

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG
KHOA CÔNG NGHỆ THÔNG TIN



NGUYỄN THỊ DIỄM SƯƠNG - 52000129

NGUYỄN NHÃ THẢO DUY - 52000325

XÂY DỰNG MẠNG LAN CHO TRƯỜNG HỌC SỬ DỤNG KỸ THUẬT VXLAN

DỰ ÁN CÔNG NGHỆ THÔNG TIN MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG DỮ LIỆU

THÀNH PHỐ HỒ CHÍ MINH, 2024

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG
KHOA CÔNG NGHỆ THÔNG TIN



NGUYỄN THỊ DIỄM SƯƠNG - 52000129

NGUYỄN NHÃ THẢO DUY - 52000325

XÂY DỰNG MẠNG LAN CHO TRƯỜNG HỌC SỬ DỤNG KỸ THUẬT VXLAN

DỰ ÁN CÔNG NGHỆ THÔNG TIN MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG DỮ LIỆU

Người hướng dẫn
ThS. LÊ VIẾT THANH

THÀNH PHỐ HỒ CHÍ MINH, 2024

LỜI CẢM ƠN

Chúng em xin chân thành bày tỏ sự biết ơn sâu sắc và lòng kính trọng đến ThS. LÊ VIẾT THANH, thầy là người hướng dẫn chúng em trong dự án lần này. Trong quá trình học tập và làm việc, thầy đã truyền đạt cho chúng em vô vàn kiến thức hay và bổ ích, giúp chúng em có được cơ sở lý thuyết vững vàng để em có thể hoàn thành dự án này.

Tuy nhiên, vì sự hiểu biết còn hạn chế của chúng em, bài báo cáo còn nhiều sai sót và chưa chỉnh chu như chúng em mong muốn. Chúng em rất mong nhận được nhận xét và đánh giá của thầy cẩn thận để có thể rút kinh nghiệm cũng như sửa chữa lỗi sai của bản thân.

Chúng em xin kính chúc quý thầy, quý cô và quý nhà trường luôn mạnh khỏe, hạnh phúc và ngày một thành công hơn trong sự nghiệp trồng người của mình.

Chúng em xin chân thành cảm ơn!

TP.Hồ Chí Minh, Ngày ... tháng ... năm 2024.

Tác giả

(ký và ghi rõ họ tên)

Nguyễn Thị DiễmƯơng

Nguyễn Nhã Thảo Duy

CÔNG TRÌNH ĐƯỢC HOÀN THÀNH TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG

Nhóm chúng em xin cam đoan đây là công trình nghiên cứu của riêng chúng em và được sự hướng dẫn khoa học của ThS. LÊ VIỆT THANH. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong báo cáo còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

Nếu phát hiện có bất kỳ sự gian lận nào nhóm chúng em xin hoàn toàn chịu trách nhiệm về nội dung Báo cáo Dự án Công nghệ thông tin của mình. Trường Đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do chúng em gây ra trong quá trình thực hiện (nếu có).

TP.Hồ Chí Minh, Ngày ... tháng ... năm 2024.

Tác giả

(ký và ghi rõ họ tên)

Nguyễn Thị Diễm Sương

Nguyễn Nhã Thảo Duy

XÂY DỰNG MẠNG LAN CHO TRƯỜNG HỌC SỬ DỤNG KỸ THUẬT VXLAN TÓM TẮT

- **Vấn đề nghiên cứu:** Báo cáo gồm 7 chương:

- Chương 1 - Tổng quan đề tài
- Chương 2 - Cơ sở lý thuyết
- Chương 3 - Khảo sát yêu cầu hệ thống
- Chương 4 - Phân tích thiết kế hệ thống
- Chương 5 - Triển khai hệ thống
- Chương 6 - Kiểm tra và đánh giá
- Chương 7 - Tổng kết

- **Các hướng tiếp cận:**

- Lý thuyết
- Thực hành

- **Cách giải quyết vấn đề:** Xem lại những nội dung đã học qua slide bài giảng, các kiến thức được ghi chép lại trong quá trình học và nghiên cứu thêm các video bài giảng trên mạng. Vận dụng chúng vào để giải quyết các nội dung trong dự án.

- **Một số kết quả đạt được:** Ôn lại được những kiến thức đã học, nắm vững các lý thuyết và phương pháp đã được học trong các môn về mạng máy tính. Rèn luyện tư duy logic cho việc học tập sau này.

BUILDING A LAN FOR SCHOOLS USING VXLAN TECHNIQUE ABSTRACT

- **Research issues:** The report includes 7 chapters:

- Chapter 1 - Overview of the topic
- Chapter 2 - Theoretical basis
- Chapter 3 - System requirements survey
- Chapter 4 - System design analysis
- Chapter 5 - System deployment
- Chapter 6 - Testing and evaluation
- Chapter 7 - Summary

- **Approach:**

- Theory
- Practice

- **How to solve problems:** Review the content learned through lecture slides, the knowledge recorded during the learning process and study more video lectures online. Apply them to solve project contents.
- **Some results were achieved:** Review the knowledge learned, master the theories and methods learned in computer network subjects. Practice logical thinking for future learning.

MỤC LỤC

DANH MỤC HÌNH VẼ	vi
DANH MỤC BẢNG BIỂU	viii
DANH MỤC CÁC CHỮ VIẾT TẮT	ix
CHƯƠNG 1 - TỔNG QUAN ĐỀ TÀI	1
1.1 Giới thiệu	1
1.1.1 Giới thiệu về đề tài và lý do chọn đề tài	1
1.1.2 Mục tiêu thực hiện đề tài	2
1.2 Nội dung đề tài	3
1.3 Đối tượng, phạm vi nghiên cứu đề tài	4
1.4 Phương pháp nghiên cứu	4
1.5 Ý nghĩa lý luận và thực tiễn	5
1.6 Cấu trúc bài báo cáo	5
CHƯƠNG 2 - CƠ SỞ LÝ THUYẾT	7
2.1 Tìm hiểu về mạng LAN	7
2.1.1 Mạng LAN là gì?	7
2.1.2 Phạm vi sử dụng của mạng LAN	8
2.1.3 Phân loại mạng LAN	8

2.1.4	Các thành phần cơ bản của hệ thống mạng LAN	9
2.1.5	Mạng LAN hoạt động như thế nào?	10
2.1.6	Công dụng của mạng LAN	11
2.1.7	Các kiểu Topology cơ bản của mạng LAN	12
2.2	Công nghệ VXLAN	17
2.2.1	VXLAN là gì?	17
2.2.2	Cách hoạt động của VXLAN	18
2.2.3	Overlay và Underlay	19
2.2.4	Cấu trúc gói tin VXLAN	21
2.2.5	Một số khái niệm trong VXLAN	23
2.2.6	Ưu điểm của mô hình triển khai VXLAN	25
2.2.7	Ứng dụng VXLAN	25
2.3	Phần mềm EVE-NG	26
2.3.1	Giới thiệu sơ lược về công cụ EVE-NG	26
2.3.2	Một số ưu điểm vượt trội của EVE-NG	27
2.3.3	Cài đặt EVE-NG	28
2.4	Bảo mật hệ thống	29
2.4.1	Giới thiệu	29
2.4.2	Các giải pháp bảo mật mạng	30

3.1	Phân tích yêu cầu của trường học	34
3.1.1	Xác định các thông tin phạm vi trường học	34
3.1.2	Yêu cầu người dùng	35
3.1.3	Yêu cầu về bảo mật	36
3.1.4	Sơ đồ cấu trúc trường học	37
3.2	Mục tiêu xây dựng hệ thống mạng	45
3.3	Định hướng thiết kế hệ thống	46
CHƯƠNG 4 - PHÂN TÍCH THIẾT KẾ HỆ THỐNG		49
4.1	Thiết kế mô hình mạng	49
4.1.1	Sơ đồ vật lý	49
4.1.2	Sơ đồ luận lý	50
4.2	Thông tin cài đặt cấu hình hệ thống	50
4.2.1	Thông tin VLAN, VXLAN trong hệ thống	50
4.2.2	Thông tin kết nối port trong hệ thống	54
4.2.3	Thông tin địa chỉ IP planning	60
CHƯƠNG 5 - TRIỂN KHAI HỆ THỐNG		63
5.1	Cấu hình cơ bản trên các thiết bị	63
5.2	Cấu hình các server	103
5.2.1	Cấu hình server RADIUS	103
CHƯƠNG 6 - KIỂM TRA VÀ ĐÁNH GIÁ		139

6.1	Demo sản phẩm	139
6.1.1	Kiểm tra kết nối với ISP	139
6.1.2	Kiểm tra giao thức NAT	140
6.1.3	Kiểm tra DHCP	141
6.1.4	Kiểm tra kết nối giữa các VLAN	141
6.1.5	Kiểm tra kết nối giữa các VXLAN	141
6.1.6	Kiểm tra giao thức dự phòng gateway HSRP	143
6.1.7	Kiểm tra Etherchannel	144
6.1.8	Kiểm tra kết nối VPC	146
6.1.9	Kiểm tra khả năng dự phòng của hệ thống	147
6.2	Kết luận và tổng kết dự án	151
6.3	Bài học kinh nghiệm	152
6.4	Hướng phát triển và nghiên cứu tiếp theo	152

TÀI LIỆU THAM KHẢO

154

DANH MỤC HÌNH VẼ

Hình 2.1	Mạng LAN là gì?	7
Hình 2.2	Mạng LAN hoạt động như thế nào?	10
Hình 2.3	Cấu trúc liên kết hình sao gồm các hệ thống được kết nối với một điểm kết nối duy nhất	13
Hình 2.4	Cấu trúc liên kết bus với cáp đường trực dùng chung. Các nút được kết nối với kênh thông qua các đường dây thả.	15
Hình 2.5	Cấu trúc liên kết vòng bao gồm các trạm được kết nối với nhau tạo thành một vòng.	16
Hình 2.6	Cách hoạt động của VXLAN	19
Hình 2.7	Lớp Underlay và lớp Overlay	20
Hình 2.8	VXLAN Tunnel Endpoint (VTEP)	23
Hình 3.1	Sơ đồ tổng quan cấu trúc trường	37
Hình 3.2	Sơ đồ kiến trúc của tòa A ở trụ sở chính	38
Hình 3.3	Sơ đồ kiến trúc của tòa B ở trụ sở chính	39
Hình 3.4	Sơ đồ kiến trúc của tòa C ở trụ sở chính	40
Hình 3.5	Sơ đồ kiến trúc của tòa D ở chi nhánh	41
Hình 3.6	Mặt cắt bằng của phòng hành chính	42
Hình 3.7	Mặt cắt bằng của phòng đào tạo	42
Hình 3.8	Mặt cắt bằng của phòng tuyển sinh	43
Hình 3.9	Mặt cắt bằng của phòng lab	43

Hình 3.10	Mặt cắt bằng của văn phòng khoa	44
Hình 3.11	Mặt cắt bằng của phòng học	44
Hình 3.12	Mặt cắt bằng của phòng kỹ thuật	45
Hình 3.13	Mặt cắt bằng của thư viện	45
Hình 4.1	Sơ đồ vật lý	49
Hình 4.2	Sơ đồ luận lý	50
Hình 5.1	Đặt Team name là Po8 -> Chọn Ethernet và Ethernet2 -> Chọn Teaming mode là LACP -> Apply	104
Hình 5.2	Điền địa chỉ IPv4 và DNS -> chọn OK	105
Hình 5.3	Chọn Manage -> Add Roles and Features để thêm dịch vụ server .	105
Hình 5.4	Chọn Server Roles là DNS Server	106
Hình 5.5	Chọn Install để thêm dịch vụ DNS Server	106
Hình 5.6	Chọn DNS Manager	107
Hình 5.7	Cấu hình Zone Name cmu.edu	107
Hình 5.8	Cấu hình Forward Lookup Zones	108
Hình 5.9	Cấu hình Reverse Lookup Zones	108
Hình 5.10	Chọn New Host	109
Hình 5.11	Điền địa chỉ IP -> Chọn Add Host	109
Hình 5.12	Chọn Properties	110
Hình 5.13	Cấu hình Advanced	111
Hình 5.14	Cấu hình Forwarders -> Chọn Apply	112

Hình 5.15 Chọn Add Host	113
Hình 5.16 Cấu hình Zone Transfers	114
Hình 5.17 Allow Zone Transfers	114
Hình 5.18 Chọn Add Role and Features	115
Hình 5.19 Chọn Active Directory Domain Service	115
Hình 5.20 Deployment Configuration	116
Hình 5.21 Nhập password là Admin1@123	116
Hình 5.22 Chọn Active Directory Domains and Trusts	116
Hình 5.23 Chọn Manage	117
Hình 5.24 Chọn New -> Chọn Organizational Unit	117
Hình 5.25 Nhập tên là HO	117
Hình 5.26 Nhập tên là BO	118
Hình 5.27 Chọn New -> Chọn Group	118
Hình 5.28 Nhập tên phòng ban	119
Hình 5.29 Chọn New -> Chọn User	119
Hình 5.30 Tạo User 1	120
Hình 5.31 Tạo User 2	120
Hình 5.32 Add User vào Group	120
Hình 5.33 Chọn Groups	121
Hình 5.34 Chọn service Active Directory Domain Services và Network Policy and Access Service	121

Hình 5.35 Cấu hình Active Directory Certificate Services	122
Hình 5.36 Chọn Certification Authority	122
Hình 5.37 Tạo Policy	122
Hình 5.38 Nhập tên	123
Hình 5.39 Chọn Properties	123
Hình 5.40 Chọn OK	124
Hình 5.41 Tạo Policy	124
Hình 5.42 Nhập tên	125
Hình 5.43 Chọn Security -> Chọn Properties	126
Hình 5.44 Bỏ chọn Verify the server's identity	127
Hình 5.45 Chọn Network Policy Server	128
Hình 5.46 Chọn Configure VPN or Dial-Up	128
Hình 5.47 Chọn VPN	129
Hình 5.48 Chọn Add	129
Hình 5.49 Nhập tên của các thiết bị sao cho dễ quản lý và IP tương ứng và Shared Secret là Admin1@123	130
Hình 5.50 Chọn Add	130
Hình 5.51 Nhập Team name là Po7 -> chọn Ethernet và Ethernet2 -> chọn Teaming mode là LACP	131
Hình 5.52 Điền địa chỉ IPv4 và DNS -> chọn OK	132

Hình 5.53 Vào DNS Manager -> Tạo New Zone -> Chọn Zone Type là Secondary zone	133
Hình 5.54 Nhập Zone Name	133
Hình 5.55 Nhập địa chỉ IP của Master Servers	133
Hình 5.56 Thêm dịch vụ DHCP cho Server	134
Hình 5.57 Install DHCP Server	134
Hình 5.58 Tạo Scope Name cho các VLAN	135
Hình 5.59 Nhập dải địa chỉ IP của VLAN	135
Hình 5.60 Nhập địa chỉ gateway	136
Hình 5.61 Nhập domain name và địa chỉ IP của DNS Server	136
Hình 5.62 Thêm dịch vụ IIS cho Server	137
Hình 5.63 Tắt trang web mặc định của web server	137
Hình 5.64 Thêm Source Web vào các ổ đĩa của Server	138
Hình 5.65 Gán các đường dẫn của Website mới	138
Hình 6.1 Router R1 và Router R2 kết nối với 2 ISP	139
Hình 6.2 Hai Router sau khi được kết nối với ISP	140
Hình 6.3 Kết quả kiểm tra giao thức NAT	140
Hình 6.4 Kiểm tra DHCP của từng phòng ban	141
Hình 6.5 Kiểm tra kết nối giữa các VLAN	141
Hình 6.6 Kiểm tra kết nối VXLAN tại NXOS3	142
Hình 6.7 Xem Interface NVE 1	142

Hình 6.8 Xem NVE VNI	143
Hình 6.9 Kiểm tra giao thức dự phòng gateway HSRP tại NXOS3	143
Hình 6.10 Kiểm tra giao thức dự phòng gateway HSRP tại NXOS4	144
Hình 6.11 Kiểm tra Port-channel 1 trên Sw_A	144
Hình 6.12 Kiểm tra Port-channel 2 trên Sw_B	145
Hình 6.13 Kiểm tra Port-channel 3 trên Sw_C	145
Hình 6.14 Kiểm tra Port-channel 4 trên Sw_DC1	146
Hình 6.15 Kiểm tra VPC domain 1 trên switch NXOS1	146
Hình 6.16 Kiểm tra VPC domain 2 trên switch NXOS3	147
Hình 6.17 VPC Status	147
Hình 6.18 Switch là Leaf nếu xảy ra sự cố vẫn lấy được địa chỉ IP DHCP . .	148
Hình 6.19 Switch là Spine nếu xảy ra sự cố vẫn lấy được địa chỉ IP DHCP . .	149
Hình 6.20 Các thiết bị redundant làm cho hệ thống vẫn hoạt động bình thường khi xảy ra sự cố	150

DANH MỤC BẢNG BIỂU

Bảng 4.1	Thông tin VLAN, VXLAN trong hệ thống	50
Bảng 4.1	Thông tin VLAN, VXLAN trong hệ thống	51
Bảng 4.1	Thông tin VLAN, VXLAN trong hệ thống	52
Bảng 4.1	Thông tin VLAN, VXLAN trong hệ thống	53
Bảng 4.1	Thông tin VLAN, VXLAN trong hệ thống	54
Bảng 4.2	Thông tin kết nối port trong hệ thống	54
Bảng 4.2	Thông tin kết nối port trong hệ thống	55
Bảng 4.2	Thông tin kết nối port trong hệ thống	56
Bảng 4.2	Thông tin kết nối port trong hệ thống	57
Bảng 4.2	Thông tin kết nối port trong hệ thống	58
Bảng 4.2	Thông tin kết nối port trong hệ thống	59
Bảng 4.3	Thông tin quy hoạch địa chỉ IP	60
Bảng 4.3	Thông tin quy hoạch địa chỉ IP	61
Bảng 4.3	Thông tin quy hoạch địa chỉ IP	62
Bảng 5.1	Quy trình cấu hình của các thiết bị trong hệ thống	63
Bảng 5.2	Các lệnh cấu hình của Router ISP1	67
Bảng 5.3	Các lệnh cấu hình của Router ISP2	68
Bảng 5.4	Các lệnh cấu hình của Router R1	69
Bảng 5.5	Các lệnh cấu hình của Router R2	70

Bảng 5.6 Các lệnh cấu hình của Firewall FW1	71
Bảng 5.7 Các lệnh cấu hình của Firewall FW2	72
Bảng 5.8 Các lệnh cấu hình của NXOS1	74
Bảng 5.9 Các lệnh cấu hình của NXOS2	76
Bảng 5.10 Các lệnh cấu hình của NXOS3	79
Bảng 5.11 Các lệnh cấu hình của NXOS4	86
Bảng 5.12 Các lệnh cấu hình của Switch Sw_A	93
Bảng 5.13 Các lệnh cấu hình của Switch Sw_B	94
Bảng 5.14 Các lệnh cấu hình của Switch Sw_C	96
Bảng 5.15 Các lệnh cấu hình của Switch Sw_DC1	97
Bảng 5.16 Các lệnh cấu hình của Switch Sw_DC2	98
Bảng 5.17 Các lệnh cấu hình của Router R3	99
Bảng 5.18 Các lệnh cấu hình của Switch Sw_BO	100
Bảng 5.19 Các lệnh cấu hình của Switch Sw_D1	101
Bảng 5.20 Các lệnh cấu hình của Switch Sw_D2	102

DANH MỤC CÁC CHỮ VIẾT TẮT

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
LAN	Local Area Network
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
LAN	Local Area Network
VLAN	Virtual Local Area Network
VXLAN	Virtual Extensible LAN
VTEPs	VXLAN Tunnel Endpoints
VNI	Virtual Network Instance
SSH	Secure SHell
HSRP	Hot Standby Router Protocol
OSPF	Open Shortest Path First
EVE-NG	Emulated Virtual Environment – Netx Generation

CHƯƠNG 1 - TỔNG QUAN ĐỀ TÀI

1.1 Giới thiệu

1.1.1 Giới thiệu về đề tài và lý do chọn đề tài

Mạng Local Area Network (LAN) là một phần không thể thiếu đối với hệ thống giáo dục, có vai trò then chốt đối với việc nâng cao hiệu quả giảng dạy và học tập. Một số ứng dụng điển hình của mạng LAN đối với giáo dục là:

- Mạng LAN tạo ra một môi trường chia sẻ thông tin, giúp giáo viên và học sinh có thể kết nối và chia sẻ kiến thức. Nhờ vậy, việc truyền tải thông tin trở nên nhanh chóng và hiệu quả hơn bao giờ hết.
- Khả năng kết nối với Internet và mạng LAN mở ra một thế giới thông tin vô tận. Học sinh và giáo viên có thể tận dụng nguồn thông tin phong phú nhằm nâng cao kiến thức và kỹ năng của mình.
- Mạng LAN hỗ trợ việc triển khai hình thức giảng dạy trực tuyến (E-Learning), tạo điều kiện cho việc học từ xa có thể tiếp cận nhanh chóng các nguồn tư liệu giảng dạy.

Chúng em chọn đề tài "Thiết kế mạng LAN cho trường học sử dụng kỹ thuật VXLAN" với lý do nhằm tối ưu hóa hiệu suất, linh hoạt và bảo mật của mạng trong môi trường giáo dục. Trường học đòi hỏi một hạ tầng mạng mạnh mẽ để đáp ứng nhu cầu ngày càng tăng về kết nối internet, phục vụ cho việc học tập trực tuyến, quản lý dữ liệu sinh viên và giảng dạy. Trong những năm gần đây, Virtual Extensible LAN (VXLAN) đã được sử dụng rộng rãi bởi các tổ chức để cải thiện khả năng linh hoạt và quản lý tài nguyên mạng một cách tối ưu.

Việc triển khai VXLAN trong mạng LAN của trường học không chỉ giúp giảm chi

phi phí vận hành và quản lý mạng mà còn mang lại sự đơn giản hóa trong việc mở rộng hạ tầng mạng và thích ứng với các thay đổi về cấu trúc mạng và vị trí vật lý của thiết bị. Từ đó, việc nghiên cứu và thực hiện đề tài này không chỉ mang lại lợi ích ngay trong việc xây dựng một mạng LAN hiệu quả cho trường học mà còn cung cấp kiến thức và kinh nghiệm quý báu về việc áp dụng công nghệ mới trong môi trường mạng hiện đại.

1.1.2 *Mục tiêu thực hiện đề tài*

Thiết kế mạng LAN cho trường học sử dụng kỹ thuật VXLAN để tạo mạng ảo cho giảng dạy và học tập.

Trong việc thiết kế mạng Local Area Network (LAN) dùng cho giảng dạy và học tập, mục tiêu quan trọng nhất là tạo ra một hệ thống linh hoạt, an toàn và hiệu quả. Đầu tiên và quan trọng nhất là tính khả dụng.

Cần đảm bảo mạng luôn sẵn có, cho phép giáo viên và học sinh truy cập internet từ bất cứ vị trí nào trên thế giới hoặc thậm chí từ xa. Điều này có thể đạt được thông qua việc áp dụng các giải pháp và công nghệ có khả năng cao về tính khả dụng và kết nối mạng.

Trong đó bảo mật thông tin là một mục tiêu quan trọng. Hệ thống cần bảo vệ an toàn các thông tin cá nhân, dữ liệu học tập và tài nguyên mạng trước mọi đe doạ an ninh. Sử dụng các biện pháp an toàn như firewalls, mã hoá dữ liệu và xác thực đáng tin cậy sẽ giúp đảm bảo sự riêng tư và an toàn của hệ thống.

Hiệu suất của mạng là một yếu tố quan trọng giúp cho việc truyền dẫn hình ảnh, video và âm thanh được suôn sẻ. Điều này đòi hỏi băng thông mạng được tối ưu và sử dụng các thiết bị mạng chất lượng cao. Việc tối ưu hoá băng thông mạng cũng đóng vai trò quan trọng đối với việc duy trì hiệu suất mạng.

Tối ưu việc quản lý hệ thống thiết bị đầu cuối và băng thông mạng, áp dụng các

công cụ giám sát và quản lý tài nguyên một cách hiệu quả. Điều này giúp tăng tính linh động và hiệu quả của hệ thống.

Triển khai các kỹ thuật như VXLAN để tạo mạng ảo và duy trì sự cô lập giữa các cá nhân và nhóm làm việc là quan trọng. Điều này giúp tạo ra môi trường linh động và đáp ứng được từng yêu cầu cụ thể của mỗi đối tượng sử dụng.

1.2 Nội dung đề tài

Nội dung của đề tài bao gồm:

- Tìm hiểu và nghiên cứu các kiến thức về mạng Lan, kỹ thuật xây dựng VXLAN và cách sử dụng phần mềm EVE-NG.
- Từ đó thiết kế nên một mạng LAN dựa trên các yêu cầu của trường học. Xác định rõ các yêu cầu để tiến hành thiết kế mạng LAN sử dụng kỹ thuật VXLAN để tạo mạng ảo cho giảng dạy và học tập. Các yêu cầu cần tìm hiểu và làm rõ bao gồm: số lượng người dùng mạng, số lượng thiết bị mạng, các ứng dụng đang sử dụng và các yêu cầu bảo mật.
- Sử dụng phần mềm EVE-NG để thiết kế mô hình mạng LAN, bao gồm cấu hình và cách kết nối các thiết bị mạng như Switch, Router và Server.
- Sau khi thiết kế được một mô hình mạng, cần cấu hình các thiết bị mạng, bao gồm cấu hình VLAN, cấu hình VXLAN, cấu hình định tuyến và bảo mật.
- Khi đã hoàn thành việc cấu hình, sử dụng EVE-NG để mô phỏng hoạt động của mạng LAN, kiểm tra tính năng và hiệu suất của hệ thống mạng.
- Cuối cùng là phân tích và đánh giá kết quả của mô phỏng, từ đó đưa ra kết luận về hiệu quả của việc sử dụng kỹ thuật VXLAN để tạo mạng ảo cho giảng dạy và học tập ở trường học.

1.3 Đối tượng, phạm vi nghiên cứu đề tài

Đối tượng nghiên cứu của đề tài là các trường học có nhu cầu triển khai các mạng ảo để ứng dụng giảng dạy và học tập.

Phạm vi nghiên cứu bao gồm các công nghệ ảo hóa mạng, mô hình mạng ảo, và kỹ thuật VXLAN. Đề tài sẽ nghiên cứu và đánh giá hiệu quả của việc sử dụng kỹ thuật VXLAN trong thiết kế một hệ thống mạng LAN để tạo mạng ảo.

1.4 Phương pháp nghiên cứu

Phương pháp nghiên cứu giải quyết đề tài:

- Tìm hiểu lý thuyết và tài liệu: Bắt đầu bằng việc tìm hiểu các tài liệu, sách, bài báo, hướng dẫn và tài liệu trực tuyến liên quan đến mạng LAN, kỹ thuật xây dựng VXLAN và EVE-NG. Các nguồn tài liệu có thể bao gồm sách chuyên ngành, tài liệu học trực tuyến, tài liệu công ty và bài viết từ các chuyên gia trong lĩnh vực.
- Xây dựng môi trường thí nghiệm: Để áp dụng và thực hành các kiến thức, bạn cần có một môi trường thí nghiệm. Trong trường hợp này, bạn có thể sử dụng phần mềm EVE-NG để tạo môi trường mạng ảo và thực hiện các thí nghiệm liên quan đến mạng LAN và VXLAN. Hãy tìm hiểu về cách cài đặt và sử dụng EVE-NG thông qua tài liệu và hướng dẫn của nhà phát triển.
- Thực hiện các thí nghiệm và nghiên cứu: Sử dụng môi trường thí nghiệm EVE-NG, xây dựng mạng LAN, triển khai VXLAN, tìm hiểu về các tính năng và cấu hình của VXLAN, và thực hiện các kịch bản thử nghiệm.
- Ghi lại và phân tích kết quả: Ghi lại kết quả triển khai. Phân tích dữ liệu và kết quả thu được để hiểu rõ hơn về mạng LAN, kỹ thuật xây dựng VXLAN và sử dụng EVE-NG.
- Đánh giá và cải thiện: Đánh giá mức độ đạt được mục tiêu đề ra và xác định các

cải tiến tiềm năng trong tương lai của ứng dụng.

1.5 Ý nghĩa lý luận và thực tiễn

- Ý nghĩa lý luận: Dự án góp phần làm rõ tính khả thi khi xây dựng hệ thống mạng LAN bằng cách sử dụng kỹ thuật VXLAN để tạo mạng ảo.
- Ý nghĩa thực tiễn: Kết quả của dự án đề ra giải pháp thực tiễn giúp trường học có phương pháp dạy tối ưu hơn, tiết kiệm chi phí hơn. Ngoài ra, các tổ chức có thể phát triển thêm các dịch vụ và ứng dụng vào các lĩnh vực khác.

1.6 Cấu trúc bài báo cáo

Bài làm gồm có 7 chương:

- **Chương 1: Tổng quan đề tài:**

Giới thiệu sơ lược, tổng quan về đề tài Tìm hiểu và nghiên cứu các kiến thức về mạng Lan, kỹ thuật xây dựng VXLAN và cách sử dụng phần mềm EVE-NG.

- **Chương 2: Cơ sở lý thuyết:**

Giới thiệu cơ sở lý thuyết cần có để thực hiện đề tài, cũng như các lý thuyết liên quan đến đề tài.

- **Chương 3: Khảo sát yêu cầu hệ thống:**

Khảo sát, thu nhập thông tin để xây dựng mạng LAN với kỹ thuật VXLAN.

- **Chương 4: Phân tích thiết kế hệ thống:**

Xây dựng và thiết kế hệ thống mạng.

- **Chương 5: Triển khai hệ thống:**

Triển khai hệ thống mạng trên ứng dụng mô phỏng EVE-NG.

- **Chương 6: Kiểm tra và đánh giá:**

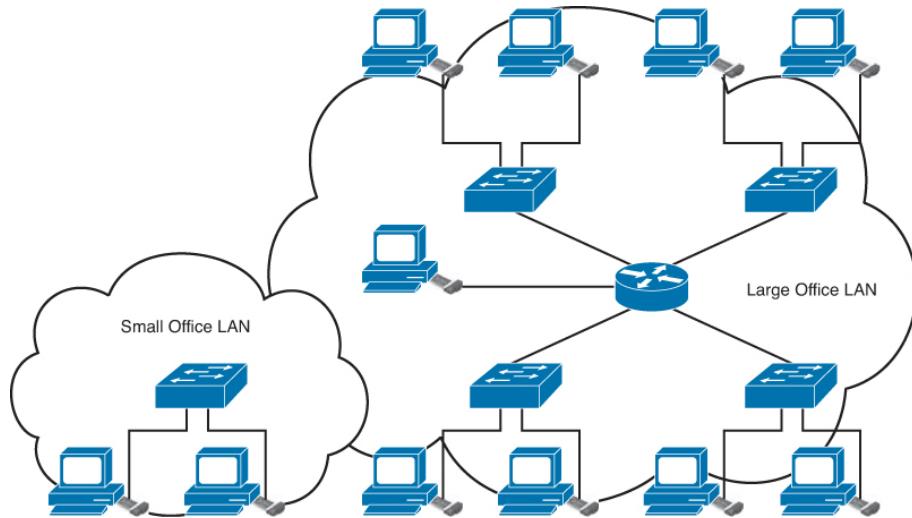
Trình bày kết quả demo hệ thống và đánh giá chất lượng hệ thống.

- **Chương 7: Tổng kết:**

Trình bày các kết quả đạt được và hướng phát triển dự án trong tương lai.

CHƯƠNG 2 - CƠ SỞ LÝ THUYẾT

2.1 Tìm hiểu về mạng LAN



Hình 2.1 Mạng LAN là gì?

2.1.1 *Mạng LAN là gì?*

Local Area Network (LAN) là một mạng hợp nhất các thiết bị tại cùng một vị trí vật lý như tòa nhà, văn phòng, hoặc căn nhà, có thể có quy mô từ nhỏ đến lớn, từ một mạng gia đình với một người dùng đến một mạng doanh nghiệp với hàng nghìn người dùng và thiết bị tại văn phòng hoặc trường học.

Liên kết trong mạng LAN thường được thực hiện thông qua dây cáp mạng hoặc kết nối không dây (Wi-Fi) trong một phạm vi hạn chế như cơ quan, gia đình, hoặc công ty.

Mạng LAN tạo điều kiện cho việc chia sẻ dữ liệu và tài nguyên như tập tin, máy in, và phần mềm giữa các thiết bị, tạo ra môi trường thuận lợi để hợp tác và chia sẻ trong một phạm vi địa phương.

2.1.2 Phạm vi sử dụng của mạng LAN

Phạm vi hoạt động của mạng LAN (Local Area Network) bị giới hạn trong các khu vực như văn phòng, nhà riêng, lớp học, phòng game hoặc doanh nghiệp. Thông thường, phạm vi này không vượt quá 100m.

Các thiết bị máy tính trong phạm vi của mạng LAN có thể kết nối và tương tác với nhau để trao đổi dữ liệu và thông tin. Trong trường hợp không thể kết nối từ khoảng cách xa hơn, mạng LAN sẽ sử dụng mạng Internet để chia sẻ thông tin.

2.1.3 Phân loại mạng LAN

Có hai dạng chính của mạng LAN được biết đến: mạng LAN có dây và mạng LAN không dây.

- **Mạng LAN có dây (Wire LAN):** Sử dụng các thiết bị chuyển mạch và cáp Ethernet để kết nối các thiết bị đầu cuối, máy chủ hoặc các thiết bị IoT với mạng của tổ chức. Trong các doanh nghiệp nhỏ có ít thiết bị, mạng LAN có dây thường bao gồm các bộ chuyển mạch không quản lý với đủ cổng Ethernet để kết nối tất cả các thiết bị.

Tuy nhiên, trong các mạng LAN lớn hơn, cần kết nối hàng nghìn thiết bị, việc này đòi hỏi các bước như cấu hình, phần cứng hoặc phần mềm bổ sung để đảm bảo hoạt động của mạng một cách hiệu quả nhất. Đây cũng là lúc mạng LAN ảo (VLAN) xuất hiện. VLAN chia lưu lượng truy cập trên cùng một mạng vật lý thành hai mạng để quản lý mạng, đặc biệt là trong các mạng LAN lớn.

- **Mạng LAN không dây (Wireless LAN hay WLAN):** Sử dụng kỹ thuật IEEE 802.11 để truyền dữ liệu giữa các thiết bị đầu cuối và mạng thông qua phổi không dây. Trong nhiều trường hợp, mạng LAN không dây được ưu tiên hơn kết nối mạng LAN có dây vì tính linh hoạt và tiết kiệm chi phí, không cần phải triển khai hệ thống cáp ở toàn bộ tòa nhà. Công ty thường đánh giá mạng WLAN là phương tiện kết nối chính vì người dùng phụ thuộc vào điện thoại thông minh, máy tính bảng và các thiết bị di động khác.

2.1.4 Các thành phần cơ bản của hệ thống mạng LAN

Mạng LAN bao gồm cables, access points, switches, routers và các thành phần khác cho phép thiết bị kết nối với máy chủ nội bộ, máy chủ web và các mạng LAN khác thông qua mạng diện rộng như:

- **Computer** Máy tính đóng vai trò quan trọng trong mạng LAN, chúng là các thiết bị dùng để chia sẻ tài nguyên và giao tiếp với nhau. Các máy tính có thể là máy tính cá nhân, laptop, điện thoại thông minh và máy tính bảng. Mỗi máy tính trong mạng được xem như một nút.[1]

- **Server**

Thiết bị máy chủ (server) là một máy tính đảm nhận vai trò quản lý tài nguyên trên mạng. Nó có thể phục vụ nhiều chức năng khác nhau, bao gồm lưu trữ tệp tin hoặc cơ sở dữ liệu.

- **Client**

Các máy trạm (client) là những thiết bị được liên kết với nhau và dưới sự quản lý của máy chủ.

- **Network Interface Card**

Network Interface Cards (NICs) là các thiết bị phần cứng đảm nhận vai trò xử lý giao diện với mạng, cho phép các thiết bị có khả năng kết nối mạng liên kết với mạng. Chúng chuyển đổi các gói dữ liệu giữa máy tính và định dạng dữ liệu mạng.[1]

- **Cable**

Cáp mạng (cable) được sử dụng để liên kết các thiết bị trên mạng. Loại cáp mạng phổ biến nhất trong mạng LAN là cáp Ethernet, được dùng để kết nối các thiết bị như máy tính, router và switch trong mạng cục bộ.

- Hub

Hub cung cấp các thiết bị tổng hợp hoạt động ở Lớp 1 của mô hình tham chiếu OSI. Tuy nhiên, vai trò của các hub trong chức năng này đã được thay thế bằng các switch, và hiện nay rất ít khi thấy các hub được sử dụng trong mạng LAN.[2]

- Switch

Bộ chuyển mạch (switch) là các thiết bị mạng dùng để kết nối các thiết bị trong mạng máy tính bằng cách sử dụng chuyển mạch gói để nhận và chuyển tiếp dữ liệu đến thiết bị đích. Bộ chuyển mạch cho phép các thiết bị khác nhau trên mạng giao tiếp một cách hiệu quả.

- Router

Bộ định tuyến (router): cung cấp phương tiện để kết nối các phân đoạn mạng LAN[2]. Router là thiết bị giúp chuyển các gói dữ liệu sang một mạng khác và định tuyến chúng đến các đầu cuối thông qua quá trình định tuyến. Ngoài ra, router còn có khả năng liên kết các mạng LAN khác nhau, ngay cả khi chúng ở xa nhau.

2.1.5 Mạng LAN hoạt động như thế nào?



Hình 2.2 Mạng LAN hoạt động như thế nào?

Nhiệm vụ cơ bản của mạng LAN là xây dựng một môi trường kết nối giữa các máy tính, cho phép chúng chia sẻ tài nguyên và truy cập vào các dịch vụ như máy in, tệp tin và ứng dụng. Mạng LAN thường được phân loại thành hai dạng chính: mạng ngang hàng (peer-to-peer) và mạng máy khách-máy chủ (client-server). Trong mạng LAN máy khách-máy chủ, các máy tính khách kết nối với một máy chủ trung tâm, nơi quản lý và điều khiển quyền truy cập vào ứng dụng, thiết bị và dữ liệu lưu trữ.

Các ứng dụng hoạt động trên máy chủ của mạng LAN cung cấp một loạt các dịch vụ quan trọng như truy cập vào cơ sở dữ liệu, chia sẻ tài liệu, gửi và nhận email, và in ấn. Trong khi đó, trong mạng LAN ngang hàng, các máy tính chia sẻ dữ liệu trực tiếp với nhau thông qua các thiết bị chuyển mạch hoặc định tuyến mà không cần sự trung gian của một máy chủ.

Mạng LAN cũng có khả năng liên kết với các mạng LAN khác thông qua các kết nối truyền dẫn hoặc dịch vụ thuê riêng, và thậm chí có thể kết nối với Internet bằng cách sử dụng các công nghệ mạng riêng ảo. Điều này tạo ra nhiều cơ hội để tăng cường giao tiếp và chia sẻ thông tin giữa các mạng LAN khác nhau..

Nhiệm vụ cơ bản của mạng LAN là tạo ra một môi trường kết nối giữa các máy tính, cho phép chúng chia sẻ tài nguyên và truy cập vào các dịch vụ khác nhau như máy in, tệp tin và ứng dụng. Mạng LAN thường được phân loại thành hai loại chính: mạng ngang hàng (peer-to-peer) và mạng máy khách-máy chủ (client-server).

2.1.6 Công dụng của mạng LAN

Các công dụng chính của mạng LAN:

- **Chia sẻ tài nguyên:** Mạng LAN hỗ trợ việc phân chia và chia sẻ các nguồn lực như máy tính, thiết bị mạng, ổ cứng và ứng dụng giữa các máy tính trong mạng. Bằng cách này, không cần phải mua thêm thiết bị cho mỗi máy tính, điều này giúp cải thiện hiệu suất làm việc và giảm chi phí sản xuất.

- **Trao đổi thông tin:** Các mạng LAN cho phép truyền thông nhanh chóng giữa các thiết bị trong cùng một mạng. Người dùng có thể chia sẻ file, hình ảnh, email, tin nhắn và tài liệu khác một cách dễ dàng và nhanh chóng.
- **Quản lý dữ liệu:** Mạng LAN hỗ trợ tính năng sao lưu và khôi phục dữ liệu trên một máy chủ trung tâm, tăng cường bảo mật và khả năng phục hồi dữ liệu khi cần thiết.
- **Tích hợp ứng dụng trong mạng LAN:** Mạng LAN cho phép tích hợp các ứng dụng và dịch vụ như email, truyền thông âm thanh, hội nghị video và các ứng dụng doanh nghiệp khác. Việc này tạo điều kiện cho việc hợp tác và cải thiện hiệu quả công việc trong hệ thống LAN.
- **Bảo mật dữ liệu:** Hệ thống LAN được xây dựng với các giao thức bảo mật như mật khẩu, mã hóa và phân quyền truy cập để bảo vệ dữ liệu quan trọng khỏi truy cập trái phép một cách hiệu quả hơn.
- **Quản lý mạng dễ dàng:** Việc tích hợp các công cụ quản lý mạng như phần mềm quản lý mạng và giao diện quản lý đồ họa giúp nâng cao hiệu quả quản lý mạng. Điều này giúp người quản trị dễ dàng quản lý và vận hành mạng một cách hiệu quả hơn.

2.1.7 Các kiểu Topology cơ bản của mạng LAN

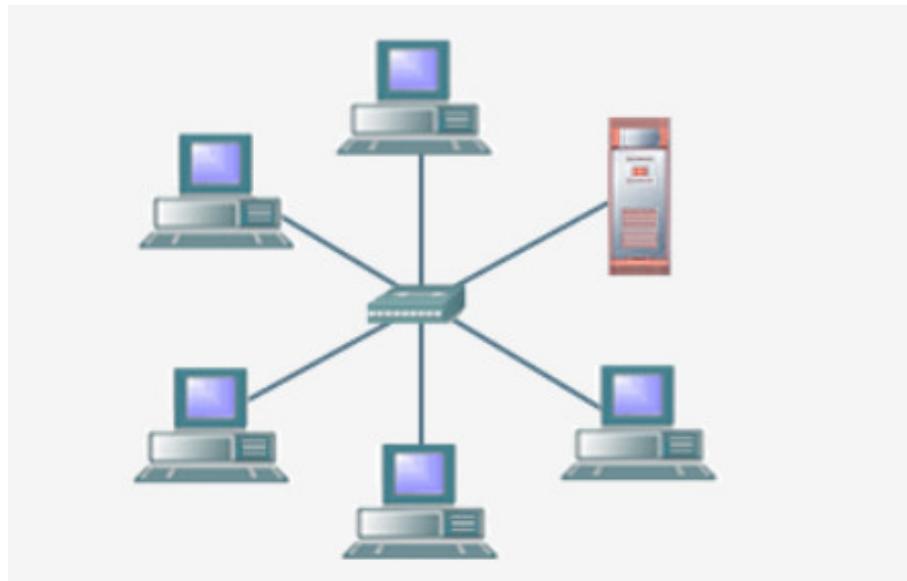
Cấu trúc mạng LAN, hay còn gọi là topology, biểu thị cách các thành phần của mạng được tổ chức và kết nối với nhau. Mạng LAN có nhiều loại topology khác nhau, nhưng đa số chúng thường bao gồm ba loại phổ biến sau đây:

- **Mạng hình sao (Star Topology):**

- Trong Topology này, tất cả các thiết bị được kết nối với một hub hoặc switch thông qua cáp riêng biệt. Hub hoặc switch là điểm trung tâm của

mạng và phân phối dữ liệu đến các thiết bị khác. Đây là một trong những kiểu Topology phổ biến nhất trong mạng LAN.

- Ở trung tâm này, nó có vai trò quản lý và điều khiển toàn bộ hoạt động của mạng như [3]:
 - Thông báo về trạng thái của mạng.
 - Xác định cặp địa chỉ gửi - địa chỉ nhận và cho phép chúng trao đổi thông tin để liên lạc với nhau.
 - Theo dõi và xử lý các lỗi trong quá trình trao đổi thông tin,...



Hình 2.3 Cấu trúc liên kết hình sao gồm các hệ thống được kết nối với một điểm kết nối duy nhất

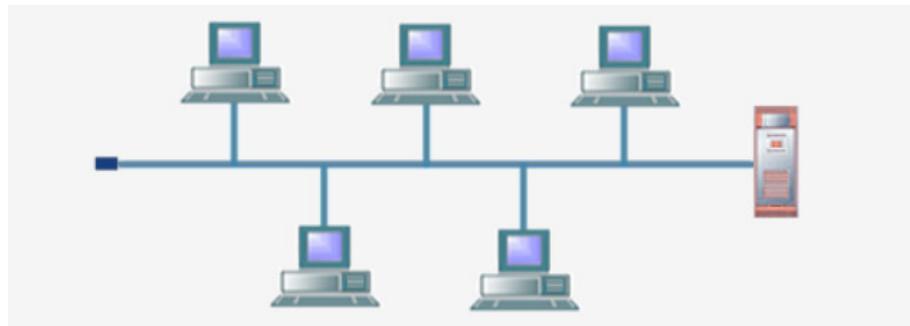
- **Ưu điểm:**

- Dễ cài đặt và bảo trì: Topology Hình sao đơn giản để triển khai và cấu hình, đặc biệt là với việc sử dụng hub hoặc switch, giúp quản trị mạng dễ dàng thêm hoặc loại bỏ thiết bị mà không gây ảnh hưởng đến các thiết bị khác trong mạng.

- Dễ dàng phát hiện và cô lập lỗi: Vì mỗi thiết bị được kết nối trực tiếp với hub hoặc switch, việc phát hiện và xử lý lỗi trở nên dễ dàng hơn.
- Hiệu suất cao: Dữ liệu được truyền trực tiếp giữa hai thiết bị mà không cần phải đi qua nhiều nút trung gian, do đó giảm thiểu độ trễ và tăng hiệu suất mạng.
- Nhược điểm:
 - Điểm trung tâm duy nhất: Toàn bộ mạng phụ thuộc vào hub hoặc switch. Nếu hub hoặc switch gặp sự cố, toàn bộ mạng có thể bị gián đoạn.
 - Hạn chế về khả năng mở rộng: Số lượng cổng trên hub hoặc switch là hạn chế, điều này có thể làm hạn chế khả năng mở rộng của mạng khi số lượng thiết bị tăng lên.
 - Chi phí cao: Việc triển khai mạng Hình sao có thể đòi hỏi chi phí cao hơn so với một số kiểu Topology khác, đặc biệt là khi cần sử dụng hub hoặc switch chất lượng cao để đảm bảo hiệu suất và độ ổn định của mạng.

- **Mạng hình tuyến (Bus Topology)[3]:**

- Trong Topology này, tất cả các thiết bị được kết nối với một đường truyền chính. Dữ liệu được truyền từ một thiết bị đến tất cả các thiết bị khác trên đường truyền.



Hình 2.4 Cấu trúc liên kết bus với cáp đường trực dùng chung. Các nút được kết nối với kênh thông qua các đường dây thả.

- **Ưu điểm:**

- Dễ cài đặt: Topology tuyến là một trong những kiểu Topology đơn giản nhất để triển khai. Các thiết bị chỉ cần được kết nối với một đường truyền chính.
- Chi phí thấp: Việc triển khai mạng theo Topology tuyến thường rất chi phí hiệu quả, do sử dụng ít dây cáp hơn so với các kiểu Topology khác.
- Dễ dàng mở rộng: Thêm thiết bị mới vào mạng dạng tuyến là một quá trình đơn giản, chỉ cần kết nối thiết bị mới vào đường truyền chính.

- **Nhược điểm:**

- Điểm yếu tại nút trung tâm: Nếu nút trung tâm (bus) gặp sự cố, toàn bộ mạng có thể bị gián đoạn.
- Hiệu suất giảm khi tăng số lượng thiết bị: Khi số lượng thiết bị trên mạng tăng lên, hiệu suất của mạng có thể giảm do xung đột dữ liệu trên đường truyền chính.
- Khó phát hiện và xử lý lỗi: Việc xác định và sửa chữa lỗi trên mạng

dạng tuyễn có thể phức tạp hơn so với các kiểu Topology khác do mỗi thiết bị không trực tiếp kết nối với nhau.

- - Mạng dạng vòng (Ring Topology)[3]:

- Mạng dạng vòng là một loại mạng phổ biến, được tổ chức và triển khai dưới dạng một vòng tròn kín. Tín hiệu được truyền theo một hướng nhất định, và mỗi máy trạm chỉ truyền tín hiệu qua một nút tại mỗi thời điểm. Do đó, thông tin được chuyển đi phải kèm theo địa chỉ cụ thể của mỗi máy trạm sẽ nhận thông tin đó.



Hình 2.5 Cấu trúc liên kết vòng bao gồm các trạm được kết nối với nhau tạo thành một vòng.

- **Ưu điểm:**

- Dễ mở rộng: Topology vòng cho phép dễ dàng thêm hoặc loại bỏ các thiết bị trong mạng mà không ảnh hưởng đến các thiết bị khác.
- Hiệu suất cao: Dữ liệu được truyền qua mỗi thiết bị trong mạng theo

một hướng duy nhất, giúp giảm xung đột và đảm bảo hiệu suất cao.

- **Khả năng tự phục hồi:** Trong một số hệ thống vòng, có các cơ chế tự phục hồi tự động khi có sự cố xảy ra, giúp duy trì tính liên tục của mạng.

- **Nhược điểm:**

- **Độ tin cậy thấp:** Nếu có sự cố xảy ra tại một điểm nào đó trong vòng, toàn bộ mạng có thể bị ảnh hưởng.
- **Khó phát hiện và xử lý lỗi:** Việc xác định và sửa chữa lỗi trên mạng vòng có thể phức tạp hơn do dữ liệu được truyền liên tục và không có một điểm trung tâm để kiểm soát.
- **Hiệu suất giảm khi tăng số lượng thiết bị:** Khi số lượng thiết bị trên mạng tăng lên, hiệu suất của mạng có thể giảm do xung đột dữ liệu trên vòng.

2.2 Công nghệ VXLAN

2.2.1 VXLAN là gì?

Virtual Extensible LAN (VXLAN) là một công nghệ tiên tiến cho phép mở rộng các mạng Layer 2 qua cơ sở hạ tầng Layer 3 bằng cách sử dụng kỹ thuật đóng gói MAC vào giao thức UDP và tunneling. Tính năng này cho phép thiết kế kết cấu trung tâm dữ liệu ảo hóa và nhiều bên thuê trên cơ sở hạ tầng vật lý chung được chia sẻ và còn mang lại nhiều lợi ích. VXLAN cho phép sắp xếp linh hoạt các công việc trên vải dữ liệu trung tâm dữ liệu, giúp đặt các công việc của người thuê trên các pod vật lý trong một trung tâm dữ liệu duy nhất hoặc thậm chí trải rộng qua nhiều trung tâm dữ liệu có đặc điểm địa lý khác nhau.

Ngoài ra, VXLAN cung cấp khả năng mở rộng cao hơn bằng cách sử dụng một ID đoạn 24 bit, gọi là bộ nhận dạng mạng VXLAN (VNID), cho phép tối đa 16 triệu đoạn

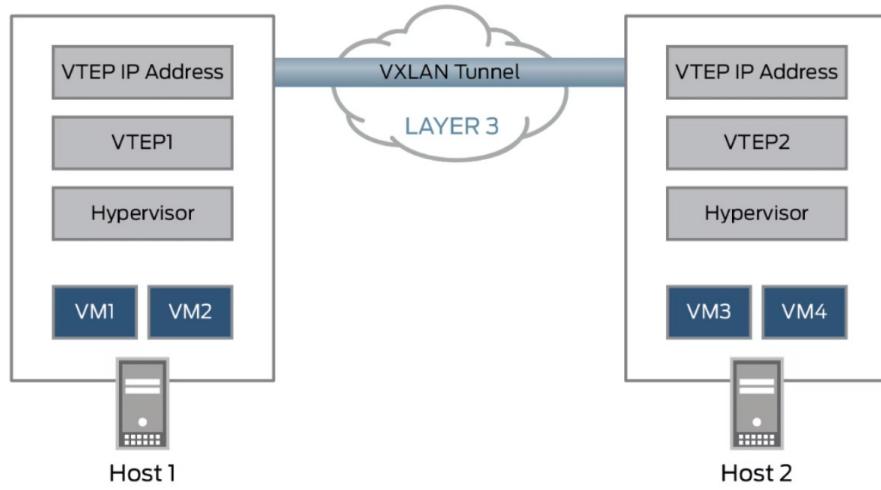
VXLAN tồn tại trong cùng một miền quản trị, so với VLAN truyền thống chỉ hỗ trợ tối đa 4096 VLAN.[4]

2.2.2 *Cách hoạt động của VXLAN*

Giao thức tunneling VXLAN đóng gói các khung Ethernet Layer 2 vào các gói UDP Layer 4, cho phép bạn tạo ra các mạng con Layer 2 ảo mở rộng trên các mạng Layer 3 vật lý. Mỗi mạng con được phân đoạn được định danh duy nhất bằng một VXLAN Network Identifier (VNI).[5]

Đơn vị thực hiện việc đóng gói và giải mã các gói tin được gọi là VXLAN Tunnel Endpoint (VTEP). Một VTEP có thể là một thiết bị mạng độc lập, chẳng hạn như một router hoặc switch vật lý, hoặc là một switch ảo triển khai trên một máy chủ. VTEP đóng gói các khung Ethernet thành các gói VXLAN, sau đó gửi đến VTEP đích qua mạng IP hoặc mạng Layer 3 khác, nơi chúng được giải gói và chuyển tiếp đến máy chủ đích.

Để hỗ trợ các thiết bị không thể hoạt động như một VTEP trên riêng của mình, chẳng hạn như các máy chủ metal chưa có hệ điều hành, các VTEP phần cứng như các switch và bộ định tuyến Juniper có thể đóng gói và giải gói các gói dữ liệu. Ngoài ra, các VTEP có thể tồn tại trên các máy chủ hypervisor, chẳng hạn như máy ảo dựa trên kernel (KVM), để hỗ trợ trực tiếp các công việc ảo hóa. Loại VTEP này được gọi là VTEP phần mềm.

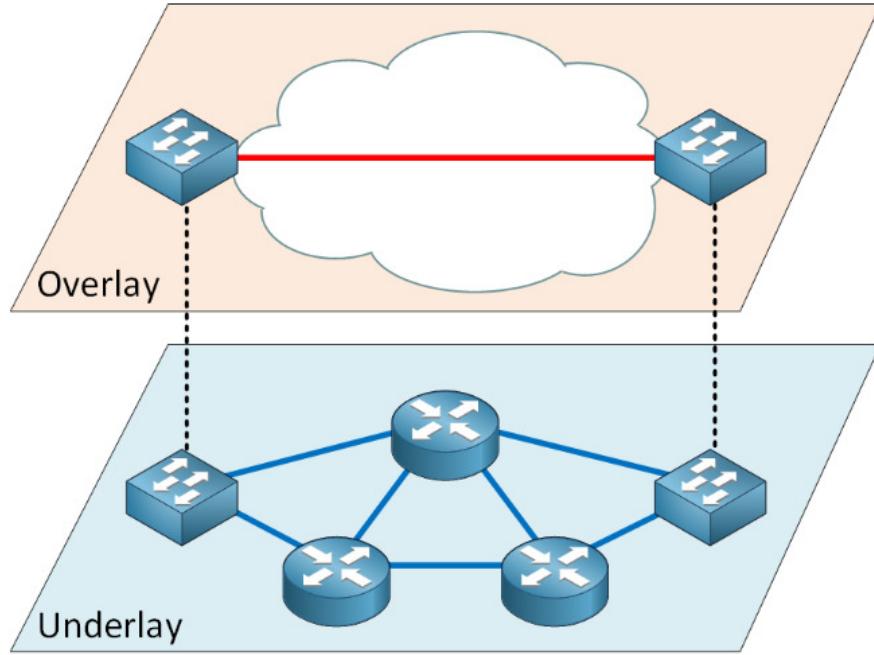


Hình 2.6 Cách hoạt động của VXLAN

Trong hình trên, khi VTEP1 nhận khung Ethernet từ Máy ảo 1 (VM1) được gửi đến Máy ảo 3 (VM3), nó sử dụng VNI và MAC đích để tra cứu trong bảng chuyển tiếp của nó để VTEP gửi gói đến . VTEP1 thêm tiêu đề VXLAN chứa VNI vào khung Ethernet, đóng gói khung trong gói UDP lớp 3 và định tuyến gói đến VTEP2 qua mạng Lớp 3. VTEP2 giải mã khung Ethernet ban đầu và chuyển tiếp nó tới VM3. VM1 và VM3 hoàn toàn không biết về đường hầm VXLAN và mạng Layer 3 giữa chúng.

2.2.3 Overlay và Underlay

Mô hình mạng cho VXLAN được xây dựng dựa trên hai lớp: lớp Underlay và lớp Overlay[6]:



Hình 2.7 Lớp Underlay và lớp Overlay

- **Underlay** Lớp Underlay trong VXLAN chủ yếu tập trung vào cung cấp hạ tầng mạng vật lý để hỗ trợ việc triển khai mạng overlay VXLAN. Underlay đóng vai trò quan trọng trong việc liên kết các VTEP (VXLAN Tunnel Endpoint) và chuyển tiếp gói tin VXLAN trong mạng VXLAN.

Để chuyển tiếp gói tin VXLAN qua mạng Underlay, cần sử dụng các giao thức định tuyến. OSPF (Open Shortest Path First) và IS-IS (Intermediate System to Intermediate System) là những giao thức định tuyến phổ biến, được áp dụng để đảm bảo việc lựa chọn đường đi tối ưu và cung cấp khả năng chuyển tiếp gói tin một cách hiệu quả trong mạng Underlay.

Mạng Underlay có khả năng quảng bá thông tin về địa chỉ IP của các VTEP và định tuyến của mạng VXLAN. BGP (Border Gateway Protocol) và OSPF là những giao thức thường được sử dụng để quảng bá thông tin này trong mạng Underlay.

- **Underlay** Lớp Overlay trong VXLAN là một phần quan trọng trong kiến trúc VXLAN, nó cung cấp mạng ảo Overlay trên mạng Underlay vật lý. Lớp Overlay này cho phép tạo ra các mạng ảo độc lập (Virtual networks) trên mạng vật lý duy nhất, cung cấp khả năng mở rộng và độ phân phối tốt hơn.

Lớp Overlay cho phép tạo ra hàng ngàn mạng ảo độc lập trên một mạng Underlay duy nhất. Điều này mang lại khả năng mở rộng linh hoạt và quản lý hiệu quả cho các mạng ảo trong môi trường Data Center hoặc các mạng lớn. Mỗi mạng ảo trong lớp Overlay có địa chỉ IP, địa chỉ MAC và bảng định tuyến riêng biệt. Điều này tạo điều kiện cho độ phân tách cao giữa các mạng ảo và ngăn chặn sự xung đột hay sự can thiệp giữa chúng.

Trong lớp Overlay, BGP-EVPN (Border Gateway Protocol - Ethernet VPN) là giao thức control plane được sử dụng để phân phối thông tin về địa chỉ MAC (Media Access Control), IP và các thông tin liên quan đến định tuyến[5]. BGP-EVPN cho phép các VTEP trao đổi thông tin về địa chỉ MAC và IP của các thiết bị kết nối trong mạng VXLAN. Điều này giúp xác định địa chỉ đích của các gói tin và cung cấp khả năng di chuyển ảo hóa và cân bằng tải.

2.2.4 Cấu trúc gói tin VXLAN

Hình

Cấu trúc gói tin VXLAN:

- VXLAN Tunnel Endpoint (VTEP) đóng gói các header sau vào khung Ethernet gốc (khung L2 gốc) được gửi bởi VM:
- Header VXLAN: Header VXLAN (8 bytes) chứa trường VNI 24-bit, được sử dụng để xác định các đối tượng thuê khác nhau trên mạng VXLAN. Nó cũng chứa trường VXLAN Flag (8 bit, được đặt thành 00001000) và hai trường dành riêng (lần lượt là 24 bit và 8 bit).

- Header UDP: Header VXLAN và khung Ethernet gốc được sử dụng làm dữ liệu UDP. Trong tiêu đề UDP, số cổng đích (VXLAN Port) được cố định ở mức 4789 và số cổng nguồn (UDP Src. Port) được tính toán bằng thuật toán băm dựa trên khung Ethernet gốc.
- Outer IP Header: Trong Outer IP Header, địa chỉ IP nguồn (Outer Src. IP) là địa chỉ IP của VTEP được kết nối với VM nguồn và địa chỉ IP đích (Outer Dst. IP) là địa chỉ IP của VTEP được kết nối với VM đích.
- Outer MAC Header: Outer MAC Header còn được gọi là Outer Ethernet Header. Trong header này, địa chỉ MAC nguồn (Src. MAC Addr.) là địa chỉ MAC của VTEP được kết nối với VM nguồn và địa chỉ MAC đích (Dst. MAC Addr.) là địa chỉ MAC của bước nhảy tiếp theo dọc theo đường dẫn tới VTEP đích.

VXLAN là một kiểu đóng gói có dùng UDP. Phần tận cùng bên ngoài của gói tin là định dạng chuẩn UDP và như vậy có thể định tuyến được bởi bất kỳ thiết bị IP nào. Phần bên trong là một phần được đóng gói bao gồm toàn bộ một Ethernet frame, địa chỉ MAC nguồn ban đầu, địa chỉ MAC đích và phần Ethernet header nguyên thủy ban đầu, thêm vào đó là gói tin IP được chứa bên trong nó. Cách đóng gói của VXLAN này là quan trọng vì nó có nghĩa là VxLAN là một công nghệ có thể hỗ trợ cho các giải pháp mạng ảo ở cả lớp 2 và lớp 3.

Phần VXLAN header nằm giữa UDP header và phần frame layer 2 nguyên bản. Có hai thông tin rất quan trọng: giá trị SGT (Security Group Tag) và giá trị mạng ảo VNI (Virtual Network Identifier). Kết hợp hai giá trị này lại với nhau, chúng ta sẽ có đủ thông tin về phần gói tin được đóng gói bên trong, đặc biệt các thông tin về các phân đoạn mạng.

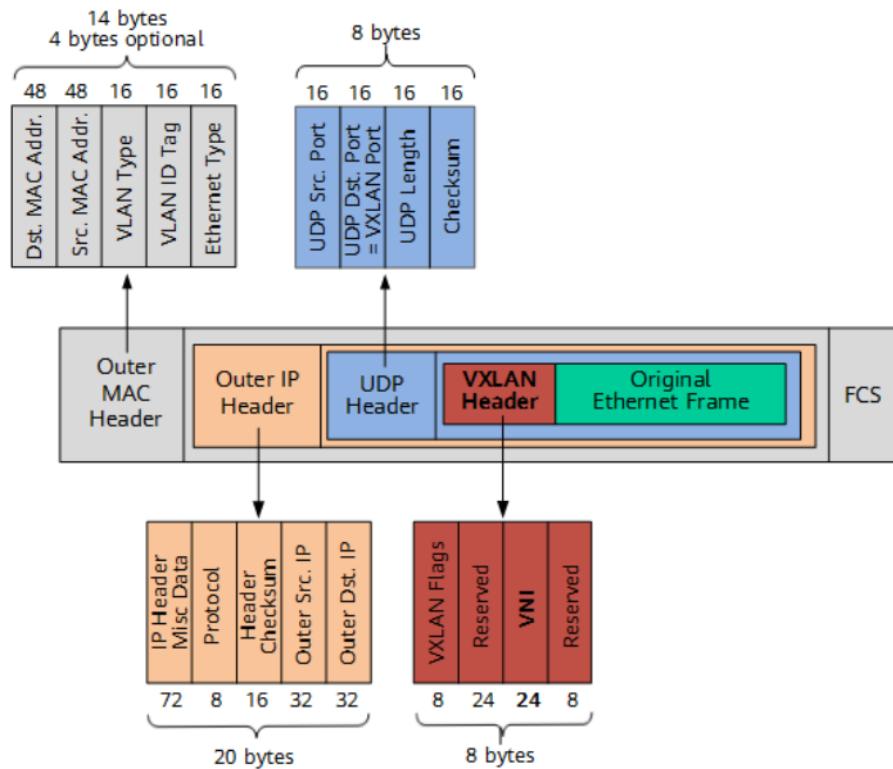
Với việc sử dụng kiểu đóng gói UDP như là header bên ngoài, bất kỳ thiết bị định tuyến IP nào cũng có thể mang một gói tin VXLAN. Địa chỉ IP nguồn trong header này

sẽ là địa chỉ của node mạng đang đóng gói tin vào trong VXLAN (còn được biết đến với tên gọi VXLAN Tunnel Endpoint – VTEP), còn địa chỉ IP đích trong header này sẽ là địa chỉ IP của node mạng sẽ mở gói VXLAN. Với việc sử dụng UDP, các node mạng trung gian không biết, không cần hiểu và không cần diễn dịch các header VXLAN bên trong. Đặc điểm này cho phép VXLAN hoạt động như một lớp trung chuyển bên trên của một hạ tầng mạng IP bên dưới.

2.2.5 Một số khái niệm trong VXLAN

- **VXLAN Tunnel Endpoint (VTEP):**

- Các thiết bị biên trên mạng VXLAN được gọi là VTEP. Điểm cuối hoặc điểm bắt đầu là điểm tại đó các khung dữ liệu người dùng ban đầu được đóng gói hoặc giải mã trong đường hầm VXLAN.



Hình 2.8 VXLAN Tunnel Endpoint (VTEP)

- VTEP có thể là một thiết bị mạng độc lập hoặc một bộ chuyển mạch ảo được triển khai trên máy chủ. Các nguồn VTEP đóng gói các khung dữ liệu gốc được máy chủ nguồn gửi vào các gói VXLAN, sau đó các gói này được gửi đến VTEP đích qua mạng IP. Các gói VXLAN sau đó được VTEP đích giải mã thành các khung dữ liệu gốc và chuyển tiếp đến máy chủ đích.
- Thông qua giao diện IP, thiết bị VTEP cũng phát hiện các VTEP từ xa cho các phân đoạn VXLAN của nó và tìm hiểu ánh xạ từ các địa chỉ MAC từ xa tới VTEP. VTEP là các đơn vị chức năng tạo ra kết nối Lớp 2 qua mạng IP truyền tải dựa trên cấu trúc liên kết logic.
- Các phân đoạn VXLAN không phụ thuộc vào cấu trúc liên kết mạng cơ bản và ngược lại, mạng IP cơ bản giữa các VTEP không phụ thuộc vào lớp phủ VXLAN. Các gói được định tuyến dựa trên tiêu đề địa chỉ IP bên ngoài, trong đó có địa chỉ VTEP khởi tạo là địa chỉ nguồn và địa chỉ VTEP kết thúc làm địa chỉ đích.

- **Virtual Network Identifier(VNI):**

- VNI là giá trị xác định một mạng ảo cụ thể trong mặt phẳng dữ liệu. Nó thường là phần giá trị 24 bit của tiêu đề VXLAN, có thể hỗ trợ tối 16 triệu phân đoạn mạng riêng lẻ. (Giá trị VNI hợp lệ là từ 4096 đến 16.777.215.)[5]
- VNI tương tự như VLAN ID trên mạng truyền thống và nó xác định phân đoạn VXLAN. Người thuê trên các phân đoạn VXLAN khác nhau không thể giao tiếp ở Lớp 2. Một người thuê có thể có một hoặc nhiều VNI.
- Đóng gói gói VXLAN, VNI 24-bit được thêm vào gói VXLAN, cho phép VXLAN cách ly một số lượng lớn người thuê.

2.2.6 Ưu điểm của mô hình triển khai VXLAN

Hỗ trợ nhiều khách hàng trên cùng 1 hệ thống: VXLAN Fabric hỗ trợ nhiều khách hàng trên cả Lớp 2 (mỗi VNID định danh cho 1 khách hàng khác nhau) và Lớp 3 (dùng VRF khác nhau cho từng khách hàng khác nhau).

Tính di động: VXLAN cung cấp khả năng triển khai các mạng Layer 2 overlay trên các mạng Layer 3 sẵn có, cung cấp tính linh hoạt và di động khi thiết kế các mạng Layer 2.

Tăng số lượng segments lớp 2: Các thiết kế dựa trên Vlan bị giới hạn tối đa 4.096 phân đoạn Lớp 2 do sử dụng Vlan ID 12 bit. VXLAN giới thiệu một VNID 24 bit về mặt lý thuyết hỗ trợ tới 16 triệu segments.

Multi-path Layer 2: các mạng lớp 2 chỉ hỗ trợ 1 tuyến đường hoạt động vì STP sẽ Block các đường dự phòng để tránh loop. VXLAN hoạt động dựa trên các mạng Lớp 3 cung cấp nhiều tuyến đường tới đích mà không phụ thuộc vào STP.

2.2.7 Ứng dụng VXLAN

Các trường hợp sử dụng VXLAN cho các nhà cung cấp dịch vụ và nhà cung cấp đám mây là khá rõ ràng: những nhà điều hành này có số lượng lớn người thuê hoặc khách hàng, và có nhiều lý do về pháp lý, quyền riêng tư và bảo mật thông tin khách hàng khiến cho các nhà cung cấp phải phân chia lưu lượng mạng của một khách hàng khỏi khách hàng khác.

Trong môi trường doanh nghiệp, người thuê có thể là một nhóm người dùng, bộ phận hoặc bất kỳ tập hợp nào của người dùng hoặc thiết bị được phân đoạn mạng tạo ra vì lý do bảo mật nội bộ. Ví dụ, các thiết bị Internet of Things (IoT) như cảm biến môi trường trung tâm dữ liệu có thể dễ bị tấn công, vì vậy việc cách ly lưu lượng mạng IoT khỏi lưu lượng ứng dụng mạng sản xuất là một thực hành an toàn.

2.3 Phần mềm EVE-NG

2.3.1 Giới thiệu sơ lược về công cụ EVE-NG

UnetLab (Unified Networking Lab) là một bản phân phối của Linux cho phép bạn xây dựng hệ thống các bài lab network. UNetLab có thể xem như là một hypervisor cho các image thường chạy trên các thiết bị mạng vật lý hoặc các máy ảo tách biệt bên trong.

Nó cho phép triển khai giả lập các thiết bị mạng như switch, router, firewall, ... và các thiết bị cuối để kiểm tra thiết kế, kiểm thử các hoạt động của mô hình lab thực tế.

Điều tuyệt vời về UnetLab (và do đó cũng về EVE-NG) là tất cả mọi thứ được chứa trong một máy ảo, và bạn sử dụng một giao diện web để tạo và quản lý các bài lab bạn. Chỉ cần đẩy image vào đó (EVE-NG hỗ trợ rất nhiều image các thiết bị từ nhiều nhà cung cấp khác nhau), và từ đó cấu hình bắt đầu lab.

EVE-NG (Emulated Virtual Environment – Netx Generation) là phiên bản kế thừa những tính năng mạnh mẽ và vượt trội hơn so với Unetlab.

EVE-NG là một công cụ mô phỏng mạng cung cấp giao diện người dùng thông qua trình duyệt. Người dùng có thể tạo các node mạng từ một thư viện các template sẵn có, kết nối chúng lại với nhau và cấu hình chúng. Người dùng chuyên nghiệp hoặc quản trị viên có thể thêm các image phần mềm vào thư viện và tạo các mẫu các thiết bị mạng tùy chỉnh để hỗ trợ hầu hết các mô hình lab.

EVE-NG hỗ trợ cấu hình nhiều hypervisors trên một máy ảo. Nó chạy phần mềm thiết bị mạng thương mại trên Dynamips và IOU và chạy các thiết bị mạng khác, chẳng hạn như bộ định tuyến router mã nguồn mở, trên QEMU.

Tóm lại, EVE-NG là một phần mềm mạng ảo mạnh mẽ và linh hoạt, cung cấp một môi trường mô phỏng mạng để thử nghiệm, phát triển và kiểm tra các giải pháp mạng. Với khả năng hỗ trợ đa nhà cung cấp, giao diện người dùng đồ họa, tích hợp đám mây,

hỗ trợ SDN và NFV, cùng với khả năng chia sẻ và hợp tác, EVE-NG là một công cụ quan trọng cho các chuyên gia mạng, nhà phát triển và những người quan tâm đến việc nghiên cứu và phát triển các giải pháp mạng tiên tiến.

2.3.2 Một số ưu điểm vượt trội của EVE-NG

Những đặc điểm và tính năng quan trọng của phần mềm EVE-NG:

- Mô phỏng mạng mạnh mẽ: EVE-NG cho phép bạn tạo ra mô hình mạng ảo với hàng trăm thiết bị mạng như router, switch, firewall, máy chủ và nhiều hơn nữa. Bạn có thể tạo ra các mạng LAN, mạng WAN, mạng viễn thông, và thậm chí mạng phân tán phức tạp với EVE-NG. Việc mô phỏng mạng trên EVE-NG giúp bạn thử nghiệm các cấu hình, kiểm tra tính tương thích và giải quyết sự cố mạng một cách an toàn và hiệu quả.
- Hỗ trợ đa nhà cung cấp thiết bị: EVE-NG hỗ trợ nhiều nhà cung cấp thiết bị mạng phổ biến như Cisco, Juniper, Palo Alto, Fortinet, Arista, và nhiều hơn nữa. Điều này cho phép bạn tạo ra môi trường mạng ảo với các thiết bị từ nhiều nhà cung cấp khác nhau và kiểm tra tương tác giữa chúng. EVE-NG cung cấp các ảnh hỗ trợ cho các thiết bị mạng phổ biến, giúp bạn dễ dàng cài đặt và cấu hình chúng trong môi trường mạng ảo.
- Giao diện người dùng đồ họa: EVE-NG có giao diện người dùng trực quan và dễ sử dụng. Bạn có thể kéo và thả các thiết bị mạng, kết nối chúng với nhau, và cấu hình chúng thông qua giao diện đồ họa. Điều này giúp giảm đáng kể thời gian và công sức cần thiết để tạo ra mô hình mạng ảo. EVE-NG cung cấp các công cụ quản lý và giám sát mạng tích hợp, giúp bạn quản lý và theo dõi hiệu suất mạng trong quá trình thử nghiệm và triển khai.
- Tích hợp đám mây: EVE-NG tích hợp với các dịch vụ đám mây như Amazon Web Services (AWS) và Microsoft Azure. Điều này cho phép bạn tạo ra mô hình mạng

kết hợp giữa mạng ảo trên EVE-NG với các dịch vụ đám mây để kiểm tra và triển khai các giải pháp đám mây. Bạn có thể tạo ra các kịch bản mạng phức tạp, kiểm tra tính tương thích với môi trường đám mây, và thực hiện các tác vụ như cấu hình VPN, tạo mạng riêng ảo (VPC), và quản lý tài nguyên đám mây.

- Hỗ trợ SDN và NFV: EVE-NG hỗ trợ các công nghệ mạng mới như mạng quản lý bằng phần mềm (SDN) và mạng chức năng (NFV). Bạn có thể triển khai và kiểm tra các giải pháp SDN và NFV trong môi trường mạng ảo của EVE-NG. EVE-NG cung cấp các hình ảnh và mô-đun hỗ trợ cho các nền tảng SDN phổ biến như Cisco ACI (Application Centric Infrastructure), VMware NSX, và OpenContrail. Bằng cách tích hợp SDN và NFV, bạn có thể thử nghiệm và phát triển các kiến trúc mạng tiên tiến và linh hoạt hơn trong môi trường ảo.
- Chia sẻ và hợp tác: EVE-NG cho phép người dùng chia sẻ và hợp tác trong việc xây dựng và thử nghiệm mạng. Bạn có thể chia sẻ mô hình mạng, bài lab, hướng dẫn và tài liệu tham khảo với cộng đồng người dùng EVE-NG khác. Điều này giúp tạo ra một môi trường học tập và trao đổi kiến thức mạng rộng lớn, nơi mọi người có thể học hỏi và chia sẻ kinh nghiệm của mình.

2.3.3 Cài đặt EVE-NG

- Yêu cầu hệ thống:

Để cài đặt phần mềm EVE-NG, cần có máy tính với hệ điều hành Windows, macOS hoặc Linux. Và cần cài đặt phần mềm VirtualBox.

- Hệ điều hành: Windows 7, 8, 10, macOS 10.10 trở lên, hoặc Linux
- RAM: 16 GB trở lên
- Dung lượng ổ cứng trống: 50 GB trở lên
- Bộ xử lý: Intel Core i5 hoặc tương đương

- Cài đặt máy ảo:

Trước khi cài đặt EVE-NG, cần cài đặt phần mềm VMware Workstation.

- Cài đặt EVE-NG:

Sau khi cài đặt máy ảo, có thể tải xuống EVE-NG từ trang web của EVE-NG. Và tạo máy ảo EVE trên máy ảo VMware.

- Cấu hình EVE-NG:

Sau khi cài đặt EVE-NG, cần cấu hình nó để có thể sử dụng, sau đó:

- Tải các ứng dụng hỗ trợ khi sử dụng EVE như Putty, WinSCP...
- Thêm các images cần thiết để sử dụng các thiết bị trên EVE.
- Cài đặt các server cần thiết.

- Cấu hình thiết bị mạng:

- Sau khi thêm một thiết bị mạng vào dự án, có thể thực hiện cấu hình thiết bị này. Trước tiên là khơi động thiết bị đó lên.
- Sử dụng các tập lệnh CLI để cấu hình thiết bị.

2.4 Bảo mật hệ thống

2.4.1 Giới thiệu

Bảo mật hệ thống mạng là lĩnh vực quan trọng trong công nghệ thông tin, nghiên cứu và triển khai các biện pháp để đảm bảo tính bảo mật và an toàn cho hệ thống mạng máy tính. Bảo mật hệ thống mạng đóng vai trò quan trọng trong việc bảo vệ dữ liệu quan trọng, ngăn chặn truy cập trái phép, đảm bảo quyền riêng tư và ngăn chặn các cuộc tấn công mạng. Có nhiều mối đe dọa bảo mật hệ thống mạng khác nhau, bao gồm:

- Xâm nhập: là hành vi cố gắng truy cập trái phép vào một hệ thống mạng.
- Tấn công: là hành vi sử dụng các kỹ thuật trái phép để gây hại cho một hệ thống mạng.

- Gián điệp: là hành vi thu thập thông tin trái phép từ một hệ thống mạng.
- Phá hoại: là hành vi cố gắng làm hỏng hoặc vô hiệu hóa một hệ thống mạng.

Một hệ thống mạng bảo mật tốt sẽ triển khai một loạt các biện pháp và kỹ thuật để đối phó với các mối đe dọa và cuộc tấn công mạng. Điều này bao gồm xác thực và ủy quyền, sử dụng tường lửa và phân đoạn mạng để kiểm soát lưu lượng mạng, mã hóa thông tin để bảo vệ dữ liệu, sử dụng mạng riêng ảo (VPN) để tạo kết nối an toàn, quản lý xác thực và khóa, giám sát mạng để phát hiện các hoạt động không bình thường, cập nhật và vá lỗi thường xuyên để khắc phục các lỗ hổng bảo mật, bảo vệ chống từ chối dịch vụ (DDoS Protection) và đào tạo người dùng về bảo mật thông tin.

Bảo mật hệ thống mạng là một quá trình liên tục và không ngừng nghỉ. Các mối đe dọa mạng liên tục tiến bộ và phát triển, do đó, các biện pháp bảo mật cũng cần được cải tiến và cập nhật liên tục để đối phó với những mối đe dọa mới.

Trong tổ chức và doanh nghiệp, chuyên gia bảo mật hệ thống đóng vai trò quan trọng trong việc triển khai, giám sát và duy trì tính bảo mật của hệ thống mạng. Các chuyên gia này phải có kiến thức sâu về các công nghệ bảo mật, phân tích mối đe dọa, phục hồi sau sự cố và nắm vững quy trình bảo mật.

2.4.2 Các giải pháp bảo mật mạng

- **IP Filtering (Lọc IP)** hay còn gọi là Packet Filtering, là một kỹ thuật bảo mật mạng sử dụng để kiểm soát và lọc các gói tin dựa trên địa chỉ IP nguồn và đích, cổng giao tiếp, giao thức và các tiêu chí khác. Kỹ thuật này cho phép quản trị viên mạng quyết định xem gói tin nào được chấp nhận hoặc từ chối dựa trên các quy tắc xác định trước. IP Filtering thường được triển khai trên các tường lửa mạng để ngăn chặn truy cập trái phép hoặc các cuộc tấn công từ các địa chỉ IP cụ thể.
- **NAT: Network Address Translation (Chuyển đổi địa chỉ mạng)** là một kỹ thuật được sử dụng để chuyển đổi địa chỉ IP của các gói tin trong mạng. Nó cho phép

nhiều máy tính trong mạng nội bộ chia sẻ một địa chỉ IP công cộng duy nhất. Khi các gói tin đi ra ngoài mạng, NAT sẽ thay đổi địa chỉ IP nguồn của chúng thành địa chỉ IP công cộng của mạng. Khi các gói tin trả về từ bên ngoài, NAT sẽ dịch ngược và chuyển gói tin đến máy tính trong mạng nội bộ tương ứng.

- **IPSec: IP Security Architecture (Kiến trúc IP an toàn)** là một kiến trúc bảo mật mạng được sử dụng để bảo vệ tính bảo mật và toàn vẹn của dữ liệu truyền qua mạng. Nó cung cấp các phương thức mã hóa và xác thực để đảm bảo rằng thông tin truyền đi không bị xâm phạm và chỉ có người được ủy quyền mới có thể truy cập vào nó. IPSec được sử dụng phổ biến trong việc thiết lập các kết nối VPN (Virtual Private Network) an toàn và bảo mật.
- **Application Proxies (Proxy ứng dụng)** hay còn gọi là Application-level Gateways, là các thành phần trung gian giữa người dùng và một dịch vụ hoặc ứng dụng trên mạng. Các Proxy ứng dụng hoạt động theo cách thức của một ứng dụng, giúp kiểm soát và giám sát các giao tiếp giữa người dùng và dịch vụ mục tiêu. Proxy ứng dụng có thể thực hiện các chức năng như lọc gói tin, kiểm tra xác thực, kiểm soát truy cập và ghi lại hoạt động mạng.
- **Firewalls (Tường lửa)** là một hệ thống phần cứng hoặc phần mềm được sử dụng để kiểm soát và giám sát lưu lượng mạng vào và ra khỏi một mạng. Nó áp dụng các quy tắc và chính sách bảo mật để ngăn chặn truy cập trái phép, tấn công mạng và lọc các gói tin không mong muốn. Firewalls có thể hoạt động ở nhiều tầng của mô hình OSI và có thể sử dụng các phương pháp như IP Filtering, Stateful Inspection và Application-level Gateway để kiểm soát lưu lượng mạng.
- **Tunnel Protocols (Các giao thức đường hầm)** là các giao thức được sử dụng để tạo ra các đường hầm ảo (tunnels) thông qua mạng công cộng hoặc mạng không tin cậy như Internet. Các đường hầm này cho phép truyền dữ liệu an toàn và bảo

mật giữa hai hoặc nhiều điểm cuối trong mạng. Giao thức đường hầm giúp bảo vệ dữ liệu bằng cách mã hóa và đóng gói các gói tin gốc trong gói tin mới có địa chỉ đích và nguồn mới, đi qua các đường hầm mạng công cộng và được giải mã và giải nén tại điểm cuối.

- **SOCKS** là một chuẩn cho các gateway circuit-level. Nó không cần proxy nhưng người sử dụng có thể thực hiện kết nối đến Firewall trước, sau đó yêu cầu một kết nối thứ hai đến server đích. Người sử dụng khởi tạo một ứng dụng client với địa chỉ IP của server đích. Thay vì khởi tạo một session trực tiếp với server đích, client khởi tạo một session đến SOCKS server trên Firewall. Sau đó SOCKS sẽ xác nhận tính hợp lệ của địa chỉ nguồn và user ID, nếu hợp lệ sẽ cho phép user thiết lập kết nối hướng đến mạng không an toàn (non-secure)/bên ngoài, và rồi tạo một session thứ hai.
- **SSH: Secure Shell** Có thể được sử dụng để kết nối an toàn giữa các hệ thống. Nó cho phép mã hoá và nén các traffic được sinh ra bởi TELNET, FTP, POP3,... SSH thường sử dụng nén trên các liên kết modem tốc độ chậm. SSH cũng cho phép người sử dụng chọn lựa phương pháp mã hoá khi cài đặt nó. Các phần mềm client thường hỗ trợ cả 2 SSH là SSH1 (DES, 3DES, RC4), SSH2 (3DES, RC4). Người sử dụng và các hệ thống ở xa được xác thực bởi password hoặc khoá public/private. SSH thiết lập một kết nối đơn từ client đến server, tất cả traffic gửi qua kết nối này đều được mã hoá, và có thể được nén.
- **SSL:**

Secure Sockets Layer: Là một giao thức an toàn được phát triển bởi tập đoàn Netscap Communications và RSA Data Security. Mục tiêu chính của giao thức SSL là cung cấp một kênh riêng giữa các ứng dụng truyền thông cần có sự xác thực các đối tác truyền thông và đảm bảo tính toàn vẹn và riêng tư của dữ liệu.

SSL cung cấp một sự thay thế cho các socket API chuẩn TCP/IP, trong đó có cài đặt các tính năng an toàn. Do đó, về lý thuyết nó có thể chạy bất kỳ ứng dụng TCP/IP nào trong một môi trường an toàn mà không cần thay đổi ứng dụng. SSL thường được cài đặt để hỗ trợ các traffic như HTTP, NNTP, Telnet, ...

CHƯƠNG 3 - KHẢO SÁT YÊU CẦU HỆ THỐNG

3.1 Phân tích yêu cầu của trường học

3.1.1 Xác định các thông tin phạm vi trường học

Khảo sát quy mô hệ thống mạng của một trường đại học vừa và nhỏ muốn phát triển hệ thống mạng để phục vụ nhu cầu ngày càng tăng của cộng đồng đại học. Trường này mong muốn cung cấp môi trường giảng dạy chất lượng cao thông qua sự kết hợp linh hoạt giữa học trực tuyến và học tại trường. Hiện tại trường đang có nhu cầu xây dựng một hệ thống mạng mạng ảo cho giảng dạy và học tập. Dự án thiết kế mạng LAN sử dụng kỹ thuật VXLAN được triển khai nhằm nâng cao hiệu suất mạng, cung cấp tính linh hoạt cao cho giáo viên và học sinh trong việc truy cập tài nguyên mạng ảo. Mục tiêu chính là tạo ra một hệ thống mạng an toàn, có thể mở rộng và tích hợp tốt với cơ sở hạ tầng hiện tại của trường, từ đó tối ưu hóa trải nghiệm học tập và giảng dạy trong môi trường ảo.

Quy mô hệ thống:

Trụ sở chính tại TP. Hồ Chí Minh và chi nhánh ở Cần Thơ. Trụ sở chính gồm 3 tòa chính A, B, C và chi nhánh có 1 tòa D:

- Tòa A có các phòng ban: phòng hành chính, phòng đào tạo, phòng tuyển sinh và phòng lab.
- Tòa B có các phòng ban: phòng khoa xã hội và nhân văn, khoa dược, khoa ngoại ngữ, khoa tài chính ngân hàng và các lớp học.
- Tòa C có các phòng ban: phòng kỹ thuật, phòng khoa công nghệ thông tin, khoa quản trị kinh doanh; các phòng học và thư viện.
- Tòa D có các phòng ban: phòng kỹ thuật, văn phòng khoa; các phòng học và thư viện.

Số lượng người sử dụng:

- Sinh viên: Hơn 6,000 sinh viên.
- Giảng viên và nhân viên: Gần 300 người, bao gồm giảng viên, nhân viên hành chính và đội ngũ quản lý.

3.1.2 Yêu cầu người dùng

- Khả năng kết nối và truy cập:
 - Truy cập dễ dàng: Khả năng truy cập mạng và tài nguyên một cách dễ dàng từ bất kỳ đâu, bất kỳ thiết bị nào.
 - Kết nối ổn định: Yêu cầu mạng ổn định và có băng thông đủ để hỗ trợ các hoạt động giảng dạy và học tập trực tuyến.
- An toàn và bảo mật:
 - Bảo mật tài khoản và đăng nhập: Có chính sách đăng nhập an toàn, cũng như khả năng bảo mật tài khoản.
 - Quyền riêng tư: Yêu cầu đảm bảo sự riêng tư của thông tin tổ chức và dữ liệu tổ chức trong quá trình sử dụng mạng và các ứng dụng liên quan.
 - Chia sẻ dữ liệu nội bộ.
- Trải nghiệm: Tương Thích Đa Nền Tảng: Yêu cầu khả năng sử dụng trên nhiều nền tảng và thiết bị, bao gồm cả máy tính, điện thoại di động và máy tính bảng.
- Khả năng mở rộng:
 - Mở rộng dễ dàng: Có thể đề xuất yêu cầu về khả năng mở rộng để hỗ trợ sự phát triển và mở rộng trong tương lai.
 - Khả năng thích nghi: Yêu cầu hệ thống có khả năng thích nghi để đáp ứng với các yêu cầu và thay đổi của môi trường giáo dục.

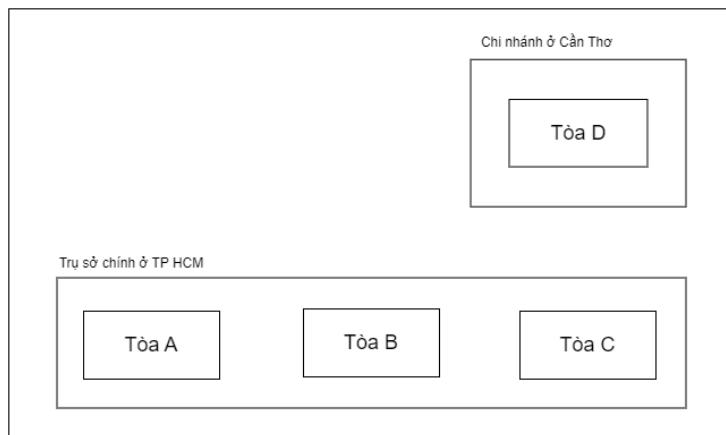
- Chất lượng dịch vụ:

- Độ ổn định và hiệu suất: Yêu cầu độ ổn định và hiệu suất cao khi sử dụng các ứng dụng và tài nguyên trên mạng.
- Hỗ trợ kỹ thuật: Đòi hỏi sự hỗ trợ kỹ thuật nhanh chóng để giải quyết mọi vấn đề kỹ thuật phát sinh.

3.1.3 *Yêu cầu về bảo mật*

- Quản lý quyền VXLAN: Chặn và quản lý quyền truy cập vào các mạng ảo được tạo bởi VXLAN để đảm bảo chỉ người dùng được ủy quyền mới có thể truy cập.
- Áp dụng mã hóa cho dữ liệu lưu trữ trên các thiết bị và máy chủ để ngăn chặn truy cập trái phép.
- Kiểm soát truy cập tới tạng ảo: Sử dụng kiểm soát truy cập (ACLs) để quản lý và kiểm soát truy cập vào các mạng ảo được tạo bởi VXLAN.
- Quản lý quyền truy cập người dùng: Thiết lập quyền truy cập dựa trên vai trò của người dùng để giảm rủi ro từ việc truy cập không ủy quyền.
- Triển khai firewall để kiểm soát lưu lượng mạng và sử dụng hệ thống phát hiện và ngăn chặn xâm nhập để đối phó với các mối đe dọa.
- Yêu cầu các biện pháp phòng ngừa để đối phó với tấn công mạng và bảo vệ khỏi sự gián đoạn dịch vụ.
- Thực hiện kiểm tra an ninh vật lý định kỳ để đảm bảo rằng các thiết bị và máy chủ đều được bảo vệ vật lý.
- Hạn chế truy cập vật lý vào các trung tâm dữ liệu và phòng máy chủ.
- Cập nhật định kỳ: Duy trì chính sách cập nhật định kỳ cho hệ thống.

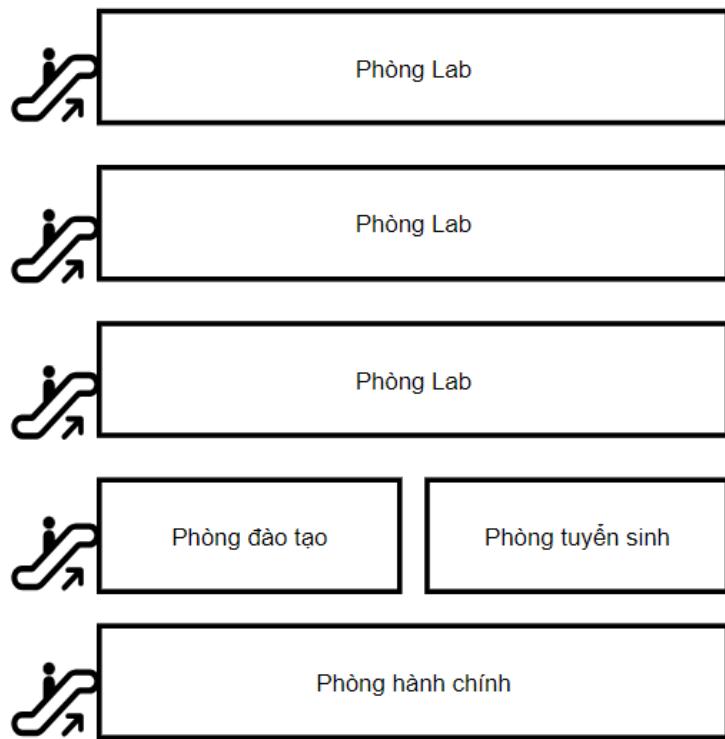
3.1.4 Sơ đồ cấu trúc trường học



Hình 3.1 Sơ đồ tổng quan cấu trúc trường

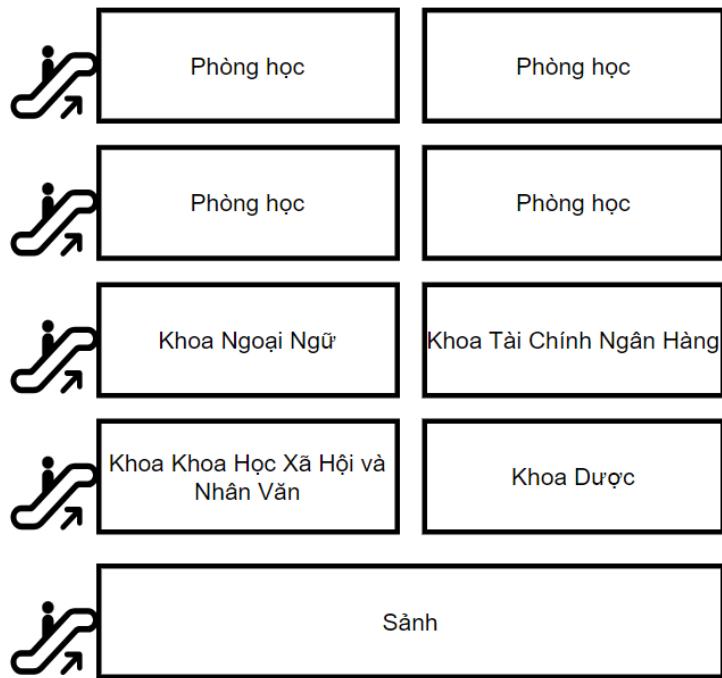
Sơ đồ kiến trúc của trường:

- Trụ sở chính: Tòa A



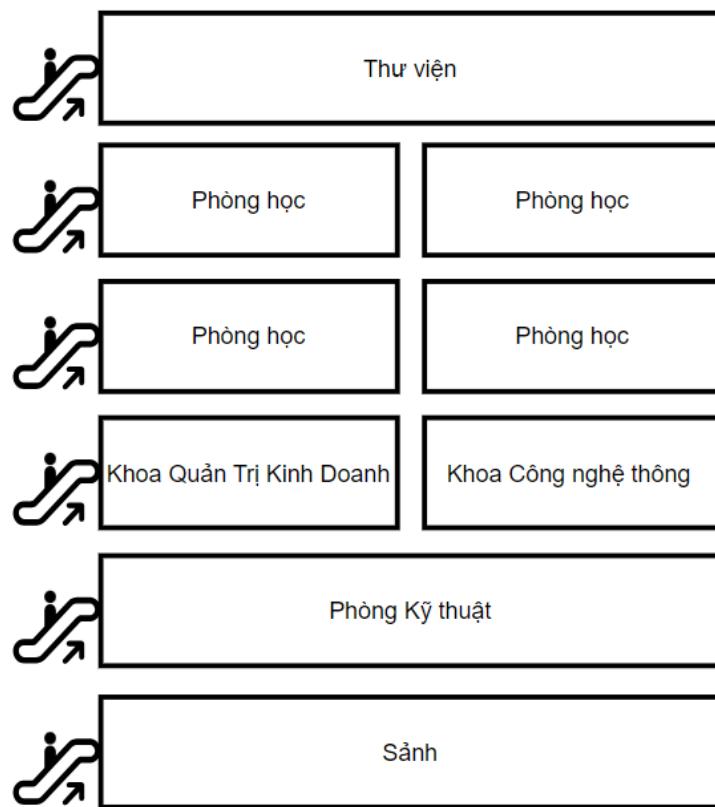
Hình 3.2 Sơ đồ kiến trúc của tòa A ở trụ sở chính

- Trụ sở chính: Tòa B



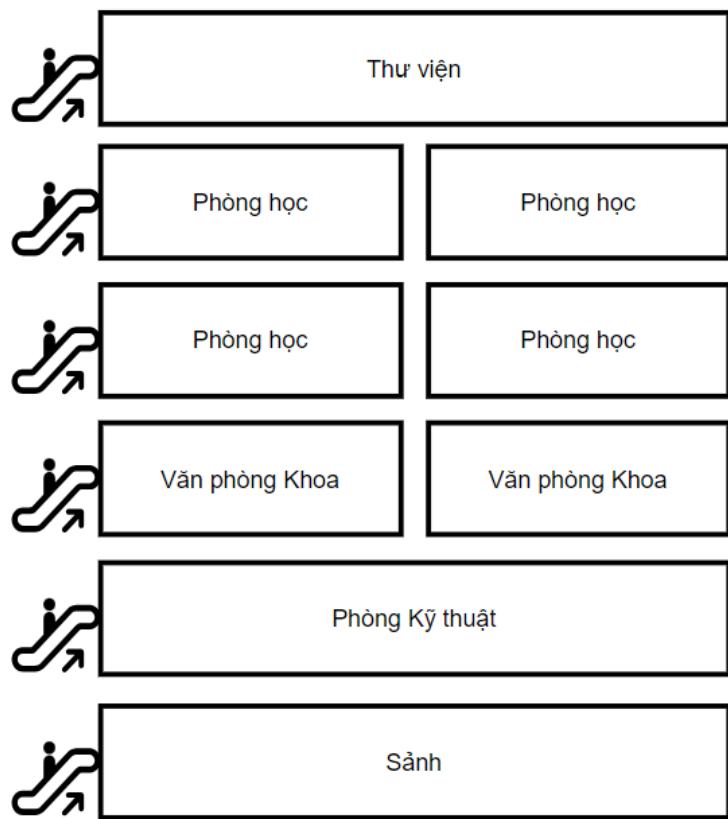
Hình 3.3 Sơ đồ kiến trúc của tòa B ở trụ sở chính

- Trụ sở chính: Tòa C



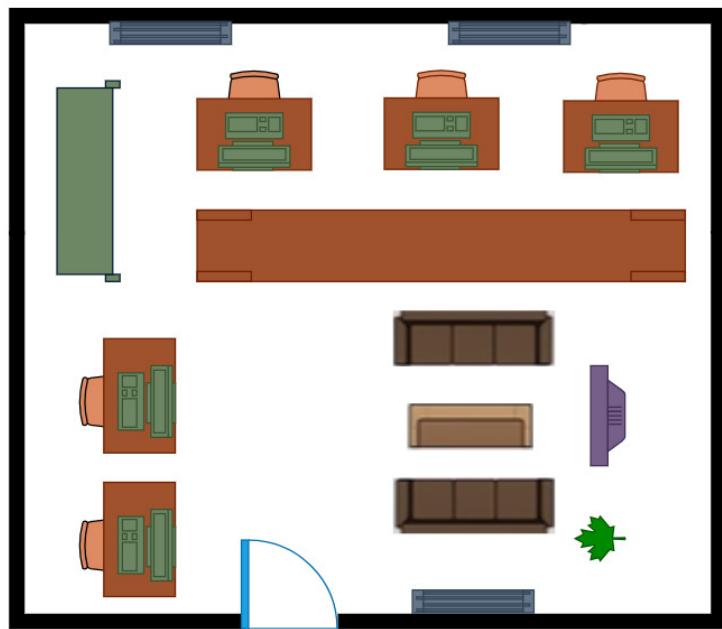
Hình 3.4 Sơ đồ kiến trúc của tòa C ở trụ sở chính

- Chi nhánh:

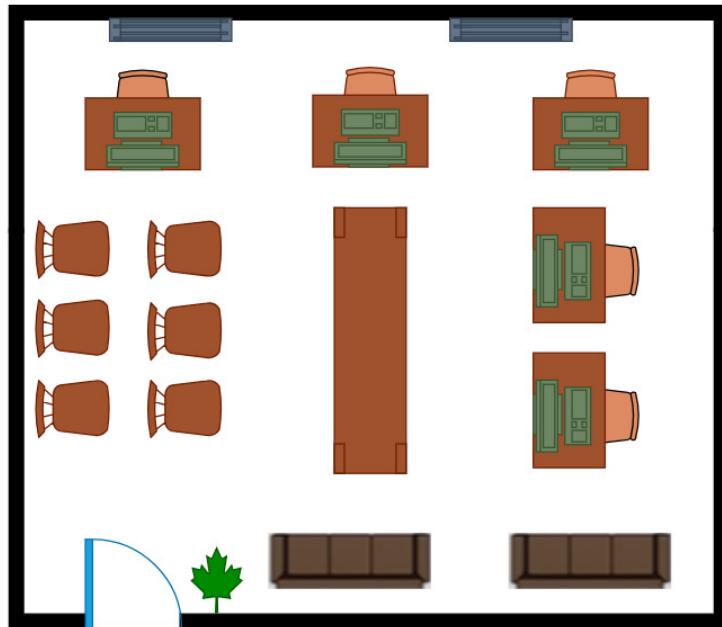


Hình 3.5 Sơ đồ kiến trúc của toà D ở chi nhánh

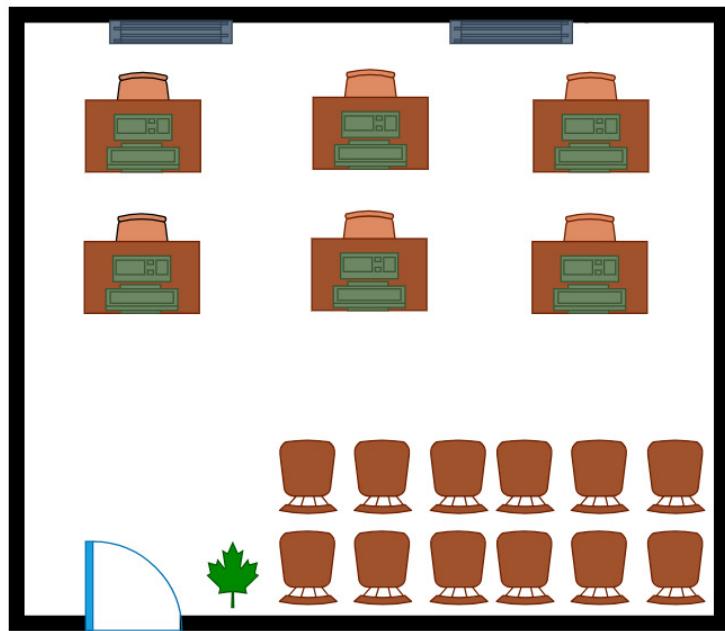
Mặt cắt bằng của các phòng:



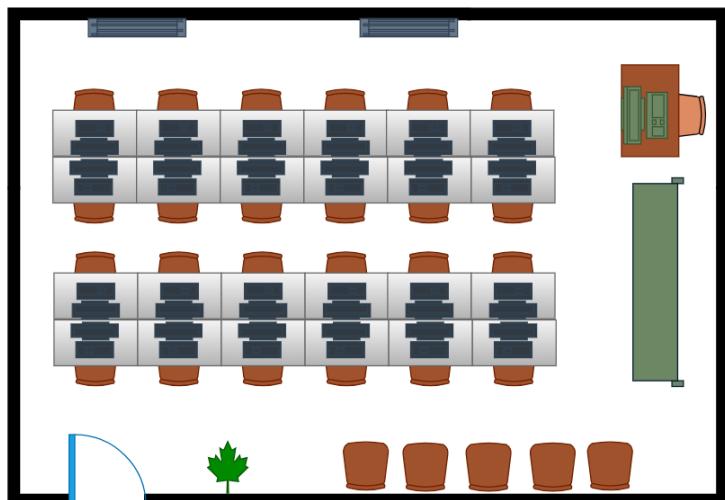
Hình 3.6 Mặt cắt bằng của phòng Hành chính



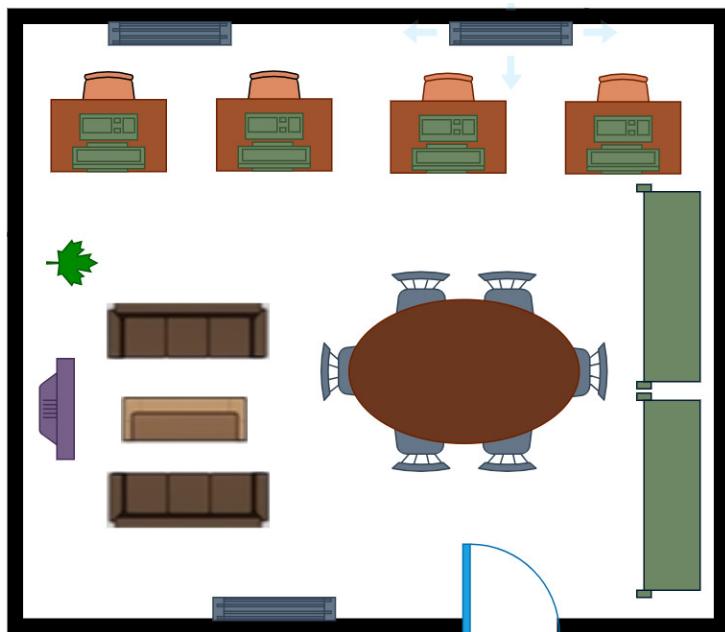
Hình 3.7 Mặt cắt bằng của phòng đào tạo



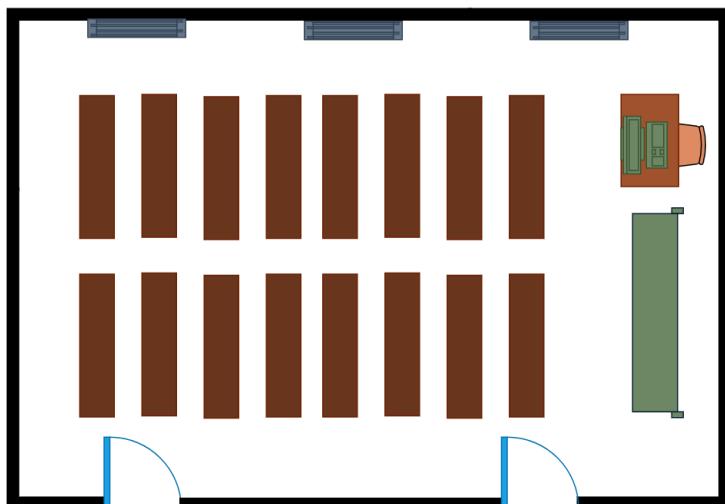
Hình 3.8 Mặt cắt bằng của phòng tuyển sinh



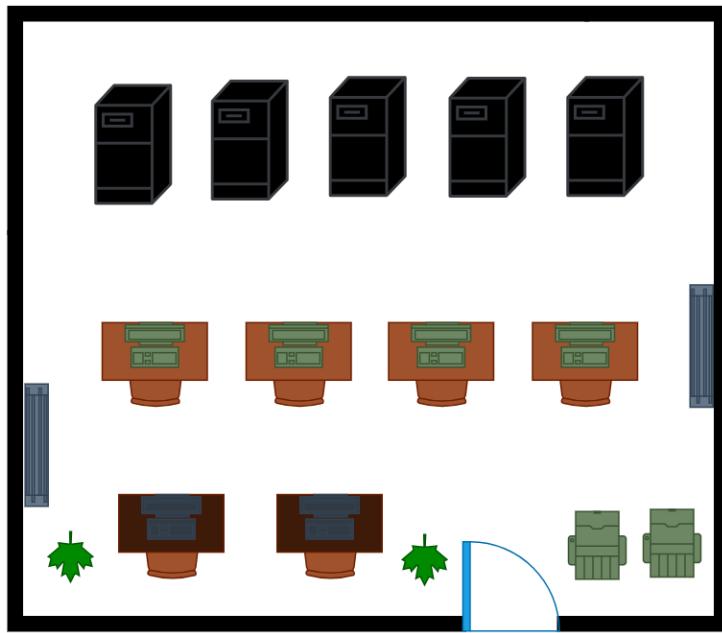
Hình 3.9 Mặt cắt bằng của phòng lab



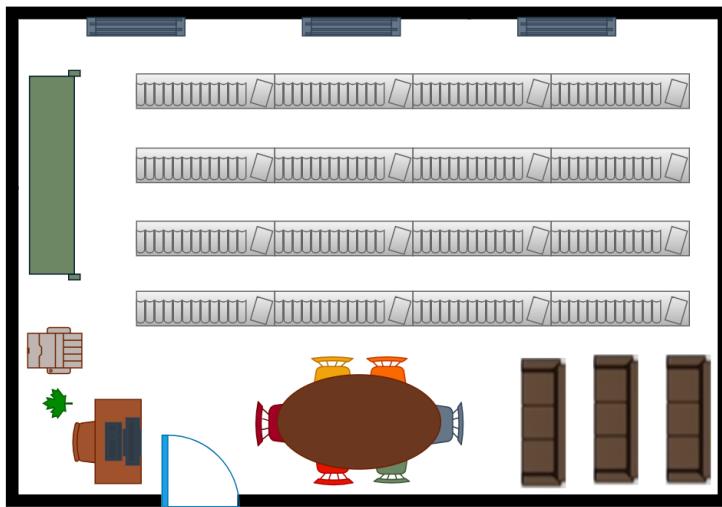
Hình 3.10 Mặt cắt băng của văn phòng khoa



Hình 3.11 Mặt cắt băng của phòng học



Hình 3.12 Mặt cắt bằng của phòng kỹ thuật



Hình 3.13 Mặt cắt bằng của thư viện

3.2 Mục tiêu xây dựng hệ thống mạng

- Sử dụng kỹ thuật VXLAN để tạo mạng ảo và chia thành các môi trường học tập độc lập tạo ra một môi trường học tập linh hoạt và tiện ích, hỗ trợ cả giảng dạy

trực tuyến và học tập từ xa.

- Triển khai các biện pháp bảo mật như mã hóa dữ liệu, xác thực đa yếu tố, và quản lý ủy quyền chặt chẽ để bảo vệ thông tin cá nhân và đảm bảo an toàn cho dữ liệu giáo dục quan trọng.
- Tối ưu hóa băng thông, sử dụng công nghệ hiệu suất cao, và kiểm soát tốc độ dữ liệu để giữ cho mạng hoạt động mượt mà để cung cấp một hạ tầng mạng hiệu suất cao để đảm bảo trải nghiệm mượt mà cho cả giáo viên và sinh viên.
- Sử dụng VXLAN để tạo mạng ảo và đảm bảo khả năng mở rộng dễ dàng khi nhu cầu tăng lên.
- Thực hiện kiểm tra an ninh vật lý định kỳ, giới hạn truy cập vật lý và thiết lập các biện pháp an ninh vật lý để bảo vệ hạ tầng vật lý và đảm bảo an ninh cho các thiết bị và máy chủ.

3.3 Định hướng thiết kế hệ thống

- Sử dụng EVE-NG để xây dựng, thử nghiệm và kiểm tra topology của hệ thống mạng trước khi triển khai nó trong môi trường thực tế. EVE-NG hỗ trợ giả lập nhiều thiết bị mạng phổ biến từ nhiều nhà cung cấp khác nhau, bao gồm Cisco, Juniper, VMware,... Điều này giúp mô phỏng các thiết bị thực tế sẽ được triển khai trong mạng VXLAN.
- Sử dụng VLAN để phân loại và phân đoạn mạng trong trường học. Các VLAN có thể được thiết lập cho từng khoa, tòa nhà, giúp cô lập và quản lý hiệu quả lưu lượng mạng. Sử dụng VLAN để quản lý địa chỉ IP trong mỗi VLAN riêng biệt giúp đơn giản hóa quá trình quản lý IP và ngăn chặn xung đột địa chỉ IP giữa các phân đoạn mạng. VLAN giúp tối ưu hóa hiệu suất mạng bằng cách giảm lưu lượng broadcast và multicast. Các VLAN cô lập broadcast chỉ đến thành viên trong cùng một VLAN, giảm tải trên mạng.

- Sử dụng VXLAN giúp cung cấp mạng ảo linh hoạt và dễ quản lý cho các máy ảo trong môi trường ảo hóa. Nó giúp loại bỏ các hạn chế về kích thước VLAN (4096 VLAN IDs) và tăng cường khả năng mở rộng. VXLAN được sử dụng để tạo ra môi trường đa người dùng, giúp cung cấp dịch vụ đa người dùng mà không gây xung đột về không gian địa chỉ IP hay VLAN. Cấu hình VXLAN interface trên Spine và Leaf, xác định VXLAN ID cho từng VLAN, tạo ra các tunnel giữa chúng để chuyển lưu lượng mạng. Sử dụng các giao thức như BGP hoặc mô hình unicast, các VXLAN tunnels được kết nối, tạo nên một hệ thống mạng hiệu suất cao và có khả năng mở rộng dễ dàng.
- Các dịch vụ mạng: Sử dụng DHCP server để tự động cấp phát địa chỉ IP động trong hệ thống, giúp đơn giản hóa quản lý địa chỉ IP và tăng tính linh hoạt của mạng. Sử dụng Web server để thực hiện khả năng truyền thông nội bộ thông qua trang web, tạo điều kiện thuận lợi cho việc chia sẻ thông tin và tương tác trong môi trường nội bộ. Sử dụng Mail server để gửi mail nội bộ nhanh chóng và an toàn, đảm bảo tính hiệu quả trong giao tiếp nội bộ trong tổ chức. Sử dụng DNS server để phân giải tên miền trang web, giúp người dùng truy cập trang web dễ dàng và nhanh chóng thông qua việc chuyển đổi tên miền thành địa chỉ IP tương ứng. Sử dụng FTP server để quản lý file, với tính năng sao lưu và hồi phục, nhằm đảm bảo an toàn cho dữ liệu và thuận tiện trong việc chia sẻ tệp tin.
- Sử dụng tường lửa và tích hợp anti-virus để ngăn chặn sự tấn công từ kẻ thù, bảo vệ hệ thống khỏi các mối đe dọa và đảm bảo hoạt động ổn định và an toàn.
- Sử dụng NAT để che giấu địa chỉ IP nội bộ và cung cấp bảo vệ cho mạng khỏi các cuộc tấn công từ bên ngoài.
- Sử dụng VPN để tạo kênh kết nối an toàn giữa các chi nhánh hoặc người dùng từ xa và mạng nội bộ. Điều này giúp bảo vệ dữ liệu truyền qua mạng công cộng và

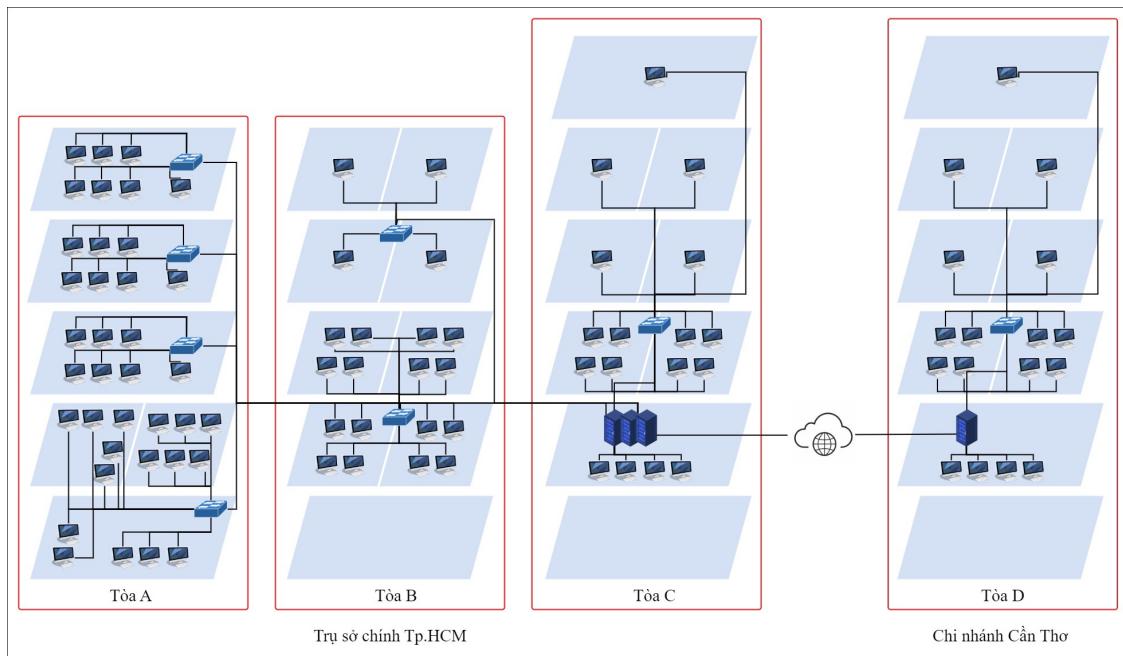
tăng cường tính riêng tư.

- Triển khai hệ thống IDS và IPS để phát hiện và ngăn chặn các hành vi tấn công độc hại. IDS theo dõi và báo cáo về các sự cố, trong khi IPS có thể thực hiện các biện pháp tự động để ngăn chặn sự tấn công.

CHƯƠNG 4 - PHÂN TÍCH THIẾT KẾ HỆ THỐNG

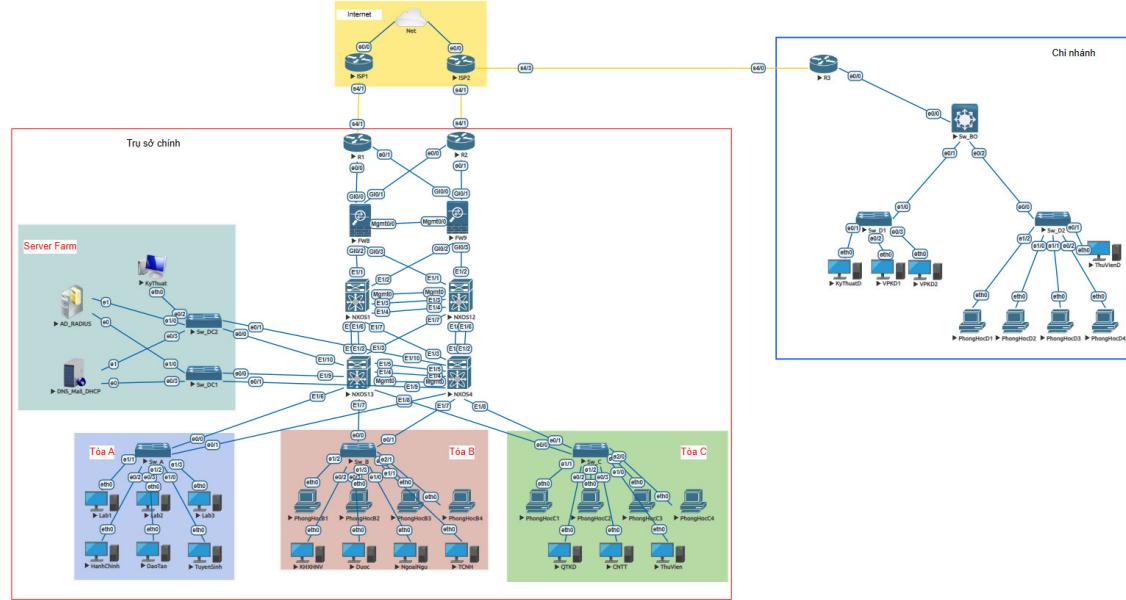
4.1 Thiết kế mô hình mạng

4.1.1 Sơ đồ vật lý



Hình 4.1 Sơ đồ vật lý

4.1.2 Sơ đồ luân lý



Hình 4.2 Sơ đồ luân lý

4.2 Thông tin cài đặt cấu hình hệ thống

4.2.1 Thông tin VLAN, VXLAN trong hệ thống

Bảng 4.1 Thông tin VLAN, VXLAN trong hệ thống

Tên VLAN	VLAN ID	VXLAN ID	Mô tả	Subnet	Default Gateway
Trụ sở chính TP.HCM					
HanhChinh	11	10011	VLAN cho các thiết bị thuộc phòng hành chính	172.16.11.0/26	172.16.11.3

Bảng 4.1 Thông tin VLAN, VXLAN trong hệ thống

Tên VLAN	VLAN ID	VXLAN ID	Mô tả	Subnet	Default Gateway
DaoTao	12	10012	VLAN cho các thiết bị thuộc phòng đào tạo	172.16.12.0/26	172.16.12.3
TuyenSinh	13	10013	VLAN cho các thiết bị thuộc phòng tuyển sinh	172.16.13.0/26	172.16.13.3
Lab	14	10014	VLAN cho các thiết bị thuộc phòng lab	172.16.14.0/26	172.16.14.3
KHXHNV	15	10015	VLAN cho các thiết bị thuộc khoa khoa học xã hội nhân văn	172.16.15.0/26	172.16.15.3
Duoc	16	10016	VLAN cho các thiết bị thuộc khoa dược	172.16.16.0/26	172.16.16.3
NgoaiNgu	17	10017	VLAN cho các thiết bị thuộc khoa ngoại ngữ	172.16.17.0/26	172.16.17.3

Bảng 4.1 Thông tin VLAN, VXLAN trong hệ thống

Tên VLAN	VLAN ID	VXLAN ID	Mô tả	Subnet	Default Gateway
TCNH	18	10018	VLAN cho các thiết bị thuộc khoa tài chính ngân hàng	172.16.18.0/26	172.16.18.3
PhongHocB	19	10019	VLAN cho các thiết bị thuộc phòng học tòa B	172.16.19.0/27	172.16.19.3
QTKD	20	10020	VLAN cho các thiết bị thuộc khoa quản trị kinh doanh	172.16.20.0/26	172.16.20.3
CNTT	21	10021	VLAN cho các thiết bị thuộc khoa công nghệ thông tin	172.16.21.0/26	172.16.21.3
ThuVien	22	10022	VLAN cho các thiết bị thuộc thư viện	172.16.22.0/24	172.16.22.3

Bảng 4.1 Thông tin VLAN, VXLAN trong hệ thống

Tên VLAN	VLAN ID	VXLAN ID	Mô tả	Subnet	Default Gateway
PhongHocC	23	10023	VLAN cho các thiết bị thuộc phòng học tòa C	172.16.23.0/27	172.16.23.3
KyThuat	99	10099	VLAN cho các thiết bị thuộc phòng kỹ thuật	172.16.99.0/24	172.16.99.3
Chi nhánh Cần Thơ					
KyThuat_CT	109		VLAN cho các thiết bị thuộc phòng kỹ thuật tại chi nhánh Cần Thơ	172.17.109.0/24	172.17.109.1
VPK	24		VLAN cho các thiết bị thuộc phòng văn phòng khoa	172.17.24.0/26	172.17.24.1
ThuVien_CT	25		VLAN cho các thiết bị thuộc thư viện tại chi nhánh Cần Thơ	172.17.25.0/24	172.17.25.1

Bảng 4.1 Thông tin VLAN, VXLAN trong hệ thống

Tên VLAN	VLAN ID	VXLAN ID	Mô tả	Subnet	Default Gateway
PhongHocD	26		VLAN cho các thiết bị thuộc phòng học tại chi nhánh Cần Thơ	172.17.26.0/27	172.17.26.1

4.2.2 Thông tin kết nối port trong hệ thống**Bảng 4.2 Thông tin kết nối port trong hệ thống**

Source		Destination		VLAN/Port-channel
Tên thiết bị	Interface	Tên thiết bị	Interface	
Trụ sở chính TP.HCM				
R1	s4/1	ISP1	s4/1	
	e0/0	FW1	g0/0	
	e0/1	FW2	g0/0	
R2	s4/1	ISP2	s4/1	
	e0/0	FW1	g0/1	
	e0/1	FW2	g0/1	
FW1	m0/0	FW2	m0/0	
	g0/0	R1	e0/0	
	g0/1	R2	e0/0	
	g0/2	NXOS1	e1/1	
	g0/3	NXOS2	e1/1	

Bảng 4.2 Thông tin kết nối port trong hệ thống

Source		Destination		VLAN/Port-channel
Tên thiết bị	Interface	Tên thiết bị	Interface	
FW2	m0/0	FW1	m0/0	
	g0/0	R1	e0/0	
	g0/1	R2	e0/0	
	g0/2	NXOS1	e1/1	
	g0/3	NXOS2	e1/2	
NXOS1	e1/1	FW1	g0/2	
	e1/2	FW2	g0/2	
	e1/3	NXOS2	e1/3	Po51
	e1/4	NXOS2	e1/4	
	e1/5	NXOS3	e1/1	
	e1/6	NXOS3	e1/2	
	e1/7	NXOS4	e1/3	
NXOS2	e1/1	FW1	g0/3	
	e1/2	FW2	g0/3	
	e1/3	NXOS1	e1/3	Po51
	e1/4	NXOS1	e1/4	
	e1/5	NXOS4	e1/1	
	e1/6	NXOS4	e1/2	
	e1/7	NXOS3	e1/3	

Bảng 4.2 Thông tin kết nối port trong hệ thống

Source		Destination		VLAN/Port-channel
Tên thiết bị	Interface	Tên thiết bị	Interface	
NXOS3	e1/1	NXOS1	e1/5	
	e1/2	NXOS1	e1/6	
	e1/3	NXOS2	e1/7	
	e1/4	NXOS4	e1/4	Po54
	e1/5	NXOS4	e1/5	
	e1/6	Sw_A	e0/0	Po1
	e1/7	Sw_B	e0/0	Po2
	e1/8	Sw_C	e0/0	Po3
	e1/9	Sw_DC1	e0/0	Po4
	e1/10	Sw_DC2	e0/0	Po5
NXOS4	e1/1	NXOS2	e1/5	
	e1/2	NXOS2	e1/6	
	e1/3	NXOS1	e1/7	
	e1/4	NXOS3	e1/4	Po54
	e1/5	NXOS3	e1/5	
	e1/6	Sw_A	e0/1	Po1
	e1/7	Sw_B	e0/2	Po2
	e1/8	Sw_C	e0/3	Po3
	e1/9	Sw_DC1	e0/4	Po4
	e1/10	Sw_DC2	e0/5	Po5

Bảng 4.2 Thông tin kết nối port trong hệ thống

Source		Destination		VLAN/Port-channel
Tên thiết bị	Interface	Tên thiết bị	Interface	
Sw_A	e0/0	NXOS3	e1/6	Po1
	e0/1	NXOS4	e1/6	
	e0/2	HanhChinh	eth0	VLAN 11
	e0/3	DaoTao	eth0	VLAN 12
	e1/0	TuyenSinh	eth0	VLAN 13
	e1/1	Lab1	eth0	VLAN 14
	e1/2	Lab2	eth0	VLAN 14
	e1/3	Lab3	eth0	VLAN 14
Sw_B	e0/0	NXOS3	e1/7	Po2
	e0/1	NXOS4	e1/7	
	e0/2	KHXHNV	eth0	VLAN 15
	e0/3	Duoc	eth0	VLAN 16
	e1/0	NgoaiNgu	eth0	VLAN 17
	e1/1	TCNH	eth0	VLAN 18
	e1/2	PhongHocB1	eth0	VLAN 19
	e1/3	PhongHocB2	eth0	VLAN 19
	e2/0	PhongHocB3	eth0	VLAN 19
	e2/1	PhongHocB4	eth0	VLAN 19

Bảng 4.2 Thông tin kết nối port trong hệ thống

Source		Destination		VLAN/Port-channel
Tên thiết bị	Interface	Tên thiết bị	Interface	
Sw_C	e0/0	NXOS3	e1/8	Po3
	e0/1	NXOS4	e1/8	
	e0/2	QTKD	eth0	VLAN 20
	e0/3	CNTT	eth0	VLAN 21
	e1/0	ThuVien	eth0	VLAN 22
	e1/1	PhongHocC1	eth0	VLAN 23
	e1/2	PhongHocC2	eth0	VLAN 23
	e1/3	PhongHocC3	eth0	VLAN 23
	e2/0	PhongHocC4	eth0	VLAN 23
Sw_DC1	e0/0	NXOS3	e1/9	Po4
	e0/1	NXOS4	e1/9	
	e0/3	DNS_Mail_DHCP	e0	Po7
	e1/0	AD_RADIUS	e0	Po8
Sw_DC2	e0/0	NXOS3	e1/10	Po5
	e0/1	NXOS4	e1/10	
	e0/3	DNS_Mail_DHCP	e1	Po7
	e1/0	AD_RADIUS	e1	Po8
	e1/1	KyThuat	eth0	VLAN99

Bảng 4.2 Thông tin kết nối port trong hệ thống

Source		Destination		VLAN/Port-channel
Tên thiết bị	Interface	Tên thiết bị	Interface	
Chi nhánh Cần Thơ				
R3	s4/0	ISP2	s4/3	
	e0/0	Sw_BO	g0/0	
Sw_BO	e0/0	R3	e0/0	
	e0/1	Sw_D1	e1/0	
	e0/2	Sw_D2	e0/0	
Sw_D1	e1/0	Sw_BO	e1/3	
	e0/1	KyThuatD	eth0	VLAN109
	e0/2	VPKD1	eth0	VLAN24
	e0/3	VPKD2	eth0	VLAN24
Sw_D2	e0/0	Sw_BO	e1/4	
	e0/1	ThuVienD	eth0	VLAN25
	e0/2	PhongHocD1	eth0	VLAN26
	e0/3	PhongHocD2	eth0	VLAN26
	e1/0	PhongHocD3	eth0	VLAN26
	e1/1	PhongHocD4	eth0	VLAN26

4.2.3 Thông tin địa chỉ IP planning

Bảng 4.3 Thông tin quy hoạch địa chỉ IP

Tên thiết bị	Interface	Subnet	IPv4
Trụ sở chính TP.HCM			
R1	s4/1	14.16.240.0/30	14.16.240.2
	e0/0	172.16.0.4/30	172.16.0.5
	e0/1	172.16.0.8/30	172.16.0.9
R2	s4/1	14.16.241.0/30	14.16.241.2
	e0/0	172.16.0.12/30	172.16.0.13
	e0/1	172.16.0.16/30	172.16.0.17
FW1	m0/0	172.16.0.20/30	172.16.0.21
	g0/0	172.16.0.4/30	172.16.0.6
	g0/1	172.16.0.12/30	172.16.0.14
	g0/2	172.16.0.24/30	172.16.0.25
	g0/3	172.16.0.28/30	172.16.0.29
FW2	m0/0	172.16.0.20/30	172.16.0.22
	g0/0	172.16.0.8/30	172.16.0.10
	g0/1	172.16.0.16/30	172.16.0.18
	g0/2	172.16.0.32/30	172.16.0.33
	g0/3	172.16.0.36/30	172.16.0.37

Bảng 4.3 Thông tin quy hoạch địa chỉ IP

Tên thiết bị	Interface	Subnet	IPv4
NXOS1	e1/1	172.16.0.24/30	172.16.0.26
	e1/2	172.16.0.32/30	172.16.0.34
	mgmt0	172.16.0.40/30	172.16.0.41
	e1/5	172.16.0.48/30	172.16.0.49
	e1/6	172.16.0.52/30	172.16.0.53
	e1/7	172.16.0.56/30	172.16.0.57
NXOS2	e1/1	172.16.0.28/30	172.16.0.30
	e1/2	172.16.0.36/30	172.16.0.38
	mgmt0	172.16.0.40/30	172.16.0.42
	e1/5	172.16.0.64/30	172.16.0.65
	e1/6	172.16.0.68/30	172.16.0.69
	e1/7	172.16.0.60/30	172.16.0.62
NXOS3	e1/1	172.16.0.48/30	172.16.0.50
	e1/2	172.16.0.52/30	172.16.0.54
	e1/3	172.16.0.60/30	172.16.0.61
NXOS4	e1/1	172.16.0.64/30	172.16.0.66
	e1/2	172.16.0.68/30	172.16.0.70
	e1/3	172.16.0.56/30	172.16.0.58
NXOS3	mgmt0	172.16.0.44/30	172.16.0.45
NXOS4	mgmt0	172.16.0.44/30	172.16.0.46
KyThuat	eth0	172.16.99.0/24	172.16.99.3
AD_RADIUS	e0		
	e1	172.16.99.0/24	172.16.99.4

Bảng 4.3 Thông tin quy hoạch địa chỉ IP

Tên thiết bị	Interface	Subnet	IPv4
DNS_Mail_DHCP	e0	172.16.99.0/24	172.16.99.5
	e1		
Chi nhánh Cần Thơ			
R3	s0/4	14.16.242.0/30	14.16.242.2
	e0/0	172.17.0.4/30	172.17.0.5
Sw_BO	e0/0	172.17.0.4/30	172.17.0.6

CHƯƠNG 5 - TRIỂN KHAI HỆ THỐNG

5.1 Cấu hình cơ bản trên các thiết bị

Bảng 5.1 Quy trình cấu hình của các thiết bị trong hệ thống

STT	Tên thiết bị	Mô tả	Quy trình cấu hình
Trụ sở chính TP.HCM			
1	ISP1 ISP2	Router ISP kết nối mạng nội bộ với Internet, kết nối mạng WAN và NAT địa chỉ IP.	1. Cấu hình cơ bản 2. Cấu hình địa chỉ IP 3. Cấu hình định tuyến OSPF 4. Cấu hình định tuyến static 5. Cấu hình NAT
2	R1 R2	Router kết nối với nhà cung cấp dịch vụ và phân đoạn mạng nội bộ khu vực trụ sở chính.	1. Cấu hình cơ bản 2. Cấu hình địa chỉ IP 3. Cấu hình định tuyến OSPF 4. Cấu hình định tuyến static 5. Cấu hình Telnet/SSH
3	FW1 FW2	Tường lửa ngăn cách mạng nội bộ và mạng bên ngoài.	1. Cấu hình cơ bản 2. Cấu hình địa chỉ IP 3. Cấu hình định tuyến OSPF 4. Cấu hình định tuyến static 5. Cấu hình ACL

4	NXOS1 NXOS2	<p>Switch Nexus 9000v có vai trò là điểm tập trung cho việc kết nối các leaf switch và cung cấp khả năng mở rộng linh hoạt cho mạng.</p>	<ol style="list-style-type: none"> 1. Cấu hình cơ bản 2. Cấu hình địa chỉ IP 3. Cấu hình định tuyến OSPF 4. Cấu hình định tuyến static 5. Cấu hình VXLAN 6. Cấu hình vPC 7. Cấu hình Telnet/SSH
5	NXOS3 NXOS4	<p>Switch Nexus 9000v có nhiệm vụ định tuyến các VXLAN, phân phối lưu lượng mạng VXLAN.</p>	<ol style="list-style-type: none"> 1. Cấu hình cơ bản 2. Cấu hình địa chỉ IP 3. Cấu hình định tuyến OSPF 4. Tạo VLAN 5. Cấu hình Trunking mode 6. Cấu hình Interface Vlan 7. Cấu hình VXLAN 8. Cấu hình vPC 9. Cấu hình HSRP 10. Cấu hình DHCP Relay 11. Cấu hình Telnet/SSH

			<ol style="list-style-type: none"> 1. Cấu hình cơ bản 2. Cấu hình VLAN 3. Cấu hình Port-channel 4. Cấu hình Access mode 5. Cấu hình Telnet/SSH 6. Cấu hình chế độ Port-security 7. Thiết lập cơ chế AAA 8. Cấu hình mật khẩu cho các quyền truy cập
6	Sw_A Sw_B Sw_C	Có nhiệm vụ kết nối giữa các Leaf Switch với End Device.	<ol style="list-style-type: none"> 1. Cấu hình cơ bản 2. Cấu hình VLAN 3. Cấu hình Port-channel 4. Cấu hình Access mode 5. Cấu hình Telnet/SSH 6. Cấu hình chế độ Port-security 7. Thiết lập cơ chế AAA 8. Cấu hình mật khẩu cho các quyền truy cập
7	Sw_DC1 Sw_DC2	Có nhiệm vụ kết nối giữa các Leaf Switch với các Server ở khu vực Server farm.	<ol style="list-style-type: none"> 1. Cấu hình cơ bản 2. Cấu hình VLAN 3. Cấu hình Port-channel 4. Cấu hình Access mode 5. Cấu hình Telnet/SSH 6. Thiết lập cơ chế AAA 7. Cấu hình mật khẩu cho các quyền truy cập
8	Các Server	Có nhiệm vụ cung cấp các dịch vụ cho người dùng và các thiết bị khác trong mạng.	<ol style="list-style-type: none"> 1. Cài đặt hệ điều hành 2. Cấu hình địa chỉ IP 3. Cấu hình dịch vụ
Chi nhánh Cần Thơ			

9	R3	Router kết nối với nhà cung cấp dịch vụ và phân đoạn mạng nội bộ khu vực chi nhánh.	<ol style="list-style-type: none"> 1. Cấu hình cơ bản 2. Cấu hình địa chỉ IP 3. Cấu hình định tuyến OSPF 4. Cấu hình định tuyến static 5. Cấu hình Telnet/SSH
10	Sw_BO	Có nhiệm vụ chính là định tuyến, đảm bảo chuyển tiếp dữ liệu giữa các subnet, tạo kết nối Layer 3 đến các mạng khác, và cung cấp khả năng mở rộng cho mạng.	<ol style="list-style-type: none"> 1. Cấu hình cơ bản 2. Cấu hình địa chỉ IP 3. Cấu hình định tuyến OSPF 4. Tạo VLAN 5. Cấu hình Trunking mode 6. Cấu hình Interface VLAN
11	Sw_D1 Sw_D2	Có nhiệm vụ phân phối lưu lượng mạng ở Layer 2 của khu vực chi nhánh Cần Thơ.	<ol style="list-style-type: none"> 1. Cấu hình cơ bản 2. Tạo VLAN 3. Cấu hình Trunking mode 4. Cấu hình Access mode 5. Cấu hình Telnet/SSH 6. Cấu hình chế độ Port-security 7. Thiết lập cơ chế AAA 8. Cấu hình mật khẩu cho các quyền truy cập

Bảng 5.2 Các lệnh cấu hình của Router ISP1

ISP1		
1. Cấu hình cơ bản	3. Cấu hình định tuyến	
#hostname ISP1	OSPF	
#ip name-server 8.8.8.8	#router ospf 1	5. Cấu hình NAT
#ip domain-lookup	#router-id 1.1.1.1	#access-list 10 permit any
	#interface s4/1	#ip nat inside source
2. Cấu hình địa chỉ IP	#ip ospf 1 area 1	list 10 interface e0/0
#interface s4/1	#interface e0/0	overload
#ip address 14.16.240.1	#ip ospf 1 area 1	#interface e0/0
255.255.255.252		#ip nat outside
#no shutdown	4. Cấu hình định tuyến	#interface s4/1
#interface e0/0	static	#ip nat inside
#ip address dhcp	#ip route 0.0.0.0 0.0.0.0	
#no shutdown	192.168.1.1	

Bảng 5.3 Các lệnh cấu hình của Router ISP2

ISP2	
1. Cấu hình cơ bản #hostname ISP2 #ip name-server 8.8.8.8 #ip domain-lookup	#interface e0/0 #ip address dhcp #no shutdown <hr/> 3. Cấu hình định tuyến OSPF #router ospf 1 #router-id 1.1.1.2 #interface s4/1 #ip ospf 1 area 1 #interface s4/3 #ip ospf 1 area 1 #interface e0/0 #ip ospf 1 area 1
2. Cấu hình địa chỉ IP #interface s4/1 #ip address 14.16.241.1 255.255.255.252 #no shutdown #interface s4/3 #ip address 14.16.242.1 255.255.255.252 #no shutdown	4. Cấu hình định tuyến static #ip route 0.0.0.0 0.0.0.0 192.168.1.1 <hr/> 5. Cấu hình NAT #access-list 10 permit any #ip nat inside source list 10 interface e0/0 overload #interface e0/0 #ip nat outside #interface s4/1 #ip nat inside

Bảng 5.4 Các lệnh cấu hình của Router R1

R1	
1. Cấu hình cơ bản <pre>>enable #configure terminal #hostname R1 #ip domain-name cmu.edu #no ip domain-lookup</pre> <hr/> 2. Cấu hình địa chỉ IP <pre>#interface s4/1 #ip address 14.16.240.2 255.255.255.252 #no shutdown #interface e0/0 #ip address 172.16.0.5 255.255.255.252 #no shutdown</pre>	3. Cấu hình định tuyến OSPF <pre>#interface e0/1 #ip address 172.16.0.9 255.255.255.252 #no shutdown</pre> <hr/> 4. Cấu hình định tuyến static <pre>#ip route 0.0.0.0 0.0.0.0 14.16.240.1</pre> <hr/> 5. Cấu hình Telnet/SSH <pre>#crypto key generate rsa generatal-keys 1024 #username adminHO secret AdminHO@123 #ip ssh ver 2 #line vty 0 4 #login local #transport input SSH</pre>

Bảng 5.5 Các lệnh cấu hình của Router R2

R2		
1. Cấu hình cơ bản <pre>>enable #configure terminal #hostname R2 #ip domain-name cmu.edu #no ip domain-lookup</pre>	2. Cấu hình địa chỉ IP <pre>#interface s4/1 #ip address 14.16.241.2 255.255.255.252 #no shutdown #interface e0/0 #ip address 172.16.0.13 255.255.255.252 #no shutdown</pre>	3. Cấu hình định tuyến OSPF <pre>#interface e0/1 #ip address 172.16.0.17 255.255.255.252 #no shutdown</pre> <hr/> 4. Cấu hình định tuyến static <pre>#ip route 0.0.0.0 0.0.0.0 14.16.241.1</pre> <hr/> 5. Cấu hình Telnet/SSH <pre>#crypto key generate rsa genral-keys 1024 #username adminHO secret AdminHO@123 #ip ssh ver 2 #line vty 0 4 #login local #transport input SSH</pre>

Bảng 5.6 Các lệnh cấu hình của Firewall FW1

FW1		
1. Cấu hình cơ bản		
>enable	#no shutdown	5. Cấu hình ACL
#configure terminal	#interface g0/3	#access-list outside_access
#hostname FW1	#nameif IN-2	extended permit icmp any
	#security-level 100	any echo-reply
	#ip address 172.16.0.29	
	255.255.255.252	#access-list outside_access
	#no shutdown	extended permit icmp any
	#interface m0/0	any time-exceeded
	#ip address 172.16.0.21	#access-list outside_access
	255.255.255.252	extended permit icmp any
	#no shutdown	any timestamp-reply
		#access-list outside_access
2. Cấu hình địa chỉ IP		extended permit icmp any
#interface g0/0	#no shutdown	any unreachable
#nameif OUT-1	#interface m0/0	#access-list outside_access
#security-level 50	#ip address 172.16.0.21	extended deny tcp any
#ip address 172.16.0.6	255.255.255.252	172.16.0.0 255.255.0.0 eq
255.255.255.252	#no shutdown	telnet
#no shutdown		#access-list outside_access
#interface g0/1		extended deny tcp any
#nameif OUT-2	3. Cấu hình định tuyến	172.16.0.0 255.255.0.0 eq
#security-level 50	OSPF	
#ip address 172.16.0.14	#router ospf 1	#access-list outside_access
255.255.255.252	#router-id 11.0.0.3	extended deny tcp any
#no shutdown	#network 172.16.0.0	172.16.0.0 255.255.0.0 eq
#interface g0/2	255.255.255.0	telnet
#nameif IN-1	area 0.0.0.0	#access-list outside_access
#security-level 100		extended deny tcp any
#ip address 172.16.0.25	4. Cấu hình định tuyến static	172.16.0.0 255.255.0.0 eq
255.255.255.252	#route OUT-1 0.0.0.0 0.0.0.0	ssh
	172.16.0.5	

#access-list outside_access extended deny udp any any eq domain #access-list outside_access extended deny icmp any any #access-group outside_access in interface OUT-1 #access-group outside_access in interface OUT-2 #access-list inside_access extended permit tcp	172.16.99.0 255.255.255.0 any eq telnet #access-list inside_access extended permit tcp 172.16.99.0 255.255.255.0 any eq ssh #access-list inside_access extended deny tcp 172.16.0.0 255.255.0.0 any eq telnet #access-list inside_access extended deny tcp 172.16.0.0 255.255.0.0 any eq ssh	#access-list inside_access extended permit tcp 172.16.0.0 255.255.0.0 any eq www #access-list inside_access extended permit icmp any any #access-group inside_access in interface IN-1 #access-group inside_access in interface IN-2
--	---	--

Bảng 5.7 Các lệnh cấu hình của Firewall FW2

FW2		
1. Cấu hình cơ bản	#nameif OUT-1	#security-level 50
>enable	#security-level 50	#ip address 172.16.0.18
#configure terminal	#ip address 172.16.0.10	255.255.255.252
#hostname FW2	255.255.255.252	#no shutdown
-----	#no shutdown	#interface g0/2
2. Cấu hình địa chỉ IP	#interface g0/1	#nameif IN-1
#interface g0/0	#nameif OUT-2	#security-level 100

#ip address 172.16.0.33 255.255.255.252 #no shutdown #interface g0/3 #nameif IN-2 #security-level 100 #ip address 172.16.0.37 255.255.255.252 #no shutdown #interface m0/0 #ip address 172.16.0.22 255.255.255.252 #no shutdown	5. Cấu hình ACL #access-list outside_access extended permit icmp any any echo-reply #access-list outside_access extended permit icmp any any time-exceeded #access-list outside_access extended permit icmp any any timestamp-reply #access-list outside_access extended permit icmp any any unreachable #access-list outside_access extended deny tcp any 172.16.0.0 255.255.0.0 eq telnet #access-list outside_access extended deny tcp any 172.16.0.0 255.255.0.0 eq ssh #access-list outside_access extended deny udp any any eq domain	#access-list outside_access extended deny icmp any any #access-group outside_access in interface OUT-1 #access-group outside_access in interface OUT-2 #access-list inside_access extended permit tcp 172.16.99.0 255.255.255.0 any eq telnet #access-list inside_access extended permit tcp 172.16.99.0 255.255.255.0 any eq ssh #access-list inside_access extended deny tcp 172.16.0.0 255.255.0.0 any eq telnet #access-list inside_access extended deny tcp 172.16.0.0 255.255.0.0 any eq ssh
3. Cấu hình định tuyến OSPF #router ospf 1 #router-id 11.0.0.4 #network 172.16.0.0 255.255.255.0 area 0.0.0.0		
4. Cấu hình định tuyến static #route OUT-2 0.0.0.0 0.0.0.0 172.16.0.17		

#access-list inside_access extended permit tcp 172.16.0.0 255.255.0.0 any eq www	#access-list inside_access extended permit icmp any any #access-group inside_access in interface	IN-1 #access-group inside_access in interface IN-2
---	--	---

Bảng 5.8 Các lệnh cấu hình của NXOS1

NXOS1		
1. Cấu hình cơ bản #hostname NXOS1 #ip domain-name cmu.edu #no ip domain-lookup #username admin1 password Admin1@123 role network-admin	#ip address 172.16.0.34 255.255.255.252 #no shutdown #interface e1/5 #no switchport #ip address 172.16.0.49 255.255.255.252 #no shutdown #interface loopback0	#ip address 172.16.0.57 255.255.255.252 #no shutdown #interface mgmt0 #ip address 172.16.0.41 255.255.255.252 #no shutdown #interface loopback0
2. Cấu hình địa chỉ IP #interface e1/1 #no switchport #ip address 172.16.0.26 255.255.255.252 #no shutdown #interface e1/2 #no switchport	#ip address 172.16.0.53 255.255.255.252 #no shutdown #interface e1/7 #no switchport	#ip address 1.0.0.2/32 #interface loopback1 #ip address 1.0.0.1/32
		3. Cấu hình định tuyến OSPF #license smart enable #feature ospf

#router ospf 1	#ip router ospf 1 area 0	#ip pim sparse-mode
#router-id 11.0.0.5	#interface e1/7	#interface e1/4
#interface e1/1	#no switchport	#ip pim sparse-mode
#ip router ospf 1 area 0	#ip ospf network	#interface e1/5
#interface e1/2	point-to-point	#ip pim sparse-mode
#ip router ospf 1 area 0	#ip router ospf 1 area 0	#interface e1/6
#interface e1/3	#interface loopback0	#ip pim sparse-mode
#no switchport	#ip ospf network	#interface e1/7
#ip ospf network	point-to-point	#ip pim sparse-mode
point-to-point	#ip router ospf 1 area 0	#interface loopback0
#ip router ospf 1 area 0	#interface loopback1	#ip pim sparse-mode
#interface e1/4	#ip ospf network	#interface loopback1
#no switchport	point-to-point	#ip pim sparse-mode
#ip ospf network	#ip router ospf 1 area 0	#ip pim rp-address 1.0.0.1
point-to-point	_____	group-list 224.0.0.0/4
#ip router ospf 1 area 0	4. Cấu hình định tuyến static	#ip pim anycast-rp 1.0.0.1
#interface e1/5	#ip route 0.0.0.0 0.0.0.0	1.0.0.2
#no switchport	172.16.0.25	#ip pim anycast-rp 1.0.0.1
#ip ospf network	_____	1.0.0.3
point-to-point	5. Cấu hình VXLAN	_____
#ip router ospf 1 area 0	#system jumbo mtu 9216	6. Cấu hình vPC
#interface e1/6	#feature pim	#feature vpc
#no switchport	#interface e1/1	#feature lacp
#ip ospf network	#ip pim sparse-mode	#vpc domain 1
point-to-point	#interface e1/2	#peer-switch

#peer-gateway	#channel-group 51 mode active	7. Cấu hình Telnet/SSH
#role priority 10	#no shutdown	#feature telnet
#graceful consistency-check	#interface po51	#telnet server enable
#auto-recover	#description vPC-PeerLink	#feature ssh
#ip arp synchronize	#switchport	#ssh server enable
#ipv6 nd synchronize	#switchport mode trunk	#username adminHO
#peer-keepalive destination 172.16.0.42 source	#vpc peer-link	password AdminHO@123
172.16.0.41 vrf management	#spanning-tree port type	#username adminHO role
#interface e1/3-4	network	network-admin
#description vPC-PeerLink	#no shutdown	

Bảng 5.9 Các lệnh cấu hình của NXOS2

NXOS2		
1. Cấu hình cơ bản	#no switchport	#no switchport
#hostname NXOS2	#ip address 172.16.0.30	#ip address 172.16.0.65
#ip domain-name cmu.edu	255.255.255.252	255.255.255.252
#no ip domain-lookup	#no shutdown	#no shutdown
#username admin1 password Admin1@123 role network-admin	#interface e1/2 #no switchport #ip address 172.16.0.38 255.255.255.252	#interface e1/6 #no switchport #ip address 172.16.0.69 255.255.255.252
2. Cấu hình địa chỉ IP	#no shutdown	#no shutdown
#interface e1/1	#interface e1/5	#interface e1/7

#no switchport #ip address 172.16.0.62 255.255.255.252 #no shutdown #interface mgmt0 #ip address 172.16.0.42 255.255.255.252 #no shutdown #interface loopback0 #ip address 1.0.0.3/32 #interface loopback1 #ip address 1.0.0.1/32	#ip ospf network point-to-point #ip router ospf 1 area 0 #interface e1/4 #no switchport #ip ospf network point-to-point #ip router ospf 1 area 0 #interface e1/5 #no switchport #ip ospf network point-to-point #ip router ospf 1 area 0	point-to-point #ip router ospf 1 area 0 #interface loopback1 #ip ospf network point-to-point #ip router ospf 1 area 0
3. Cấu hình định tuyến OSPF #license smart enable #feature ospf #router ospf 1 #router-id 11.0.0.6 #interface e1/1 #ip router ospf 1 area 0 #interface e1/2 #ip router ospf 1 area 0 #interface e1/3 #no switchport	#ip ospf network point-to-point #ip router ospf 1 area 0 #interface e1/6 #no switchport #ip ospf network point-to-point #ip router ospf 1 area 0 #interface e1/7 #no switchport #ip ospf network point-to-point #ip router ospf 1 area 0 #interface loopback0 #ip ospf network	4. Cấu hình định tuyến static #ip route 0.0.0.0 0.0.0.0 172.16.0.37
		5. Cấu hình VXLAN #system jumbomtu 9216 #feature pim #interface e1/1 #ip pim sparse-mode #interface e1/2 #ip pim sparse-mode #interface e1/4 #ip pim sparse-mode #interface e1/5 #ip pim sparse-mode #interface e1/6 #ip pim sparse-mode

#interface e1/7	#peer-switch	#switchport
#ip pim sparse-mode	#peer-gateway	#switchport mode trunk
#interface loopback0	#role priority 10	#vpc peer-link
#ip pim sparse-mode	#graceful consistency-check	#spanning-tree port type
#interface loopback1	#auto-recover	network
#ip pim sparse-mode	#ip arp synchronize	#no shutdown
#ip pim rp-address 1.0.0.1	#ipv6 nd synchronize	
group-list 224.0.0.0/4	#peer-keepalive destination	
#ip pim anycast-rp 1.0.0.1	172.16.0.41 source	#feature telnet
1.0.0.2	172.16.0.42 vrf management	#telnet server enable
#ip pim anycast-rp 1.0.0.1	#interface e1/3-4	#feature ssh
1.0.0.3	#description vPC-PeerLink	#ssh server enable
<hr/>		
6. Cấu hình vPC	#channel-group 51 mode	#username adminHO
#feature vpc	active	password
#feature lacp	#no shutdown	AdminHO@123
#vpc domain 1	#interface po51	#username adminHO role
	#description vPC-PeerLink	network-admin
<hr/>		
7. Cấu hình Telnet/SSH		

Bảng 5.10 Các lệnh cấu hình của NXOS3

NXOS3		
1. Cấu hình cơ bản		
#hostname NXOS3	#no shutdown	#ip ospf network
#ip domain-name cmu.edu	#interface mgmt0	point-to-point
#no ip domain-lookup	#ip address 172.16.0.45	#ip router ospf 1 area 0
#username admin1 password	255.255.255.252	#interface e1/3
Admin1@123 role	#no shutdown	#no switchport
network-admin	#interface loopback0	#ip ospf network
	#ip address 1.1.1.5/32	point-to-point
	#ip address 1.1.1.4/32	#ip router ospf 1 area 0
	secondary	#interface loopback0
2. Cấu hình địa chỉ IP		
#interface e1/1		#ip ospf network
#no switchport		point-to-point
#ip address 172.16.0.50		#ip router ospf 1 area 0
255.255.255.252		
#no shutdown	#license smart enable	
#interface e1/2	#feature ospf	
#no switchport	#router ospf 1	
#ip address 172.16.0.54	#router-id 11.0.0.7	
255.255.255.252	#interface e1/1	
#no shutdown	#no switchport	
#interface e1/3	#ip ospf network	
#no switchport	point-to-point	
#ip address 172.16.0.61	#ip router ospf 1 area 0	
255.255.255.252	#interface e1/2	
	#no switchport	
3. Cấu hình định tuyến OSPF		
	#vlan 11	
	#name HanhChinh	
	#vlan 12	
	#name DaoTao	
	#vlan 13	
	#name TuyenSinh	
	#vlan 14	
	#name Lab	
	#vlan 15	
4. Tạo VLAN		

#name KHXHNV	vlan 11-23,99	#switchport
#vlan 16	#no shutdown	#switchport mode trunk
#name Duoc	#exit	#switchport trunk allow
#vlan 17	#interface e1/5	vlan 21,22,23
#name NgoaiNgu	#switchport	#no shutdown
#vlan 18	#switchport mode trunk	#exit
#name TCNH	#switchport trunk allow	#interface e1/9
#vlan 19	vlan 11-23,99	#switchport
#name PhongHocB	#no shutdown	#switchport mode trunk
#vlan 20	#exit	#switchport trunk allow
#name QTKD	#interface e1/6	vlan 99
#vlan 21	#switchport	#no shutdown
#name CNTT	#switchport mode trunk	#exit
#vlan 22	#switchport trunk allow	#interface e1/10
#name ThuVien	vlan 11,12,13,14	#switchport
#vlan 23	#no shutdown	#switchport mode trunk
#name PhongHocC	#exit	#switchport trunk allow
#vlan 99	#interface e1/7	vlan 99
#name KyThuat	#switchport	#no shutdown
<hr/>		#exit
5. Cấu hình Trunking mode	#switchport mode trunk	<hr/>
#interface e1/4	#switchport trunk allow	6. Cấu hình Interface Vlan
#switchport	vlan 15,16,17,18,19,20	#feature interface-vlan
#switchport mode trunk	#no shutdown	#interface vlan 11
#switchport trunk allow	#exit	#ip address 171.16.11.1
	#interface e1/8	

255.255.255.192	#ip router ospf 1 area 0	#mtu 9216
#ip router ospf 1 area 0	#mtu 9216	#no shutdown
#mtu 9216	#no shutdown	#interface vlan 20
#no shutdown	#interface vlan 16	#ip address 171.16.20.1
#interface vlan 12	#ip address 171.16.16.1	255.255.255.192
#ip address 171.16.12.1	255.255.255.192	#ip router ospf 1 area 0
255.255.255.192	#ip router ospf 1 area 0	#mtu 9216
#ip router ospf 1 area 0	#mtu 9216	#no shutdown
#mtu 9216	#no shutdown	#interface vlan 21
#no shutdown	#interface vlan 17	#ip address 171.16.21.1
#interface vlan 13	#ip address 171.16.17.1	255.255.255.192
#ip address 171.16.13.1	255.255.255.192	#ip router ospf 1 area 0
255.255.255.192	#ip router ospf 1 area 0	#mtu 9216
#ip router ospf 1 area 0	#mtu 9216	#no shutdown
#mtu 9216	#no shutdown	#interface vlan 22
#no shutdown	#interface vlan 18	#ip address 171.16.22.1
#interface vlan 14	#ip address 171.16.18.1	255.255.255.0
#ip address 171.16.14.1	255.255.255.192	#ip router ospf 1 area 0
255.255.255.192	#ip router ospf 1 area 0	#mtu 9216
#ip router ospf 1 area 0	#mtu 9216	#no shutdown
#mtu 9216	#no shutdown	#interface vlan 23
#no shutdown	#interface vlan 19	#ip address 171.16.23.1
#interface vlan 15	#ip address 171.16.19.1	255.255.255.192
#ip address 171.16.15.1	255.255.255.224	#ip router ospf 1 area 0
255.255.255.192	#ip router ospf 1 area 0	#mtu 9216

#no shutdown	#interface loopback0	#vlan 18
#interface vlan 99	#ip pim sparse-mode	#vn-segment 10018
#ip address 171.16.99.1	#ip pim rp-address 1.1.1.4	#vlan 19
255.255.255.0	group-list 224.0.0.0/4	#vn-segment 10019
#ip router ospf 1 area 0	#ip pim anycast-rp 1.1.1.4	#vlan 20
#mtu 9216	1.1.1.5	#vn-segment 10020
#no shutdown	#ip pim anycast-rp 1.1.1.4	#vlan 21
<hr/>		
7. Cấu hình VXLAN	#feature nv overlay	#vlan 22
#system jumbo mtu 9216	#feature	#vn-segment 10022
#feature pim	vn-segment-vlan-based	#vlan 23
#interface e1/4	#vlan 11	#vn-segment 10023
#ip pim sparse-mode	#vn-segment 10011	#vlan 99
#interface e1/5	#vlan 12	#vn-segment 10099
#ip pim sparse-mode	#vn-segment 10012	#interface nve1
#interface e1/6	#vlan 13	#no shutdown
#ip pim sparse-mode	#vn-segment 10013	#source-interface
#interface e1/7	#vlan 14	loopback0
#ip pim sparse-mode	#vn-segment 10014	#member vni 10011
#interface e1/8	#vlan 15	mcast-group 239.1.1.11
#ip pim sparse-mode	#vn-segment 10015	#member vni 10012
#interface e1/9	#vlan 16	mcast-group 239.1.1.12
#ip pim sparse-mode	#vn-segment 10016	#member vni 10013
#interface e1/10	#vlan 17	mcast-group 239.1.1.13
#ip pim sparse-mode	#vn-segment 10017	#member vni 10014

mcast-group 239.1.1.14 #member vni 10015 mcast-group 239.1.1.15 #member vni 10016 mcast-group 239.1.1.16 #member vni 10017 mcast-group 239.1.1.17 #member vni 10018 mcast-group 239.1.1.18 #member vni 10019 mcast-group 239.1.1.19 #member vni 10020 mcast-group 239.1.1.20 #member vni 10021 mcast-group 239.1.1.21 #member vni 10022 mcast-group 239.1.1.22 #member vni 10023 mcast-group 239.1.1.23 #member vni 10099 mcast-group 239.1.1.99	#interface mgmt0 #ip address 172.16.0.45/30 #no shutdown #vpc domain 2 #peer-switch #peer-gateway #role priority 10 #graceful consistency-check #auto-recover #ip arp synchronize #ipv6 nd synchronize #peer-keepalive destination 172.16.0.46 source 172.16.0.45 vrf management #interface e1/4-5 #description vPC-PeerLink #channel-group 54 mode active #no shutdown #switchport #description vPC-PeerLink	network #no shutdown #interface e1/6 #channel-group 1 mode active #no shutdown #interface po1 #switchport mode trunk #vpc 1 #no shutdown #interface e1/7 #channel-group 2 mode active #no shutdown #interface po2 #switchport mode trunk #vpc 2 #no shutdown #interface e1/8 #channel-group 3 mode active #no shutdown #interface po3 #switchport mode trunk #vpc 3
8. Cấu hình vPC #feature vpc #feature lacp	#switchport #switchport mode trunk #vpc peer-link #spanning-tree port type	#no shutdown #interface po3 #switchport mode trunk #vpc 3

#no shutdown	#interface vlan 12	#interface vlan 17
#interface e1/9	#hsrp 12	#hsrp 17
#channel-group 4 mode active	#ip 172.16.12.3 #preempt	#ip 172.16.17.3 #preempt
#no shutdown	#priority 200	#priority 200
#interface po4	#interface vlan 13	#interface vlan 18
#switchport mode trunk	#hsrp 13	#hsrp 18
#vpc 4	#ip 172.16.13.3	#ip 172.16.18.3
#no shutdown	#preempt	#preempt
#interface e1/10	#priority 200	#priority 200
#channel-group 5 mode active	#interface vlan 14 #hsrp 14	#interface vlan 19 #hsrp 19
#no shutdown	#ip 172.16.14.3	#ip 172.16.19.3
#interface po5	#preempt	#preempt
#switchport mode trunk	#priority 200	#priority 200
#vpc 5	#interface vlan 15	#interface vlan 20
#no shutdown	#hsrp 15	#hsrp 20
	#ip 172.16.15.3	#ip 172.16.20.3
9. Cấu hình HSRP	#preempt	#preempt
#feature hsrp	#priority 200	#priority 200
#interface vlan 11	#interface vlan 16	#interface vlan 21
#hsrp 11	#hsrp 16	#hsrp 21
#ip 172.16.11.3	#ip 172.16.16.3	#ip 172.16.21.3
#preempt	#preempt	#preempt
#priority 200	#priority 200	#priority 200

#interface vlan 22 #hsrp 22 #ip 172.16.22.3 #preempt #priority 200 #interface vlan 23 #hsrp 23 #ip 172.16.23.3 #preempt #priority 200 #interface vlan 99 #hsrp 99 #ip 172.16.99.3 #preempt #priority 200	#interface vlan 11 #ip dhcp relay address 172.16.99.5 use-vrf default #interface vlan 12 #ip dhcp relay address 172.16.99.5 use-vrf default #interface vlan 13 #ip dhcp relay address 172.16.99.5 use-vrf default #interface vlan 14 #ip dhcp relay address 172.16.99.5 use-vrf default #interface vlan 15 #ip dhcp relay address 172.16.99.5 use-vrf default #interface vlan 16 #ip dhcp relay address 172.16.99.5 use-vrf default #interface vlan 17 #ip dhcp relay address 172.16.99.5 use-vrf default #interface vlan 18 #ip dhcp relay address 172.16.99.5 use-vrf default #interface vlan 19	#ip dhcp relay address 172.16.99.5 use-vrf default #interface vlan 20 #ip dhcp relay address 172.16.99.5 use-vrf default #interface vlan 21 #ip dhcp relay address 172.16.99.5 use-vrf default #interface vlan 22 #ip dhcp relay address 172.16.99.5 use-vrf default #interface vlan 23 #ip dhcp relay address 172.16.99.5 use-vrf default
10. Cấu hình DHCP Relay #feature dhcp #service dhcp #ip dhcp relay #ip dhcp relay information option #ip dhcp relay information option vpn #ipv6 dhcp relay		11. Cấu hình Telnet/SSH #feature telnet #telnet server enable #feature ssh #ssh server enable #username adminHO password AdminHO@123 #username adminHO role network-admin

Bảng 5.11 Các lệnh cấu hình của NXOS4

NXOS4

1. Cấu hình cơ bản		
#hostname NXOS4	#no shutdown	#ip ospf network
#ip domain-name cmu.edu	#interface mgmt0	point-to-point
#no ip domain-lookup	#ip address 172.16.0.46	#ip router ospf 1 area 0
#username admin1 password	255.255.255.252	#interface e1/3
Admin1@123 role	#no shutdown	#no switchport
network-admin	#interface loopback0	#ip ospf network
	#ip address 1.1.1.6/32	point-to-point
	#ip address 1.1.1.4/32	#ip router ospf 1 area 0
	secondary	#interface loopback0
2. Cấu hình địa chỉ IP		
#interface e1/1		#ip ospf network
#no switchport		point-to-point
#ip address 172.16.0.66		#ip router ospf 1 area 0
255.255.255.252		
#no shutdown	#license smart enable	
#interface e1/2	#feature ospf	
#no switchport	#router ospf 1	
#ip address 172.16.0.70	#router-id 11.0.0.8	
255.255.255.252	#interface e1/1	
#no shutdown	#no switchport	
#interface e1/3	#ip ospf network	
#no switchport	point-to-point	
#ip address 172.16.0.58	#ip router ospf 1 area 0	
255.255.255.252	#interface e1/2	
	#no switchport	
3. Cấu hình định tuyến OSPF		
	#feature ospf	
	#router ospf 1	
	#router-id 11.0.0.8	
	#interface e1/1	
	#no switchport	
	#ip ospf network	
	point-to-point	
	#ip router ospf 1 area 0	
4. Tạo VLAN		
	#vlan 11	
	#name HanhChinh	
	#vlan 12	
	#name DaoTao	
	#vlan 13	
	#name TuyenSinh	
	#vlan 14	
	#name Lab	
	#vlan 15	

#name KHXHNV	vlan 11-23,99	#switchport
#vlan 16	#no shutdown	#switchport mode trunk
#name Duoc	#exit	#switchport trunk allow
#vlan 17	#interface e1/5	vlan 21,22,23
#name NgoaiNgu	#switchport	#no shutdown
#vlan 18	#switchport mode trunk	#exit
#name TCNH	#switchport trunk allow	#interface e1/9
#vlan 19	vlan 11-23,99	#switchport
#name PhongHocB	#no shutdown	#switchport mode trunk
#vlan 20	#exit	#switchport trunk allow
#name QTKD	#interface e1/6	vlan 99
#vlan 21	#switchport	#no shutdown
#name CNTT	#switchport mode trunk	#exit
#vlan 22	#switchport trunk allow	#interface e1/10
#name ThuVien	vlan 11,12,13,14	#switchport
#vlan 23	#no shutdown	#switchport mode trunk
#name PhongHocC	#exit	#switchport trunk allow
#vlan 99	#interface e1/7	vlan 99
#name KyThuat	#switchport	#no shutdown
<hr/>		#exit
5. Cấu hình Trunking mode	#switchport mode trunk	<hr/>
#interface e1/4	#switchport trunk allow	6. Cấu hình Interface Vlan
#switchport	vlan 15,16,17,18,19,20	#feature interface-vlan
#switchport mode trunk	#no shutdown	#interface vlan 11
#switchport trunk allow	#exit	#ip address 171.16.11.2
	#interface e1/8	

255.255.255.192	#ip router ospf 1 area 0	#mtu 9216
#ip router ospf 1 area 0	#mtu 9216	#no shutdown
#mtu 9216	#no shutdown	#interface vlan 20
#no shutdown	#interface vlan 16	#ip address 171.16.20.2
#interface vlan 12	#ip address 171.16.16.2	255.255.255.192
#ip address 171.16.12.2	255.255.255.192	#ip router ospf 1 area 0
255.255.255.192	#ip router ospf 1 area 0	#mtu 9216
#ip router ospf 1 area 0	#mtu 9216	#no shutdown
#mtu 9216	#no shutdown	#interface vlan 21
#no shutdown	#interface vlan 17	#ip address 171.16.21.2
#interface vlan 13	#ip address 171.16.17.2	255.255.255.192
#ip address 171.16.13.2	255.255.255.192	#ip router ospf 1 area 0
255.255.255.192	#ip router ospf 1 area 0	#mtu 9216
#ip router ospf 1 area 0	#mtu 9216	#no shutdown
#mtu 9216	#no shutdown	#interface vlan 22
#no shutdown	#interface vlan 18	#ip address 171.16.22.2
#interface vlan 14	#ip address 171.16.18.2	255.255.255.0
#ip address 171.16.14.2	255.255.255.192	#ip router ospf 1 area 0
255.255.255.192	#ip router ospf 1 area 0	#mtu 9216
#ip router ospf 1 area 0	#mtu 9216	#no shutdown
#mtu 9216	#no shutdown	#interface vlan 23
#no shutdown	#interface vlan 19	#ip address 171.16.23.2
#interface vlan 15	#ip address 171.16.19.2	255.255.255.192
#ip address 171.16.15.2	255.255.255.224	#ip router ospf 1 area 0
255.255.255.192	#ip router ospf 1 area 0	#mtu 9216

#no shutdown	#interface loopback0	#vlan 18
#interface vlan 99	#ip pim sparse-mode	#vn-segment 10018
#ip address 171.16.99.2 255.255.255.0	#ip pim rp-address 1.1.1.4 group-list 224.0.0.0/4	#vlan 19
#ip router ospf 1 area 0	#ip pim anycast-rp 1.1.1.4	#vn-segment 10019
#mtu 9216	1.1.1.5	#vlan 20
#no shutdown	#ip pim anycast-rp 1.1.1.4	#vn-segment 10020
<hr/>		
7. Cấu hình VXLAN	1.1.1.6	#vlan 21
#system jumbo mtu 9216	#feature nv overlay	#vn-segment 10021
#feature pim	#feature	#vlan 22
#interface e1/4	vn-segment-vlan-based	#vn-segment 10022
#ip pim sparse-mode	#vlan 11	#vlan 23
#interface e1/5	#vn-segment 10011	#vn-segment 10023
#ip pim sparse-mode	#vlan 12	#vlan 99
#interface e1/6	#vn-segment 10012	#vn-segment 10099
#ip pim sparse-mode	#vlan 13	#interface nve1
#interface e1/7	#vn-segment 10013	#no shutdown
#ip pim sparse-mode	#vlan 14	#source-interface
#interface e1/8	#vn-segment 10014	loopback0
#ip pim sparse-mode	#vlan 15	#member vni 10011
#interface e1/9	#vn-segment 10015	mcast-group 239.1.1.11
#ip pim sparse-mode	#vlan 16	#member vni 10012
#interface e1/10	#vn-segment 10016	mcast-group 239.1.1.12
#ip pim sparse-mode	#vlan 17	#member vni 10013
	#vn-segment 10017	mcast-group 239.1.1.13
		#member vni 10014

mcast-group 239.1.1.14 #member vni 10015 mcast-group 239.1.1.15 #member vni 10016 mcast-group 239.1.1.16 #member vni 10017 mcast-group 239.1.1.17 #member vni 10018 mcast-group 239.1.1.18 #member vni 10019 mcast-group 239.1.1.19 #member vni 10020 mcast-group 239.1.1.20 #member vni 10021 mcast-group 239.1.1.21 #member vni 10022 mcast-group 239.1.1.22 #member vni 10023 mcast-group 239.1.1.23 #member vni 10099 mcast-group 239.1.1.99	#interface mgmt0 #ip address 172.16.0.46/30 #no shutdown #interface e1/6 #vpc domain 2 #peer-switch #peer-gateway #role priority 10 #graceful consistency-check #auto-recover #ip arp synchronize #ipv6 nd synchronize #peer-keepalive destination 172.16.0.45 source 172.16.0.46 vrf management #interface e1/4-5 #description vPC-PeerLink #channel-group 54 mode active #no shutdown #interface po54 #description vPC-PeerLink	network #no shutdown #channel-group 1 mode active #no shutdown #interface po1 #switchport mode trunk #vpc 1 #no shutdown #interface e1/7 #channel-group 2 mode active #no shutdown #interface po2 #switchport mode trunk #vpc 2 #no shutdown #interface e1/8 #channel-group 3 mode active #no shutdown #interface po3 #switchport mode trunk #vpc 3
8. Cấu hình vPC #feature vpc #feature lacp	#switchport #switchport mode trunk #vpc peer-link #spanning-tree port type	#no shutdown #interface po3 #switchport mode trunk #vpc 3

#no shutdown	#hsrp 12	#ip 172.16.18.3
#interface e1/9	#ip 172.16.12.3	#preempt
#channel-group 4 mode active	#preempt	#interface vlan 19
	#interface vlan 13	#hsrp 19
#no shutdown	#hsrp 13	#ip 172.16.19.3
#interface po4	#ip 172.16.13.3	#preempt
#switchport mode trunk	#preempt	#interface vlan 20
#vpc 4	#interface vlan 14	#hsrp 20
#no shutdown	#hsrp 14	#ip 172.16.20.3
#interface e1/10	#ip 172.16.14.3	#preempt
#channel-group 5 mode active	#preempt	#interface vlan 21
	#interface vlan 15	#hsrp 21
#no shutdown	#hsrp 15	#ip 172.16.21.3
#interface po5	#ip 172.16.15.3	#preempt
#switchport mode trunk	#preempt	#interface vlan 22
#vpc 5	#interface vlan 16	#hsrp 22
#no shutdown	#hsrp 16	#ip 172.16.22.3
	#ip 172.16.16.3	#preempt
9. Cấu hình HSRP	#preempt	#interface vlan 23
#feature hsrp	#interface vlan 17	#hsrp 23
#interface vlan 11	#hsrp 17	#ip 172.16.23.3
#hsrp 11	#ip 172.16.17.3	#preempt
#ip 172.16.11.3	#preempt	#interface vlan 99
#preempt	#interface vlan 18	#hsrp 99
#interface vlan 12	#hsrp 18	#ip 172.16.99.3

#preempt	172.16.99.5 use-vrf default #interface vlan 16 #ip dhcp relay address	#ip dhcp relay address 172.16.99.5 use-vrf default #interface vlan 20 #ip dhcp relay address
10. Cấu hình DHCP Relay		
#feature dhcp	172.16.99.5 use-vrf default #interface vlan 17 #ip dhcp relay address	172.16.99.5 use-vrf default #interface vlan 21 #ip dhcp relay address
#service dhcp	172.16.99.5 use-vrf default #interface vlan 18 #ip dhcp relay address	172.16.99.5 use-vrf default #interface vlan 22 #ip dhcp relay address
#ip dhcp relay	172.16.99.5 use-vrf default #interface vlan 19 #ip dhcp relay address	172.16.99.5 use-vrf default #interface vlan 23 #ip dhcp relay address
#ip dhcp relay information option	172.16.99.5 use-vrf default #interface vlan 20 #ip dhcp relay address	172.16.99.5 use-vrf default
#ip dhcp relay information option vpn	172.16.99.5 use-vrf default #interface vlan 21 #ip dhcp relay address	
#ipv6 dhcp relay	172.16.99.5 use-vrf default #interface vlan 22 #ip dhcp relay address	
#interface vlan 11	172.16.99.5 use-vrf default #interface vlan 23 #ip dhcp relay address	
#ip dhcp relay address	172.16.99.5 use-vrf default #interface vlan 20 #ip dhcp relay address	
172.16.99.5 use-vrf default	172.16.99.5 use-vrf default #interface vlan 21 #ip dhcp relay address	
#interface vlan 12	172.16.99.5 use-vrf default #interface vlan 22 #ip dhcp relay address	
#ip dhcp relay address	172.16.99.5 use-vrf default #interface vlan 23 #ip dhcp relay address	
172.16.99.5 use-vrf default	172.16.99.5 use-vrf default #interface vlan 20 #ip dhcp relay address	
#interface vlan 13	172.16.99.5 use-vrf default #interface vlan 21 #ip dhcp relay address	
#ip dhcp relay address	172.16.99.5 use-vrf default #interface vlan 22 #ip dhcp relay address	
172.16.99.5 use-vrf default	172.16.99.5 use-vrf default #interface vlan 23 #ip dhcp relay address	
#interface vlan 14	172.16.99.5 use-vrf default #interface vlan 20 #ip dhcp relay address	
#ip dhcp relay address	172.16.99.5 use-vrf default #interface vlan 21 #ip dhcp relay address	
172.16.99.5 use-vrf default	172.16.99.5 use-vrf default #interface vlan 22 #ip dhcp relay address	
#interface vlan 15	172.16.99.5 use-vrf default #interface vlan 23 #ip dhcp relay address	
#ip dhcp relay address	172.16.99.5 use-vrf default	
		11. Cấu hình Telnet/SSH
		#feature telnet
		#telnet server enable
		#feature ssh
		#ssh server enable
		#username adminHO
		password AdminHO@123
		#username adminHO role
		network-admin

Bảng 5.12 Các lệnh cấu hình của Switch Sw_A

Sw_A		
1. Cấu hình cơ bản		
#hostname Sw_A	#no shutdown	#switchport mode access
#ip domain-name cmu.edu	#interface range e0/0-1	#switchport access vlan 13
#no ip domain-lookup	#switchport trunk encapsulation dot1q	#no shutdown #interface range
	#switchport mode trunk	Ethernet1/1-3
2. Cấu hình VLAN	#channel-protocol lacp	#switchport mode access
#vlan 11	#channel-group 1 mode	#switchport access vlan 14
#name HanhChinh	active	#no shutdown
#vlan 12	#no shutdown	
#name DaoTao		
#vlan 13		
#name TuyenSinh	4. Cấu hình Access mode	5. Cấu hình Telnet/SSH
#vlan 14	#interface Ethernet0/2	#crypto key generate rsa generatal-keys 1024
#name Lab	#switchport mode access	#username adminHO
	#switchport access vlan 11	secret AdminHO@123
	#no shutdown	
3. Cấu hình Port-channel	#interface Ethernet0/3	#ip ssh ver 2
#interface Port-channel1	#switchport mode access	#line vty 0 4
#switchport trunk	#switchport access vlan 12	#login local
encapsulation dot1q	#no shutdown	#transport input SSH
#switchport mode trunk	#interface Ethernet1/0	

6. Cấu hình chế độ Port-security	7. Thiết lập cơ chế AAA	8. Cấu hình mật khẩu cho các quyền truy cập
#interface range e0/2-3, e1/0-3 #switchport port-security #switchport port-security maximum 1 #switchport port-security violation shutdown	#aaa new-model #aaa authentication login default local #aaa authorization exec default local #aaa accounting exec default start-stop local	#enable secret AdminHO@123 #line console 0 #password AdminHO@123 #login #line vty 0 4 #password AdminHO@

Bảng 5.13 Các lệnh cấu hình của Switch Sw_B

Sw_B		
1. Cấu hình cơ bản	#vlan 18 #name TCNH #vlan 19 #name PhongHocB	#switchport trunk encapsulation dot1q #switchport mode trunk #channel-protocol lacp #channel-group 2 mode active
2. Cấu hình VLAN	3. Cấu hình Port-channel	#no shutdown
#vlan 15 #name KHXHNV #vlan 16 #name Duoc #vlan 17 #name NgoaiNgu	#interface Port-channel2 #switchport trunk encapsulation dot1q #switchport mode trunk #no shutdown #interface range e0/0-1	#interfce Ethernet0/2 #switchport mode access #switchport access vlan 15
		4. Cấu hình Access mode

#no shutdown #interface Ethernet0/3 #switchport mode access #switchport access vlan 16 #no shutdown #interface Ethernet1/0 #switchport mode access #switchport access vlan 17 #no shutdown #interface Ethernet1/1 #switchport mode access #switchport access vlan 18 #no shutdown #interface range Ethernet1/2-3 #switchport mode access #switchport access vlan 19 #no shutdown #interface range Etherne2/0-1 #switchport mode access	#switchport access vlan 19 #no shutdown 5. Cấu hình Telnet/SSH #crypto key generate rsa generatal-keys 1024 #username adminHO secret AdminHO@123 #ip ssh ver 2 #line vty 0 4 #login local #transport input SSH	violation shutdown 7. Thiết lập cơ chế AAA #aaa new-model #aaa authentication login default local #aaa authorization exec default local #aaa accounting exec default start-stop local
	 6. Cấu hình chế độ Port-security #interface range e0/2-3, e1/0-3, e2/0-1 #switchport port-security maximum 1 #switchport port-security	 8. Cấu hình mật khẩu cho các quyền truy cập #enable secret AdminHO@123 #line console 0 #password AdminHO@123 #login #line vty 0 4 #password AdminHO@

Bảng 5.14 Các lệnh cấu hình của Switch Sw_C

Sw_C		
1. Cấu hình cơ bản		
#hostname Sw_C	#no shutdown	#switchport mode access
#ip domain-name cmu.edu	#interface range e0/0-1	#switchport access vlan 22
#no ip domain-lookup	#switchport trunk encapsulation dot1q	#no shutdown #interface range
	#switchport mode trunk	Ethernet1/1-3
2. Cấu hình VLAN		
#vlan 20	#channel-protocol lacp	#switchport mode access
#name QTKD	#channel-group 3 mode active	#switchport access vlan 23
#vlan 21	#no shutdown	#no shutdown
#name CNTT		#interface Etherne2/0
#vlan 22		#switchport mode access
#name ThuVien		#switchport access vlan 23
#vlan 23		#no shutdown
#name PhongHocC		
	4. Cấu hình Access mode	
	#interface Ethernet0/2	#switchport access vlan 20
	#switchport mode access	#no shutdown
	#switchport access vlan 20	
	#no shutdown	
	#interface Ethernet0/3	#crypto key generate rsa
3. Cấu hình Port-channel		generatal-keys 1024
#interface Port-channel3	#switchport mode access	#username adminHO
#switchport trunk	#switchport access vlan 21	secret AdminHO@123
encapsulation dot1q	#no shutdown	#ip ssh ver 2
#switchport mode trunk	#interface Ethernet1/0	#line vty 0 4

#login local #transport input SSH	#switchport port-security violation shutdown	8. Cấu hình mật khẩu cho các quyền truy cập
6. Cấu hình chế độ Port-security #interface range e0/2-3, e1/0-3, e2/0 #switchport port-security #switchport port-security maximum 1	7. Thiết lập cơ chế AAA #aaa new-model #aaa authentication login default local #aaa authorization exec default local #aaa accounting exec default start-stop local	#enable secret AdminHO@123 #line console 0 #password AdminHO@123 #login #line vty 0 4 #password AdminHO@

Bảng 5.15 Các lệnh cấu hình của Switch Sw_DC1

Sw_DC1		
1. Cấu hình cơ bản #hostname Sw_DC1 #ip domain-name cmu.edu #no ip domain-lookup	#interface Port-channel4 #switchport trunk encapsulation dot1q #switchport mode trunk #no shutdown	#channel-group 4 mode active #no shutdown
2. Cấu hình VLAN #vlan 99 #name KyThuat	#interface range e0/0-1 #switchport trunk encapsulation dot1q #switchport mode trunk	4. Cấu hình Access mode #interface range Ethernet0/2-3 #switchport mode access #switchport access vlan 99
3. Cấu hình Port-channel	#channel-protocol lacp	#no shutdown

#interface Etherne1/0 #switchport mode access #switchport access vlan 99 #no shutdown	#login local #transport input SSH	7. Cấu hình mật khẩu cho các quyền truy cập 6. Thiết lập cơ chế AAA
5. Cấu hình Telnet/SSH #crypto key generate rsa generatal-keys 1024 #username adminHO secret AdminHO@123 #ip ssh ver 2 #line vty 0 4	#aaa new-model #aaa authentication login default local #aaa authorization exec default local #aaa accounting exec default start-stop local	#enable secret AdminHO@123 #line console 0 #password AdminHO@123 #login #line vty 0 4 #password AdminHO@

Bảng 5.16 Các lệnh cấu hình của Switch Sw_DC2

Sw_DC2		
1. Cấu hình cơ bản #hostname Sw_DC2 #ip domain-name cmu.edu #no ip domain-lookup	3. Cấu hình Port-channel #interface Port-channel5 #switchport trunk encapsulation dot1q #switchport mode trunk #no shutdown	encapsulation dot1q #switchport mode trunk #channel-protocol lacp #channel-group 5 mode active #no shutdown
2. Cấu hình VLAN #vlan 99 #name KyThuat	#interface range e0/0-1 #switchport trunk	4. Cấu hình Access mode

#interface range Ethernet0/2-3 #switchport mode access #switchport access vlan 99 #no shutdown #interface range Etherne1/0-1 #switchport mode access #switchport access vlan 99 #no shutdown	generatal-keys 1024 #username adminHO secret AdminHO@123 #ip ssh ver 2 #line vty 0 4 #login local #transport input SSH	default local #aaa accounting exec default start-stop local
5. Cấu hình Telnet/SSH #crypto key generate rsa	6. Thiết lập cơ chế AAA #aaa new-model #aaa authentication login default local #aaa authorization exec	7. Cấu hình mật khẩu cho các quyền truy cập #enable secret AdminHO@123 #line console 0 #password AdminHO@123 #login #line vty 0 4 #password AdminHO@

Khu vực chi nhánh:

Bảng 5.17 Các lệnh cấu hình của Router R3

R3		
1. Cấu hình cơ bản #hostname R3 #ip domain-name cmu.edu #no ip domain-lookup	#ip address 14.16.242.2 255.255.255.252 #no shutdown #interface e0/0 #ip address 172.17.0.05 255.255.255.252	3. Cấu hình định tuyến OSPF #router ospf 1 #router-id 12.0.0.1 #interface s4/0 #ip ospf 1 area 1 #interface e0/0
2. Cấu hình địa chỉ IP #interface s4/0	#no shutdown	

#ip ospf 1 area 0 4. Cấu hình định tuyến static #ip route 0.0.0.0 0.0.0.0 14.16.242.1	5. Cấu hình Telnet/SSH #crypto key generate rsa general-keys 1024 #username adminHO	secret AdminBO@123 #ip ssh ver 2 #line vty 0 4 #login local #transport input SSH
---	---	--

Bảng 5.18 Các lệnh cấu hình của Switch Sw_BO

Sw_BO		
1. Cấu hình cơ bản #hostname Sw_BO #ip domain-name cmu.edu #no ip domain-lookup	#ip ospf 1 area 0	#switchport trunk allow vlan all
2. Cấu hình địa chỉ IP #interface e0/0 #ip address 172.17.0.06 255.255.255.252 #no shutdown	4. Tạo VLAN #vlan 109 #name KyThuat_CT #vlan 24 #name VPK #vlan 25 #name ThuVien_CT #vlan 26 #name PhongHocD	#no shutdown #interface e0/2 #switchport #switchport mode trunk #switchport trunk allow vlan all #no shutdown
3. Cấu hình định tuyến OSPF #router ospf 1 #router-id 12.0.0.2 #interface e0/0	5. Cấu hình Trunking mode #interface e0/1 #switchport #switchport mode trunk	6. Cấu hình Access mode #interface e0/1 #switchport mode access #switchport access vlan 109 #no shutdown

#interface e0/2 #switchport mode access #switchport access vlan 24	#no shutdown #interface e0/3	#switchport mode access #switchport access vlan 24
--	---------------------------------	---

Bảng 5.19 Các lệnh cấu hình của Switch Sw_D1

Sw_D1		
1. Cấu hình cơ bản	vlan all #no shutdown	#no shutdown
#hostname Sw_DC1 #ip domain-name cmu.edu #no ip domain-lookup	_____	5. Cấu hình Telnet/SSH #crypto key generate rsa general-keys 1024 #username adminBO secret AdminBO@123 #ip ssh ver 2 #line vty 0 4 #login local #transport input SSH
2. Tạo VLAN	#switchport mode access #switchport access vlan 109 #name KyThuat_CT	_____
	#no shutdown #interface e0/2	#line vty 0 4 #login local #transport input SSH
3. Cấu hình Trunking mode	#switchport mode access #switchport access vlan 24 #no shutdown #interface e0/3	6. Cấu hình chế độ Port-security #interface range e0/1-3 #switchport
	#switchport mode trunk #switchport trunk allow	

#switchport port-security #switchport port-security maximum 1 #switchport port-security violation shutdown <hr/> 7. Thiết lập cơ chế AAA #aaa new-model	#aaa authentication login default local #aaa authorization exec default local #aaa accounting exec default start-stop local <hr/> 8. Cấu hình mật khẩu cho	các quyền truy cập #enable secret AdminBO@123 #line console 0 #password AdminBO@123 #login #line vty 0 4 #password AdminBO@
--	---	--

Bảng 5.20 Các lệnh cấu hình của Switch Sw_D2

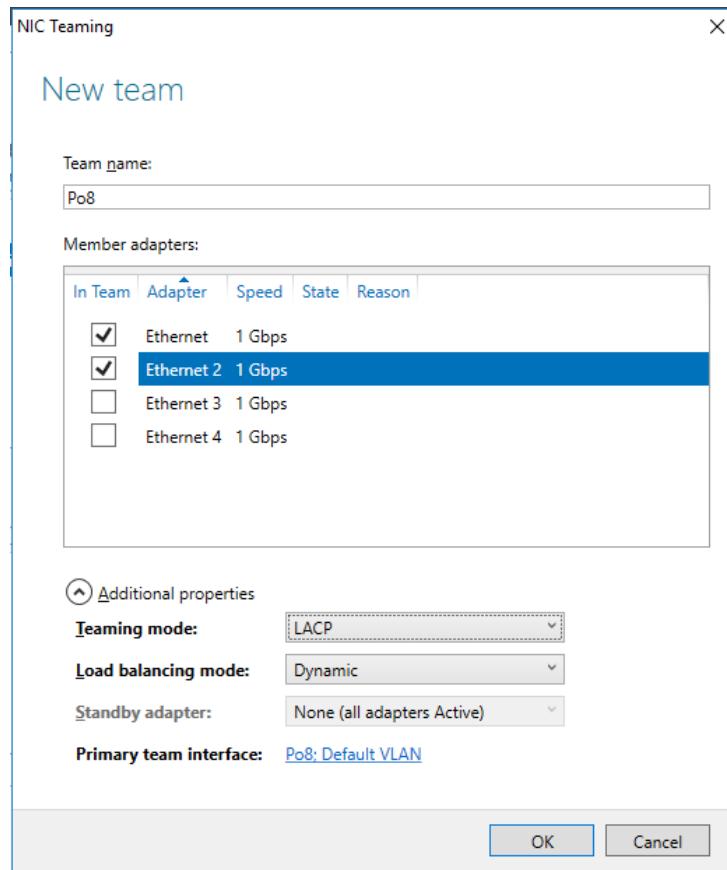
Sw_D2		
1. Cấu hình cơ bản #hostname Sw_DC2 #ip domain-name cmu.edu #no ip domain-lookup <hr/>	#interface e1/0 #switchport #switchport mode trunk #switchport trunk allow vlan all <hr/>	#interface e0/2 #switchport mode access #switchport access vlan 26 #no shutdown #interface e1/0 <hr/>
2. Tạo VLAN #vlan 25 #name ThuVien_CT #vlan 26 #name PhongHocD <hr/>	#no shutdown <hr/> 4. Cấu hình Access mode #interface e0/1 #switchport mode access #switchport access vlan 25 <hr/>	#switchport mode access #switchport access vlan 26 #no shutdown #interface e1/1 #switchport mode access #switchport access vlan 26 <hr/>
3. Cấu hình Trunking mode	#no shutdown	#no shutdown

#interface e1/2 #switchport mode access #switchport access vlan 26 #no shutdown	6. Cấu hình chế độ Port-security #interface range e0/1-2, e1/0-2 #switchport port-security	#aaa authorization exec default local #aaa accounting exec default start-stop local
5. Cấu hình Telnet/SSH #crypto key generate rsa general-keys 1024 #username adminBO secret AdminBO@123 #ip ssh ver 2 #line vty 0 4 #login local #transport input SSH	#switchport port-security maximum 1 #switchport port-security violation shutdown	8. Cấu hình mật khẩu cho các quyền truy cập #enable secret AdminBO@123 #line console 0 #password AdminBO@123 #login #line vty 0 4 #password AdminBO@
	7. Thiết lập cơ chế AAA #aaa new-model #aaa authentication login default local	

5.2 Cấu hình các server

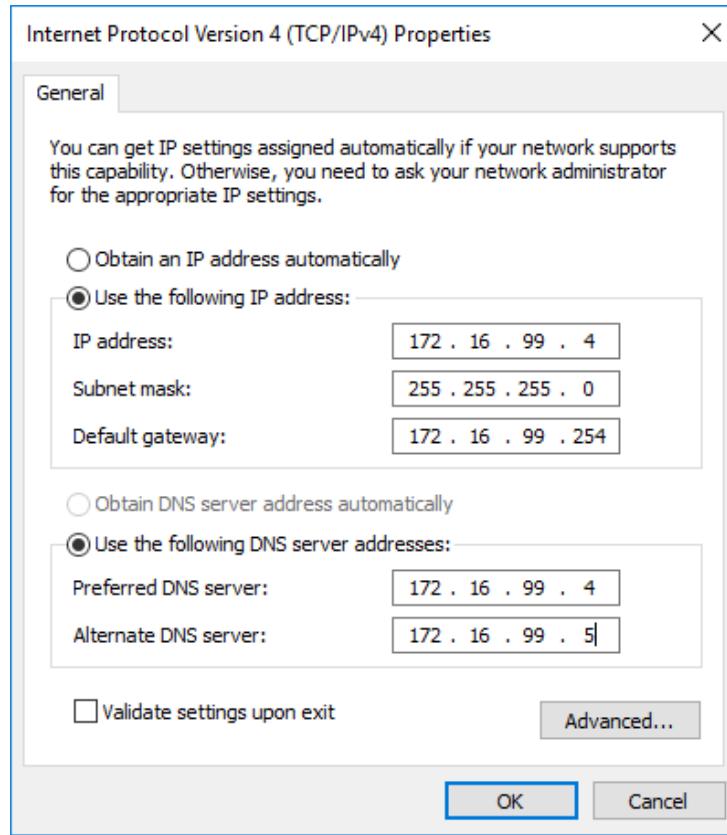
5.2.1 Cấu hình server RADIUS

a) Cấu hình NIC Teaming



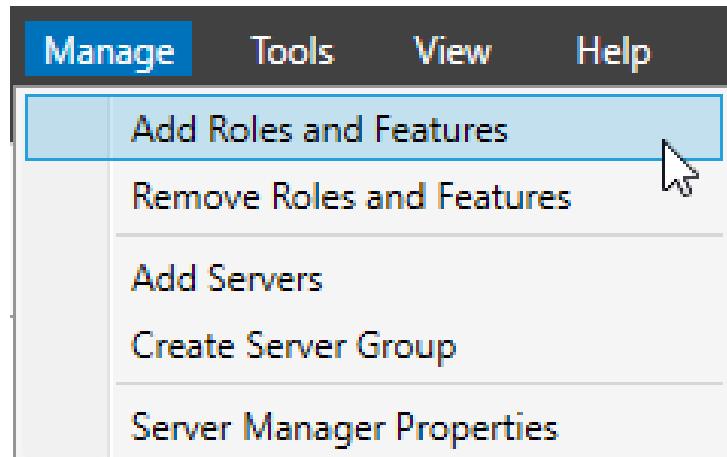
Hình 5.1 Đặt Team name là Po8 -> Chọn Ethernet và Ethernet2 -> Chọn Teaming mode là LACP -> Apply

b) Cấu hình địa chỉ IPv4 cho NIC Teaming

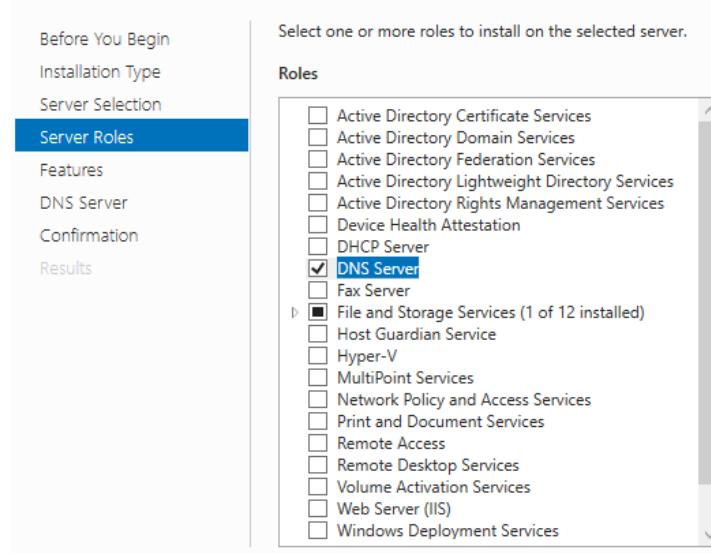


Hình 5.2 ĐIỀN ĐỊA CHỈ IPv4 VÀ DNS -> CHỌN OK

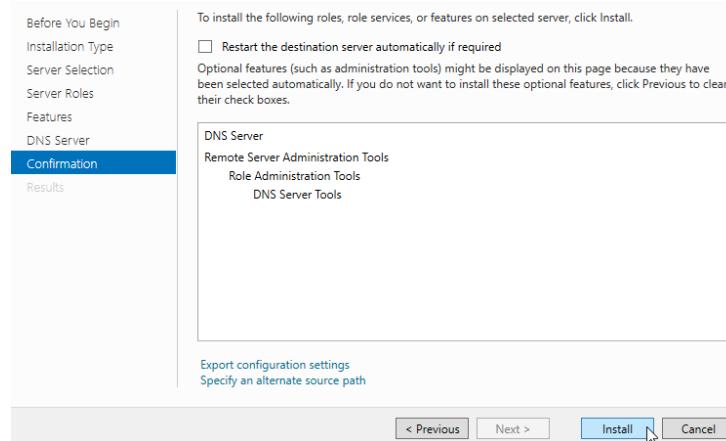
c) Cấu hình dịch vụ DNS Server



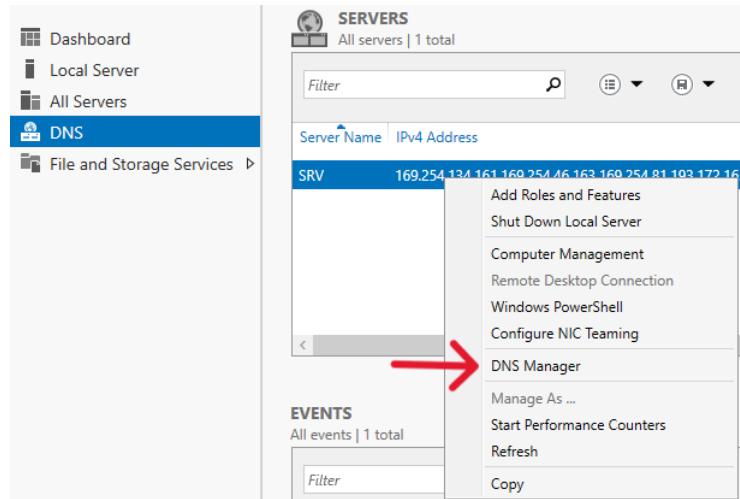
Hình 5.3 Chọn Manage -> Add Roles and Features để thêm dịch vụ server



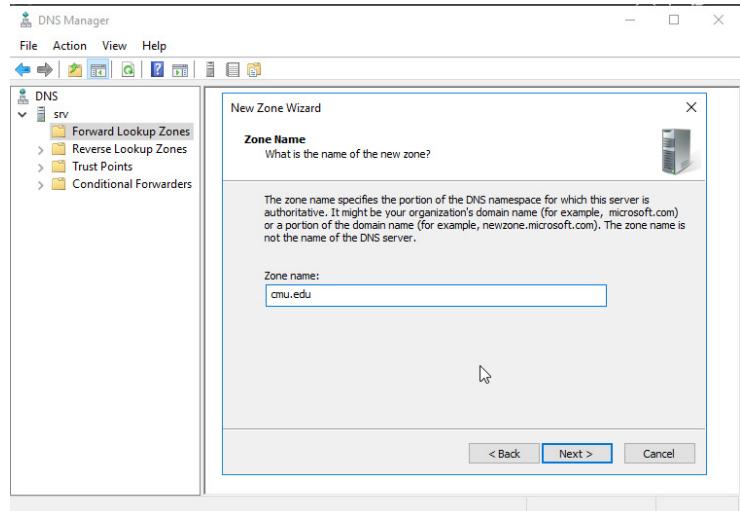
Hình 5.4 Chọn Server Roles là DNS Server



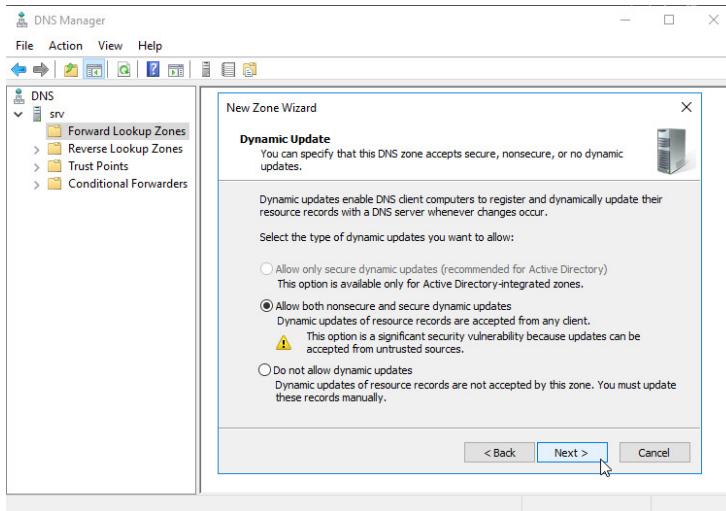
Hình 5.5 Chọn Install để thêm dịch vụ DNS Server



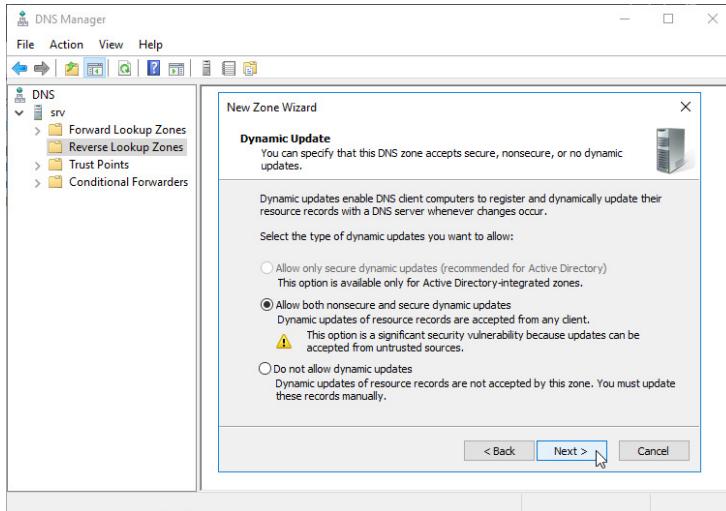
Hình 5.6 Chọn DNS Manager



Hình 5.7 Cấu hình Zone Name cmu.edu

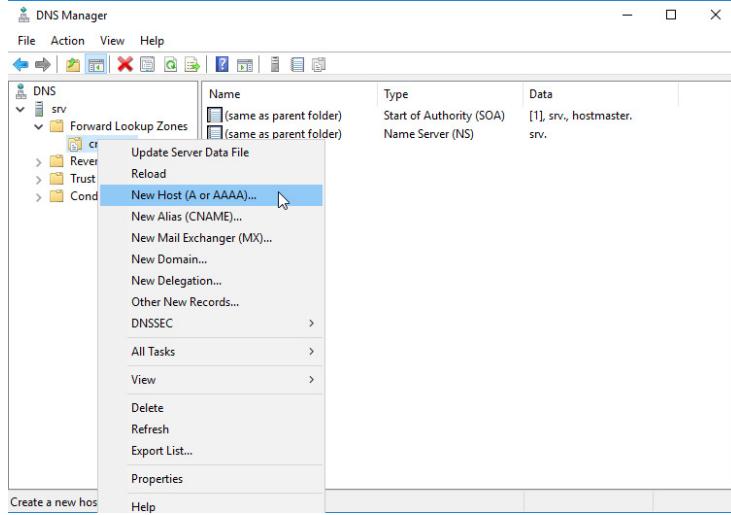


Hình 5.8 Cấu hình Forward Lookup Zones

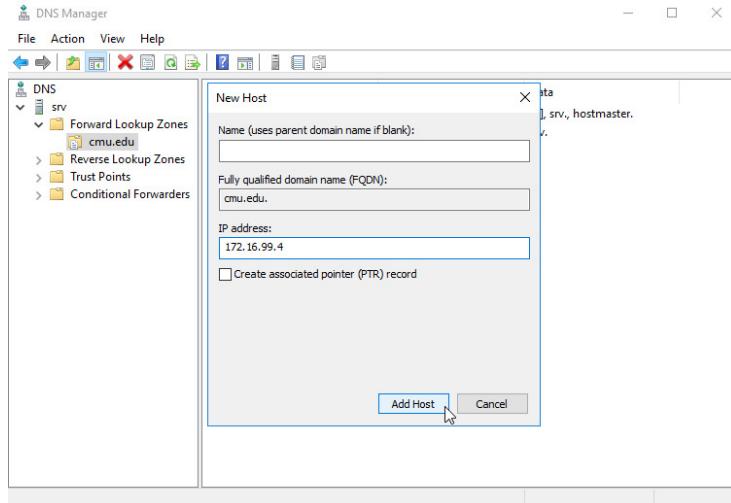


Hình 5.9 Cấu hình Reverse Lookup Zones

Tạo bản ghi A cho domain của Web Server:

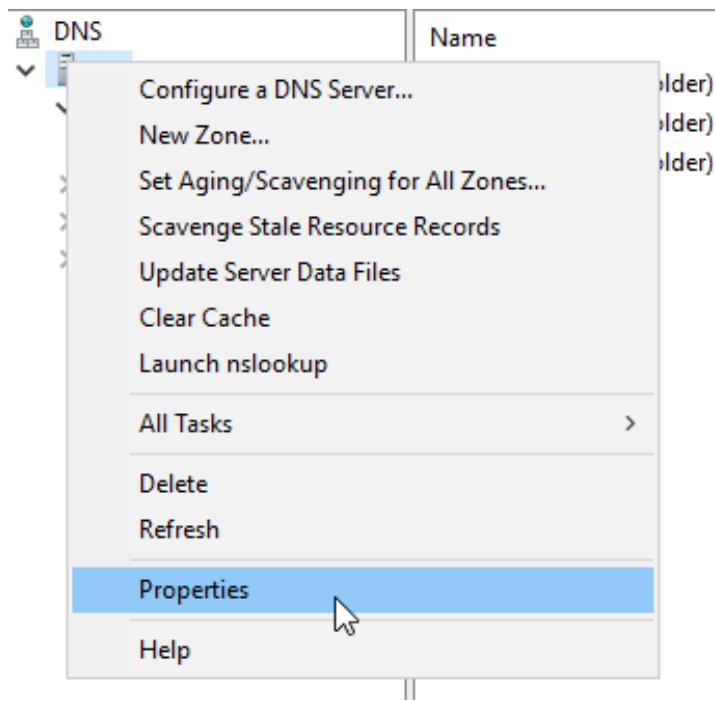


Hình 5.10 Chọn New Host

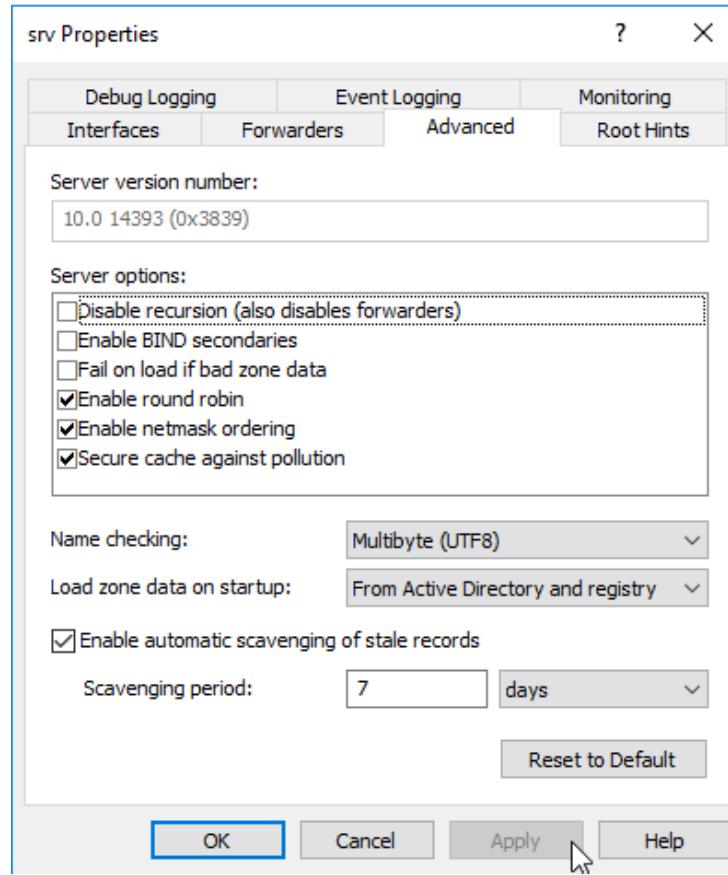


Hình 5.11 Điền địa chỉ IP -> Chọn Add Host

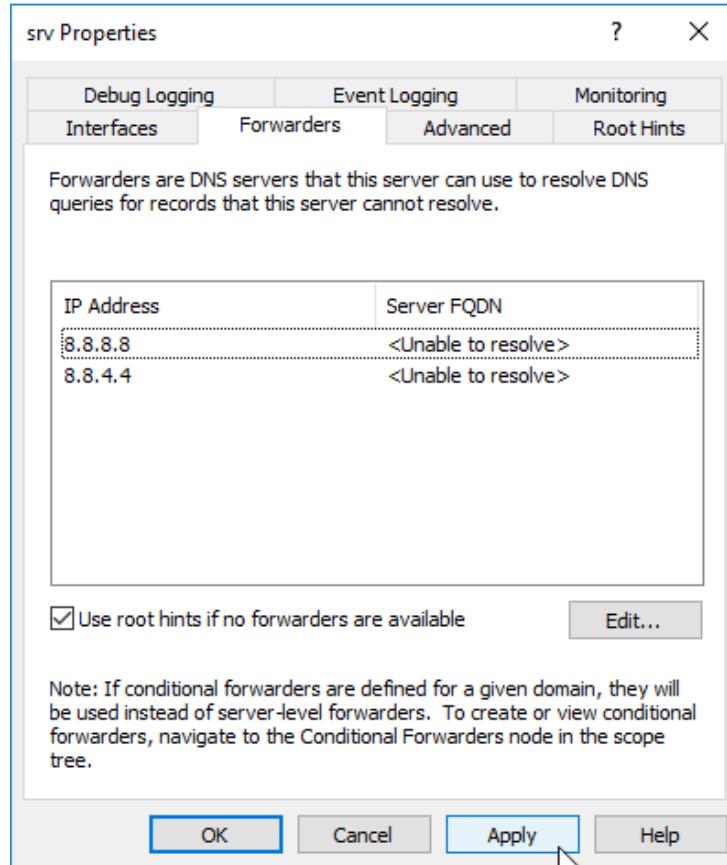
Cấu hình DNS recursive để phân giải tên miền các địa chỉ ở bên ngoài mạng LAN:



Hình 5.12 Chọn Properties



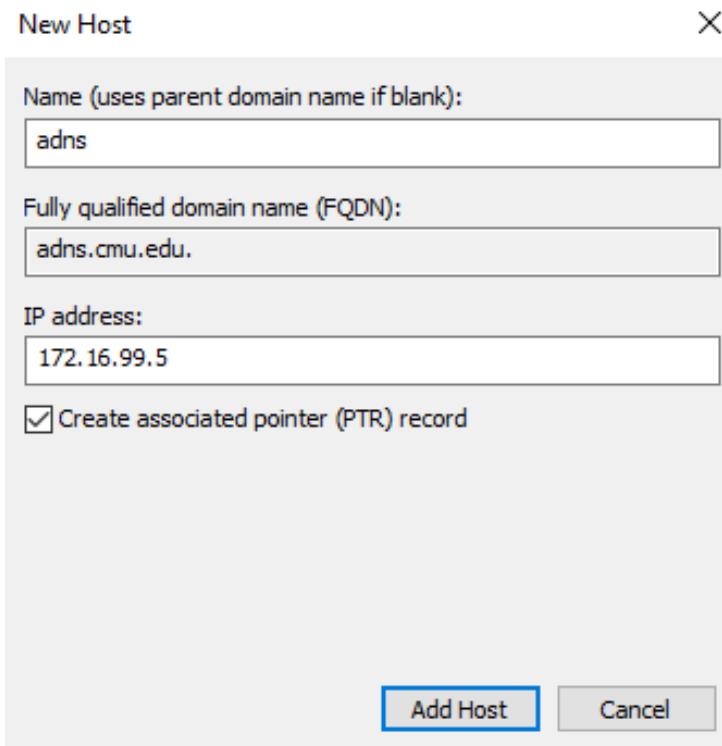
Hình 5.13 Cấu hình Advanced



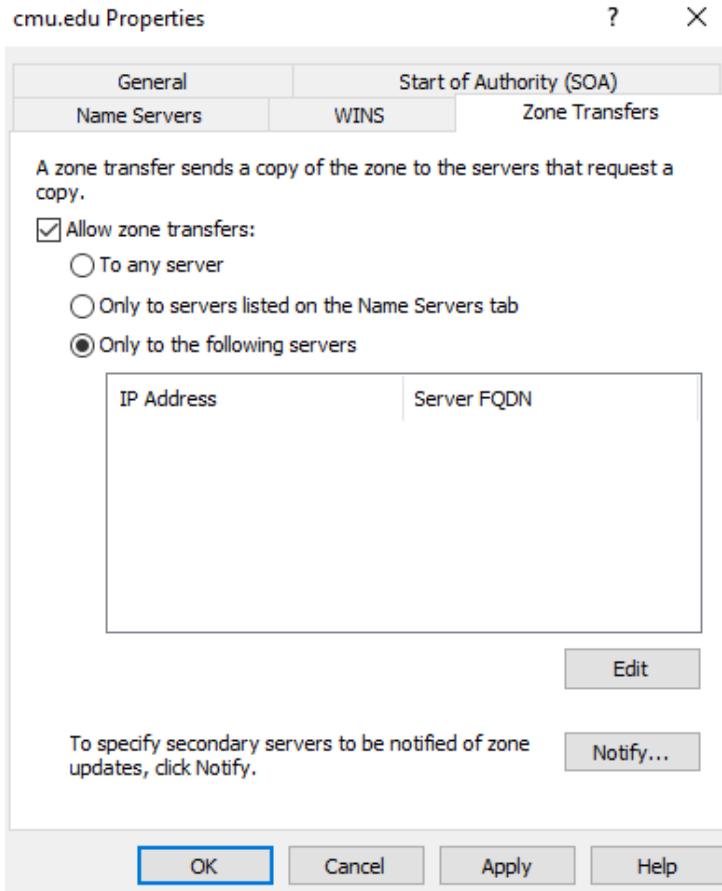
Hình 5.14 Cấu hình Forwarders -> Chọn Apply

d) Cấu hình Alternative DNS

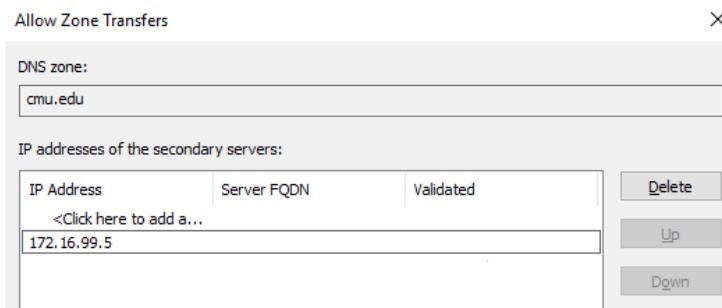
Tạo New Host với địa chỉ IP của Server DNS _Mail _DHCP làm Alternative DNS:



Hình 5.15 Chọn Add Host

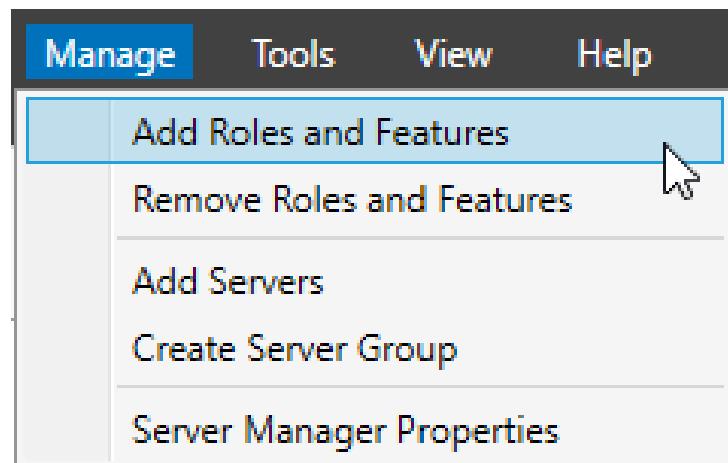


Hình 5.16 Cấu hình Zone Transfers

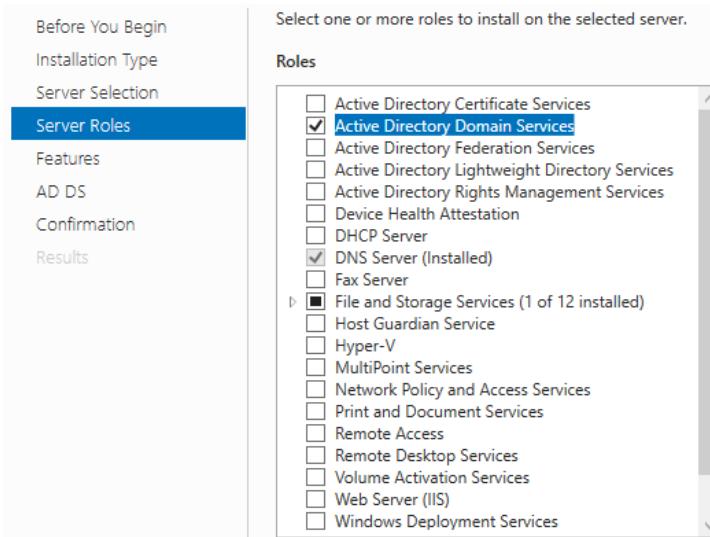


Hình 5.17 Allow Zone Transfers

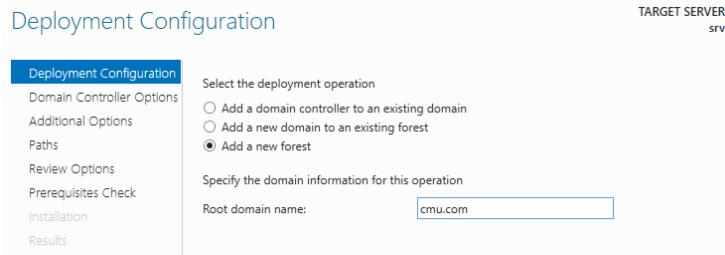
e) Cấu hình Active Directory Domain Service



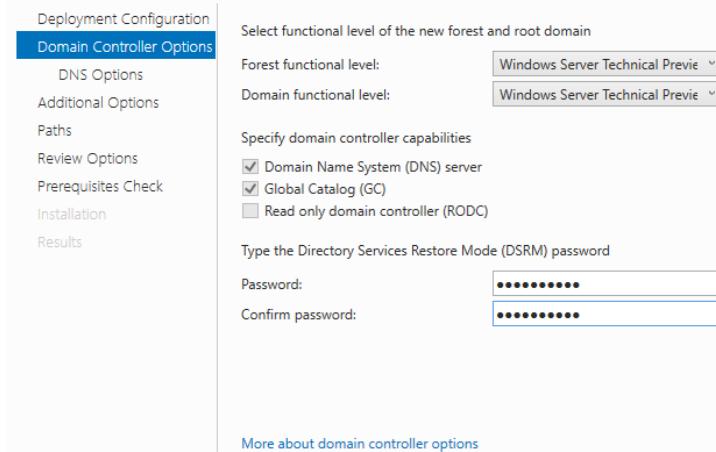
Hình 5.18 Chọn Add Role and Features



Hình 5.19 Chọn Active Directory Domain Service

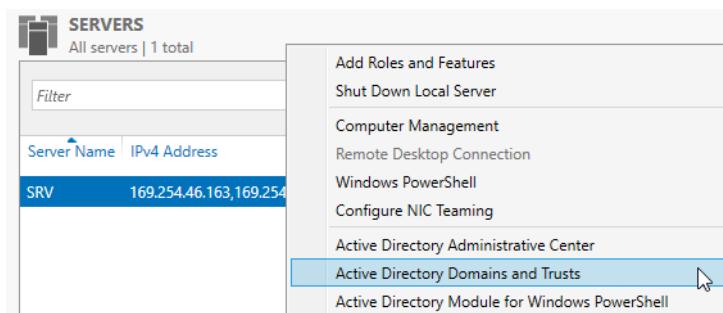


Hình 5.20 Deployment Configuration

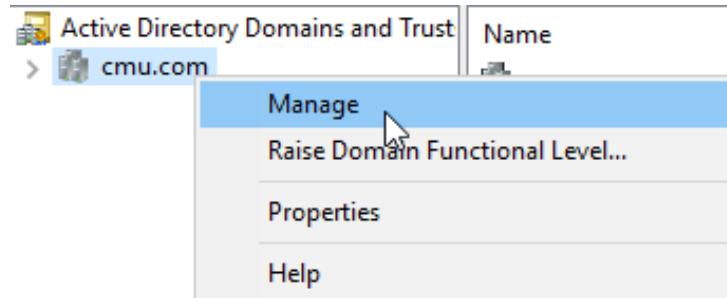


Hình 5.21 Nhập password là Admin1@123

Câu hình quản lý Active Directory Domains and Trusts:

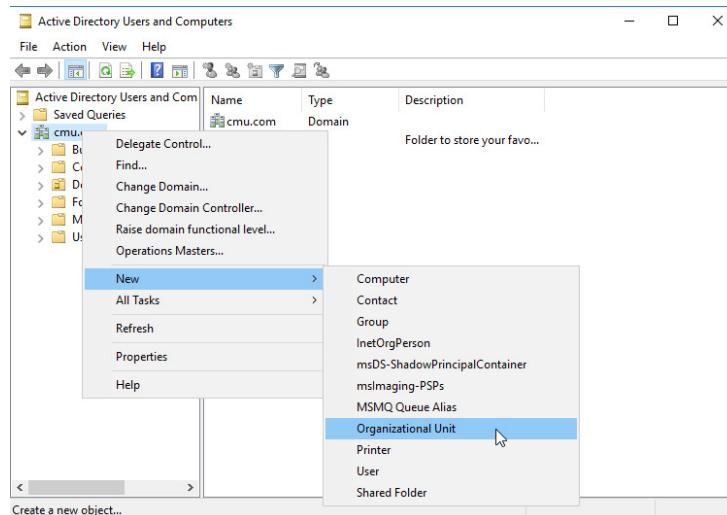


Hình 5.22 Chọn Active Directory Domains and Trusts

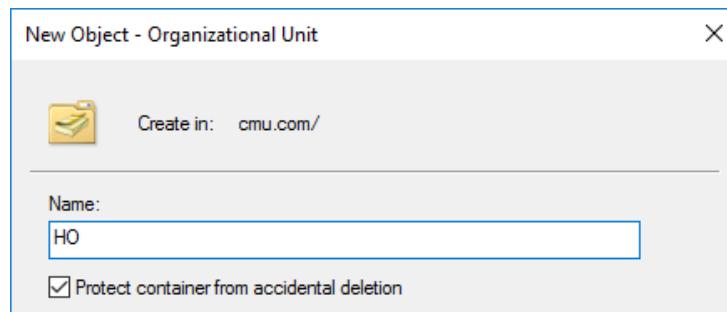


Hình 5.23 Chọn Manage

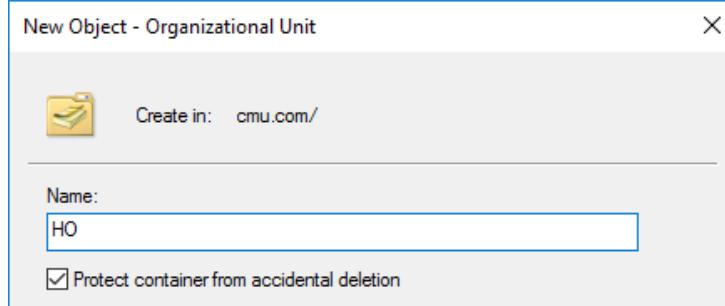
Tạo 2 Organizational Unit cho Head Office và Branch Office:



Hình 5.24 Chọn New -> Chọn Organizational Unit

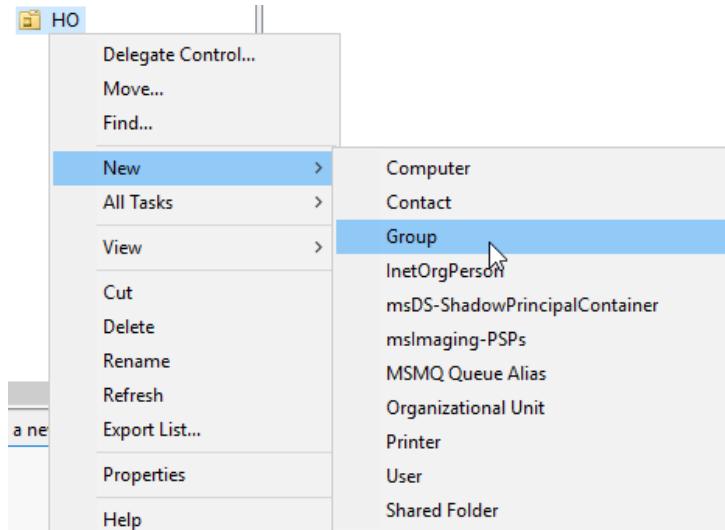


Hình 5.25 Nhập tên là HO

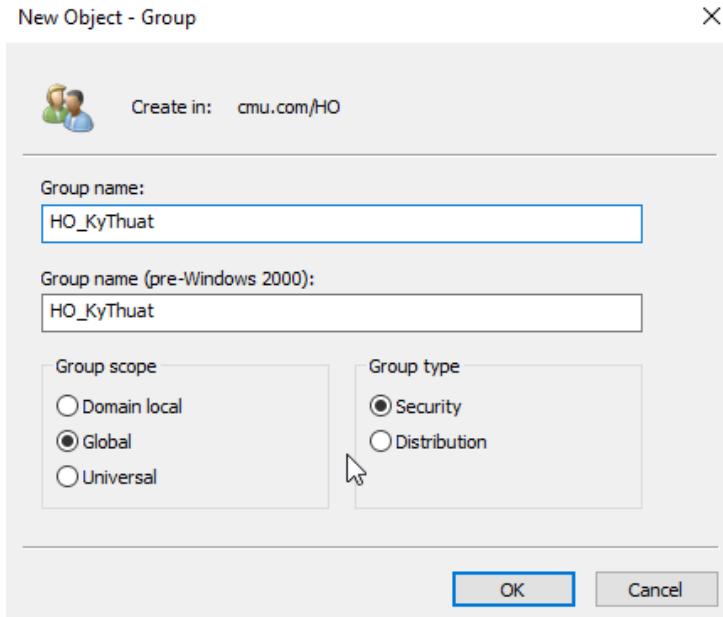


Hình 5.26 Nhập tên là BO

Tạo các Group cho các phòng ban:



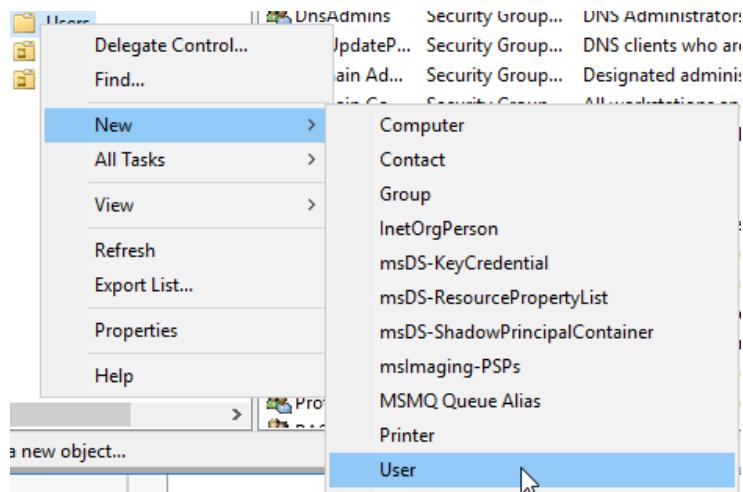
Hình 5.27 Chọn New -> Chọn Group



Hình 5.28 Nhập tên phòng ban

Làm tương tự với các phòng ban khác.

Tạo user và thêm user đó vào các phòng ban:



Hình 5.29 Chọn New -> Chọn User

New Object - User



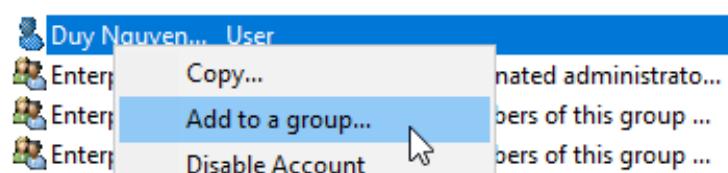
Create in: cmu.com/Users

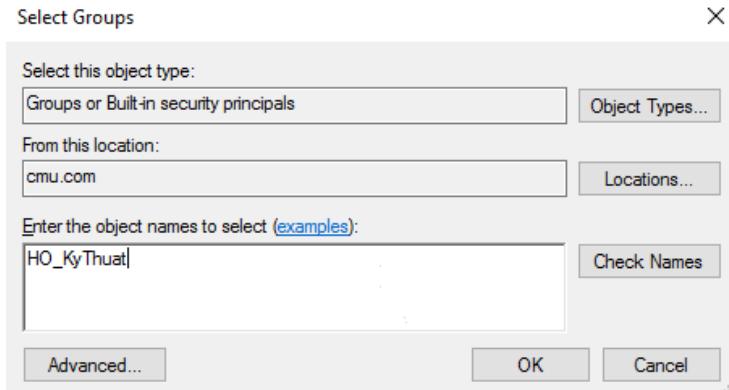
First name:	Duy	Initials:	
Last name:	Nguyen		
Full name:	Duy Nguyen Nha Thao		
User logon name:	duynnt	@cmu.com	▼
User logon name (pre-Windows 2000):	CMU\	duynnt	

Hình 5.30 Tạo User 1


Create in: cmu.com/Users

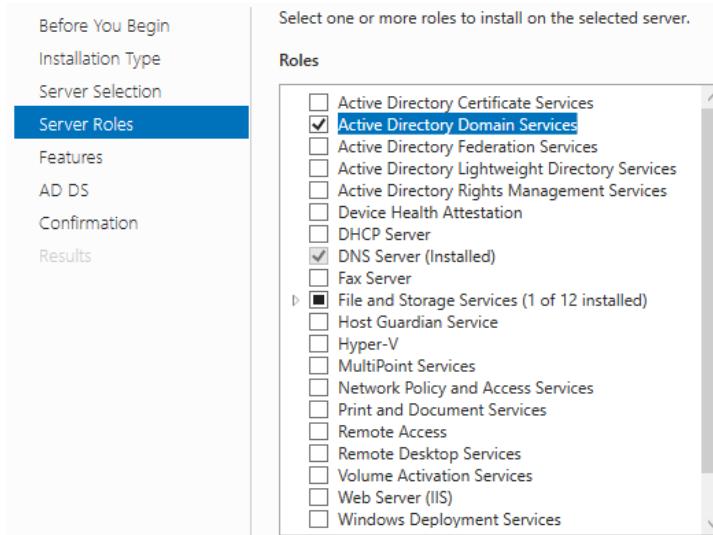
First name:	Suong	Initials:	
Last name:	Nguyen Thi Diem		
Full name:	Suong Nguyen Thi Diem		
User logon name:	suongntd	@cmu.com	▼
User logon name (pre-Windows 2000):	CMU\	suongntd	

Hình 5.31 Tạo User 2**Hình 5.32 Add User vào Group**

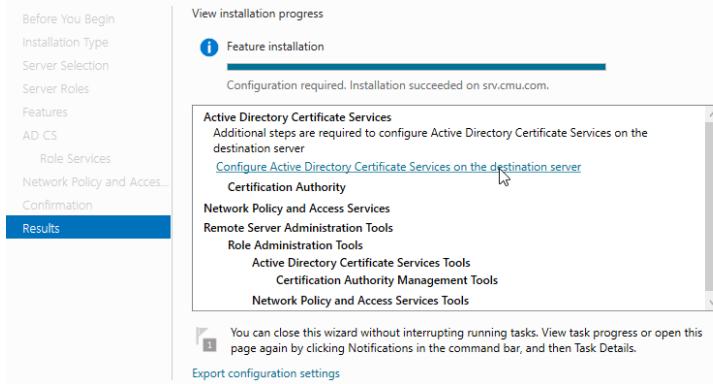


Hình 5.33 Chọn Groups

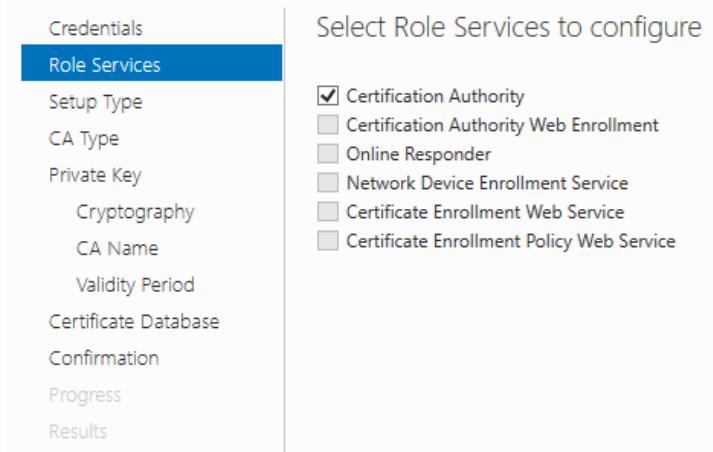
f) Cấu hình xác thực RADIUS



Hình 5.34 Chọn service Active Directory Domain Services và Network Policy and Access Service

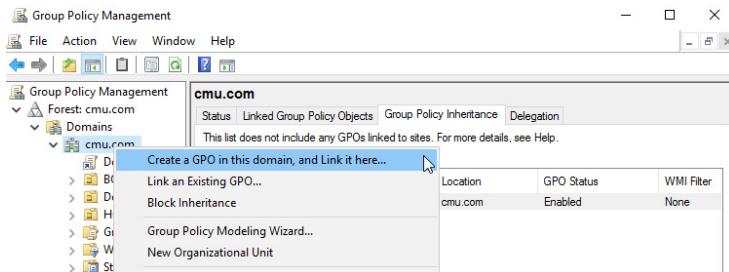


Hình 5.35 Cấu hình Active Directory Certificate Services

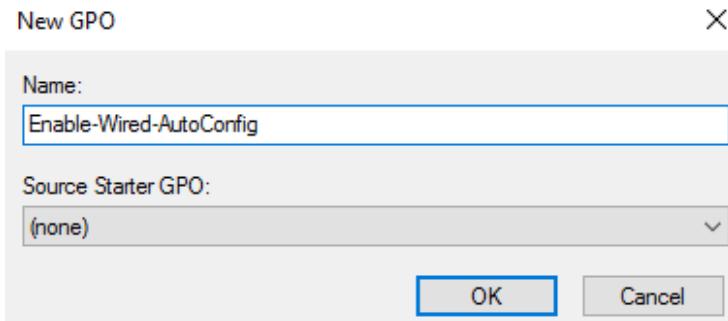


Hình 5.36 Chọn Certification Authority

Tạo Policy cho phép bật Wired AutoConfig Services:



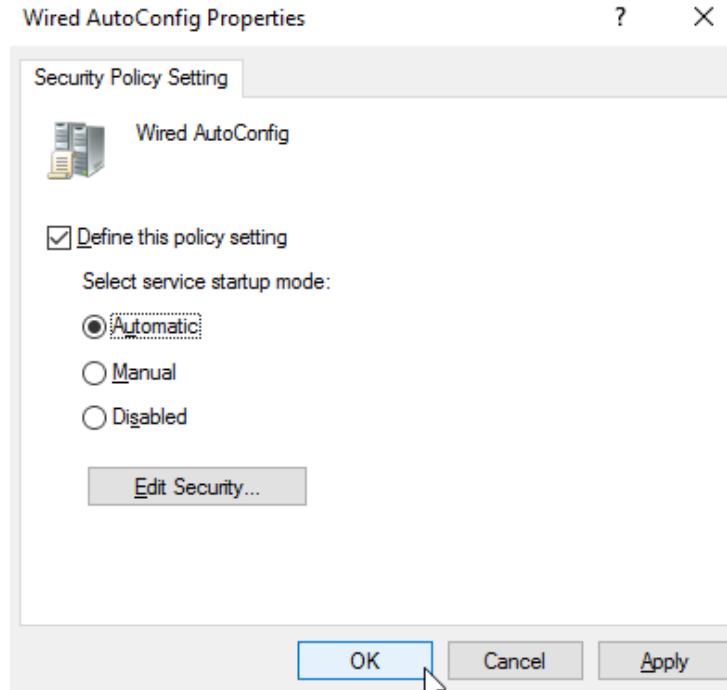
Hình 5.37 Tạo Policy



Hình 5.38 Nhập tên

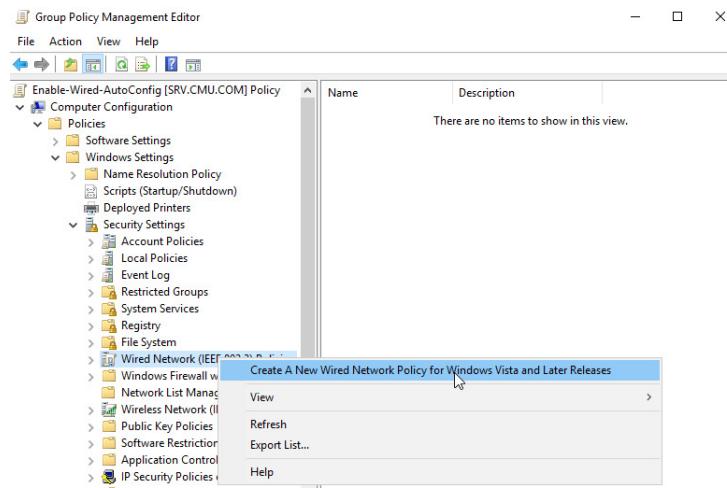
Service Name	Startup	Permission
Windows Event Log	Not Defined	Not Defined
Windows Firewall	Not Defined	Not Defined
Windows Font Cache Serv...	Not Defined	Not Defined
Windows Image Acquisiti...	Not Defined	Not Defined
Windows Insider Service	Not Defined	Not Defined
Windows Installer	Not Defined	Not Defined
Windows License Manage...	Not Defined	Not Defined
Windows Management In...	Not Defined	Not Defined
Windows Mobile Hotspot...	Not Defined	Not Defined
Windows Modules Installer	Not Defined	Not Defined
Windows Push Notificatio...	Not Defined	Not Defined
Windows Push Notificatio...	Not Defined	Not Defined
Windows Remote Manag...	Not Defined	Not Defined
Windows Search	Not Defined	Not Defined
Windows Time	Not Defined	Not Defined
Windows Update	Not Defined	Not Defined
WinHTTP Web Proxy Aut...	Not Defined	Not Defined
Wired AutoConfig	Not Defined	Not Defined
WMI Performance Adapter	Not Defined	Not Defined
Workstation	Help	Not Defined
Xbox Live Auth Manager	Not Defined	Not Defined
Xbox Live Game Save	Not Defined	Not Defined

Hình 5.39 Chọn Properties

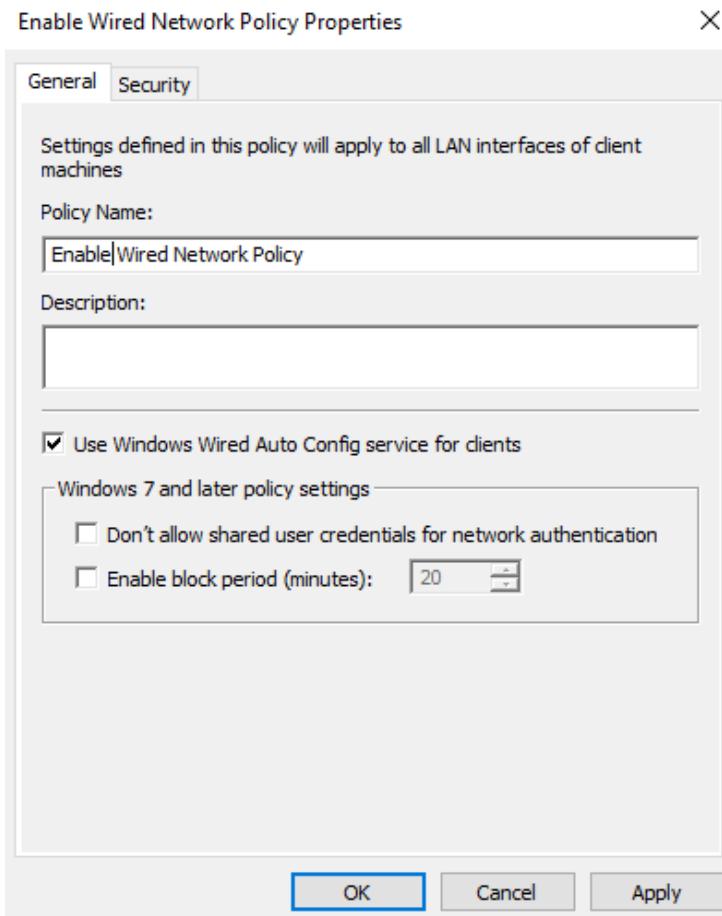


Hình 5.40 Chọn OK

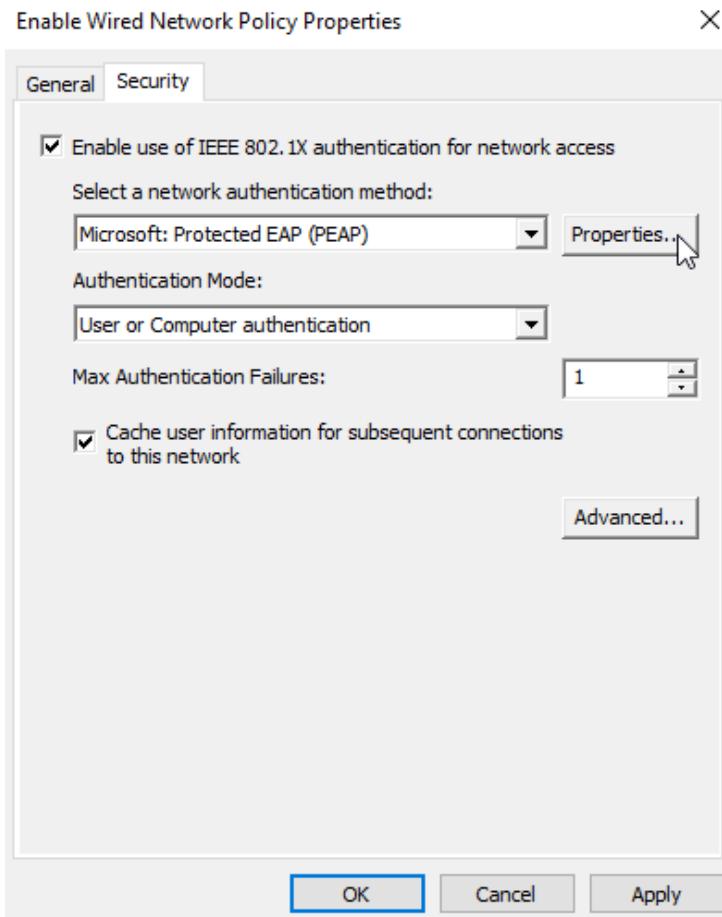
Tạo Policy cho phép bật IEEE 802.1X:



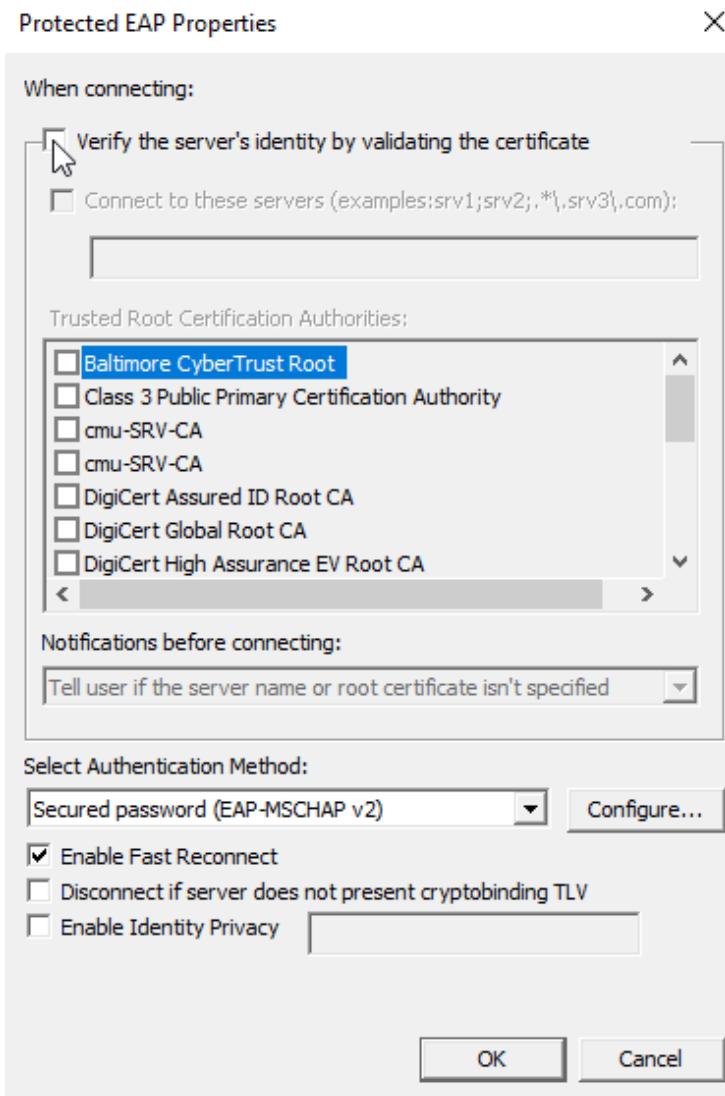
Hình 5.41 Tạo Policy



Hình 5.42 Nhập tên

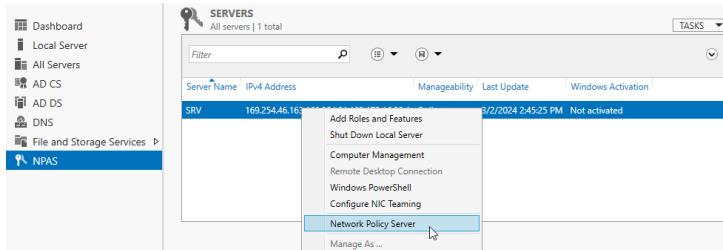


Hình 5.43 Chọn Security -> Chọn Properties

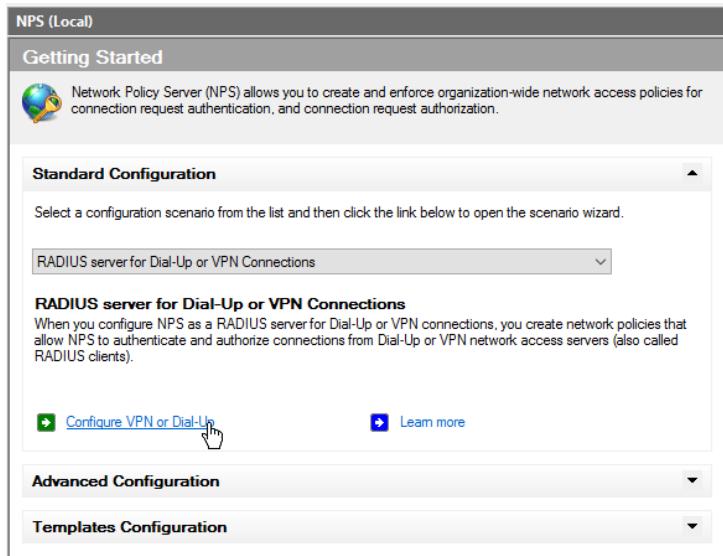


Hình 5.44 Bỏ chọn Verify the server's identity

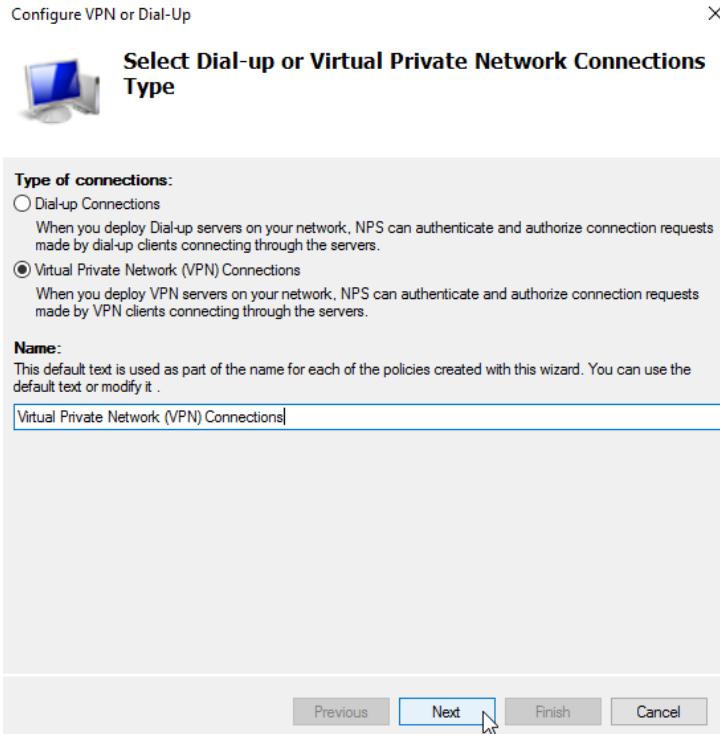
Cấu hình Radius Server theo chuẩn 802.1X:



Hình 5.45 Chọn Network Policy Server

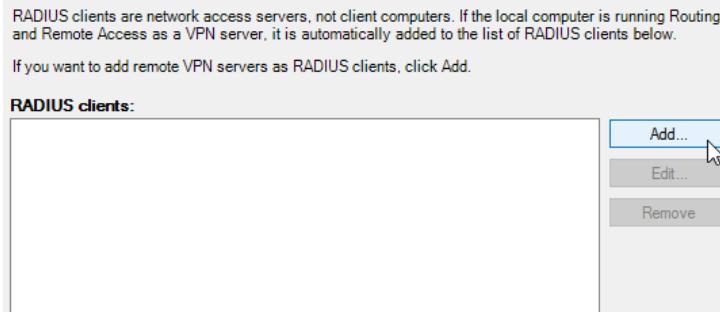


Hình 5.46 Chọn Configure VPN or Dial-Up

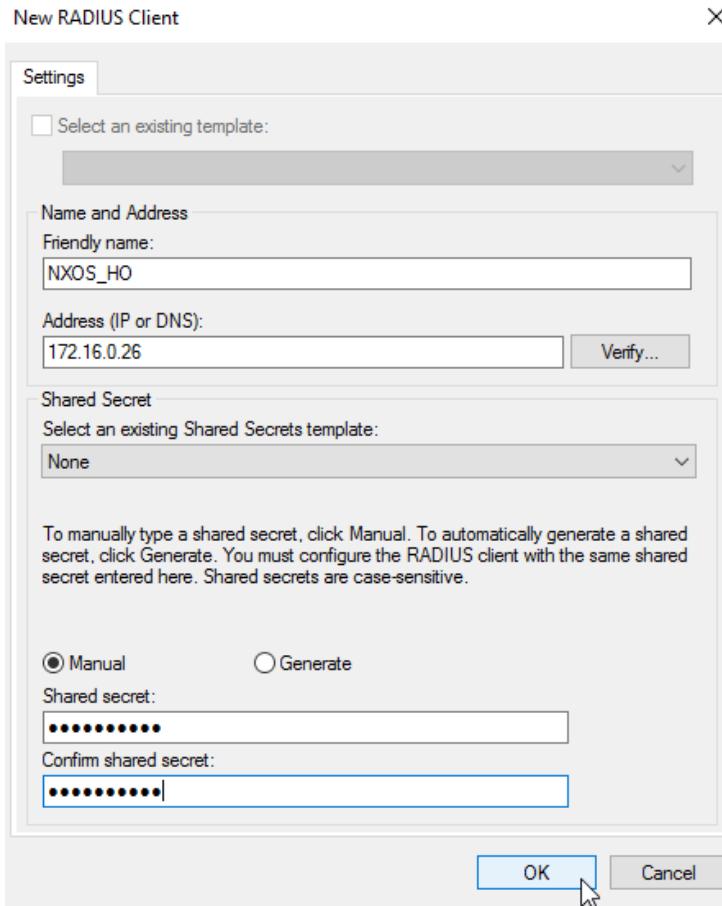


Hình 5.47 Chọn VPN

Thêm RADIUS clients là các switch Nexus trong hệ thống mạng:



Hình 5.48 Chọn Add



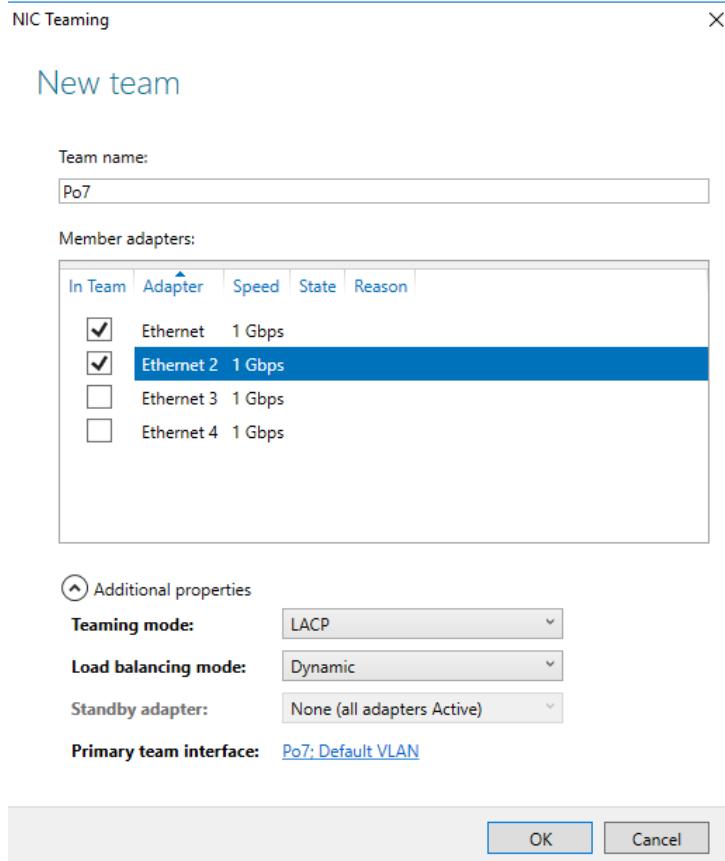
Hình 5.49 Nhập tên của các thiết bị sao cho dễ quản lý và IP tương ứng và Shared Secret là Admin1@123



Hình 5.50 Chọn Add

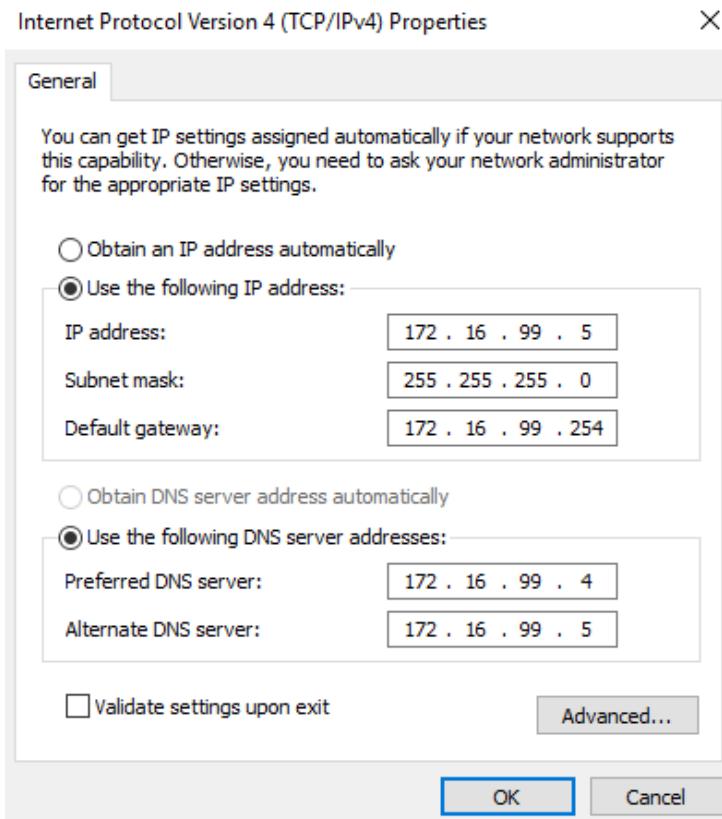
subsubsection Cấu hình server DNS_Mail_DHCP

a) Cấu hình NIC Teaming



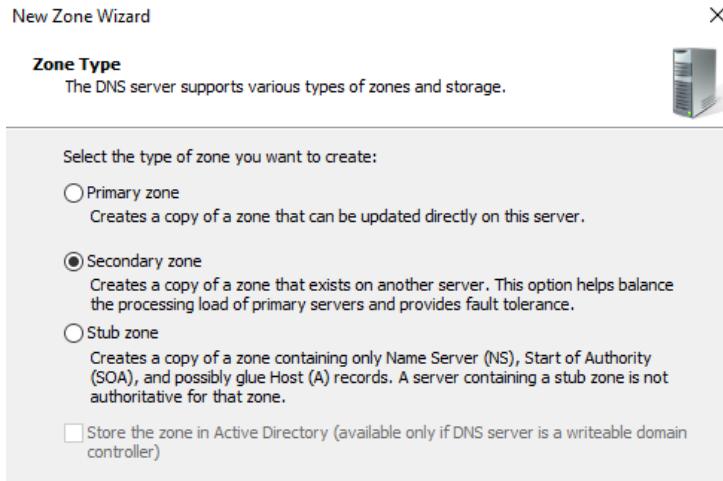
Hình 5.51 Nhập Team name là Po7 -> chọn Ethernet và Ethernet2 -> chọn Teaming mode là LACP

b) Cấu hình địa chỉ IPv4 cho NIC Teaming

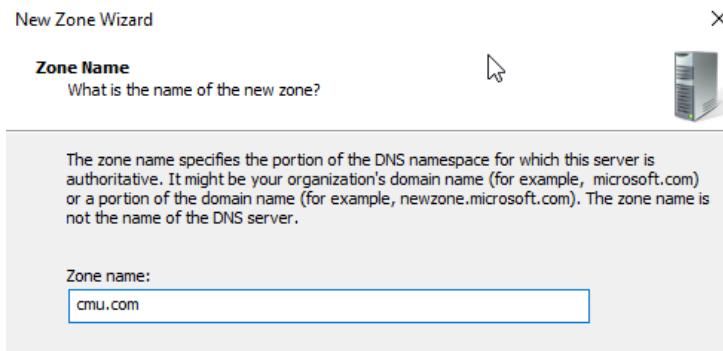


Hình 5.52 Điền địa chỉ IPv4 và DNS -> chọn OK

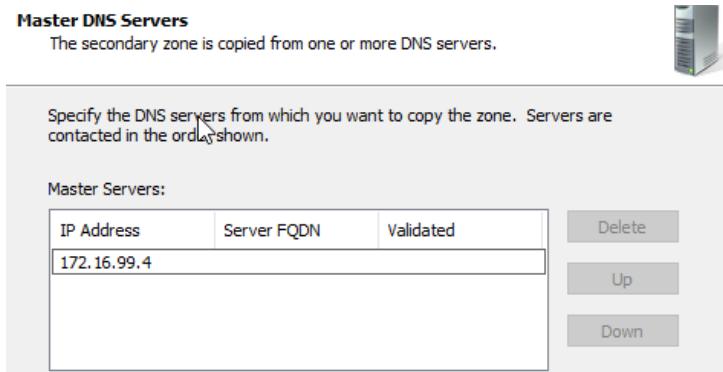
c) Cấu hình dịch vụ DNS Alternate Server



Hình 5.53 Vào DNS Manager -> Tạo New Zone -> Chọn Zone Type là Secondary zone

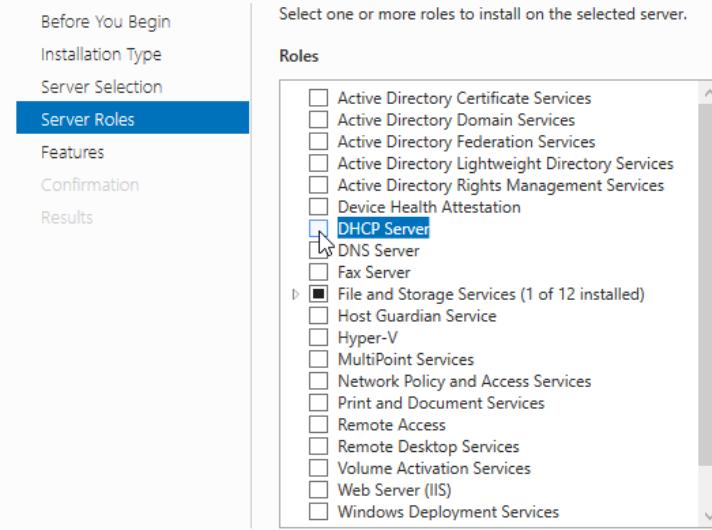


Hình 5.54 Nhập Zone Name

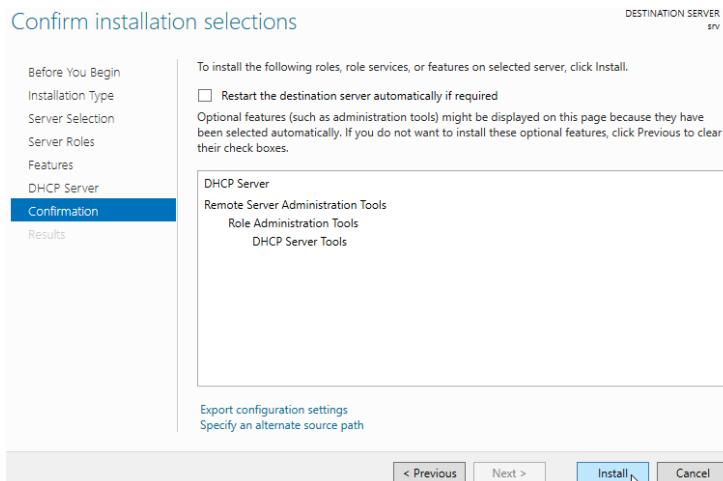


Hình 5.55 Nhập địa chỉ IP của Master Servers

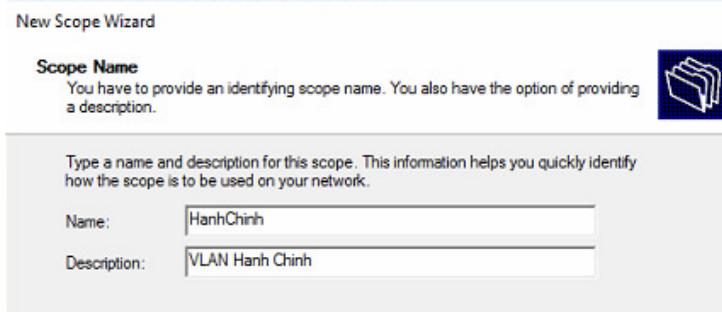
d) Cấu hình dịch vụ DHCP Server



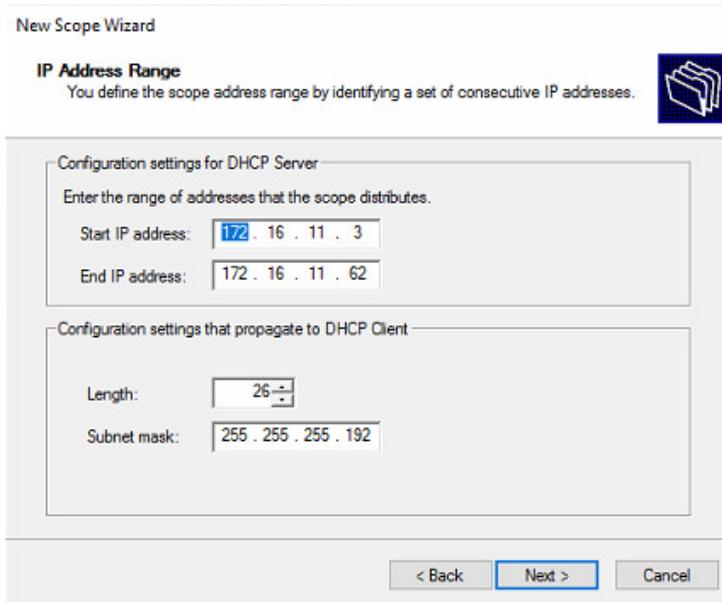
Hình 5.56 Thêm dịch vụ DHCP cho Server



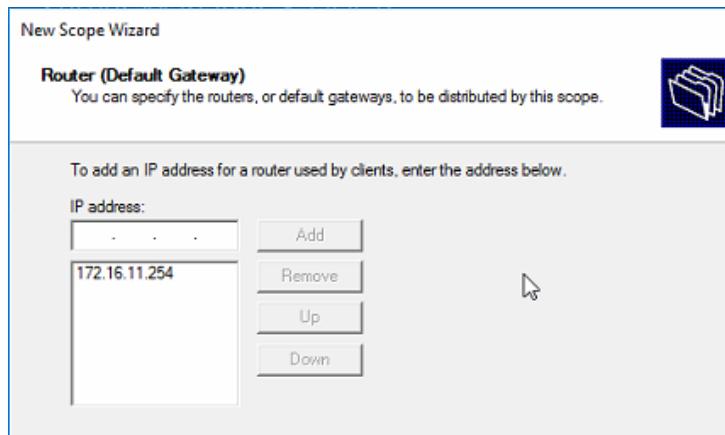
Hình 5.57 Install DHCP Server



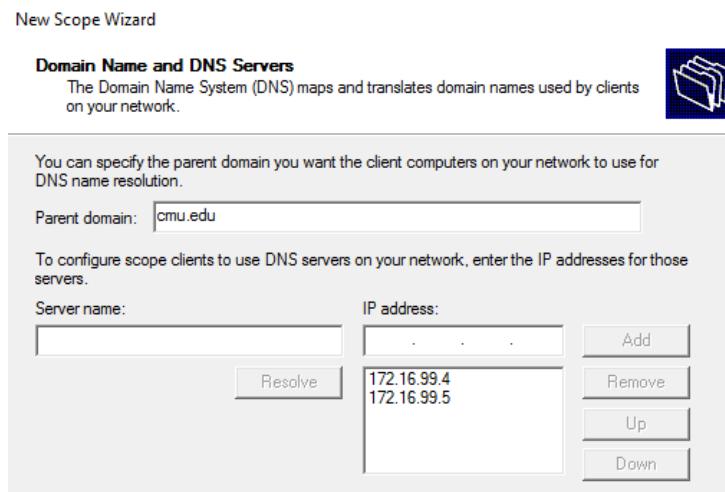
Hình 5.58 Tạo Scope Name cho các VLAN



Hình 5.59 Nhập dải địa chỉ IP của VLAN



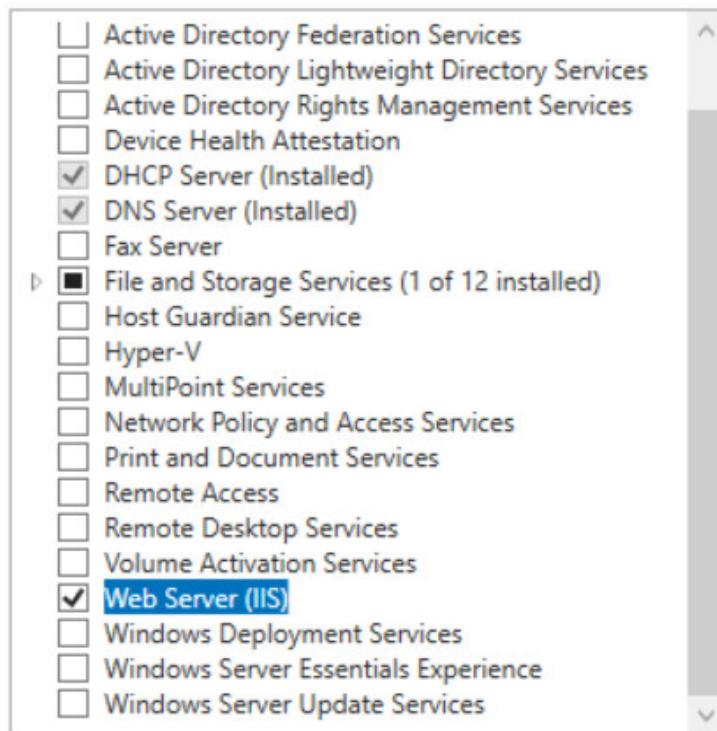
Hình 5.60 Nhập địa chỉ gateway



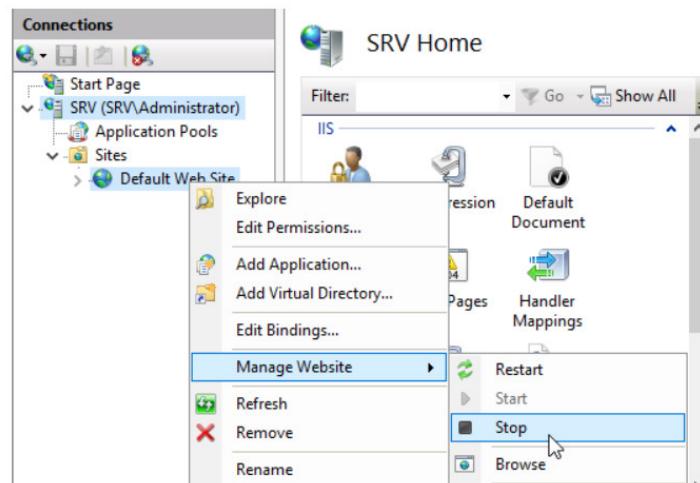
Hình 5.61 Nhập domain name và địa chỉ IP của DNS Server

Làm tương tự với những VLAN còn lại.

e) Cấu hình Web server



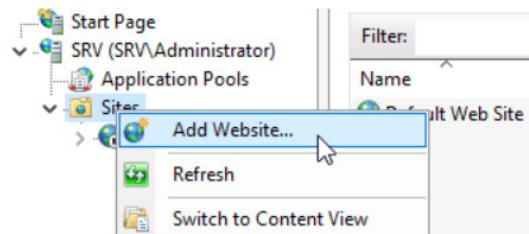
Hình 5.62 Thêm dịch vụ IIS cho Server



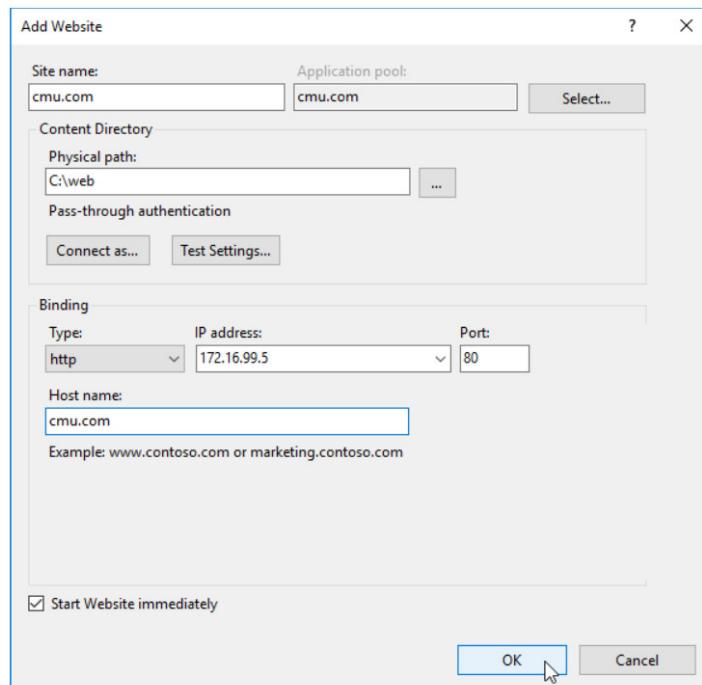
Hình 5.63 Tắt trang web mặc định của web server

Thêm source Web vào các ổ đĩa của Server và sau đó gán vào đường dẫn của website

mới:



Hình 5.64 Thêm Source Web vào các ổ đĩa của Server



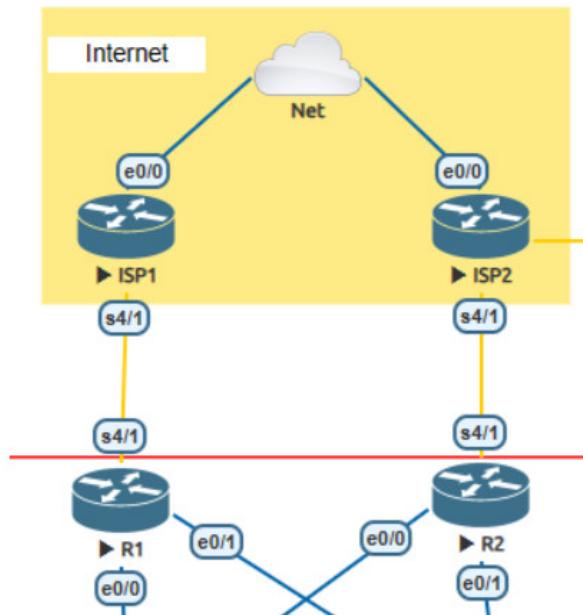
Hình 5.65 Gán các đường dẫn của Website mới

CHƯƠNG 6 - KIỂM TRA VÀ ĐÁNH GIÁ

6.1 Demo sản phẩm

6.1.1 Kiểm tra kết nối với ISP

Hai router R1 và R2 kết nối với 2 ISP để đảm bảo hệ thống mạng có tính sẵn sàng và tính dự phòng:



Hình 6.1 Router R1 và Router R2 kết nối với 2 ISP

Kết quả là 2 router R1 và R2 đều ping được tới Internet:

```

R1#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 38/39/41 ms
R1#ping google.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 142.250.199.78, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 35/36/38 ms

R2#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 38/40/44 ms
R2#ping google.com
Translating "google.com"...domain server (8.8.8.8) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.217.27.46, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 35/36/37 ms

Kiểm tra giao thức NAT:
ISP1#show ip nat translations
Pro Inside global      Inside local        Outside local       Outside global
icmp 192.168.1.7:22591 172.16.0.26:22591  8.8.8.8:22591    8.8.8.8:22591
icmp 192.168.1.7:34367 172.16.0.26:34367  8.8.8.8:34367    8.8.8.8:34367

ISP2#show ip nat translations
Pro Inside global      Inside local        Outside local       Outside global
icmp 192.168.1.2:4     14.16.241.2:4     8.8.8.8:4         8.8.8.8:4
icmp 192.168.1.2:5     14.16.241.2:5     8.8.8.8:5         8.8.8.8:5
icmp 192.168.1.2:6     14.16.241.2:6     8.8.8.8:6         8.8.8.8:6
icmp 192.168.1.2:7     14.16.241.2:7     142.250.66.78:7  142.250.66.78:7
udp 192.168.1.2:60197 14.16.241.2:60197  8.8.8.8:53       8.8.8.8:53

```

Hình 6.2 Hai Router sau khi được kết nối với ISP

6.1.2 Kiểm tra giao thức NAT

```

ISP1#show ip nat translations
Pro Inside global      Inside local        Outside local       Outside global
icmp 192.168.1.7:22591 172.16.0.26:22591  8.8.8.8:22591    8.8.8.8:22591
icmp 192.168.1.7:34367 172.16.0.26:34367  8.8.8.8:34367    8.8.8.8:34367

ISP2#show ip nat translations
Pro Inside global      Inside local        Outside local       Outside global
icmp 192.168.1.2:4     14.16.241.2:4     8.8.8.8:4         8.8.8.8:4
icmp 192.168.1.2:5     14.16.241.2:5     8.8.8.8:5         8.8.8.8:5
icmp 192.168.1.2:6     14.16.241.2:6     8.8.8.8:6         8.8.8.8:6
icmp 192.168.1.2:7     14.16.241.2:7     142.250.66.78:7  142.250.66.78:7
udp 192.168.1.2:60197 14.16.241.2:60197  8.8.8.8:53       8.8.8.8:53

```

Hình 6.3 Kết quả kiểm tra giao thức NAT

6.1.3 Kiểm tra DHCP

```
HanhChinh> ip dhcp
DORA IP 172.16.11.4/26 GW 172.16.11.3

HanhChinh> show ip

NAME      : HanhChinh[1]
IP/MASK   : 172.16.11.4/26
GATEWAY   : 172.16.11.3
DNS       : 172.16.99.4  172.16.99.5
DHCP SERVER : 172.16.99.5
DHCP LEASE  : 691196, 691200/345600/604800
DOMAIN NAME : cmu.edu
MAC        : 00:50:79:66:68:1c
LPORT      : 20000
RHOST:PORT : 127.0.0.1:30000
MTU        : 1500
```

Hình 6.4 Kiểm tra DHCP của từng phòng ban

Các PC của từng phòng ban nhận được IP DHCP thành công, bao gồm các thông tin về DNS server và Domain name.

6.1.4 Kiểm tra kết nối giữa các VLAN

```
HanhChinh> ping 172.16.12.4
172.16.12.4 icmp_seq=1 timeout
84 bytes from 172.16.12.4 icmp_seq=2 ttl=63 time=10.288 ms
84 bytes from 172.16.12.4 icmp_seq=3 ttl=63 time=21.095 ms
84 bytes from 172.16.12.4 icmp_seq=4 ttl=63 time=8.570 ms
84 bytes from 172.16.12.4 icmp_seq=5 ttl=63 time=4.025 ms
```

Hình 6.5 Kiểm tra kết nối giữa các VLAN

Giữa các PC thuộc VLAN khác nhau đều kết nối được với nhau.

6.1.5 Kiểm tra kết nối giữa các VXLAN

Tại NXOS3 và NXOS4 đóng vai trò là Leaf Switch, các VLAN được mapping với VXLAN tương ứng:

```
NXOS3# show vxlan
Vlan          VN-Segment
====          =====
11            10011
12            10012
13            10013
14            10014
15            10015
16            10016
17            10017
18            10018
19            10019
20            10020
21            10021
22            10022
23            10023
99            10099
```

Hình 6.6 Kiểm tra kết nối VXLAN tại NXOS3

Tại interface nve1, các gói tin được đóng gói theo định dạng VXLAN:

```
NXOS3# show interface nve 1
nve1 is up
admin state is up,  Hardware: NVE
    MTU 9216 bytes
    Encapsulation VXLAN
    Auto-mdix is turned off
RX
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
TX
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
```

Hình 6.7 Xem Interface NVE 1

```

NXOS3# show nve vni
Codes: CP - Control Plane          DP - Data Plane
       UC - Unconfigured           SA - Suppress ARP
       SU - Suppress Unknown Unicast
       Xconn - Crossconnect
       MS-IR - Multisite Ingress Replication

  Interface VNI      Multicast-group     State Mode Type [BD/VRF]   Flags
  ----- -----
nve1    10011    239.1.1.11      Up   DP  L2 [11]
nve1    10012    239.1.1.12      Up   DP  L2 [12]
nve1    10013    239.1.1.13      Up   DP  L2 [13]
nve1    10014    239.1.1.14      Up   DP  L2 [14]
nve1    10015    239.1.1.15      Up   DP  L2 [15]
nve1    10016    239.1.1.16      Up   DP  L2 [16]
nve1    10017    239.1.1.17      Up   DP  L2 [17]
nve1    10018    239.1.1.18      Up   DP  L2 [18]
nve1    10019    239.1.1.19      Up   DP  L2 [19]
nve1    10020    239.1.1.20      Up   DP  L2 [20]
nve1    10021    239.1.1.21      Up   DP  L2 [21]
nve1    10022    239.1.1.22      Up   DP  L2 [22]
nve1    10023    239.1.1.23      Up   DP  L2 [23]
nve1    10099    239.1.1.99      Up   DP  L2 [99]

```

Hình 6.8 Xem NVE VNI**6.1.6 Kiểm tra giao thức dự phòng gateway HSRP**

```

NXOS3# show hsrp brief
*:IPv6 group #:group belongs to a bundle
          P indicates configured to preempt.
  |
  Interface  Grp  Prio P State   Active addr   Standby addr  Group addr
  VLAN11     11   200  P Active  local        172.16.11.2  172.16.11.3
  (conf)
  VLAN12     12   200  P Active  local        172.16.12.2  172.16.12.3
  (conf)
  VLAN13     13   200  P Active  local        172.16.13.2  172.16.13.3
  (conf)
  VLAN14     14   200  P Active  local        172.16.14.2  172.16.14.3
  (conf)
  VLAN15     15   200  P Active  local        172.16.15.2  172.16.15.3
  (conf)
  VLAN16     16   200  P Active  local        172.16.16.2  172.16.16.3
  (conf)
  VLAN17     17   200  P Active  local        172.16.17.2  172.16.17.3
  (conf)
  VLAN18     18   200  P Active  local        172.16.18.2  172.16.18.3
  (conf)
  VLAN19     19   200  P Active  local        172.16.19.2  172.16.19.3
  (conf)
  VLAN20     20   200  P Active  local        172.16.20.2  172.16.20.3
  (conf)
  VLAN21     21   200  P Active  local        172.16.21.2  172.16.21.3
  (conf)
  VLAN22     22   200  P Active  local        172.16.22.2  172.16.22.3
  (conf)
  VLAN23     23   200  P Active  local        172.16.23.2  172.16.23.3
  (conf)
  VLAN99     99   200  P Active  local        172.16.99.2  172.16.99.3
  (conf)

```

Hình 6.9 Kiểm tra giao thức dự phòng gateway HSRP tại NXOS3

```

NXOS4# show hsrp brief
*:IPv6 group  #:group belongs to a bundle
                           P indicates configured to preempt.
   |
Interface  Grp  Prio P State      Active addr      Standby addr      Group addr
Vlan11     11   100  P Standby    172.16.11.1    local             172.16.11.3
           (conf)
Vlan12     12   100  P Standby    172.16.12.1    local             172.16.12.3
           (conf)
Vlan13     13   100  P Standby    172.16.13.1    local             172.16.13.3
           (conf)
Vlan14     14   100  P Standby    172.16.14.1    local             172.16.14.3
           (conf)
Vlan15     15   100  P Standby    172.16.15.1    local             172.16.15.3
           (conf)
Vlan16     16   100  P Standby    172.16.16.1    local             172.16.16.3
           (conf)
Vlan17     17   100  P Standby    172.16.17.1    local             172.16.17.3
           (conf)
Vlan18     18   100  P Standby    172.16.18.1    local             172.16.18.3
           (conf)
Vlan19     19   100  P Standby    172.16.19.1    local             172.16.19.3
           (conf)
Vlan20     20   100  P Standby    172.16.20.1    local             172.16.20.3
           (conf)
Vlan21     21   100  P Standby    172.16.21.1    local             172.16.21.3
           (conf)
Vlan22     22   100  P Standby    172.16.22.1    local             172.16.22.3
           (conf)
Vlan23     23   100  P Standby    172.16.23.1    local             172.16.23.3
           (conf)
Vlan99     99   100  P Standby    172.16.99.1    local             172.16.99.3
           (conf)

```

Hình 6.10 Kiểm tra giao thức dự phòng gateway HSRP tại NXOS4

NXOS3 đóng vai trò Active, NXOS4 đóng vai trò Standby.

6.1.7 Kiểm tra Etherchannel

Port-channel 1 trên Sw_A:

```

Sw_A#show etherchannel summary
Flags:  D - down          P - bundled in port-channel
       I - stand-alone    s - suspended
       H - Hot-standby   (LACP only)
       R - Layer3          S - Layer2
       U - in use           N - not in use, no aggregation
       f - failed to allocate aggregator

       M - not in use, minimum links not met
       m - not in use, port not aggregated due to minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

       A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol      Ports
-----+-----+-----+
1      Po1(SU)       LACP        Et0/0(P)  Et0/1(P)

```

Hình 6.11 Kiểm tra Port-channel 1 trên Sw_A

Port-channel 2 trên Sw_B:

```

Sw_B#show etherchannel summary
Flags: D - down P - bundled in port-channel
      I - stand-alone s - suspended
      H - Hot-standby (LACP only)
      R - Layer3 S - Layer2
      U - in use N - not in use, no aggregation
      f - failed to allocate aggregator

      M - not in use, minimum links not met
      m - not in use, port not aggregated due to minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port

      A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
-----+-----+-----+
2     Po2 (SU)      LACP    Et0/0 (P)  Et0/1 (P)

```

Hình 6.12 Kiểm tra Port-channel 2 trên Sw_B

Port-channel 3 trên Sw_C:

```

Sw_C#show etherchannel summary
Flags: D - down P - bundled in port-channel
      I - stand-alone s - suspended
      H - Hot-standby (LACP only)
      R - Layer3 S - Layer2
      U - in use N - not in use, no aggregation
      f - failed to allocate aggregator

      M - not in use, minimum links not met
      m - not in use, port not aggregated due to minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port

      A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
-----+-----+-----+
3     Po3 (SU)      LACP    Et0/0 (P)  Et0/1 (P)

```

Hình 6.13 Kiểm tra Port-channel 3 trên Sw_C

Kiểm tra Port-channel 4 trên Sw_DC1 và Sw_DC2, port-channel1 kết nối với AD_RADIUS servre, port-channel 2 kết nối với DNS_Mail_DHCP server:

```

Sw_DC1#show etherchannel summary
Flags: D - down          P - bundled in port-channel
      I - stand-alone   S - suspended
      H - Hot-Standby (LACP only)
      R - Layer3         L - Layer2
      U - in use          N - not in use, no aggregation
      f - failed to allocate aggregator

      M - not in use, minimum links not met
      m - not in use, port not aggregated due to minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port

      A - formed by Auto LAG

Number of channel-groups in use: 3
Number of aggregators: 3

Group Port-channel Protocol Ports
-----+-----+-----+-----+
 1    Po1 (SU)     LACP    Et1/0 (P)
 2    Po2 (SU)     LACP    Et0/3 (P)
 4    Po4 (SU)     LACP    Et0/0 (P)   Et0/1 (P)

```

Hình 6.14 Kiểm tra Port-channel 4 trên Sw_DC1

6.1.8 Kiểm tra kết nối VPC

VPC domain 1 trên switch NXOS1 và NXOS2:

```

NXOS1# show vpc
Legend:
(*) - local vPC is down, forwarding via vPC peer-link

vPC domain id : 1
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role : primary
Number of vPCs configured : 0
Peer Gateway : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Enabled, timer is off.(timeout = 240s)
Delay-restore status : Timer is off.(timeout = 30s)
Delay-restore SVI status : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router : Disabled
Virtual-peerlink mode : Disabled

vPC Peer-link status
-----
id  Port  Status Active vlans
--  ---  ----  -----
1   Po51  up     1

```

Hình 6.15 VPC domain 1 trên switch NXOS1

VPC domain 2 trên switch NXOS3 và NXOS4:

```

NXOS3# show vpc
Legend:
(*) - local vPC is down, forwarding via vPC peer-link

vPC domain id          : 2
Peer status              : peer adjacency formed ok
vPC keep-alive status   : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role                 : primary
Number of vPCs configured : 5
Peer Gateway             : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status     : Enabled, timer is off.(timeout = 240s)
Delay-restore status      : Timer is off.(timeout = 30s)
Delay-restore SVI status  : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router : Disabled
Virtual-peerlink mode    : Disabled

vPC Peer-link status
-----
id  Port  Status Active vlans
--  --   -----
1   Po54 up      11-23,99

```

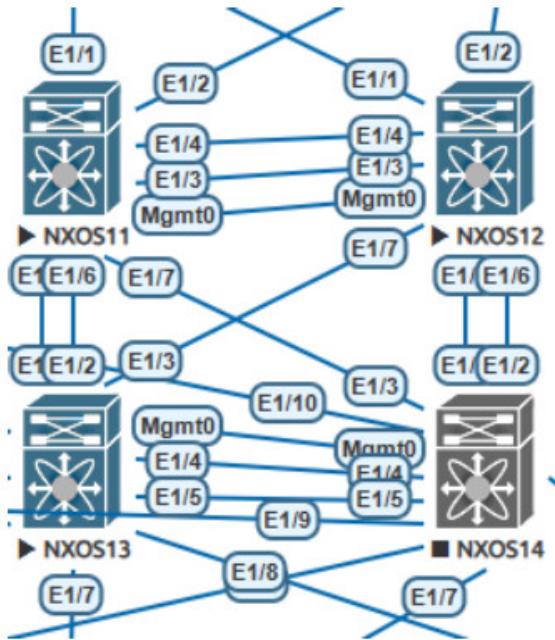
Hình 6.16 VPC domain 2 trên switch NXOS3

vPC status					
Id	Port	Status	Consistency	Reason	Active vlans
1	Po1	up	success	success	11-14
2	Po2	up	success	success	15-20
3	Po3	up	success	success	21-23
4	Po4	up	success	success	99
5	Po5	up	success	success	99

Hình 6.17 VPC Status

6.1.9 Kiểm tra khả năng dự phòng của hệ thống

Trong trường hợp 1 switch đóng vai trò là Leaf xảy ra sự cố, các PC vẫn lấy được địa chỉ IP DHCP thành công



```

NgoaiNgu> dhcp
DDORA IP 172.16.17.4/26 GW 172.16.17.3

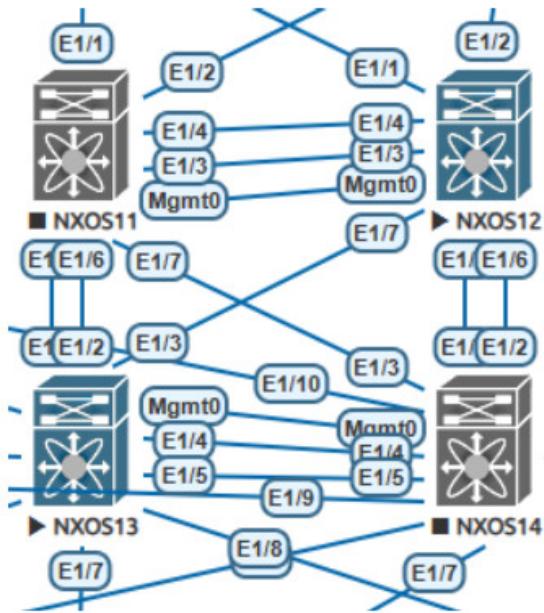
NgoaiNgu> show ip

NAME      : NgoaiNgu[1]
IP/MASK   : 172.16.17.4/26
GATEWAY   : 172.16.17.3
DNS       : 172.16.99.4  172.16.99.5
DHCP SERVER : 172.16.99.5
DHCP LEASE  : 691196, 691200/345600/604800
DOMAIN NAME : cmu.edu
MAC       : 00:50:79:66:68:24
LPORT     : 20000
RHOST:PORT : 127.0.0.1:30000
MTU      : 1500

```

Hình 6.18 Switch là Leaf nếu xảy ra sự cố vẫn lấy được địa chỉ IP DHCP

Trong trường hợp 1 switch đóng vai trò là Spine xảy ra sự cố, các PC vẫn lấy được địa chỉ IP DHCP thành công.



```

TCNH> dhcp
DORA IP 172.16.18.4/26 GW 172.16.18.3

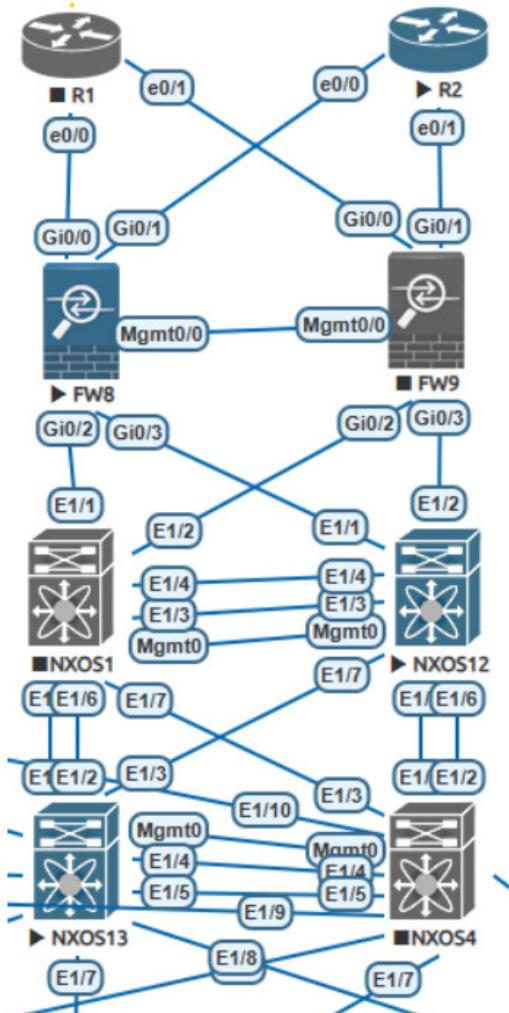
TCNH> show ip

NAME      : TCNH[1]
IP/MASK   : 172.16.18.4/26
GATEWAY   : 172.16.18.3
DNS        : 172.16.99.4  172.16.99.5
DHCP SERVER : 172.16.99.5
DHCP LEASE  : 691197, 691200/345600/604800
DOMAIN NAME : cmu.edu
MAC        : 00:50:79:66:68:25
LPORT      : 20000
RHOST:PORT : 127.0.0.1:30000
MTU       : 1500

```

Hình 6.19 Switch là Spine nếu xảy ra sự cố vẫn lấy được địa chỉ IP DHCP

Hệ thống mạng được thiết kế có các thiết bị redundant để khi xảy ra sự cố thì hệ thống vẫn hoạt động bình thường. Trong trường hợp một nửa hệ thống mạng có vấn đề thì các thiết bị trong mạng vẫn kết nối với internet được:



```

NXOS3# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=112 time=50.076 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=112 time=49.776 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=112 time=70.337 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=112 time=46.451 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=112 time=43.677 ms
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 43.677/52.063/70.337 ms

```

Hình 6.20 Các thiết bị redundant làm cho hệ thống vẫn hoạt động bình thường khi xảy ra sự cố

6.2 Kết luận và tổng kết dự án

Những kết quả đạt được sau khi chúng em hoàn thành tìm hiểu và thực hiện đề tài "Xây dựng mạng LAN cho trường học sử dụng kỹ thuật VXLAN":

- Nắm vững những kiến thức về mạng LAN. Bao gồm các kiến thức xây dựng và triển khai một hệ thống mạng.
- Hiểu rõ hơn về các yếu tố quan trọng trong việc triển khai công nghệ VXLAN trong thiết kế mạng. Với khả năng mở rộng linh hoạt qua các mạng con, điều này giúp dễ dàng quản lý và mở rộng mạng LAN theo nhu cầu thực tế của trường học.
- Tăng cường khả năng bảo mật hệ thống. Kỹ thuật VXLAN cung cấp phân đoạn mạng hiệu quả, ngăn chặn sự xâm nhập không mong muốn vào hệ thống thông qua việc tạo ra các mạng LAN ảo độc lập với nhau. Bên cạnh đó, nhờ sử dụng firewall, ACL để kiểm soát lưu lượng truy cập và các giải pháp bảo mật như Telnet/SSH, Port-security,... để giảm thiểu các cuộc tấn công mạng, hệ thống có thể đạt được các yêu cầu về bảo mật.
- Xây dựng hệ thống có tính dự phòng. Thiết kế, triển khai các thiết bị dự phòng và nhiều đường dẫn dự phòng. Điều đó giúp đảm bảo nếu có sự cố xảy ra trên một thiết bị thì hệ thống mạng vẫn hoạt động được bình thường, trường hợp một đường dẫn gặp sự cố thì vẫn có đường dẫn khác thay thế để truyền dữ liệu. Nếu một phần của mạng gặp sự cố, các kết nối dự phòng sẽ tự động kích hoạt để duy trì hoạt động của mạng.

Xây dựng hệ thống mạng LAN với kỹ thuật VXLAN mang lại những lợi ích quan trọng như tạo ra mạng ảo linh hoạt và có khả năng mở rộng. VXLAN cung cấp phân đoạn mạng hiệu quả, giúp bảo vệ dữ liệu và tài nguyên mạng khỏi sự xâm nhập không mong muốn. Hệ thống được thiết kế với tính dự phòng cao, đảm bảo rằng mạng luôn

hoạt động một cách liên tục và ổn định, ngay cả khi có sự cố xảy ra. Giúp tạo ra một môi trường mạng cho trường học an toàn, hiệu quả và dễ quản lý.

6.3 Bài học kinh nghiệm

Chúng em đã rút ra được một số bài học kinh nghiệm, sau khi chúng em hoàn thành tìm hiểu và thực hiện đề tài "Xây dựng mạng LAN cho trường học sử dụng kỹ thuật VXLAN":

- Nhận ra tầm quan trọng của mạng kiến thức về mạng máy tính và ảo hóa khi xây dựng một hệ thống mạng ảo. Nắm vững những kiến thức để có thể áp dụng các công nghệ, kỹ thuật mới vào mô hình mạng.
- Cần lựa chọn công nghệ phù hợp với mục tiêu và yêu cầu được đề ra. Việc lựa chọn kỹ thuật VXLAN đã chứng minh được tính linh hoạt và hiệu quả của nó trong việc xây dựng mạng LAN cho trường học. Cho thấy tầm quan trọng của việc nghiên cứu và lựa chọn công nghệ phù hợp với nhu cầu cụ thể của dự án.
- Bảo mật luôn là một yếu tố quan trọng trong việc xây dựng mạng LAN, đặc biệt là khi xây dựng cho các tổ chức như trường học. Cần chú ý tăng cường khả năng bảo mật trong mạng để đảm bảo hệ thống đáng tin cậy cho người dùng.
- Trước các cuộc tấn công mạng phổ biến như ngày nay, thì tính dự phòng là yếu tố không thể thiếu. Thiết kế và triển khai hệ thống mạng với tính dự phòng cao để đảm bảo rằng mạng luôn hoạt động một cách ổn định ngay cả khi có sự cố xảy ra.

6.4 Hướng phát triển và nghiên cứu tiếp theo

Trong tương lai, việc phát triển mạng LAN cho trường học sử dụng kỹ thuật VXLAN có thể phát triển theo những hướng sau:

- Trong tương lai, VXLAN có thể tích hợp với các công nghệ mới như SDN (Software Defined Networking) và NFV (Network Functions Virtualization) để tạo ra

các mạng linh hoạt và dễ quản lý hơn. Việc tích hợp này sẽ giúp tạo ra các mô hình mạng đáp ứng được yêu cầu ngày càng đa dạng và phức tạp.

- Mạng LAN của trường học cũng có thể tận dụng công nghệ AI (Artificial Intelligence) để cải thiện quản lý và bảo mật. Các hệ thống AI có thể tự động phát hiện và phản ứng với các mối đe dọa mạng một cách nhanh chóng, giúp tăng cường tính an toàn cho hệ thống mạng. VXLAN có thể được cải tiến để hỗ trợ các tính năng bảo mật mới như mã hóa dữ liệu và kiểm soát truy cập nâng cao.
- Việc tích hợp các thiết bị IoT(Internet of Things) vào mạng LAN của trường học có thể mang lại nhiều tiện ích, từ việc giám sát và quản lý thiết bị đến việc tạo ra các trải nghiệm học tập mới cho học sinh.
- Ngoài ra, việc sử dụng công nghệ Cloud trong xây dựng mạng LAN cũng là một hướng phát triển tiềm năng. Việc chuyển sang mô hình Cloud Networking giúp giảm thiểu chi phí về cơ sở hạ tầng và quản lý, đồng thời cung cấp tính linh hoạt cao hơn trong việc mở rộng mạng và triển khai dịch vụ.
- Việc xây dựng mạng LAN tương thích với môi trường học tập kỹ thuật số sẽ đóng vai trò quan trọng trong tương lai. Mạng LAN sẽ phải được thiết kế để hỗ trợ các hình thức học tập mới như học tập từ xa, học tập cá nhân hóa và học tập trải nghiệm thực tế ảo, từ đó tạo ra một môi trường học tập đa dạng và phong phú.
- Tiếp tục nghiên cứu VXLAN bao gồm việc ứng dụng các kỹ thuật có liên quan như EVPN (Ethernet Virtual Private Network), QoS (Quality of Service), Dynamic Load Balancing nhằm cải thiện hiệu suất và độ tin cậy của hệ thống.

TÀI LIỆU THAM KHẢO

- [1] Hatim, “What are the main components of a local area network (lan)?” 2018.
- [2] A. J. Sequeira, *Interconnecting Cisco Network Devices, Part 1 (ICND1) Foundation Learning Guide, 4th Edition.* Cisco Press, 2013.
- [3] W. Stallings, *Data and Computer Communication.* Prentice Hall, 2021.
- [4] C. Systems, *Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 10.1(x).* Cisco Systems, 2021.
- [5] F. A. Somit Maloo, *CCNP and CCIE Data Center Core DCCOR 350-601 Official Cert Guide.* Cisco Press, 2020.
- [6] T. Pasanen, *Virtual Extensible LAN (VXLAN): A Practical guide to VXLAN solution.* Amazon Fulfillment, 2019.