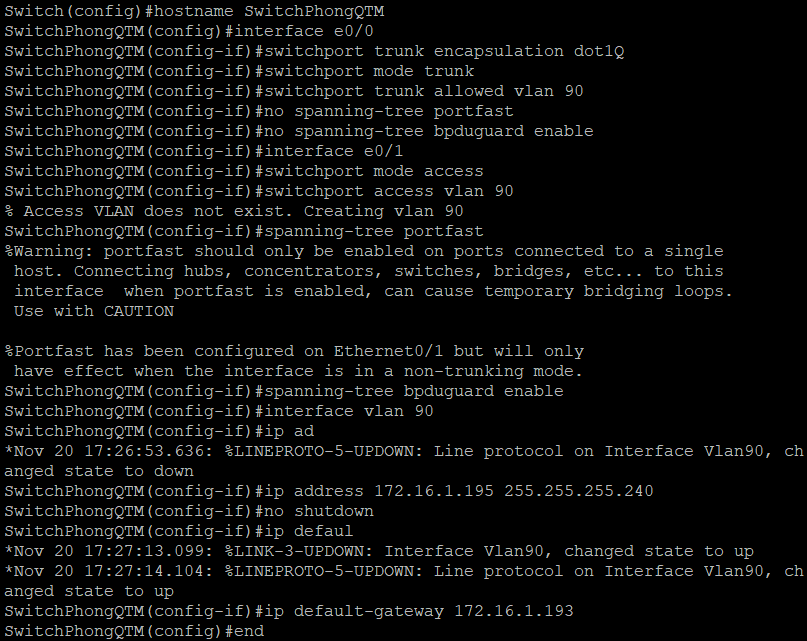
Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 8 Switch Phòng Ban Giám Hiệu**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 9 Switch Phòng Ban Giám Hiệu**



**Hình 4. 10 Switch Phòng Quản Trị Mạng**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 11 Switch Phòng Hành Chính**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 12 Switch Thư Viện 1**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 13 Switch Phòng Máy Tính 1**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 14 Switch Phòng Máy Chủ**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 15 Switch Phòng Dạy Học**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 16 Cấu hình Server VLAN**

Ảnh có chứa văn bản, ảnh chụp màn hình

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 17 Cấu hình Server VLAN**

Ảnh có chứa ảnh chụp màn hình, văn bản, mẫu

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 18 Cấu hình Server VLAN**

### *4.1.3 Các thiết bị cuối*



**Hình 4. 19 PC phòng Ban Giám Hiệu**

****

**Hình 4. 20 PC phòng Quản Trị Mạng**

****

**Hình 4. 21 PC phòng Hành Chính**

****

**Hình 4. 22 PC phòng Thư Viện 1**

****

**Hình 4. 23 PC phòng Máy Tính 1**

****

**Hình 4. 24 PC phòng Máy Chủ**

****

**Hình 4. 25 PC phòng Dạy Học 1**

## 4.2 Cấu hình mạng LAN Chi nhánh 2

### *4.2.1 Cấu hình Multilayer Switch (MLS\_CN2)*

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 26 Cấu Hình VLAN (Layer 2)**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 27 Cấu HÌnh Trunk Uplink (Router\_CN1)**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 28 Cấu Hình Access Port**



**Hình 4. 29 STP Root Primary**

### *4.2.2 Cấu hình các Switch Access*

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 30 Cấu Hình Switch Access CN2**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 31 Cấu Hình Switch Access CN2**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

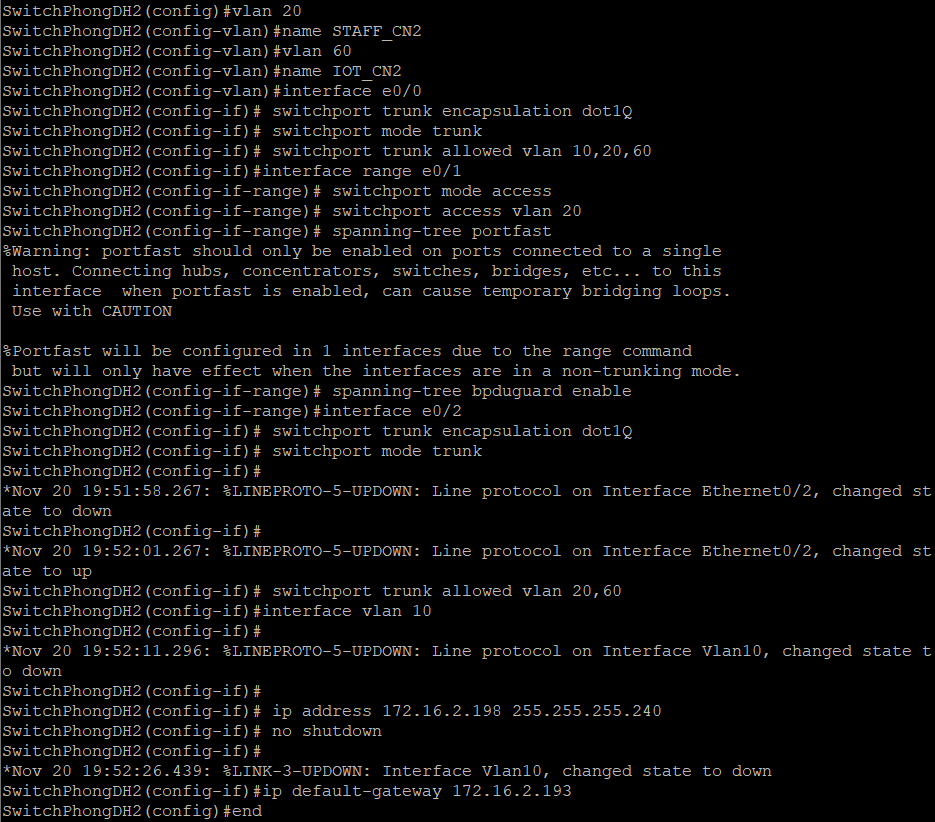
Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 32 Cấu Hình Switch Access CN2**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 33 Cấu Hình Switch Access CN2**



**Hình 4. 34 Cấu Hình Switch Access CN2**

### *4.2.3 Các thiết bị cuối*

****

**Hình 4. 35 PC Văn Phòng**

****

**Hình 4. 36 PC phòng Thư Viện 2**

****

**Hình 4. 37 PC phòng Máy Tính 2**

****

**Hình 4. 38 PC phòng Máy Tính 3**

****

**Hình 4. 39 PC phòng Dạy Học 2**

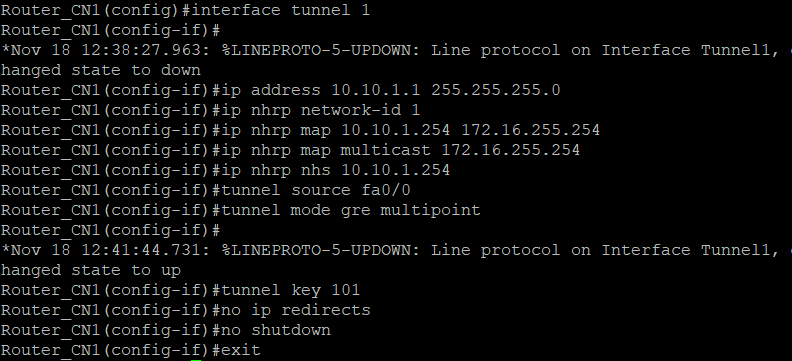
## 4.3 Cấu hình hệ thống kết nối WAN và SD-WAN Control Plane

### *4.3.1 Router\_CN1 (SD-WAN Edge chính)*

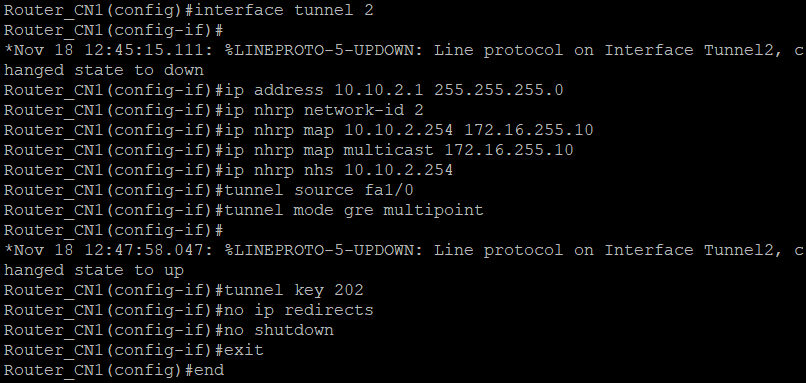
Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 40 Underlay Interfaces**

****

**Hình 4. 41 Tunnel 1: MPLS (Primary Link)**

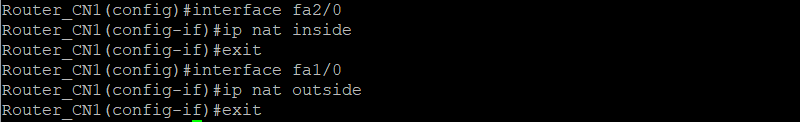


**Hình 4. 42 Tunnel 2: ISP (Backup Link)**

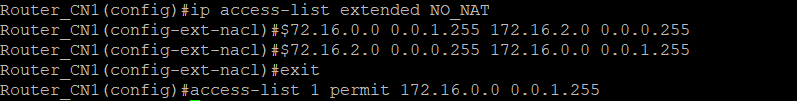
Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

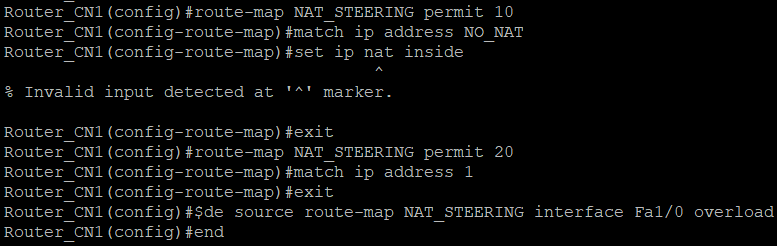
**Hình 4. 43 Routing & Failover**



**Hình 4. 44 Gán Vai trò NAT trên Interfaces**



**Hình 4. 45 Định nghĩa Trafic (ACLs)**

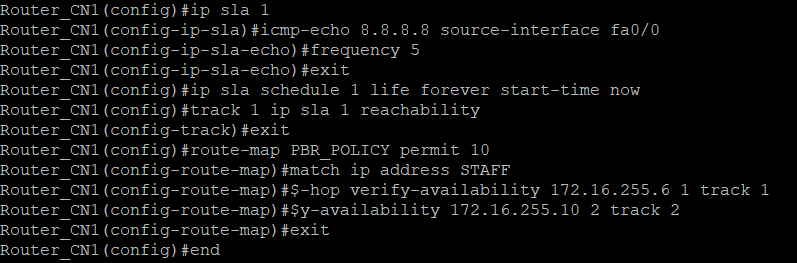


**Hình 4. 46 Cấu hình Route-Map và Áp dụng (NAT-Exempt + Overload)**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 47 Tạo ACL phân loại traffic theo VLAN/subnet**



**Hình 4. 48 IP SLA & Track (Staff failover)**

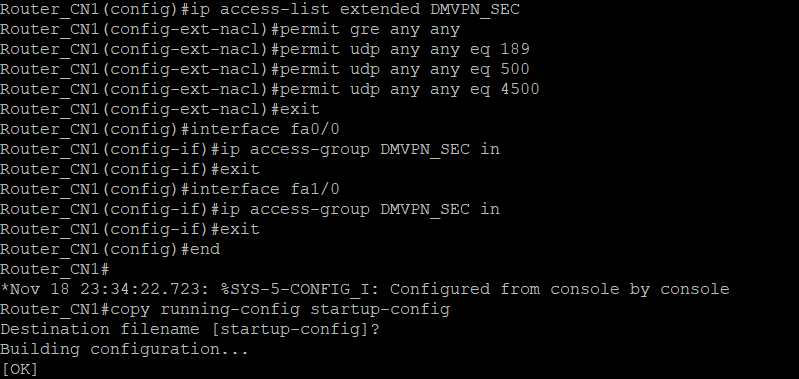
Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 49 IP SLA & Track (Staff failover)**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.**Hình 4. 50 Route-map PBR cho Staff + Student; Áp dụng PBR lên interface LAN**

**Hình 4. 51 ACL / Security (DMVPN & IPSec)**



**Hình 4. 52 Show ip policy**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 53 Show track**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 54 Show ip nhrp**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.**Hình 4. 55 Show dmvpn**

### *4.3.2 Router\_CN2 (Chi nhánh phụ)*

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 56 Underlay Interfaces**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 57 DMVPN – Tunnel**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 58 DMVPN – Tunnel**

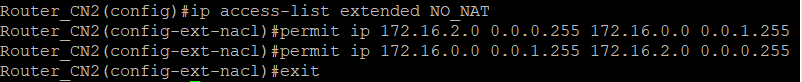


**Hình 4. 59 Routing & Failover**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, màu đen

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 60 NAT**



**Hình 4. 61 NAT**



**Hình 4. 62 NAT**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 63 NAT**



**Hình 4. 64 NAT**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, màu đen

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 65 ACL / SECURITY – GRE, NHRP, IPSec**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 66 Tạo ACL phân loại traffic theo VLAN/subnet**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 67 IP SLA & Track (Staff failover)**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 68 IP SLA & Track (Staff failover)**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 69 Route-map PBR cho Staff + Student**



**Hình 4. 70 Áp dụng PBR lên interface LAN**



**Hình 4. 71 Show ip policy**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 72 Show track**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 73 Show ip nhrp**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 74 Show dmvpn**

### *4.3.3 Router\_ISP*

Ảnh có chứa văn bản, ảnh chụp màn hình

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 75 Cấu Hình Underlay (Fa0/0 – Fa1/0 – Fa2/0) + Xóa NAT**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 76 Tạo DMVPN Hub (Tunnel2 – 10.10.2.254/24)**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 77 Định Tuyến (Routing)**

### *4.3.4 Router\_MPLS*

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.**Hình 4. 78 Underlay (MPLS cloud to branches)**

**Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.**

**Hình 4. 79 DMVPN Hub – Tunnel1 (MPLS) + NHRP (Hub)**



**Hình 4. 80 DMVPN Hub – Tunnel1 (MPLS) + NHRP (Hub)**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 81 Routing (OSPF dưới layer MPLS)**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 4. 82 Kiểm Tra**

# CHƯƠNG 5 KIỂM THỬ MẠNG

## 5.1 Kiểm thử kết nối nội bộ tại các chi nhánh

*5.1.1 Ping giữa các VLAN trong cùng chi nhánh*

Cả hai chi nhánh đều được thiết lập mạng cục bộ (LAN) ổn định và đồng nhất. Việc sử dụng các thiết bị MLS tại mỗi chi nhánh để thực hiện Inter-VLAN Routing thông qua các giao diện chuyển mạch ảo (SVI).

Các thiết bị MLS này đồng thời đóng vai trò là Gateway nội bộ cho các VLAN. Cấu hình DHCP đã hoạt động chính xác để cấp phát địa chỉ IP tự động cho các máy trạm.

Kết quả kiểm thử cho thấy, tại cả hai chi nhánh, việc ping giữa các máy trạm thuộc VLAN STAFF (172.16.0.0/25 và 172.16.2.0/24) và VLAN STUDENT (172.16.0.128/25 và 172.16.2.128/25) trong cùng một mạng LAN đều kết nối thành công.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 5. 1 Kết quả ping từ VLAN STAFF đến VLAN STUDENT ở chi nhánh 1**

**Ảnh có chứa ảnh chụp màn hình, văn bản, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.**

**Hình 5. 2 Kết quả ping từ VLAN STAFF đến VLAN STUDENT ở chi nhánh 2**

## 5.2 Kiểm thử kết nối giữa hai chi nhánh

Mục tiêu của kiểm thử này là xác minh khả năng thiết lập lớp phủ VPN (Overlay) và trao đổi thông tin định tuyến giữa chi nhánh 1 và chi nhánh 2 thông qua giao thức OSPF trên Tunnel DMVPN.

Kết quả kiểm thử cho thấy quá trình thiết lập lớp định tuyến đã đạt được thành công trên Router\_CN1: lệnh show ip ospf neighbor trên Router\_CN1 xác nhận đã thiết lập trạng thái FULL với Router Hub. Tuy nhiên, do lỗi kỹ thuật DMVPN Adjacency trên Router\_CN2, do Router\_CN2 không thấy Neighbor Hub nên Tunnel VPN không thể hoàn tất được dẫn đến việc ping liên chi nhánh thất bại.

**Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.**

**Hình 5. 3 Show ip ospf neighbor ở Router\_CN1**

****

**Hình 5. 4 Show ip ospf neighbor ở Router\_CN1**

## 5.3 Kiểm thử kết nối liên chi nhánh qua MPLS và Internet

Phần kiểm thử này tập trung vào việc xác minh Logic Phân luồng lưu lượng của hệ thống SD-WAN. Chúng tôi đã hoàn tất cấu hình Policy-Based Routing (PBR) trên Router\_CN1 để chỉ định STAFF Traffic đi MPLS và STUDENT Traffic đi ISP.

Lệnh show route-map PBR\_POLICY xác nhận logic này được áp dụng chính xác: Sequence 10 cho Staff ưu tiên Next-Hop MPLS (theo dõi bằng Track 1) và Sequence 20 cho Student ưu tiên Next-Hop ISP (theo dõi bằng Track 2). Mặc dù các lệnh ping kiểm tra thực tế ra Internet (8.8.8.8) đều thất bại do thiếu kết nối Outbound, Logic PBR đã sẵn sàng để phân luồng lưu lượng theo đúng chính sách đã đề ra khi kết nối WAN hoạt động.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 5. 5 Show route-map PBR\_POLICY ở Router\_CN1**

## 5.4 Kiểm thử cân bằng tải và chuyển mạch khi mất kết nối WAN

Mục kiểm thử này chứng minh tính năng thông minh cốt lõi của SD-WAN: cơ chế Failover tự động dựa trên sự giám sát chủ động của IP SLA/Track. Hiện tại, cả Track 1 và Track 2 đều báo Reachability is Down (Timeout) do chưa có kết nối Internet Outbound. Để chứng minh Logic chuyển mạch, chúng tôi đã mô phỏng sự cố vật lý đứt cáp bằng lệnh shutdown Interface MPLS (Fa0/0) trên Router\_CN1. Lệnh show track 1 xác nhận Track 1 ngay lập tức chuyển sang trạng thái Reachability is Down. Sự kiện này đã kích hoạt cơ chế tự động chuyển đổi của PBR. Lệnh show route-map PBR\_POLICY xác nhận Router tự động loại bỏ Next-Hop MPLS bị lỗi. Hệ thống Logic PBR đảm bảo lưu lượng Staff sẽ được định tuyến Failover tự động sang Next-Hop dự phòng ISP. Cơ chế giám sát, chuyển đổi và phục hồi (Failback) tự động này đã hoạt động hoàn toàn đúng Logic theo yêu cầu SD-WAN.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

**Hình 5. 6 Show track 1 và Show track 2 ở Router\_CN1**

## 5.5 Kiểm tra NAT và truy cập Internet từ mạng LAN

Mục tiêu kiểm tra là xác minh cấu hình NAT Outbound cho phép mạng LAN truy cập các dịch vụ bên ngoài. Cấu hình Logic NAT đã hoàn tất (bao gồm khai báo ACL, interface NAT inside/outside, và lệnh NAT chính). Tuy nhiên, do chưa hoàn tất cấu hình kết nối Internet Outbound ở lớp Underlay, mọi nỗ lực truy cập Internet từ mạng LAN đều thất bại và không thể kiểm tra NAT thực tế. Phân tích cho thấy Logic cấu hình NAT đã sẵn sàng. Khi lớp WAN Outbound được thông suốt, NAT sẽ hoạt động bình thường, cho phép các máy trạm STAFF và STUDENT truy cập Internet qua đường đi đã được PBR chỉ định.

# CHƯƠNG 6 BẢO TRÌ VÀ ĐÁNH GIÁ HỆ THỐNG

Công việc bảo trì hệ thống mạng là việc làm rất cần thiết để một hệ thống có thể hoạt động ổn định và lâu dài. Bảo trì hệ thống mạng bao gồm cả bảo trì phần cứng của thiết bị mạng và bảo trì phần mềm mạng. [3]

## 6.1 Bảo trì phần cứng

* Phải thường xuyên kiểm tra để đảm bảo các thiết bị phần cứng quan trọng thuộc hệ thống mạng như router, multilayer switch,… luôn được hoạt động ở trạng thái ổn định.
* Cần đảm bảo các dây cáp mạng được kết nối chắc chắn để kết nối luôn được hoạt động ở trạng thái tốt nhất.
* Vệ sinh định kỳ các thiết bị mạng để loại bỏ bụi bẩn bám vào các thiết bị mạng cũng như có thể kịp thời phát hiện những hư hỏng của thiết bị để kịp thời sửa chữa và thay thế.

## 6.2 Bảo trì phần mềm và sao lưu cấu hình

* Thường xuyên kiểm tra kết nối nội bộ từng chi nhánh và kết nối giữa các chi nhánh với nhau. Phải đảm bảo rằng việc kết nối luôn được hoạt động ở trạng thái ổn định.
* Nếu có sự cố về lỗi xảy ra cần có biện pháp khắc phục ngay để tránh làm hệ thống bị gián đoạn hoạt động.
* Luôn theo dõi hoạt động của hệ thống và cần lập kế hoạch định kỳ để nâng cấp và sửa chửa hệ thống.
* Đảm bảo được tính bảo mật của hệ thống để tránh những cuộc tấn công virus vào hệ thống.

## 6.3 Đánh giá ưu điểm – hạn chế của mô hình SD-WAN trường học

* Ưu điểm: Khả năng phân luồng ưu tiên (PBR), tăng cường bảo mật (IPsec) và dự phòng đường truyền, đây là những tính năng vượt trội so với mạng WAN truyền thống.
* Hạn chế: Yêu cầu độ phức tạp kỹ thuật cao khi triển khai PBR và Tunnel IPsec trên IOSv.

## 6.4 Đề xuất cải tiến và hướng phát triển mở rộng

Đề xuất mở rộng sử dụng các giải pháp SD-WAN thương mại (Cisco Viptela) để có thêm tính năng giám sát hiệu suất đường truyền theo thời gian thực và áp dụng chính sách dựa trên chất lượng dịch vụ (QoS), đồng thời tích hợp các dịch vụ bảo mật (Firewall) ngay tại biên Router Edge.

# TÀI LIỆU THAM KHẢO

|  |  |
| --- | --- |
| [1] | “CiscoShop.vn,” 2017. [Trực tuyến]. Available: https://ciscoshop.vn/. |
| [2] | “An Phát PC,” CÔNG TY CỔ PHẦN THƯƠNG MẠI MÁY TÍNH AN PHÁT, [Trực tuyến]. Available: https://www.anphatpc.com.vn/. |
| [3] | N. t. giả, trong *Giáo trình thiết kế mạng*, Đà Nẵng, Nhà xuất bản thông tin và truyền thông, 2011. |