

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 21 tháng 03 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 4 chương

- Chương 1 - Tổng quan đề tài
- Chương 2 - Phân tích thiết kế hệ thống
- Chương 3 - Triển khai hệ thống
- Chương 4 - 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 4 chapters

- Chapter 1 - Overview of the topic
- Chapter 2 - System design analysis
- Chapter 3 - System deployment
- Chapter 4 - 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	ix
DANH MỤC CÁC CHỮ VIẾT TẮT	x
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
1.1.3 Nội dung đề tài	3
1.1.4 Đối tượng, phạm vi nghiên cứu đề tài	3
1.1.5 Phương pháp nghiên cứu	4
1.1.6 Ý nghĩa lý luận và thực tiễn	4
1.1.7 Cấu trúc bài báo cáo	5
1.2 Cơ sở lý thuyết	6
1.2.1 Tìm hiểu về mạng LAN	6
1.2.2 Công nghệ VXLAN	18
1.2.3 Phần mềm EVE-NG	25
1.2.4 Bảo mật hệ thống	27

CHƯƠNG 2 - PHÂN TÍCH THIẾT KẾ HỆ THỐNG	31
2.1 Khảo sát yêu cầu của trường học	31
2.1.1 Xác định các thông tin phạm vi trường học	31
2.1.2 Yêu cầu người dùng	32
2.1.3 Yêu cầu về bảo mật	33
2.1.4 Sơ đồ cấu trúc trường học	34
2.2 Định hướng thiết kế hệ thống	36
2.3 Thiết kế mô hình mạng	37
2.3.1 Sơ đồ vật lý	37
2.3.2 Sơ đồ logic	38
2.3.3 Sơ đồ luận lý	39
2.4 Thông tin cài đặt cấu hình hệ thống	39
2.4.1 Thông tin VLAN, VXLAN trong hệ thống	39
2.4.2 Thông tin kết nối port trong hệ thống	43
2.4.3 Thông tin địa chỉ IP planning	48
CHƯƠNG 3 - TRIỂN KHAI HỆ THỐNG	52
5.1 Cấu hình cơ bản trên các thiết bị	52
5.2 Cấu hình các server	90
5.2.1 Cấu hình server RADIUS	90
5.2.2 Cấu hình server DNS_Mail_DHCP	102

5.3	Demo hệ thống	106
5.3.1	Kiểm tra kết nối với ISP	106
5.3.2	Kiểm tra giao thức NAT	108
5.3.3	Kiểm tra DHCP	108
5.3.4	Kiểm tra kết nối giữa các VLAN	108
5.3.5	Kiểm tra kết nối giữa các VXLAN	109
5.3.6	Kiểm tra giao thức dự phòng gateway HSRP	110
5.3.7	Kiểm tra Etherchannel	111
5.3.8	Kiểm tra kết nối VPC	113
5.3.9	Kiểm tra khả năng dự phòng của hệ thống	114
CHƯƠNG 4 - TỔNG KẾT		118
4.4	Kết luận và tổng kết dự án	118
4.5	Bài học kinh nghiệm	119
4.6	Hướng phát triển và nghiên cứu tiếp theo	119
TÀI LIỆU THAM KHẢO		121

DANH MỤC HÌNH VẼ

Hình 1.1	Mô hình mạng LAN	6
Hình 1.2	Mạng LAN có dây	7
Hình 1.3	Mạng LAN không dây	8
Hình 1.4	Hệ thống mạng LAN cơ bản	8
Hình 1.5	Mạng ngang hàng	11
Hình 1.6	Mạng máy khách-máy chủ	11
Hình 1.7	Hoạt động của mạng LAN	12
Hình 1.8	Cấu trúc liên kết hình sao	14
Hình 1.9	Cấu trúc liên kết bus	15
Hình 1.10	Cấu trúc liên kết vòng	17
Hình 1.11	Mô hình VXLAN	18
Hình 1.12	Cách hoạt động của VXLAN	19
Hình 1.13	Lớp Underlay và lớp Overlay	20
Hình 1.14	Cấu trúc gói tin VXLAN	22
Hình 2.1	Sơ đồ tổng quan cấu trúc trường	34
Hình 2.2	Phòng hành chính	34
Hình 2.3	Phòng đào tạo	34
Hình 2.4	Phòng tuyển sinh	35
Hình 2.5	Phòng lab	35

Hình 2.6 Văn phòng khoa	35
Hình 2.7 Phòng học	35
Hình 2.8 Phòng kỹ thuật	36
Hình 2.9 Thư viện	36
Hình 2.10 Sơ đồ vật lý	37
Hình 2.11 Sơ đồ logic	38
Hình 2.12 Sơ đồ luận lý	39
Hình 5.1 Cấu hình NIC Teaming	90
Hình 5.2 Điện địa chỉ IPv4 và DNS	90
Hình 5.3 Chọn Server Roles	91
Hình 5.4 Chọn Install	91
Hình 5.5 Chọn DNS Manager	91
Hình 5.6 Zone Name là cmu.edu	91
Hình 5.7 Forward Lookup Zones	92
Hình 5.8 Reverse Lookup Zones	92
Hình 5.9 Chọn New Host	92
Hình 5.10 Chọn Add Host	92
Hình 5.11 Cấu hình Advanced	93
Hình 5.12 Cấu hình Forwarders	93
Hình 5.15 Allow Zone Transfers	93
Hình 5.13 Nhập tên và địa chỉ	94

Hình 5.14 Chọn Zone Transfers	94
Hình 5.16 Add Role and Features	94
Hình 5.17 Chọn AD DS	94
Hình 5.18 Nhập Root domain name	95
Hình 5.19 Nhập password	95
Hình 5.20 Chọn	95
Hình 5.21 Chọn Manage	95
Hình 5.22 Chọn Organizational Unit	96
Hình 5.23 Nhập tên là HO	96
Hình 5.24 Nhập tên là BO	96
Hình 5.25 Tạo Group	97
Hình 5.26 Nhập tên phòng ban	97
Hình 5.27 Thêm User	97
Hình 5.28 Tạo User 1	98
Hình 5.29 Tạo User 2	98
Hình 5.30 Add User vào Group	98
Hình 5.31 Chọn Groups	98
Hình 5.32 Chọn Server Roles	98
Hình 5.33 Cấu hình	98
Hình 5.34 Chọn Certification Authority	99
Hình 5.35 Tạo Policy	99

Hình 5.36 Nhập tên	99
Hình 5.37 Chọn Properties	100
Hình 5.38 Chọn OK	100
Hình 5.39 Tạo Policy	100
Hình 5.40 Nhập tên	100
Hình 5.41 Chọn Properties	101
Hình 5.42 Nhấn để bỏ chọn	101
Hình 5.43 Chọn Network Policy Server	101
Hình 5.44 Chọn Configure VPN	102
Hình 5.45 Chọn VPN	102
Hình 5.46 Chọn Add	102
Hình 5.47 Cấu hình RADIUS client	102
Hình 5.48 Cấu hình NIC Teaming	103
Hình 5.49 Điền địa chỉ IPv4	103
Hình 5.50 Chọn Zone Type	103
Hình 5.51 Nhập Zone Name	104
Hình 5.52 Nhập địa chỉ IP	104
Hình 5.53 Thêm dịch vụ DHCP	104
Hình 5.54 Install DHCP Server	104
Hình 5.55 Tạo Scope Name cho VLAN	105
Hình 5.56 Nhập dải địa chỉ IP VLAN	105

Hình 5.57 Nhập địa chỉ gateway	105
Hình 5.58 Nhập domain name, địa chỉ IP	105
Hình 5.59 Thêm dịch vụ IIS	106
Hình 5.60 Tắt trang web mặc định	106
Hình 5.61 Chọn Add Website	106
Hình 5.62 Gán các đường dẫn Website	106
Hình 5.63 Router R1 và Router R2 kết nối với 2 ISP	107
Hình 5.64 Hai Router sau khi được kết nối với ISP	107
Hình 5.65 Kết quả kiểm tra giao thức NAT	108
Hình 5.66 Kiểm tra DHCP của từng phòng ban	108
Hình 5.67 Kiểm tra kết nối giữa các VLAN	108
Hình 5.68 Kiểm tra kết nối VXLAN tại NXOS3	109
Hình 5.69 Xem Interface NVE 1	109
Hình 5.70 Xem NVE VNI	110
Hình 5.71 Kiểm tra giao thức dự phòng gateway HSRP tại NXOS3	110
Hình 5.72 Kiểm tra giao thức dự phòng gateway HSRP tại NXOS4	111
Hình 5.73 Kiểm tra Port-channel 1 trên Sw_A	111
Hình 5.74 Kiểm tra Port-channel 2 trên Sw_B	112
Hình 5.75 Kiểm tra Port-channel 3 trên Sw_C	112
Hình 5.76 Kiểm tra Port-channel 4 trên Sw_DC1	113
Hình 5.77 Kiểm tra VPC domain 1 trên switch NXOS1	113

Hình 5.78 Kiểm tra VPC domain 2 trên switch NXOS3	114
Hình 5.79 VPC Status	114
Hình 5.80 Switch là Leaf nếu xảy ra sự cố vẫn lấy được địa chỉ IP DHCP . .	115
Hình 5.81 Switch là Spine nếu xảy ra sự cố vẫn lấy được địa chỉ IP DHCP . .	116
Hình 5.82 Hệ thống vẫn hoạt động bình thường nhờ các thiết bị redundant . .	117

DANH MỤC BẢNG BIỂU

Bảng 2.1	Thông tin VLAN, VXLAN trong hệ thống	39
Bảng 2.1	Thông tin VLAN, VXLAN trong hệ thống	40
Bảng 2.1	Thông tin VLAN, VXLAN trong hệ thống	41
Bảng 2.1	Thông tin VLAN, VXLAN trong hệ thống	42
Bảng 2.1	Thông tin VLAN, VXLAN trong hệ thống	43
Bảng 2.2	Thông tin kết nối port trong hệ thống	43
Bảng 2.2	Thông tin kết nối port trong hệ thống	44
Bảng 2.2	Thông tin kết nối port trong hệ thống	45
Bảng 2.2	Thông tin kết nối port trong hệ thống	46
Bảng 2.2	Thông tin kết nối port trong hệ thống	47
Bảng 2.2	Thông tin kết nối port trong hệ thống	48
Bảng 2.3	Thông tin quy hoạch địa chỉ IP	48
Bảng 2.3	Thông tin quy hoạch địa chỉ IP	49
Bảng 2.3	Thông tin quy hoạch địa chỉ IP	50
Bảng 2.4	IP dự phòng	50
Bảng 2.4	IP dự phòng	51
Bảng 5.1	Quy trình cấu hình của các thiết bị trong hệ thống	52
Bảng 5.2	Các lệnh cấu hình của Router ISP1	55
Bảng 5.3	Các lệnh cấu hình của Router ISP2	56

Bảng 5.4 Các lệnh cấu hình của Router R1	56
Bảng 5.5 Các lệnh cấu hình của Router R2	57
Bảng 5.6 Các lệnh cấu hình của Firewall FW1	58
Bảng 5.7 Các lệnh cấu hình của Firewall FW2	59
Bảng 5.8 Các lệnh cấu hình của NXOS1	61
Bảng 5.9 Các lệnh cấu hình của NXOS2	63
Bảng 5.10 Các lệnh cấu hình của NXOS3	65
Bảng 5.10 Các lệnh cấu hình của NXOS3	66
Bảng 5.10 Các lệnh cấu hình của NXOS3	67
Bảng 5.10 Các lệnh cấu hình của NXOS3	68
Bảng 5.10 Các lệnh cấu hình của NXOS3	69
Bảng 5.10 Các lệnh cấu hình của NXOS3	70
Bảng 5.10 Các lệnh cấu hình của NXOS3	71
Bảng 5.10 Các lệnh cấu hình của NXOS3	72
Bảng 5.11 Các lệnh cấu hình của NXOS4	73
Bảng 5.12 Các lệnh cấu hình của Switch Sw_A	80
Bảng 5.13 Các lệnh cấu hình của Switch Sw_B	81
Bảng 5.14 Các lệnh cấu hình của Switch Sw_C	82
Bảng 5.15 Các lệnh cấu hình của Switch Sw_DC1	84
Bảng 5.16 Các lệnh cấu hình của Switch Sw_DC2	85
Bảng 5.17 Các lệnh cấu hình của Router R3	86

Bảng 5.18 Các lệnh cấu hình của Switch Sw_BO	86
Bảng 5.19 Các lệnh cấu hình của Switch Sw_D1	87
Bảng 5.20 Các lệnh cấu hình của Switch Sw_D2	88

DANH MỤC CÁC CHỮ VIẾT TẮT

ACL	Access Control List
AD DS	Active Directory Domain Services
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EVE-NG	Emulated Virtual Environment – Netx Generation
FTP	File Transfer Protocol
GPO	Group Policy Object
HSRP	Hot Standby Router Protocol
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
LAN	Local Area Network
NAT	Network Address Translation
OSPF	Open Shortest Path First
SSH	Secure SHell
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNI	Virtual Network Instance
VTEPs	VXLAN Tunnel Endpoints
VNI	Virtual Network Instance
VPN	Virtual Private Network
VXLAN	Virtual Extensible LAN

CHƯƠNG 1 - TỔNG QUAN ĐỀ TÀI

1.1 Giới thiệu

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

Trong hệ thống giáo dục, mạng Local Area Network (LAN) là một phần không thể thiếu và đóng vai trò quan trọng đối với việc nâng cao hiệu quả giảng dạy và học tập. Mạng LAN giúp giáo viên và sinh viên có khả năng kết nối và chia sẻ thông tin một cách nhanh chóng giữa các thiết bị trong mạng. Mạng LAN còn có thể tạo điều kiện cho việc học từ xa bằng cách hỗ trợ triển khai hình thức giảng dạy trực tuyến (E-Learning), giúp giáo viên và sinh viên truy cập nhanh chóng các nguồn tài liệu giảng dạy.

Công nghệ VXLAN (Virtual Extensible LAN) và VLAN (Virtual Local Area Network) được áp dụng để phân đoạn và quản lý mạng trong môi trường mạng LAN. Trong khi VLAN bị giới hạn về số lượng ID VLAN có thể được sử dụng (4096 VLAN trên mỗi mạng LAN) thì VXLAN cho phép mở rộng số lượng mạng LAN ảo nhiều hơn đáng kể (tới hơn 16 triệu). Điều này đáp ứng được yêu cầu của các mạng có quy mô lớn và phức tạp. VXLAN cho phép kết nối các mạng LAN ảo qua các trung tâm dữ liệu khác nhau, trong khi VLAN hạn chế kết nối trong phạm vi một trung tâm dữ liệu hoặc một mạng cục bộ.

Trong những năm gần đây, VXLAN được các tổ chức sử dụng rộng rãi để mang lại hiệu quả tối ưu cho hệ thống mạng. Với công nghệ đang ngày càng phát triển thì việc sử dụng VXLAN mang lại nhiều lợi ích cho người dùng hơn so với VLAN truyền thống. Vì lý do đó, chúng em chọn công nghệ VXLAN để ứng dụng xây dựng hệ thống mạng.

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 tài liệu giảng dạy.

Việc sử dụng công nghệ VXLAN trong mạng LAN của trường học giúp giảm chi phí vận hành và quản lý mạng, 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 giúp chúng em có thêm 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.

Mục tiêu quan trọng nhất trong việc thiết kế môi trường mạng dùng cho giảng dạy và học tập là tạo ra một hệ thống an toàn, hiệu quả. Hệ thống mạng trong trường học phải luôn sẵn sàng, cho phép giáo viên và học sinh truy cập internet từ mọi vị trí hoặc thậm chí từ xa. Cần đáp ứng các yêu cầu truy cập từ phía người dùng.

Trong đó, mục tiêu vô cùng quan trọng chính là bảo mật trong tin. Trước các mối đe dọa, tấn công mạnh mẽ từ bên ngoài, hệ thống cần bảo vệ dữ liệu của người dùng bao gồm các thông tin cá nhân, tư liệu giảng dạy, tài liệu học tập và tài nguyên mạng. Cần thực hiện các chính sách bảo mật cho hệ thống mạng của trường học, có thể sử dụng các biện pháp bảo mật mạng như tường lửa, mã hoá các dữ liệu và xác thực người dùng truy cập để tăng sự riêng tư và an toàn cho hệ thống.

Triển khai công nghệ VXLAN để tạo mạng ảo và phân chia giữa các nhóm người dùng và từng bộ phận riêng biệt. Phân chia theo chức năng từng phòng ban và phân quyền cho nhóm người dùng để dễ dàng quản lý và chia sẻ tài nguyên. Điều này giúp tạo ra môi trường linh động trong hệ thống và có khả năng đáp ứng theo từng nhu cầu sử

dụng khác nhau của các nhóm đối tượng.

1.1.3 *Nội dung đề tài*

Nội dung của đề tài bao gồm:

- Tìm hiểu và nghiên cứu các kiến thức về mạng Lan, kỹ thuật 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. Trước khi tiến hành thiết kế mạng LAN sử dụng kỹ thuật VXLAN, cần xác định các yêu cầu cụ thể và rõ ràng để tạo mạng ảo cho giảng dạy và học tập. Các yêu cầu cần tìm hiểu và làm rõ bao gồm: số lượng người sử dụng mạng, số lượng các thiết bị mạng, ứng dụng đang hoạt động và các yêu cầu về bảo mật.
- Sử dụng phần mềm EVE-NG để thiết kế mô phỏng mô hình mạng LAN cho trường học, bao gồm cấu hình và 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 tiến hành mô phỏng hoạt động của hệ thống mạng và đánh giá tính khả dụng của kết nối, kiểm tra các tính năng được cấu hình và hiệu suất của hệ thống mạng.
- Cuối cùng là phân tích và đánh giá kết quả xây dựng hệ thống, 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.

1.1.4 *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 quá trình thiết kế hệ thống mạng LAN để tạo mạng ảo.

1.1.5 Phương pháp nghiên cứu

Cách tiếp cận nghiên cứu để xử lý vấn đề:

- **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 thực thi:** Để áp dụng và thực hành các kiến thức, cần có môi trường để triển khai. Phần mềm EVE-NG hỗ trợ tạo môi trường mạng ảo và thực hiện các thử nghiệm liên quan đến mạng LAN và VXLAN. Bắt đầu bằng việc nghiên cứu và 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.

1.1.6 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 giảng dạy tối ưu hơn, tiết kiệm chi phí hơn. Ngoài ra, có nhiều hướng phát triển trong tương lai bằng cách thêm các dịch vụ, công nghệ mới và có thể ứng dụng vào các lĩnh vực khác.

1.1.7 Cấu trúc bài báo cáo

Bài làm gồm có 4 chương:

- **Chương 1: Tổng quan đề tài**
 - Giới thiệu sơ lược, tổng quan về đề tài, mục tiêu của 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.
 - Giới thiệu cơ sở lý thuyết cần có để thực hiện đề tài và các lý thuyết liên quan đến đề tài.
- **Chương 2: Phân tích thiết kế hệ thống**
 - Khảo sát, phân tích thông tin về khu vực thực hiện đề tài.
 - Trình bày định hướng thiết kế hệ thống.
 - Thiết kế các sơ đồ mô phỏng mô hình mạng .
 - Liệt kê các thông tin cấu hình hệ thống.
- **Chương 3: Triển khai hệ thống**
 - Triển khai hệ thống mạng trên ứng dụng mô phỏng EVE-NG và tổng hợp các lệnh cấu hình thiết bị.
 - Trình bày kết quả demo hệ thống.
- **Chương 4: Tổng kết**

- Trình bày các kết quả đạt được sau khi hoàn thành dự án.
- Trình bày hướng phát triển dự án trong tương lai.

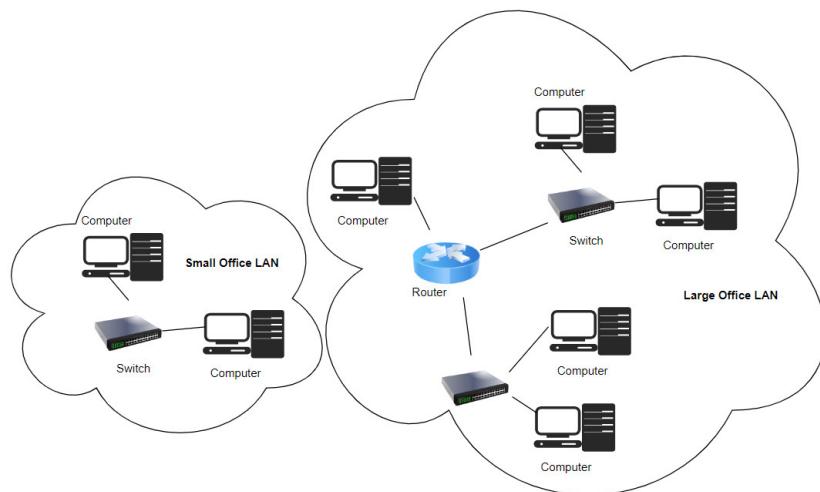
1.2 Cơ sở lý thuyết

1.2.1 Tìm hiểu về mạng LAN

a) Mạng LAN là gì?

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.

Kết nối trong mạng LAN thường được thực hiện qua dây cáp mạng hoặc kết nối không dây (Wi-Fi) trong một phạm vi giới hạn như cơ quan, gia đình hoặc doanh nghiệp.



Hình 1.1 Mô hình mạng LAN

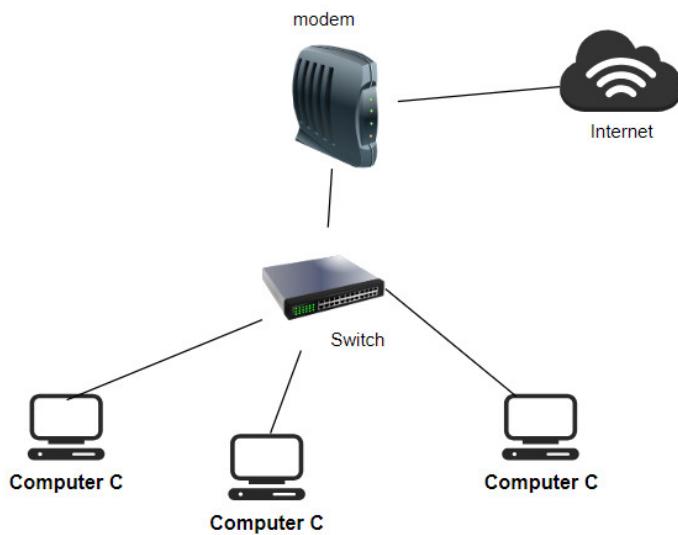
Mạng LAN tạo điều kiện cho việc chia sẻ dữ liệu và tài nguyên như tập tin, máy in, và phần mềm giữa các thiết bị, tạo ra môi trường thuận lợi để hợp tác và chia sẻ trong một phạm vi địa phương.

b) Phân loại mạng LAN

Mạng LAN có hai dạng chính là mạng LAN có dây và mạng LAN không dây:

- **Mạng LAN có dây:** Trong mạng LAN có dây, thường sử dụng các thiết bị chuyển mạch và cáp Ethernet để liên kết các thiết bị đầu cuối, máy chủ, hoặc các thiết bị IoT với mạng của tổ chức. Trong các doanh nghiệp nhỏ với số lượng thiết bị ít, mạng LAN có dây thường sử dụng các bộ chuyển mạch không quản lý, đảm bảo cung cấp đủ số lượng cổng Ethernet được sử dụng để liên kết tất cả các thiết bị.

Tuy nhiên, trong các mạng LAN lớn hơn, có nhu cầu kết nối hàng nghìn thiết bị, điều này đòi hỏi các biện pháp như cấu hình, triển khai phần cứng hoặc sử dụng phần mềm bổ sung để đảm bảo hoạt động của mạng một cách hiệu quả nhất.



Hình 1.2 Mạng LAN có dây

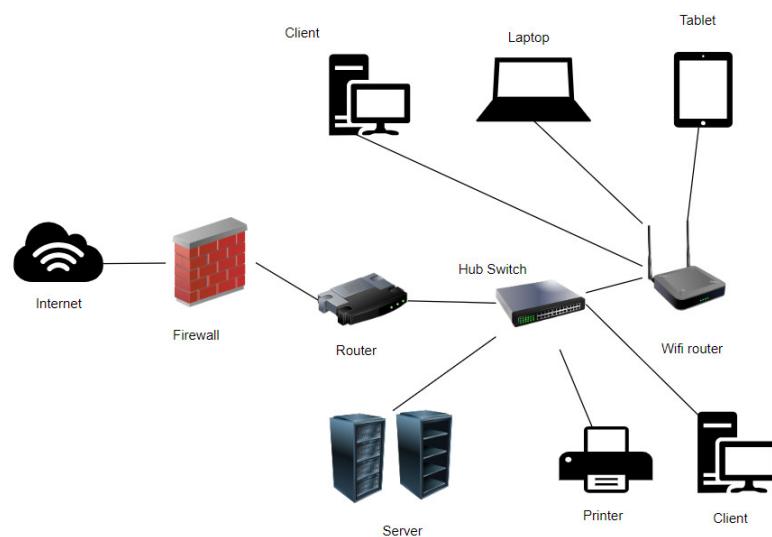
- **Mạng LAN không dây:** Sử dụng kỹ thuật IEEE 802.11 để truyền dữ liệu giữa các thiết bị đầu cuối và mạng thông qua phổ không dây. Trong nhiều trường hợp, mạng LAN không dây được ưu tiên hơn kết nối mạng LAN có dây vì tính linh hoạt và tiết kiệm

chi phí, không cần phải trải qua quá trình triển khai mạng cáp trên tất cả các khu vực của tòa nhà. Thông thường, các doanh nghiệp đánh giá mạng WLAN là phương tiện kết nối chính, bởi người dùng dựa trên điện thoại thông minh, máy tính bảng và các thiết bị di động khác.



Hình 1.3 Mạng LAN không dây

c) Các thành phần cơ bản của hệ thống mạng LAN



Hình 1.4 Hệ thống mạng LAN cơ bản

Mạng LAN bao gồm các thành phần (Sequeira, 2013) như:

- Computer

Máy tính đóng một vai trò quan trọng trong hệ thống 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.

- Server và Client

Thiết bị máy chủ (server) là một máy tính đảm nhận vai trò quản lý tài nguyên trên mạng. Server có thể phục vụ nhiều chức năng khác nhau, bao gồm lưu trữ tệp tin hoặc cơ sở dữ liệu. Các máy trạm (client) là những thiết bị được liên kết với nhau và dưới sự quản lý của máy chủ.

- Network Interface Card và Cable

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

Cáp mạng (cable) được sử dụng để kết nối 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 Layer 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 là thiết bị được sử dụng trong mạng LAN.

- **Switch**

Bộ chuyển mạch là thiết bị mạng được dùng để kết nối các thiết bị trong mạng máy tính thông qua chuyển mạch gói dữ liệu, cho phép nhận và chuyển tiếp dữ liệu đến thiết bị đích một cách hiệu quả.

- **Router**

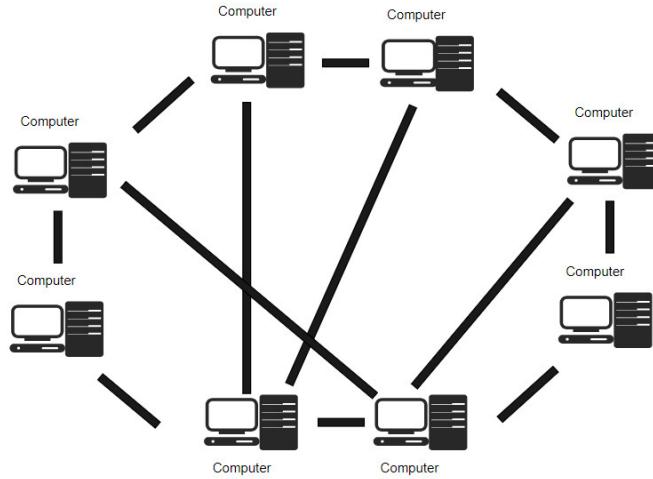
Bộ định tuyến: cung cấp phương tiện để kết nối các phân đoạn mạng LAN. Router là thiết bị giúp chuyển các gói dữ liệu sang một mạng khác và định tuyến chúng đến các đầu cuối thông qua quá trình định tuyến. Ngoài ra, router còn có khả năng liên kết các mạng LAN khác nhau, ngay cả khi chúng ở xa nhau.

d) **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.

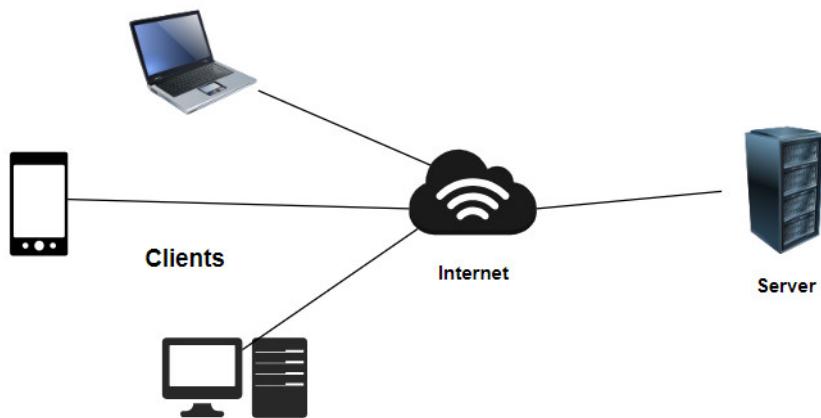
Mạng LAN thường được phân loại thành hai dạng chính: mạng ngang hàng và mạng máy khách-máy chủ. Trong mạng LAN máy khách-máy chủ, các máy tính khách kết nối với một máy chủ trung tâm, mà từ đó quản lý và điều khiển quyền truy cập vào ứng dụng, thiết bị và dữ liệu lưu trữ.

- Mạng ngang hàng là một cấu trúc mạng trong đó các máy tính kết nối với nhau thông qua Internet và chia sẻ dữ liệu mà không cần phải dựa vào một máy chủ trung tâm, thay vào đó sử dụng cơ chế phân tán.



Hình 1.5 Mạng ngang hàng

- Mô hình khách-máy chủ là một kiểu mạng máy tính có hai phần chính: máy khách và máy chủ. Máy chủ chứa tài nguyên và các dịch vụ được cài đặt dựa trên nhu cầu của máy khách. Ngược lại, máy khách gửi yêu cầu tới máy chủ và có thể kết nối đến các máy tính và các thiết bị điện tử khác.

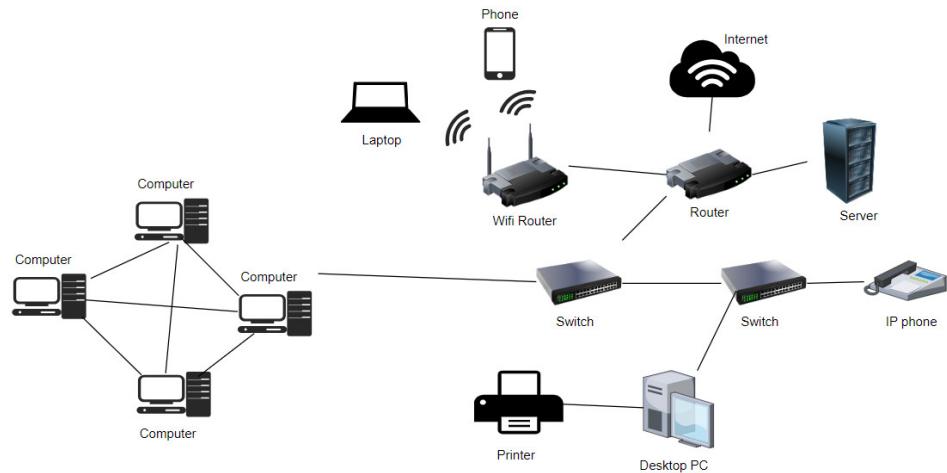


Hình 1.6 Mạng máy khách-máy chủ

Các ứng dụng chạy trên máy chủ trong mạng LAN cung cấp một loạt các dịch vụ

quan trọng như truy cập vào cơ sở dữ liệu và chia sẻ tài liệu. 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 có thể kết nối với nhau qua các kết nối truyền dẫn hoặc dịch vụ thuê riêng, và thậm chí có thể kết nối với Internet bằng cách sử dụng 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.



Hình 1.7 Hoạt động của mạng LAN

e) 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.
- **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, nâng cao tính bảo mật và khả năng khôi phục dữ liệu khi cần thiết.
- **Tích hợp ứng dụng trong mạng LAN:** Mạng LAN cung cấp khả năng tích hợp các dịch vụ và ứng dụng 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 cấu hình với các giao thức bảo mật như sử dụng 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 quản trị viên có thể dễ dàng quản lý và vận hành mạng một cách hiệu quả hơn.

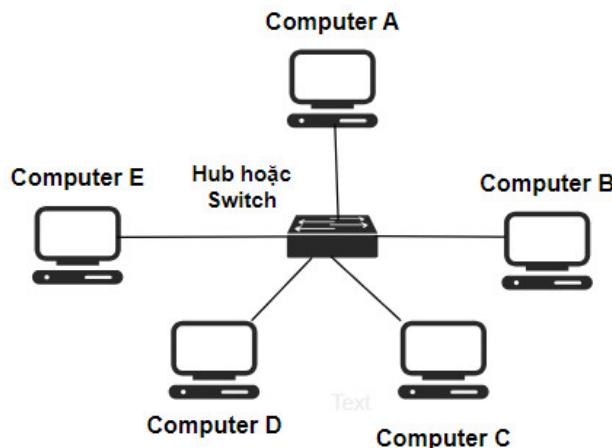
f) Các kiểu Topology cơ bản của mạng LAN

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 (Stallings, 2021) sau đây:

- **Mạng hình sao (Star Topology):**

- Mạng hình sao là một kiểu cấu trúc mạng máy tính, trong đó các thiết bị địa phương như máy tính, máy chủ và các thiết bị mạng khác được liên kết trực tiếp với một trung tâm thông qua các đường cáp riêng biệt. Trung tâm này thường là một switch hoặc hub, đóng vai trò chính trong việc quản lý kết nối và dẫn đường thông tin trong mạng. Điểm đặc biệt của mô hình này

là sự tập trung của dữ liệu và quản lý thông qua thiết bị trung tâm, giúp dễ dàng trong việc quản lý và điều chỉnh mạng.



Hình 1.8 Cấu trúc liên kết hình sao

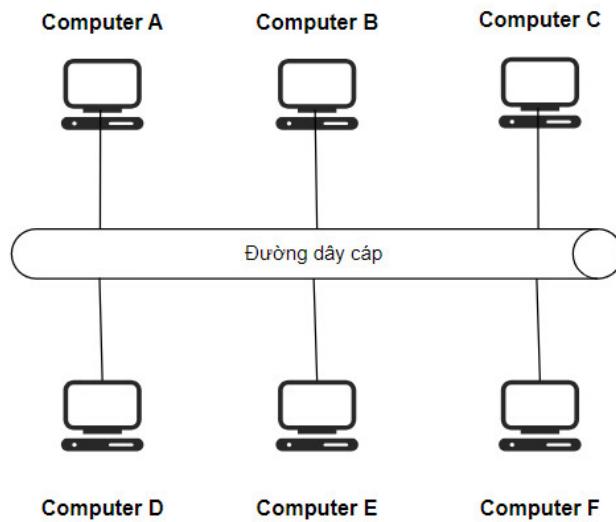
- **Ưu điểm:**

- **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 tạo ra hạn chế đối với 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):**



Hình 1.9 Cấu trúc liên kết bus

- 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 hầu hết các thiết bị trên đường truyền. 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 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.

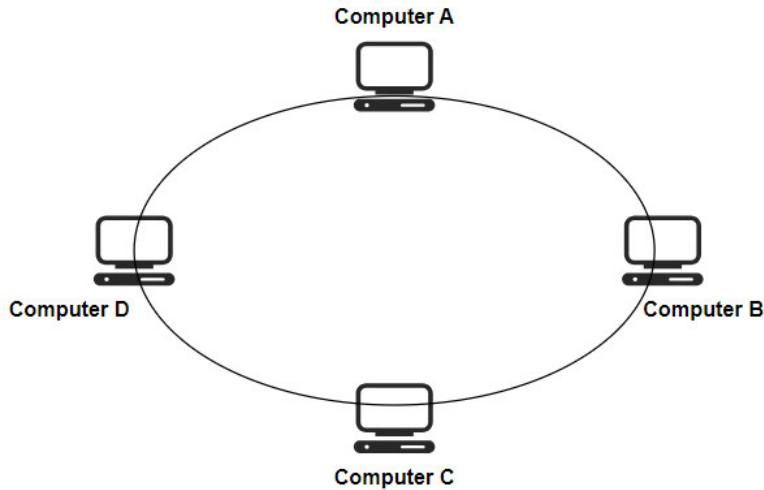
- **Nhược điểm:**

- **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 tuyến 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):**

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



Hình 1.10 Cấu trúc liên kết 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.

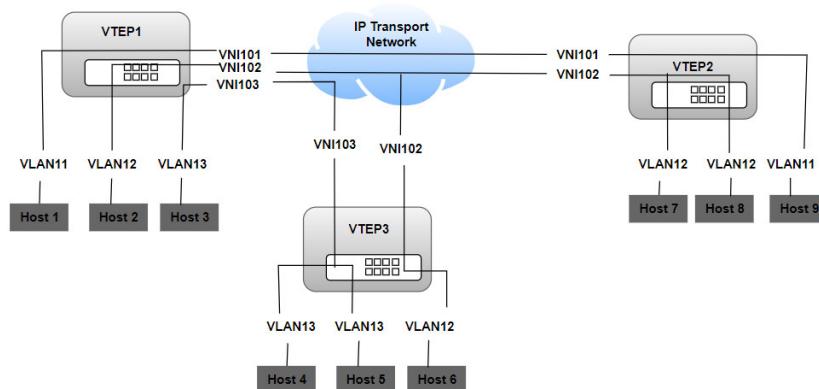
- **Hiệu suất giảm khi tăng số lượng thiết bị:** Khi số lượng thiết bị trên mạng tăng lên, hiệu suất của mạng có thể giảm do xung đột dữ liệu trên vòng.

1.2.2 Công nghệ VXLAN

a) VXLAN là gì?

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.

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.(Systems, 2021)



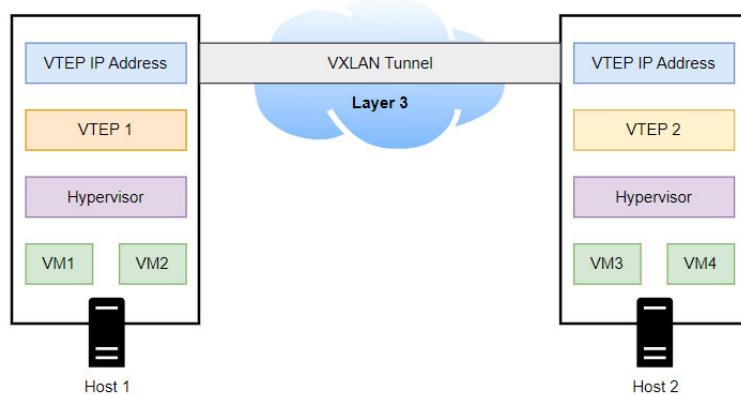
Hình 1.11 Mô hình VXLAN

b) Cách hoạt động của VXLAN

Giao thức tunneling VXLAN đóng gói các khung Ethernet ở Layer 2 vào các gói UDP ở Layer 4, tạo điều kiện cho việc tạo ra các mạng con ảo Layer 2 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). (Somit Maloo, 2020)

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 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.

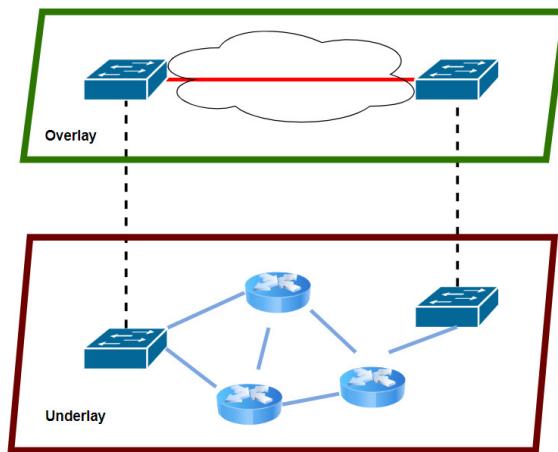


Hình 1.12 Cách hoạt động của VXLAN

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

c) Overlay và Underlay

VXLAN sử dụng mạng Underlay và mạng Overlay:



Hình 1.13 Lớp Underlay và lớp Overlay

- Underlay:

Mạng Undelay là tất cả cơ sở hạ tầng vật lý hỗ trợ các khung và gói tin được chuyển tiếp từ điểm này sang điểm khác, là nơi có thể liên kết và truyền thông với các thiết bị mạng. Underlay có vai trò quan trọng trong hỗ trợ việc di chuyển gói tin VXLAN và liên kết các VTEP trong mạng VXLAN.

Cần sử dụng các giao thức định tuyến phổ biến chẳng hạn như OSPF để hỗ trợ

việc chuyển tiếp các gói tin VXLAN hiệu quả. Các giao thức định tuyến giúp lựa chọn đường đi một cách tối ưu khi chuyển tiếp gói tin trong mạng Underlay. Ngoài ra, OSPF còn cung cấp khả năng quảng bá thông tin về địa chỉ IP của các VTEP và định tuyến của mạng VXLAN.

- **Overlay:**

Mạng Overlay là mạng ảo được xây dựng trên mạng Underlay. Overlay có khả năng tạo rất nhiều mạng ảo. Với một cơ sở hạ tầng vật lý có thể được sử dụng để xây dựng các mạng ảo khác nhau. Với khả năng mở rộng linh hoạt, Overlay đóng vai trò quan trọng trong kiến trúc của VXLAN.

Mạng Overlay triển khai các khái niệm ảo hóa mạng và sử dụng các giao thức đóng gói đường hầm Layer 2 và Layer 3 như VXLAN và IPSec. Các giao thức này cho phép vận chuyển các gói dữ liệu qua mạng Overlay, thu hẹp khoảng cách giữa các phân đoạn mạng khác nhau vốn có thể không liên lạc trực tiếp được. VXLAN là một trong những giao thức đóng gói Overlay phổ biến và hiệu quả nhất, cho phép tạo các mạng con hoặc phân đoạn Layer 2 ảo hóa trải rộng trên các mạng Layer 3 vật lý.

Mạng Overlay tạo các đường dẫn ảo trong mạng vật lý cơ bản để tối ưu hóa việc truyền dữ liệu. Các đường dẫn Overlay này định tuyến lưu lượng truy cập vào và ra khỏi trung tâm dữ liệu cũng như trong các máy ảo bên trong trung tâm dữ liệu.

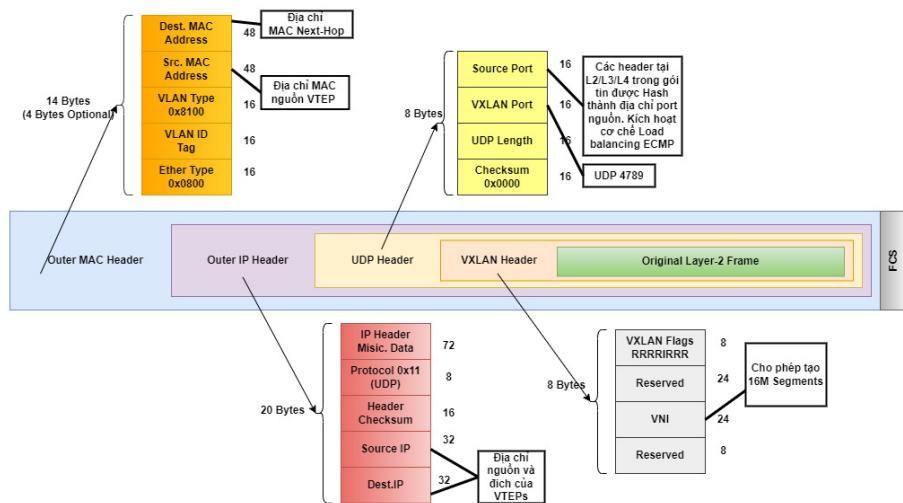
d) Cấu trúc gói tin VXLAN

Cấu trúc gói tin VXLAN:

- **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. Header VXLAN 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, chứa 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 điểm đến tiếp theo theo đường dẫn tới VTEP đích.



Hình 1.14 Cấu trúc gói tin VXLAN

e) 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.
- 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 thiết bị VTEP 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. VNI thường là phần giá trị 24 bit của tiêu đề VXLAN, có thể hỗ trợ tới 16 triệu phân đoạn mạng riêng lẻ. (Giá trị VNI hợp lệ là từ 4096 đến 16.777.215.)(Somit Maloo, 2020)
- VNI tương tự như VLAN ID trên mạng truyền thống và VNI 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.

f) **Ưu điểm của VXLAN**

- **Tính linh hoạt:** VXLAN cho phép linh hoạt hơn trong việc thiết kế mạng ảo, giúp dễ dàng điều chỉnh theo các yêu cầu thay đổi.
- **IP Mobility khả dụng:** VXLAN cung cấp hỗ trợ tốt hơn cho tính di động của IP, cho phép các máy ảo được di chuyển giữa các máy chủ vật lý mà không cần phải cấu hình lại.
- **Khả năng mở rộng:** VXLAN cho phép số lượng mạng logic lớn hơn nhiều (lên tới 16 triệu) so với VLAN truyền thống (4.094), chính vì thế nên VXLAN có khả năng mở rộng cao hơn.
- **Bảo mật:** VXLAN cung cấp mức độ bảo mật cao trên các mạng được phân đoạn. VXLAN cho phép cách ly các mạng ảo khác nhau và giảm bồ mặt tấn công.
- **Multi-tenancy:** VXLAN cung cấp hỗ trợ tốt hơn cho multi-tenancy, cho phép cách ly các mạng thuê khác nhau trong một cơ sở hạ tầng vật lý duy nhất.

g) **Ứng dụng VXLAN**

VXLAN cho phép tạo ra các mạng LAN ảo độc lập (VXLAN overlay) trên cùng một hạ tầng mạng vật lý. Điều này rất hữu ích trong các môi trường đa người dùng, nơi mà nhiều khách hàng hoặc phòng ban cần một mạng LAN riêng biệt và bảo mật. VXLAN có thể được sử dụng để kết nối các mạng LAN ảo qua các mạng WAN, cho phép truy cập dễ dàng và bảo mật giữa các chi nhánh hoặc trung tâm dữ liệu khác nhau. Ngoài ra, VXLAN là một công nghệ quan trọng trong việc xây dựng các mạng LAN ảo trong môi trường đám mây, VXLAN cho phép tự động hóa và mở rộng mạng một cách

linh hoạt.

1.2.3 Phân mềm EVE-NG

a) Giới thiệu sơ lược về EVE-NG

EVE-NG là một công cụ giả lập mô phỏng mạng. Từ một thư viện các template sẵn có, người dùng có thể tạo các node mạng, kết nối chúng lại với nhau và cấu hình chúng. Ngoài ra, người dùng còn có thể thêm các image phần mềm khác vào thư viện trên EVE để thực hiện các mô hình lab khác nhau.

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.

b) 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 người dùng tạo ra mô hình mạng ảo với hàng trăm thiết bị mạng như router, switch, firewall, máy chủ và nhiều thiết bị khác nữa. Người sử dụng có thể tạo ra các mạng LAN, mạng WAN, và thậm chí mạng phân tán phức tạp quy mô lớn với EVE-NG. Việc mô phỏng mạng trên EVE-NG hỗ trợ mô phỏng các cấu hình, triển khai hệ thống mạng 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 người dùng tạo ra môi trường mạng ảo với các thiết bị từ nhiều

nha 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 người sử dụng dễ dàng thao tác 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. 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 người sử dụng 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 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. Người dùng 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.
- **Chia sẻ và hợp tác:** EVE-NG cho phép người dùng chia sẻ và hợp tác trong việc xây dựng và thử nghiệm mạng. Người dùng có thể chia sẻ mô hình mạng, bài lab, hướng dẫn và tài liệu tham khảo với cộng đồng sử dụng EVE-NG. Vì thế, EVE-NG 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.

c) 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.

- **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 EVE 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.

1.2.4 Bảo mật hệ thống

a) 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 có thể ngăn chặn các tấn công 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.

b) Các giải pháp bảo mật mạng

- **NAT (Chuyển đổi địa chỉ mạng)** là một kỹ thuật được sử dụng để chuyển đổi địa chỉ IP của các gói tin trong mạng. 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.
- **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. Tường lửa 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.
- **ACL (Danh sách điều khiển truy cập)** là danh sách tuân tự các câu lệnh dùng để quản lý lưu lượng truy cập đến hoặc đi trên một thiết bị. ACL được sử dụng rộng rãi trong các thiết bị mạng như router, switch và firewall để xác định quyền truy cập của các gói dữ liệu dựa trên các điều kiện như địa chỉ IP nguồn và đích, cổng giao thức, hoặc các tiêu chí khác. ACL có thể được cấu hình để cho phép (allow) hoặc từ chối (deny) gói dữ liệu dựa trên các quy tắc được xác định trước, từ đó giúp kiểm soát và bảo vệ mạng khỏi các mối đe dọa bảo mật hoặc ngăn chặn truy cập không ủy quyền đến các tài nguyên mạng.

- **SSH (Vỏ bọc an toàn)** là một giao thức mạng được sử dụng để thiết lập kết nối an toàn và mã hóa giữa hai thiết bị trong mạng, cho phép truy cập từ xa và quản lý máy chủ hoặc thiết bị mạng một cách bảo mật. SSH sử dụng mã hóa để bảo vệ dữ liệu truyền qua mạng, bao gồm cả các thông tin như tên đăng nhập, mật khẩu và dữ liệu truyền qua kết nối. SSH được sử dụng rộng rãi trong các môi trường máy chủ và mạng để quản lý từ xa các máy chủ Linux, thiết bị mạng như router và switch, cũng như để truy cập vào các hệ thống điện toán đám mây và máy chủ web.

CHƯƠNG 2 - PHÂN TÍCH THIẾT KẾ HỆ THỐNG

2.1 Khảo sát yêu cầu của trường học

2.1.1 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 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. Dự án thiết kế mạng LAN cho trường học sử dụng kỹ thuật VXLAN để có thể mở rộng trong tương lai 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:

Trường đại học có trụ sở chính tại Thành phố Hồ Chí Minh và chi nhánh ở Cần Thơ. Trụ sở chính bao gồm 3 tòa chính là A, B và C và tòa D:

- Tòa A có 3 phòng ban là phòng hành chính, phòng đào tạo, phòng tuyển sinh và 5 phòng lab.
- Tòa B có 4 phòng ban là văn phòng khoa xã hội và nhân văn, khoa dược, khoa ngoại ngữ, khoa tài chính ngân hàng và 10 lớp học.
- Tòa C có 3 phòng ban là phòng kỹ thuật, phòng khoa công nghệ thông tin, khoa quản trị kinh doanh; 10 phòng học và thư viện.
- Tòa D có 2 phòng ban là phòng kỹ thuật, văn phòng khoa; 10 phòng học và thư viện.

Chức năng chính của các phòng ban:

- Phòng hành chính có chức năng quản lý các dữ liệu, hồ sơ của toàn bộ sinh viên. Chuyên xử lý các đơn từ và khiếu nại từ sinh viên.

- Phòng đào tạo có chức năng quản lý điểm số của sinh viên và xử lý các vấn đề liên quan đến học vụ.
- Phòng tuyển sinh có chức năng tiếp nhận, xử lý và quản lý các hồ sơ tuyển sinh.
- Các phòng lab tòa A được bố trí nhiều máy tính để sinh viên thực hành các môn học.
- Các văn phòng khoa có chức năng quản lý dữ liệu sinh viên, giảng viên của từng khoa, cập nhật dữ liệu khi có sự thay đổi, tiếp nhận, xử lý các vấn đề của từng khoa.
- Phòng kỹ thuật có chức năng đảm bảo khả năng kết nối và truy cập mạng ổn định cho giảng viên và học sinh, triển khai, duy trì và bảo trì hệ thống của trường học. Trong phòng kỹ thuật có khu vực Server, đây là nơi hạ tầng mạng của trường được lắp đặt và triển khai.
- Thư viện có chức năng chứa các tài liệu, sách, bài báo liên quan đến giáo dục, cho phép sinh viên tìm kiếm và truy cập bài giảng, tài liệu học tập.

2.1.2 Yêu cầu người dùng

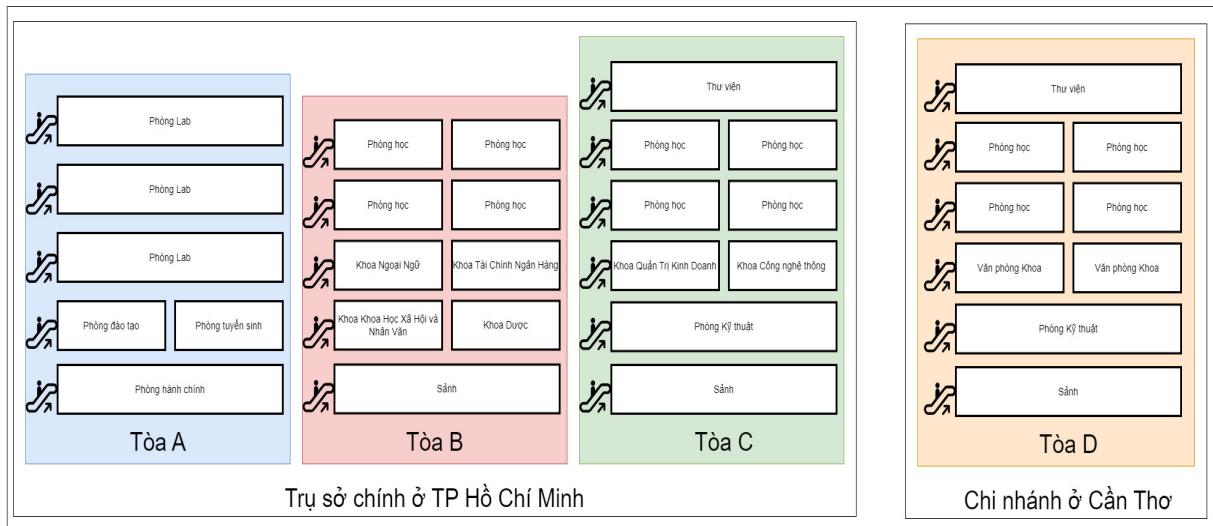
- Đảm bảo khả năng truy cập mạng vào tài nguyên một cách dễ dàng từ bất kỳ đâu, bất kỳ thiết bị nào. Hệ thống cần có độ ổn định và hiệu suất cao khi sử dụng các ứng dụng và tài nguyên trên mạng.
- Đảm bảo sự an toàn và riêng tư cho hệ thống mạng trường học. Có các chính sách quản lý truy cập, cũng như khả năng bảo mật tài khoản. Cho phép chia sẻ dữ liệu trong mạng. Bảo vệ thông tin dữ liệu của trường học trong quá trình sử dụng mạng và các khi sử dụng các ứng dụng liên quan.
- Cho phép người dùng truy cập và sử dụng các thiết bị của trường trên nhiều nền tảng, bao gồm cả máy tính, máy in, máy chiếu, điện thoại di động và máy tính bảng.

- Có khả năng mở rộng hệ thống trong tương lai để đáp ứng với các yêu cầu và thay đổi của môi trường giáo dục.
- Đòi hỏi sự hỗ trợ kỹ thuật nhanh chóng để giải quyết mọi vấn đề kỹ thuật khi có sự cố xảy ra.

2.1.3 Yêu cầu về bảo mật

- Quản lý quyền VXLAN bằng cách 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 mạng ảo bằng cách 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 bằng cách 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 bằng cách duy trì chính sách cập nhật định kỳ cho hệ thống.

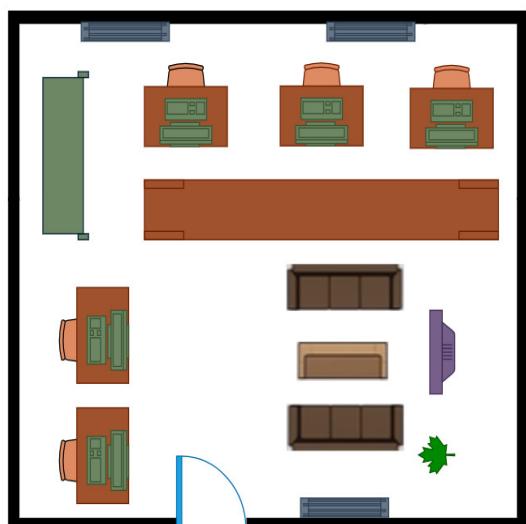
2.1.4 Sơ đồ cấu trúc trường học



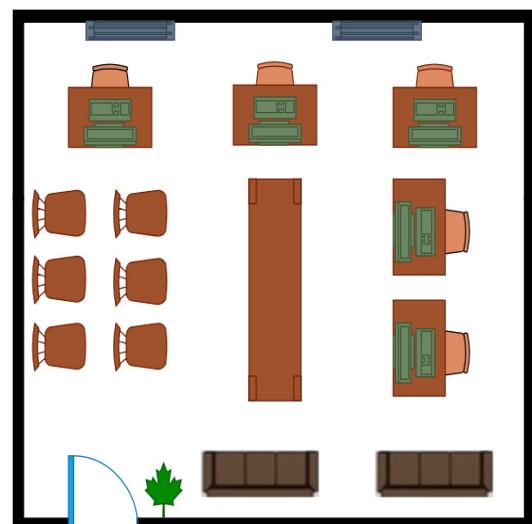
Hình 2.1 Sơ đồ tổng quan cấu trúc trường

Mặt cắt bằng của các phòng:

Mặt cắt bằng của phòng hành chính và phòng đào tạo:

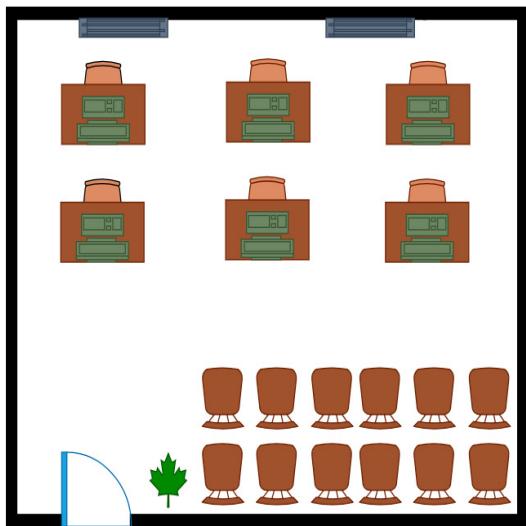


Hình 2.2 Phòng hành chính

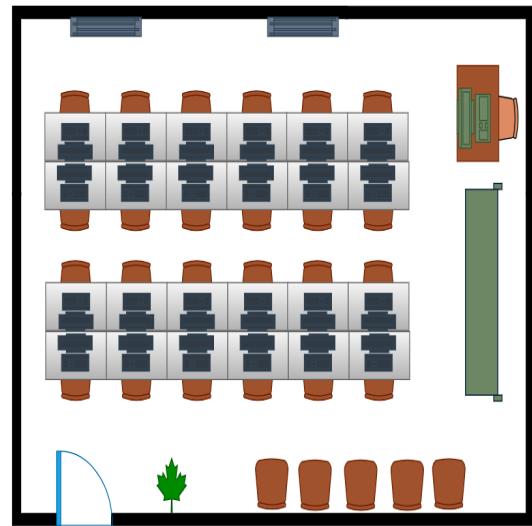


Hình 2.3 Phòng đào tạo

Mặt cắt băng của phòng tuyển sinh và phòng lab:

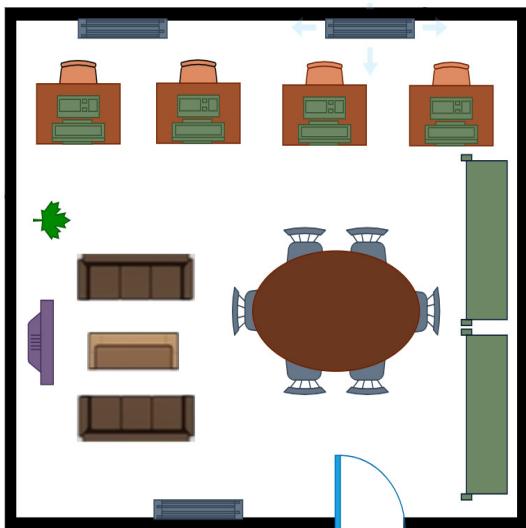


Hình 2.4 Phòng tuyển sinh

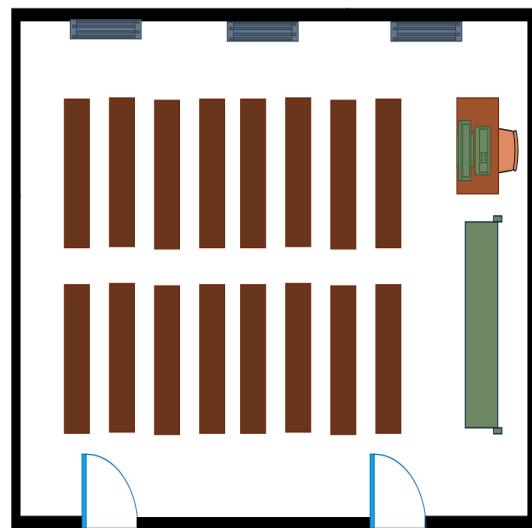


Hình 2.5 Phòng lab

Mặt cắt băng của văn phòng khoa và phòng học:

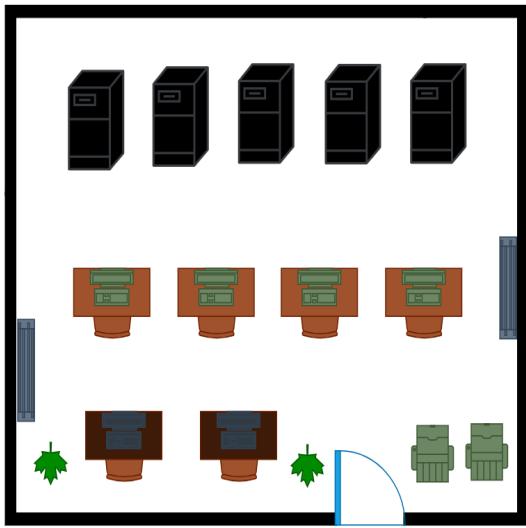


Hình 2.6 Văn phòng khoa

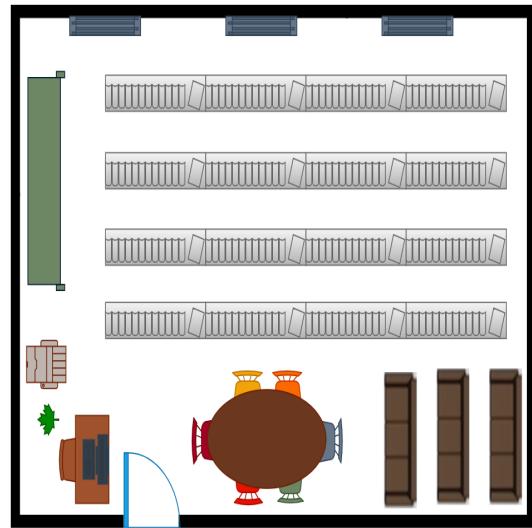


Hình 2.7 Phòng học

Mặt cắt băng của phòng kỹ thuật và thư viện:



Hình 2.8 Phòng kỹ thuật



Hình 2.9 Thư viện

2.2 Định hướng thiết kế hệ thống

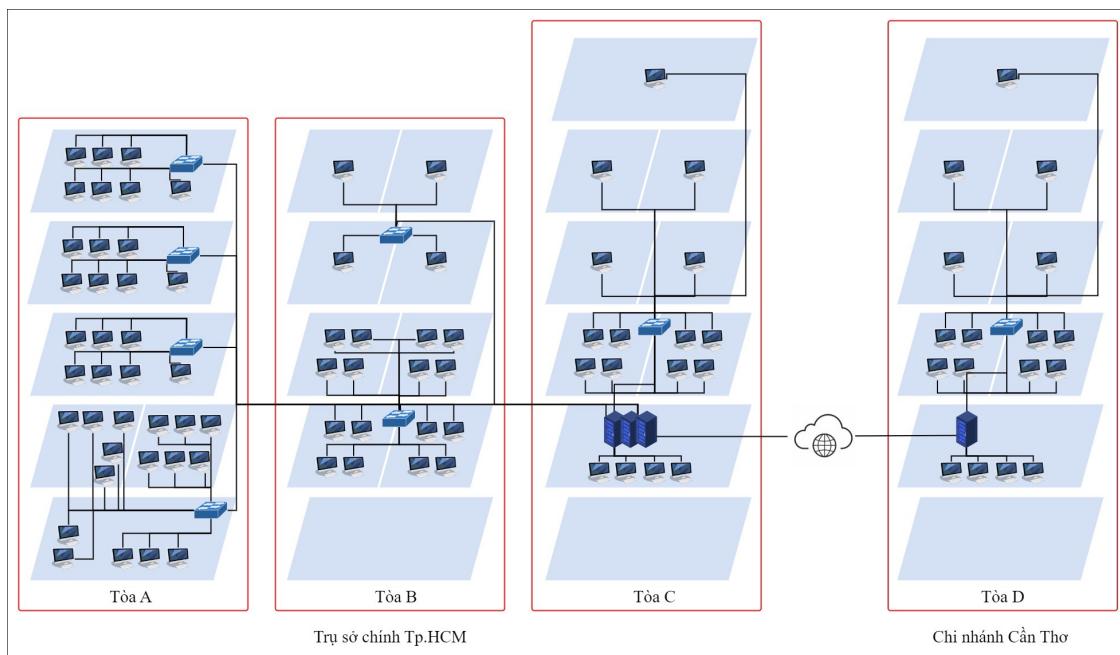
- Sử dụng EVE-NG để xây dựng, mô phỏng các thiết bị thực tế sẽ được triển khai trong mạng VXLAN.
- Sử dụng VLAN để phân loại và phân đoạn mạng trong trường học. Các VLAN có thể được thiết lập cho từng khoa, tòa nhà, giúp quản lý hiệu quả lưu lượng mạng.
- Sử dụng VXLAN giúp cung cấp mạng ảo linh hoạt và dễ quản lý cho các máy ảo trong môi trường ảo hóa. 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.
- Cài đặt các dịch vụ mạng như DHCP, DNS, Mail Server. Sử dụng DHCP server để tự động cấp phát địa chỉ IP động trong hệ thống. 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 tường lửa để ngăn chặn sự tấn công từ kẻ thù, bảo vệ hệ thống khỏi các mối đe dọa.
- 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.

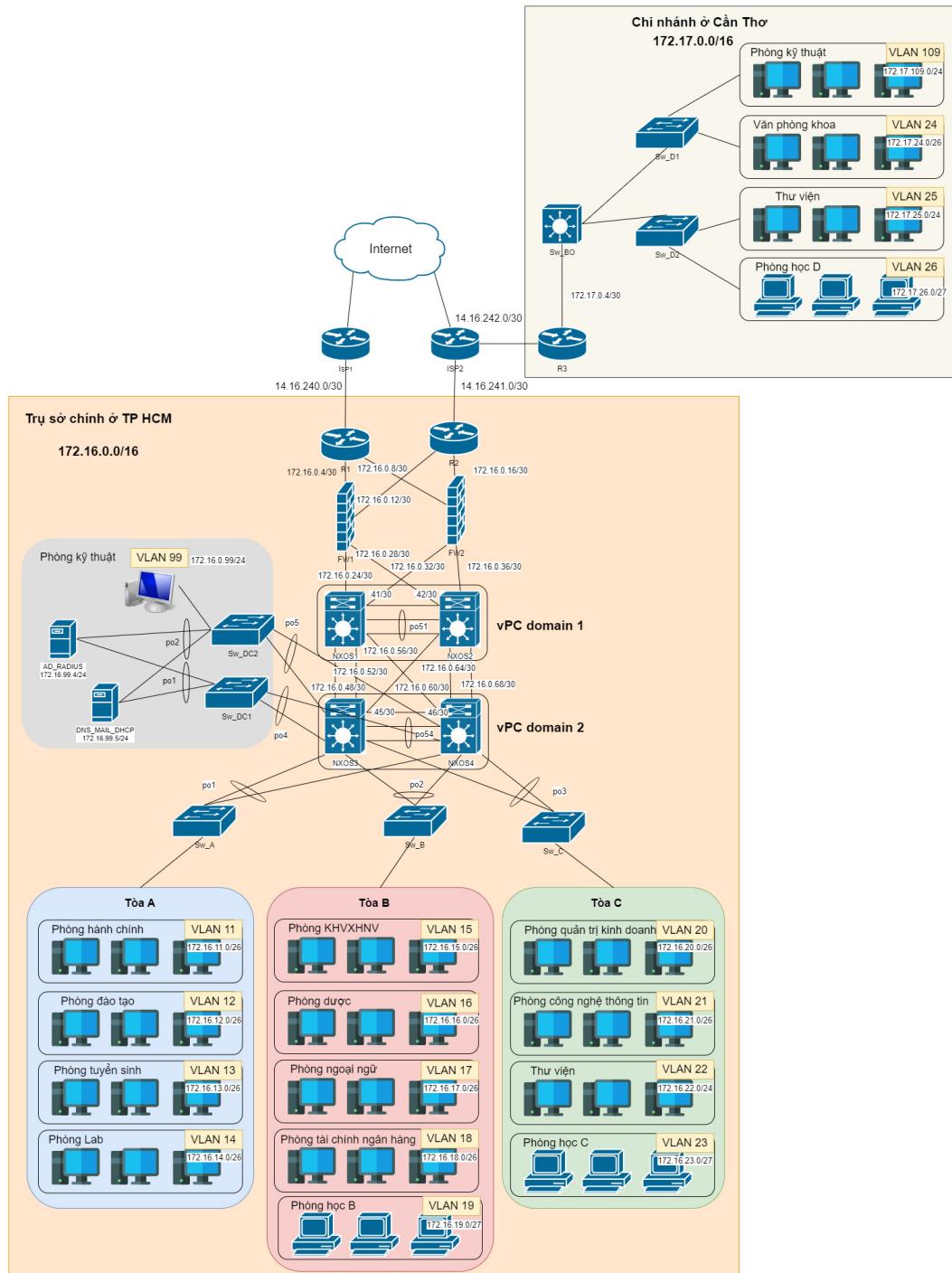
2.3 Thiết kế mô hình mạng

2.3.1 Sơ đồ vật lý



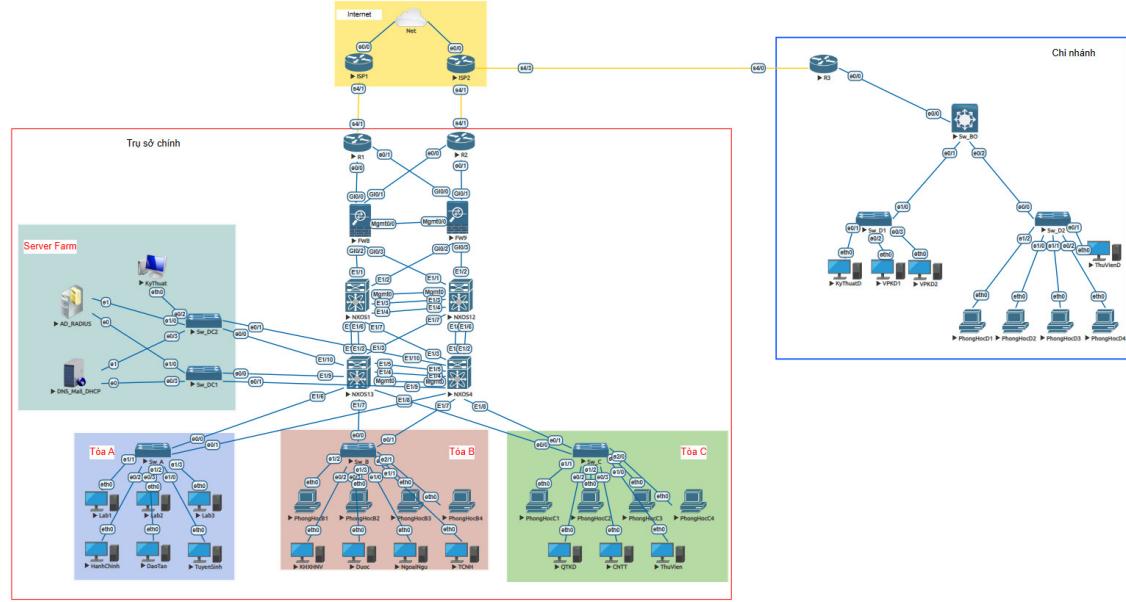
Hình 2.10 Sơ đồ vật lý

2.3.2 Sơ đồ logic



Hình 2.11 Sơ đồ logic

2.3.3 Sơ đồ luân lý



Hình 2.12 Sơ đồ luân lý

2.4 Thông tin cài đặt cấu hình hệ thống

2.4.1 Thông tin VLAN, VXLAN trong hệ thống

Bảng 2.1 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 2.1 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 2.1 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 2.1 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 2.1 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

2.4.2 Thông tin kết nối port trong hệ thống**Bảng 2.2 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 2.2 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	
NXOS3	e1/1	NXOS1	e1/5	
	e1/2	NXOS1	e1/6	
	e1/3	NXOS2	e1/7	

Bảng 2.2 Thông tin kết nối port trong hệ thống

Source		Destination		VLAN/Port- channel
Tên thiết bị	Interface	Tên thiết bị	Interface	
NXOS3	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
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

Bảng 2.2 Thông tin kết nối port trong hệ thống

Source		Destination		VLAN/Port- channel
Tên thiết bị	Interface	Tên thiết bị	Interface	
Sw_A	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
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

Bảng 2.2 Thông tin kết nối port trong hệ thống

Source		Destination		VLAN/Port- channel
Tên thiết bị	Interface	Tên thiết bị	Interface	
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
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

Bảng 2.2 Thông tin kết nối port trong hệ thống

Source		Destination		VLAN/Port- channel
Tên thiết bị	Interface	Tên thiết bị	Interface	
Sw_D2	e0/3	PhongHocD2	eth0	VLAN26
	e1/0	PhongHocD3	eth0	VLAN26
	e1/1	PhongHocD4	eth0	VLAN26

2.4.3 Thông tin địa chỉ IP planning**Bảng 2.3 Thông tin quy hoạch địa chỉ IP**

Tên thiết bị	Interface	Subnet	IPv4	Gateway
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	

Bảng 2.3 Thông tin quy hoạch địa chỉ IP

Tên thiết bị	Interface	Subnet	IPv4	Gateway
FW2	g0/2	172.16.0.32/30	172.16.0.33	
	g0/3	172.16.0.36/30	172.16.0.37	
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	
	e1/1	172.16.0.28/30	172.16.0.30	
NXOS2	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	
	e1/1	172.16.0.48/30	172.16.0.50	
NXOS3	e1/2	172.16.0.52/30	172.16.0.54	
	e1/3	172.16.0.60/30	172.16.0.61	
	e1/1	172.16.0.64/30	172.16.0.66	
NXOS4	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	172.16.99.6	172.16.99.3

Bảng 2.3 Thông tin quy hoạch địa chỉ IP

Tên thiết bị	Interface	Subnet	IPv4	Gateway
AD_RADIUS	e0	172.16.99.0/24	172.16.99.4	172.16.99.3
	e1			
DNS_Mail_DHCP	e0	172.16.99.0/24	172.16.99.5	172.16.99.3
	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_Core_BO	e0/0	172.17.0.4/30	172.17.0.6	

VXLAN có thể mở rộng mạng với quy mô rất lớn, sử dụng các dải địa chỉ mạng dự phòng, hệ thống có thể mở rộng mạng mà không gặp phải xung đột địa chỉ IP. Nhờ việc triển khai công nghệ VXLAN, sử dụng Nexus có sức chịu tải lớn, cung cấp băng thông cao và khả năng xử lý mạng lớn nên băng thông sẽ không bị ảnh hưởng, đáp ứng nhu cầu mở rộng hệ thống trong tương lai.

Bảng 2.4 IP dự phòng

STT	Dải IP	Subnet mask	Phạm vi
1	172.16.0.0/30	/30	172.16.0.1 - 172.16.0.2
2	172.16.0.64/26	/26	172.16.0.65 - 172.16.0.126
3	172.16.0.128/25	/25	172.16.0.129 - 172.16.0.254
4	172.16.1.0/24	/24	172.16.1.1 - 172.16.1.254
5	172.16.2.0/24	/24	172.16.2.1 - 172.16.2.254

Bảng 2.4 IP dự phòng

STT	Dải IP	Subnet mask	Phạm vi
6	172.16.3.0/24	/24	172.16.3.1 - 172.16.3.254
7	172.16.4.0/24	/24	172.16.4.1 - 172.16.4.254
8	172.16.5.0/24	/24	172.16.5.1 - 172.16.5.254
9	172.16.6.0/24	/24	172.16.6.1 - 172.16.6.254
10	172.16.7.0/24	/24	172.16.7.1 - 172.16.7.254
11	172.16.8.0/24	/24	172.16.8.1 - 172.16.8.254
12	172.16.9.0/24	/24	172.16.9.1 - 172.16.9.254
13	172.16.10.0/24	/24	172.16.10.1 - 172.16.10.254
14	172.16.24.0/24	/24	172.16.24.1 - 172.16.24.254
15	172.16.25.0/24	/24	172.16.25.1 - 172.16.25.254
16	172.16.26.0/24	/24	172.16.26.1 - 172.16.26.254
17	172.16.27.0/24	/24	172.16.27.1 - 172.16.27.254
18	172.16.28.0/24	/24	172.16.28.1 - 172.16.28.254
19	172.16.29.0/24	/24	172.16.29.1 - 172.16.29.254
20	172.16.30.0/24	/24	172.16.30.1 - 172.16.30.254
21	172.16.31.0/24	/24	172.16.31.1 - 172.16.31.254

CHƯƠNG 3 - 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	Switch Nexus 9000v có vai trò là điểm tập trung cho việc kết nối	1. Cấu hình cơ bản 2. Cấu hình địa chỉ IP 3. Cấu hình định tuyến OSPF

4	NXOS1 NXOS2	các leaf switch và cung cấp khả năng mở rộng linh hoạt cho mạng.	4. Cấu hình định tuyến static 5. Cấu hình VXLAN 6. Cấu hình vPC 7. Cấu hình Telnet/SSH
5	NXOS3 NXOS4	Switch Nexus 9000v có nhiệm vụ định tuyến các VXLAN, phân phối lưu lượng mạng VXLAN.	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
6	Sw_A Sw_B Sw_C	Có nhiệm vụ kết nối giữa các Leaf Switch với End Device.	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

			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
7	Sw_DC1 Sw_DC2	Có nhiệm vụ kết nối giữa các Leaf Switch với các Server ở khu vực Server farm.	
Chi nhánh Cần Thơ			
8	Các Server	Có nhiệm vụ cung cấp các dịch vụ cho người dùng và thiết bị khác trong mạng.	1. Cài đặt hệ điều hành 2. Cấu hình địa chỉ IP 3. Cấu hình dịch vụ
9	R3	Router kết nối với nhà cung cấp dịch vụ và phân đoạn mạng nội bộ khu vực chi nhánh.	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.	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

Bảng 5.2 Các lệnh cấu hình của Router ISP1

Bảng 5.3 Các lệnh cấu hình của Router ISP2

ISP2		
1.Cấu hình cơ bản #ip name-server 8.8.8.8 #ip domain-lookup	#interface e0/0 #ip address dhcp #no shutdown	4.Cấu hình định tuyến static #ip route 0.0.0.0 0.0.0.0 192.168.1.1
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	#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	3.Cấu hình định tuyến OSPF 5.Cấu hình NAT #access-list 10 permitany #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 #hostname R1 #ip domain-name cmu.edu #no ip domain-lookup	#interface s4/1 #ip address 14.16.240.2 255.255.255.252 #no shutdown #interface e0/0	255.255.255.252 #no shutdown #interface e0/1 #ip address 172.16.0.9 255.255.255.252
2.Cấu hình địa chỉ IP	#ip address 172.16.0.5	#no shutdown

3. Cấu hình OSPF	#ip ospf 1 area 0	generatal-keys 1024
#router ospf 1		#username adminHO
#router-id 11.0.0.1		secret AdminHO@123
#interface s4/1		#ip ssh ver 2
#ip ospf 1 area 1	14.16.240.1	#line vty 0 4
#interface e0/0		#login local
#ip ospf 1 area 0		#transport input SSH
#interface e0/1	#crypto key generate rsa	

Bảng 5.5 Các lệnh cấu hình của Router R2

R2			
1.Cấu hình cơ bản	#ip address 172.16.0.17 255.255.255.252 #no shutdown	4.Cấu hình định tuyến static #ip route 0.0.0.0 0.0.0.0 14.16.241.1	
2.Cấu hình địa chỉ IP	#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	3.Cấu hình OSPF #router ospf 1 #router-id 11.0.0.2 #interface s4/1 #ip ospf 1 area 1 #interface e0/0 #ip ospf 1 area 0 #interface e0/1 #ip ospf 1 area 0	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

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

<pre>#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</pre> <hr/>	<p>5. Cấu hình ACL</p> <pre>#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</pre>	<pre>#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</pre>
<p>3. Cấu hình định tuyến OSPF</p> <pre>#router ospf 1 #router-id 11.0.0.4 #network 172.16.0.0 255.255.255.0 area 0.0.0.0</pre> <hr/>		
<p>4. Cấu hình định tuyến static</p> <pre>#route OUT-2 0.0.0.0 0.0.0.0 172.16.0.17</pre>		

#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
6. Cấu hình vPC	#channel-group 51 mode	#username adminHO
	active	password
#feature vpc	#no shutdown	AdminHO@123
#feature lacp	#interface po51	#username adminHO role
#vpc domain 1	#description vPC-PeerLink	network-admin
7. Cấu hình Telnet/SSH		

Bảng 5.10 Các lệnh cấu hình của NXOS3

NXOS3		
1. Cấu hình cơ bản #hostname NXOS3 #ip domain-name cmu.edu #no ip domain-lookup	#username admin1 password Admin1@123 role network-admin	2. Cấu hình địa chỉ IP #interface e1/1 #no switchport #ip address 172.16.0.50

Bảng 5.10 Các lệnh cấu hình của NXOS3

NXOS3		
255.255.255.252	#license smart enable	4. Tạo VLAN
#no shutdown	#feature ospf	#vlan 11
#interface e1/2	#router ospf 1	#name HanhChinh
#no switchport	#router-id 11.0.0.7	#vlan 12
#ip address 172.16.0.54	#interface e1/1	#name DaoTao
255.255.255.252	#no switchport	#vlan 13
#no shutdown	#ip ospf network	#name TuyenSinh
#interface e1/3	point-to-point	#vlan 14
#no switchport	#ip router ospf 1 area 0	#name Lab
#ip address 172.16.0.61	#interface e1/2	#vlan 15
255.255.255.252	#no switchport	#name KHXHNV
#no shutdown	#ip ospf network	#vlan 16
#interface mgmt0	point-to-point	#name Duoc
#ip address 172.16.0.45	#ip router ospf 1 area 0	#vlan 17
255.255.255.252	#interface e1/3	#name NgoaiNgu
#no shutdown	#no switchport	#vlan 18
#interface loopback0	#ip ospf network	#name TCNH
#ip address 1.1.1.5/32	point-to-point	#vlan 19
#ip address 1.1.1.4/32	#ip router ospf 1 area 0	#name PhongHocB
secondary	#interface loopback0	#vlan 20
3. Cấu hình định tuyến	#ip ospf network	#name QTKD
OSPF	point-to-point	#vlan 21
	#ip router ospf 1 area 0	#name CNTT

Bảng 5.10 Các lệnh cấu hình của NXOS3

NXOS3		
#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
vlan 11-23,99	#interface e1/8	255.255.255.192
#no shutdown	#switchport	#ip router ospf 1 area 0
#exit	#switchport mode trunk	#mtu 9216
#interface e1/5	#switchport trunk allow	#no shutdown
#switchport	vlan 21,22,23	#interface vlan 12
#switchport mode trunk	#no shutdown	#ip address 171.16.12.1
#switchport trunk allow	#exit	255.255.255.192
vlan 11-23,99	#interface e1/9	#ip router ospf 1 area 0
#no shutdown	#switchport	#mtu 9216
#exit	#switchport mode trunk	#no shutdown
#interface e1/6	#switchport trunk allow	#interface vlan 13
#switchport	vlan 99	#ip address 171.16.13.1
#switchport mode trunk	#no shutdown	255.255.255.192
	#exit	

Bảng 5.10 Các lệnh cấu hình của NXOS3

NXOS3		
#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
#ip router ospf 1 area 0	#mtu 9216	#no shutdown
#mtu 9216	#no shutdown	#interface vlan 99
#no shutdown	#interface vlan 20	#ip address 171.16.99.1
#interface vlan 16	#ip address 171.16.20.1	255.255.255.0
#ip address 171.16.16.1	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	7. Cấu hình VXLAN
#no shutdown	#interface vlan 21	#system jumbomtu 9216
#interface vlan 17	#ip address 171.16.21.1	#feature pim
#ip address 171.16.17.1	255.255.255.192	#interface e1/4
255.255.255.192	#ip router ospf 1 area 0	#ip pim sparse-mode
#ip router ospf 1 area 0	#mtu 9216	

Bảng 5.10 Các lệnh cấu hình của NXOS3

NXOS3		
#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
#interface loopback0	#vlan 18	mcast-group 239.1.1.14
#ip pim sparse-mode	#vn-segment 10018	#member vni 10015
#ip pim rp-address 1.1.1.4	#vlan 19	mcast-group 239.1.1.15
group-list 224.0.0.0/4	#vn-segment 10019	#member vni 10016
#ip pim anycast-rp 1.1.1.4	#vlan 20	mcast-group 239.1.1.16
1.1.1.5	#vn-segment 10020	#member vni 10017
#ip pim anycast-rp 1.1.1.4	#vlan 21	mcast-group 239.1.1.17
1.1.1.6	#vn-segment 10021	#member vni 10018
#feature nv overlay	#vlan 22	mcast-group 239.1.1.18
#feature	#vn-segment 10022	#member vni 10019
vn-segment-vlan-based	#vlan 23	mcast-group 239.1.1.19
#vlan 11	#vn-segment 10023	#member vni 10020
#vn-segment 10011	#vlan 99	mcast-group 239.1.1.20

Bảng 5.10 Các lệnh cấu hình của NXOS3

NXOS3		
#member vni 10021	172.16.0.45 vrf management	#no shutdown
mcast-group 239.1.1.21	#interface e1/4-5	#interface po2
#member vni 10022	#description vPC-PeerLink	#switchport mode trunk
mcast-group 239.1.1.22	#channel-group 54 mode	#vpc 2
#member vni 10023	active	#no shutdown
mcast-group 239.1.1.23	#no shutdown	#interface e1/8
#member vni 10099	#interface po54	#channel-group 3 mode
mcast-group 239.1.1.99	#description vPC-PeerLink	active
<hr/>		
8. Cấu hình vPC	#switchport	#no shutdown
#feature vpc	#switchport mode trunk	#interface po3
#feature lacp	#vpc peer-link	#switchport mode trunk
#interface mgmt0	#spanning-tree port type	#vpc 3
#ip address 172.16.0.45/30	network	#no shutdown
#no shutdown	#no shutdown	#interface e1/9
#vpc domain 2	#interface e1/6	#channel-group 4 mode
#peer-switch	#channel-group 1 mode	active
#peer-gateway	active	#no shutdown
#role priority 10	#no shutdown	#interface po4
#graceful consistency-check	#interface po1	#switchport mode trunk
#auto-recover	#switchport mode trunk	#vpc 4
#ip arp synchronize	#vpc 1	#no shutdown
#ipv6 nd synchronize	#no shutdown	#interface e1/10
#peer-keepalive destination	#interface e1/7	#channel-group 5 mode
172.16.0.46 source	#channel-group 2 mode	active
	active	#no shutdown

Bảng 5.10 Các lệnh cấu hình của NXOS3

NXOS3		
#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 12	#interface vlan 17	#interface vlan 22
#hsrp 12	#hsrp 17	#hsrp 22
#ip 172.16.12.3	#ip 172.16.17.3	#ip 172.16.22.3
#preempt	#preempt	#preempt
#priority 200	#priority 200	#priority 200
#interface vlan 13	#interface vlan 18	#interface vlan 23
#hsrp 13	#hsrp 18	#hsrp 23
#ip 172.16.13.3	#ip 172.16.18.3	#ip 172.16.23.3
#preempt	#preempt	#preempt
#priority 200	#priority 200	#priority 200
#interface vlan 14	#interface vlan 19	#interface vlan 99
#hsrp 14	#hsrp 19	#hsrp 99
#ip 172.16.14.3	#ip 172.16.19.3	#ip 172.16.99.3

Bảng 5.10 Các lệnh cấu hình của NXOS3

NXOS3		
#preempt	#interface vlan 14	
#priority 200	#ip dhcp relay address	#interface vlan 21
	172.16.99.5 use-vrf default	#ip dhcp relay address
10. Cấu hình DHCP Relay	#interface vlan 15	172.16.99.5 use-vrf default
#feature dhcp	#ip dhcp relay address	#interface vlan 22
#service dhcp	172.16.99.5 use-vrf default	#ip dhcp relay address
#ip dhcp relay	#interface vlan 16	172.16.99.5 use-vrf default
#ip dhcp relay information option	#ip dhcp relay address	#interface vlan 23
#ip dhcp relay information option vpn	172.16.99.5 use-vrf default	#ip dhcp relay address
#ipv6 dhcp relay	#interface vlan 17	172.16.99.5 use-vrf default
#interface vlan 11	#ip dhcp relay address	
#ip dhcp relay address	172.16.99.5 use-vrf default	11. Cấu hình Telnet/SSH
172.16.99.5 use-vrf default	#interface vlan 18	#feature telnet
#interface vlan 12	#ip dhcp relay address	#telnet server enable
#ip dhcp relay address	172.16.99.5 use-vrf default	#feature ssh
172.16.99.5 use-vrf default	#interface vlan 19	#ssh server enable
#interface vlan 13	#ip dhcp relay address	#username adminHO
#ip dhcp relay address	172.16.99.5 use-vrf default	password AdminHO@123
172.16.99.5 use-vrf default	#interface vlan 20	#username adminHO role
	#ip dhcp relay address	network-admin
	172.16.99.5 use-vrf default	

Bảng 5.11 Các lệnh cấu hình của NXOS4

NXOS4		
1. Cấu hình cơ bản	#no shutdown #interface mgmt0 #ip address 172.16.0.46 255.255.255.252 #no shutdown #interface loopback0 #ip address 1.1.1.6/32 #ip address 1.1.1.4/32 secondary	#ip ospf network point-to-point #ip router ospf 1 area 0 #interface e1/3 #no switchport #ip ospf network point-to-point #ip router ospf 1 area 0 #interface loopback0
2. Cấu hình địa chỉ IP	#interface e1/1 #no switchport #ip address 172.16.0.66 255.255.255.252 #no shutdown #interface e1/2 #no switchport #ip address 172.16.0.70 255.255.255.252 #no shutdown #interface e1/3 #no switchport #ip address 172.16.0.58 255.255.255.252	#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 11.0.0.8 #interface e1/1 #no switchport #ip ospf network point-to-point #ip router ospf 1 area 0 #interface e1/2 #no switchport	#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 #vn-segment 10019
#ip router ospf 1 area 0	#ip pim anycast-rp 1.1.1.4 1.1.1.5	#vlan 20 #vn-segment 10020
#mtu 9216		
#no shutdown	#ip pim anycast-rp 1.1.1.4 1.1.1.6	#vlan 21 #vn-segment 10021
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 172.16.0.46/30 #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 172.16.0.45 source 172.16.0.46 vrf management #interface e1/4-5 #description vPC-PeerLink #channel-group 54 mode active #no shutdown #no shutdown #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 #switchport #switchport mode trunk	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 mode trunk #vpc peer-link #spanning-tree port type	#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 24 #ip dhcp relay address	
172.16.99.5 use-vrf default	172.16.99.5 use-vrf default #interface vlan 25 #ip dhcp relay address	
#interface vlan 12	172.16.99.5 use-vrf default #interface vlan 26 #ip dhcp relay address	
#ip dhcp relay address	172.16.99.5 use-vrf default #interface vlan 27 #ip dhcp relay address	
172.16.99.5 use-vrf default	172.16.99.5 use-vrf default #interface vlan 28 #ip dhcp relay address	
#interface vlan 13	172.16.99.5 use-vrf default #interface vlan 29 #ip dhcp relay address	
#ip dhcp relay address	172.16.99.5 use-vrf default #interface vlan 30 #ip dhcp relay address	
172.16.99.5 use-vrf default	172.16.99.5 use-vrf default #interface vlan 31 #ip dhcp relay address	
#interface vlan 14	172.16.99.5 use-vrf default #interface vlan 32 #ip dhcp relay address	
#ip dhcp relay address	172.16.99.5 use-vrf default #interface vlan 33 #ip dhcp relay address	
172.16.99.5 use-vrf default	172.16.99.5 use-vrf default #interface vlan 34 #ip dhcp relay address	
#interface vlan 15	172.16.99.5 use-vrf default #interface vlan 35 #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	encapsulation dot1q #switchport mode trunk #channel-protocol lacp #channel-group 1 mode active #no shutdown	#switchport access vlan 14 #no shutdown
2. Cấu hình VLAN	#vlan 11 #name HanhChinh #vlan 12 #name DaoTao #vlan 13 #name TuyenSinh #vlan 14 #name Lab	4. Cấu hình Access mode #interface Ethernet0/2 #switchport mode access #switchport access vlan 11 #no shutdown #interface Ethernet0/3 #switchport mode access #switchport access vlan 12 #no shutdown
3. Cấu hình Port-channel	#interface Port-channel1 #switchport trunk encapsulation dot1q #switchport mode trunk #no shutdown #interface range e0/0-1 #switchport trunk	6. Cấu hình chế độ Port-security #interface range e0/2-3, e1/0-3 #switchport port-security #switchport port-security maximum 1 #switchport port-security violation shutdown
	Ethernet1/1-3	7. Thiết lập cơ chế AAA
	#switchport mode access	

#aaa new-model #aaa authentication login default local #aaa authorization exec default local #aaa accounting exec	default start-stop local 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 5.13 Các lệnh cấu hình của Switch Sw_B

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

#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	#username adminHO secret AdminHO@123 #ip ssh ver 2 #line vty 0 4 #login local #transport input SSH	#aaa new-model #aaa authentication login default local #aaa authorization exec default local #aaa accounting exec default start-stop local
5. Cấu hình Telnet/SSH #crypto key generate rsa generatal-keys 1024	6. Cấu hình chế độ Port-security #interface range e0/2-3, e1/0-3, e2/0-1 #switchport port-security #switchport port-security maximum 1 #switchport port-security violation shutdown	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@
	7. Thiết lập cơ chế AAA	

Bảng 5.14 Các lệnh cấu hình của Switch Sw_C

Sw_C		
1. Cấu hình cơ bản #hostname Sw_C #ip domain-name cmu.edu	#no ip domain-lookup	#vlan 20 #name QTKD
	2. Cấu hình VLAN	#vlan 21

#name CNTT	#no shutdown	#line vty 0 4
#vlan 22	#interface Ethernet0/3	#login local
#name ThuVien	#switchport mode access	#transport input SSH
#vlan 23	#switchport access vlan 21	
#name PhongHocC	#no shutdown	6. Cấu hình chế độ Port-security
	#interface Ethernet1/0	#interface range
	#switchport mode access	e0/2-3, e1/0-3, e2/0
3. Cấu hình Port-channel	#switchport access vlan 22	#switchport port-security
#interface Port-channel3	#no shutdown	#switchport port-security
#switchport trunk	#interface range	maximum 1
encapsulation dot1q	Ethernet1/1-3	#switchport port-security
#switchport mode trunk	#switchport mode access	violation shutdown
#no shutdown	#switchport access vlan 23	
#interface range e0/0-1	#no shutdown	7. Thiết lập cơ chế AAA
#switchport trunk	#interface Etherne2/0	#aaa new-model
encapsulation dot1q	#switchport mode access	#aaa authentication login
#switchport mode trunk	#switchport access vlan 23	default local
#channel-protocol lacp	#no shutdown	#aaa authorization exec
#channel-group 3 mode		default local
active		#aaa accounting exec default
#no shutdown	5. Cấu hình Telnet/SSH	start-stop local
	#crypto key generate rsa	
	generatal-keys 1024	
4. Cấu hình Access mode	#username adminHO	8. Cấu hình mật khẩu cho các quyền truy cập
#interface Ethernet0/2	secret AdminHO@123	
#switchport mode access	#ip ssh ver 2	
#switchport access vlan 20		

#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	#switchport mode trunk #channel-protocol lacp #channel-group 4 mode active #no shutdown	#crypto key generate rsa generatal-keys 1024 #username adminHO secret AdminHO@123 #ip ssh ver 2 #line vty 0 4
2. Cấu hình VLAN #vlan 99 #name KyThuat	#interface range Ethernet0/2-3	#login local #transport input SSH
3. Cấu hình Port-channel #interface Port-channel4 #switchport trunk encapsulation dot1q #switchport mode trunk #no shutdown #interface range e0/0-1 #switchport trunk encapsulation dot1q	#switchport mode access #switchport access vlan 99 #no shutdown #interface Etherne1/0 #switchport mode access #switchport access vlan 99 #no shutdown	6. 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
	5. Cấu hình Telnet/SSH	

7. Cấu hình mật khẩu cho các quyền truy cập	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	encapsulation dot1q #switchport mode trunk #channel-protocol lacp #channel-group 5 mode active #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
2. Cấu hình VLAN #vlan 99 #name KyThuat	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	6. 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
3. Cấu hình Port-channel #interface Port-channel5 #switchport trunk encapsulation dot1q #switchport mode trunk #no shutdown #interface range e0/0-1 #switchport trunk		

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@
--	---	---

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	#no shutdown	#ip route 0.0.0.0 0.0.0.0 14.16.242.1
2. Cấu hình địa chỉ IP #interface s4/0 #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 #ip ospf 1 area 0	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	2. Cấu hình địa chỉ IP #interface e0/0

#ip address 172.17.0.06 255.255.255.252 #no shutdown	#vlan 25 #name ThuVien_CT #vlan 26 #name PhongHocD	vlan all #no shutdown
3. Cấu hình định tuyến OSPF	5. Cấu hình Trunking mode	6. Cấu hình Access mode
#router ospf 1 #router-id 12.0.0.2 #interface e0/0 #ip ospf 1 area 0	#interface e0/1 #switchport #switchport mode trunk #switchport trunk allow vlan all #no shutdown	#interface e0/1 #switchport mode access #switchport access vlan 109 #no shutdown
4. Tạo VLAN	#interface e0/2 #switchport #switchport mode trunk #switchport trunk allow	#interface e0/2 #switchport mode access #switchport access vlan 24
#vlan 109 #name KyThuat_CT #vlan 24 #name VPK	#interface e0/2 #switchport #switchport mode trunk #switchport trunk allow	#no shutdown #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	2. Tạo VLAN	3. Cấu hình Trunking mode
#configure terminal #hostname Sw_DC1 #ip domain-name cmu.edu #no ip domain-lookup	#vlan 109 #name KyThuat_CT #vlan 24 #name VPK	#interface e1/0 #switchport #switchport mode trunk #switchport trunk allow

vlan all #no shutdown	#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	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
4. 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 #no shutdown	6. Cấu hình chế độ Port-security #interface range e0/1-3 #switchport #switchport port-security #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@
5. Cấu hình Telnet/SSH		

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	2. Tạo VLAN #vlan 25

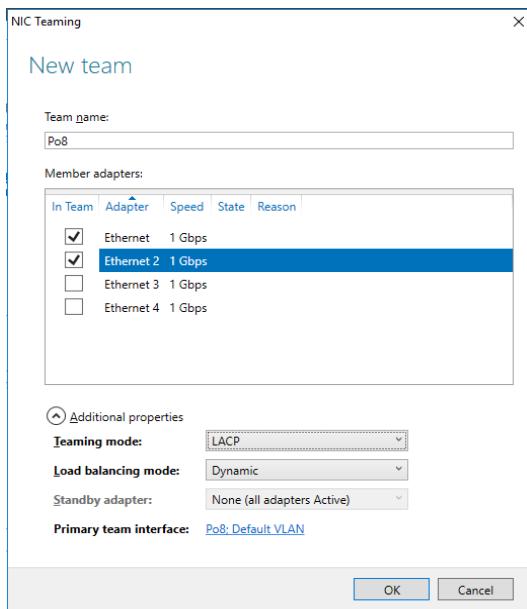
#name ThuVien_CT #vlan 26 #name PhongHocD	#no shutdown #interface e1/1 #switchport mode access #switchport access vlan 26	#switchport port-security #switchport port-security maximum 1 #switchport port-security violation shutdown
3. Cấu hình Trunking mode #interface e1/0 #switchport #switchport mode trunk #switchport trunk allow vlan all #no shutdown	#no shutdown #interface e1/2 #switchport mode access #switchport access vlan 26 #no shutdown	7. Thiết lập cơ chế AAA #aaa new-model #aaa authentication login default local #aaa authorization exec default local
4. Cấu hình Access mode #interface e0/1 #switchport mode access #switchport access vlan 25 #no shutdown #interface e0/2 #switchport mode access #switchport access vlan 26 #no shutdown #interface e1/0 #switchport mode access #switchport access vlan 26	#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	#aaa accounting exec default start-stop local 8. Cấu hình mật khẩu cho các quyền truy cập #enable secret AdminBO@123 #line console 0 6. Cấu hình chế độ Port-security #interface range e0/1-2, e1/0-2
		#password AdminBO@123 #login #line vty 0 4 #password AdminBO@

5.2 Cấu hình các server

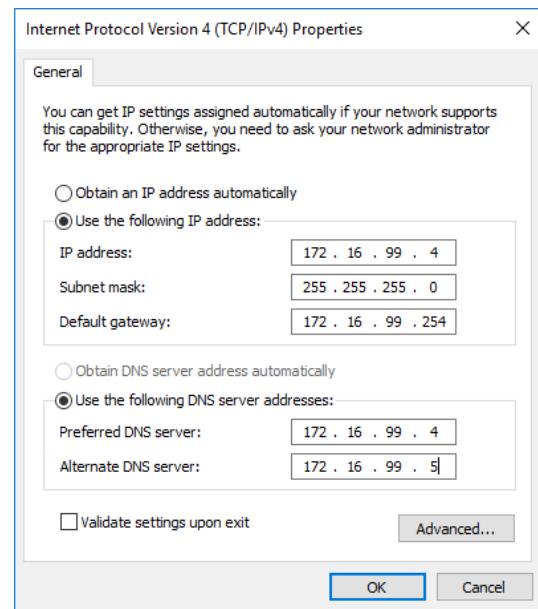
5.2.1 Cấu hình server RADIUS

a) Cấu hình NIC Teaming

- Chọn Local Server -> Nic Teaming Disabled.
- Chọn New Team.
- Đặt Team name là Po8 -> Chọn Ethernet và Ethernet2 -> Chọn Teaming mode là LACP -> Chọn Apply.
- Cấu hình địa chỉ IPv4 cho NIC Teaming.



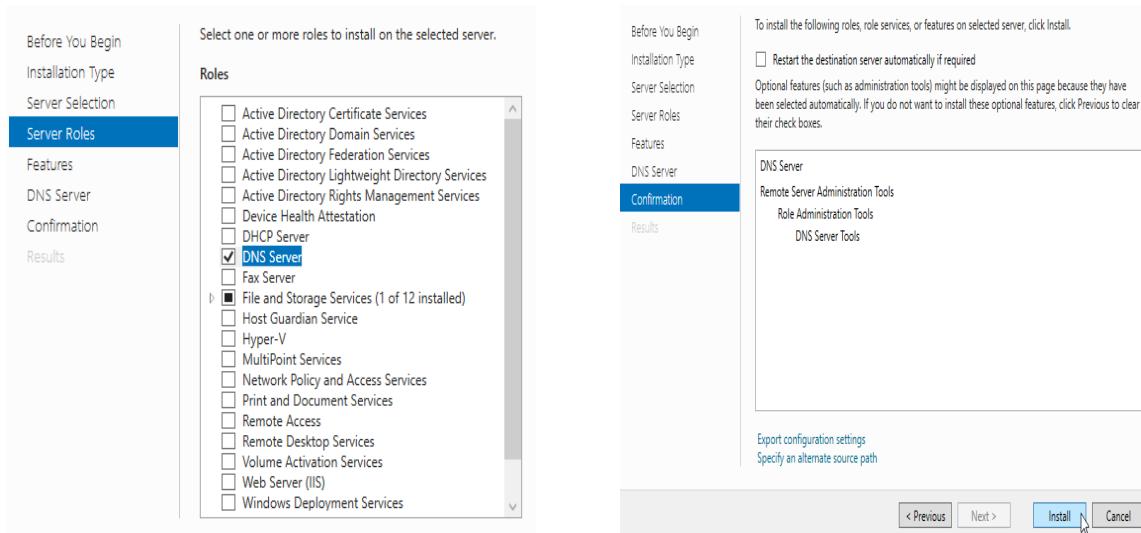
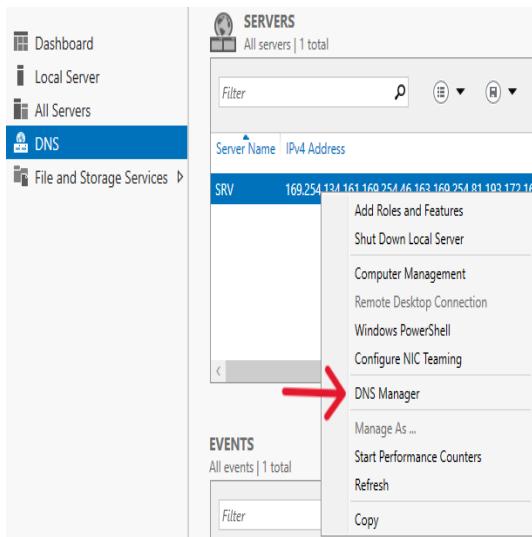
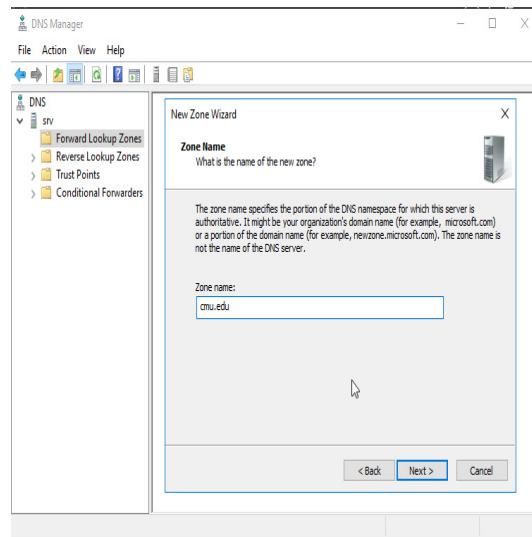
Hình 5.1 Cấu hình NIC Teaming



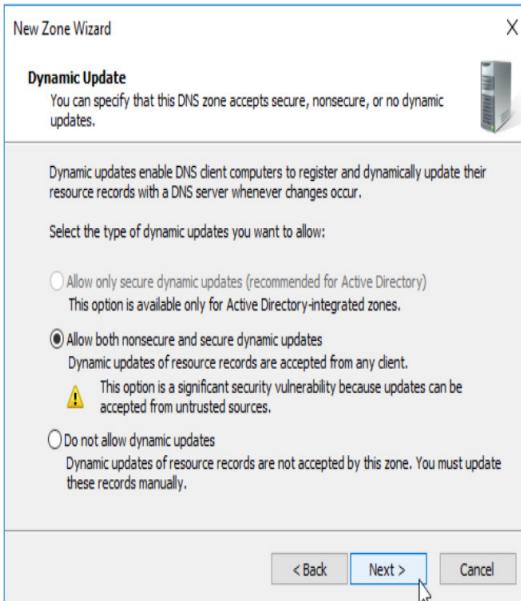
Hình 5.2 Điện địa chỉ IPv4 và DNS

b) Cấu hình dịch vụ DNS Server

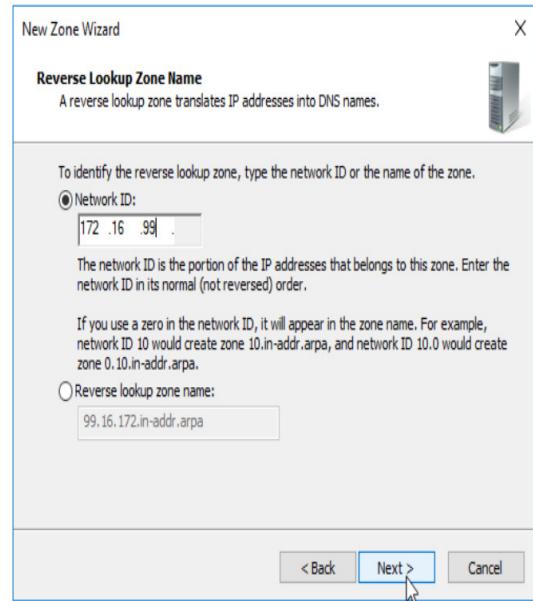
- Chọn Add Roles and Features để thêm dịch vụ server
- Chọn Server Roles là DNS Server.
- Chọn Install để thêm dịch vụ DNS Server.

**Hình 5.3 Chọn Server Roles****Hình 5.5 Chọn DNS Manager****Hình 5.6 Zone Name là cmu.edu**

- Cấu hình Forward Lookup Zones: chọn Allow both nonsecure and secure dynamic updates.
- Cấu hình Reverse Lookup Zones: nhập Network ID -> Chọn Allow both nonsecure and secure dynamic updates.



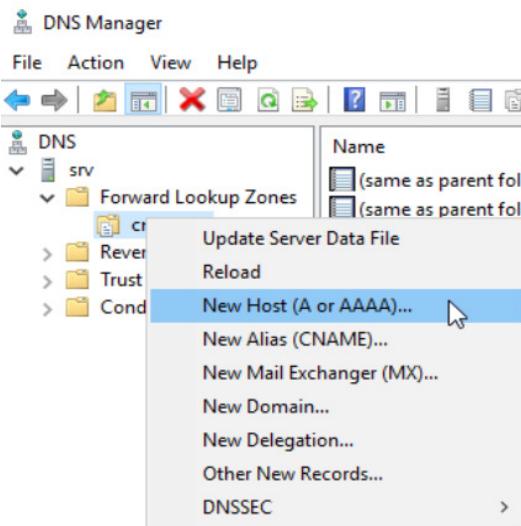
Hình 5.7 Forward Lookup Zones



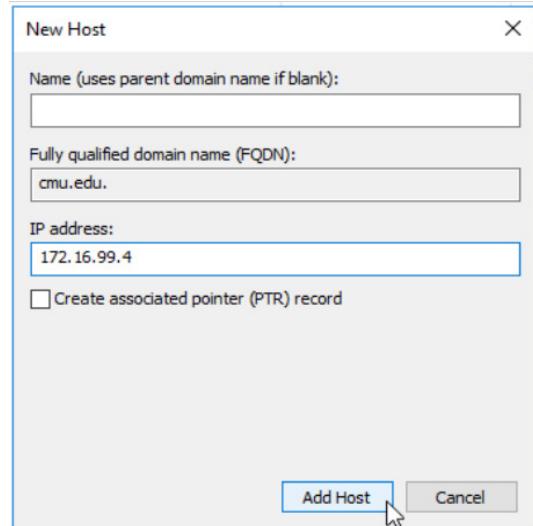
Hình 5.8 Reverse Lookup Zones

- Tạo bản ghi A cho domain của Web Server:

Tạo New Host -> Nhập địa chỉ IP -> Chọn Add Host.

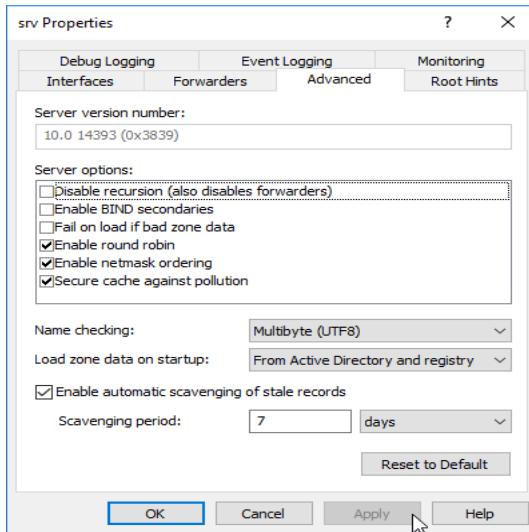


Hình 5.9 Chọn New Host

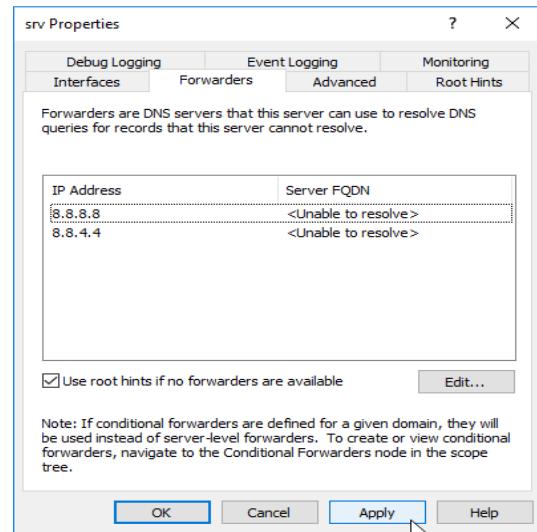


Hình 5.10 Chọn Add Host

- Cấu hình DNS recursive để phân giải tên miền các địa chỉ ở bên ngoài mạng LAN: Nhấp chuột phải vào srv -> Chọn Properties.



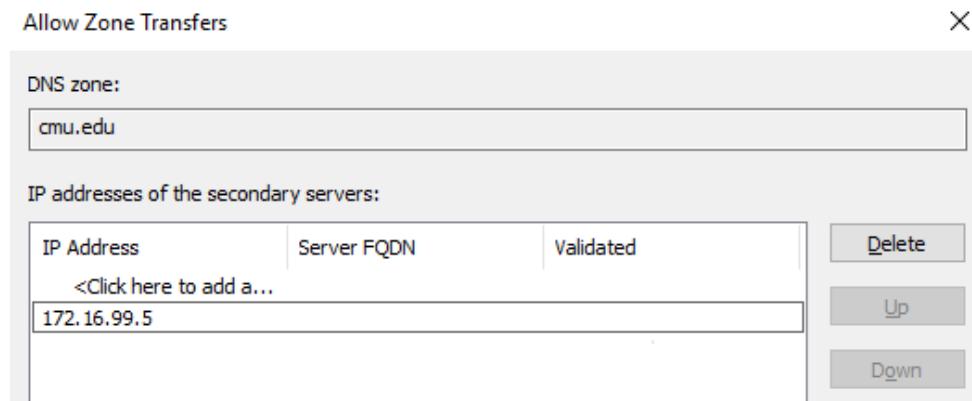
Hình 5.11 Cấu hình Advanced



Hình 5.12 Cấu hình Forwarders

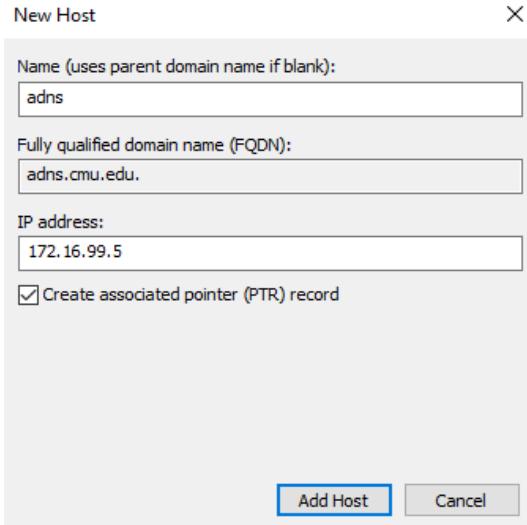
c) Cấu hình Alternative DNS

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

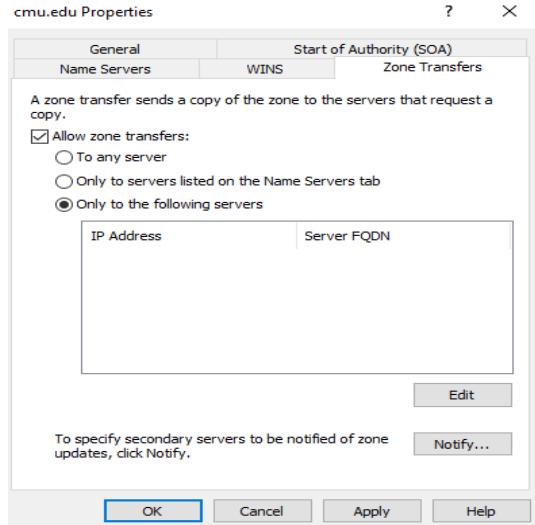


Hình 5.15 Allow Zone Transfers

- Nhập tên và địa chỉ IP -> Chọn Add Host.



Hình 5.13 Nhập tên và địa chỉ

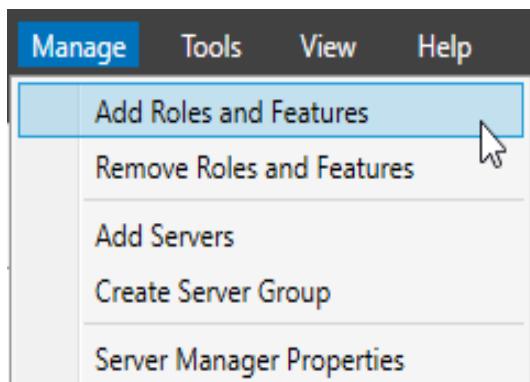


Hình 5.14 Chọn Zone Transfers

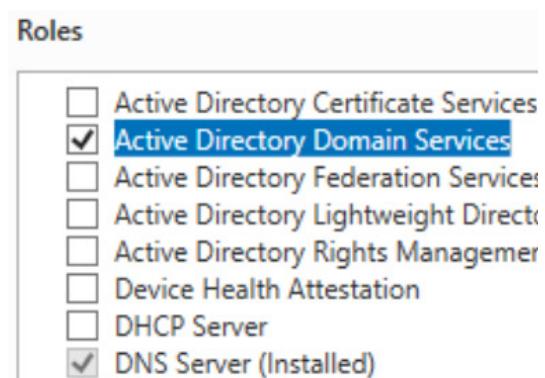
- Chọn Properties của cmu.edu -> Chọn Allow zone transfers (Only to the following server) -> Chọn Edit -> Thêm địa chỉ IP.

d) Cấu hình Active Directory Domain Service

- Chọn Manage -> Chọn Add Role and Features.
- Chọn server role là Active Directory Domain Service.



Hình 5.16 Add Role and Features



Hình 5.17 Chọn AD DS

- Tại Deployment Configuration, nhập Root domain name là cmu.com.
- Tại Domain Controller Options, nhập password là Admin1@123.

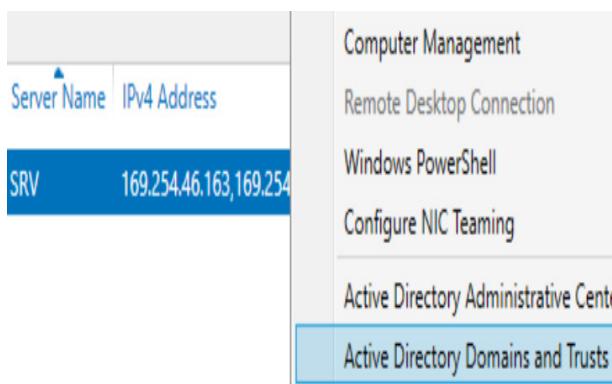
The screenshot shows the 'Deployment Configuration' wizard. The 'Domain Controller Options' step is active. In the center, it says 'Select the deployment operation' and lists three options: 'Add a domain controller to an existing domain', 'Add a new domain to an existing forest', and 'Add a new forest'. The third option is selected. Below this, it says 'Specify the domain information for this operation' and shows the 'Root domain name' field containing 'cmu.com'. On the right, there's a sidebar titled 'Domain Controller Options' with sections for 'Deployment Configuration' (selected), 'DNS Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. Under 'Deployment Configuration', it shows 'Forest functional level: Windows Server Technical Preview' and 'Domain functional level: Windows Server Technical Preview'. It also lists 'Specify domain controller capabilities' with checkboxes for 'Domain Name System (DNS) server' (checked), 'Global Catalog (GC)' (checked), and 'Read only domain controller (RODC)' (unchecked). Below that, it asks for 'Type the Directory Services Restore Mode (DSRM) password' and shows two password fields, both containing '*****'. A link 'More about domain controller options' is at the bottom.

Hình 5.18 Nhập Root domain name

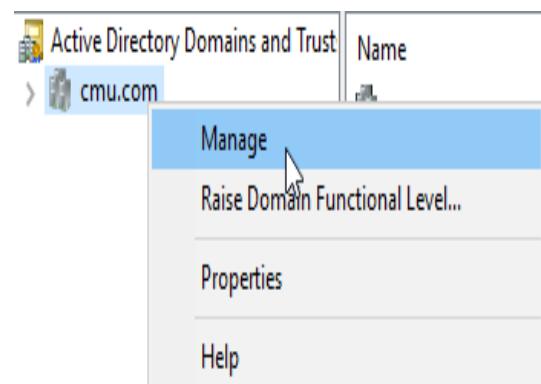
Hình 5.19 Nhập password

- Cấu hình quản lý Active Directory Domains and Trusts:

- Chọn Active Directory Domains and Trusts
- Nhấp chuột phải vào cmu.com, chọn Manage.

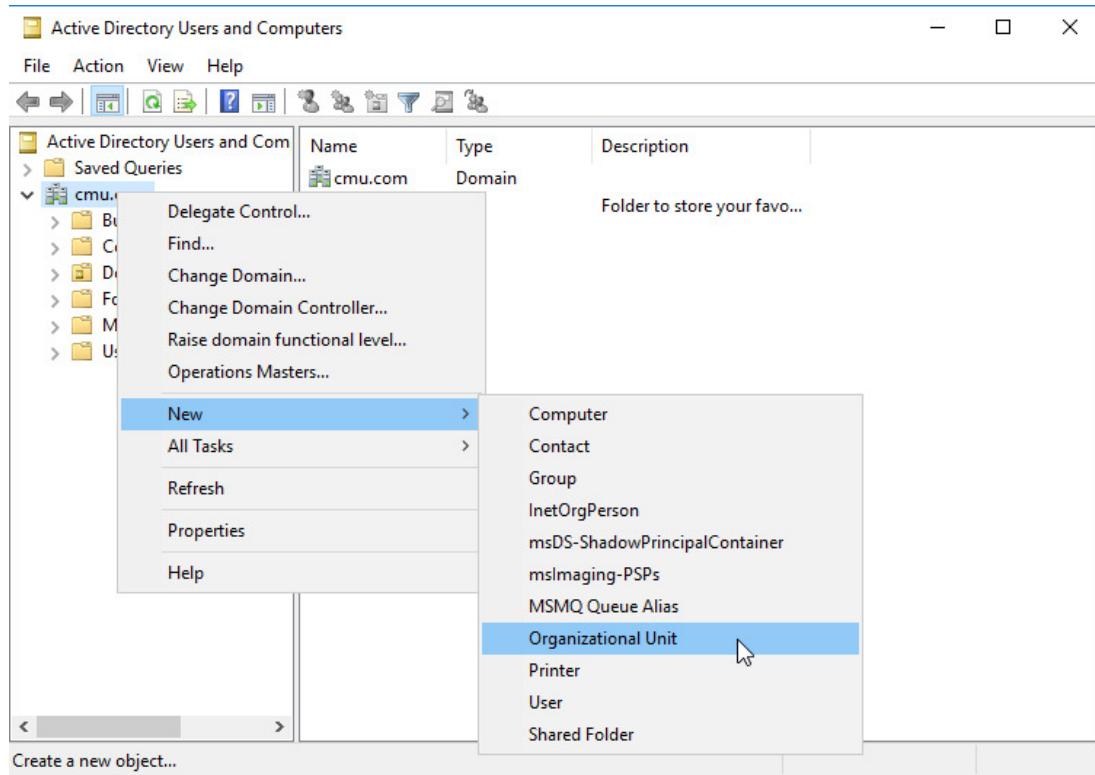


Hình 5.20 Chọn



Hình 5.21 Chọn Manage

- Tạo 2 Organizational Unit cho Head Office và Branch Office:



Hình 5.22 Chọn Organizational Unit

New Object - Organizational Unit

📁
Create in: cmu.com/

Name:

Protect container from accidental deletion

Hình 5.23 Nhập tên là HO

New Object - Organizational Unit

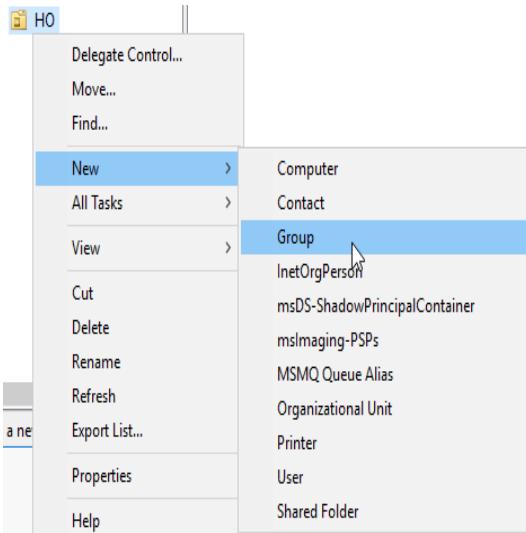
📁
Create in: cmu.com/

Name:

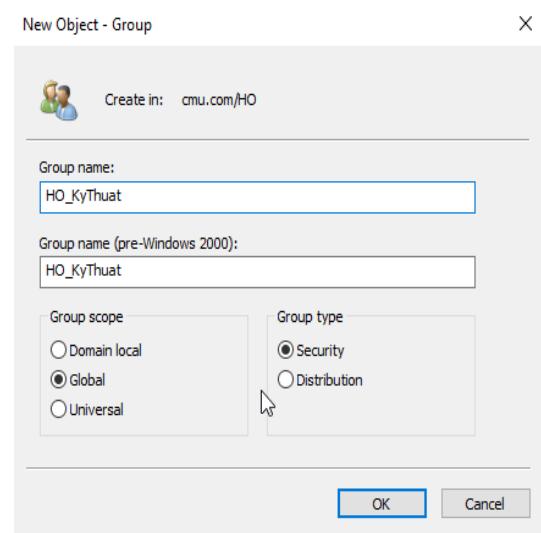
Protect container from accidental deletion

Hình 5.24 Nhập tên là BO

- Tạo các Group cho các phòng ban:



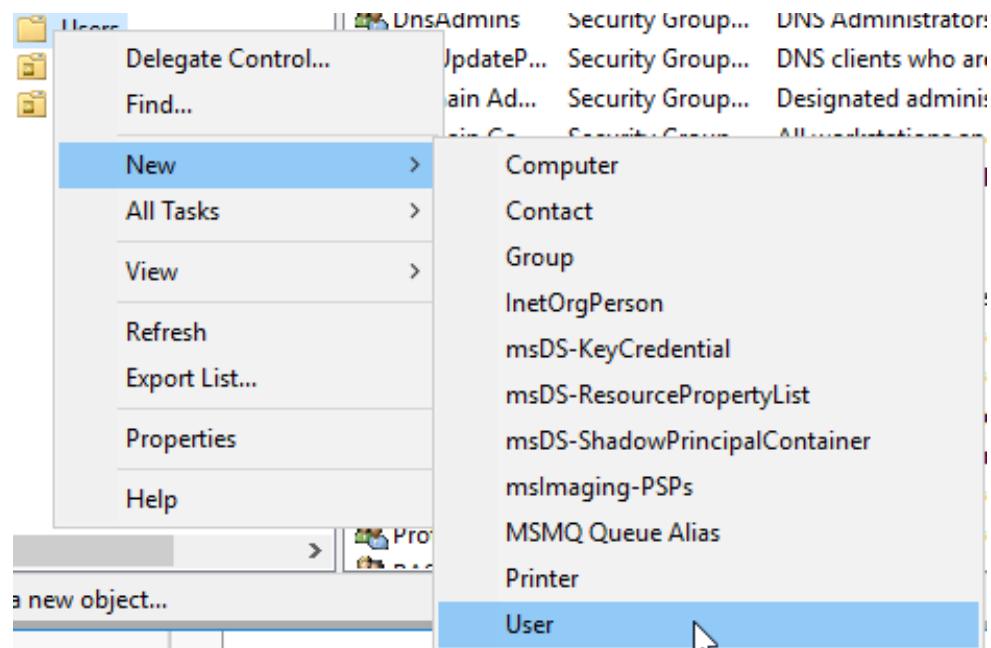
Hình 5.25 Tạo Group



Hình 5.26 Nhập tên phòng ban

Làm tương tự với các phòng ban khác.

- Tạo các user và thêm user các user đó vào các phòng ban:



Hình 5.27 Thêm User

Create in: cmu.com/Users

First name: Duy

Last name: Nguyen

Full name: Duy Nguyen Nha Thao

User logon name: duynt @cmu.com

User logon name (pre-Windows 2000): CMU\ duynt

Hình 5.28 Tạo User 1

Create in: cmu.com/Users

First name: Suong

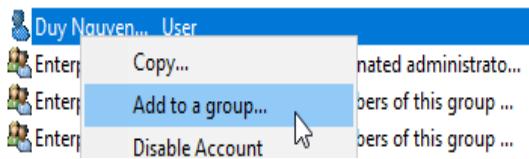
Last name: Nguyen Thi Diem

Full name: Suong Nguyen Thi Diem

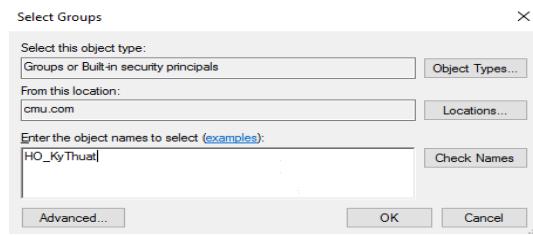
User logon name: suongntd @cmu.com

User logon name (pre-Windows 2000): CMU\ suongntd

Hình 5.29 Tạo User 2

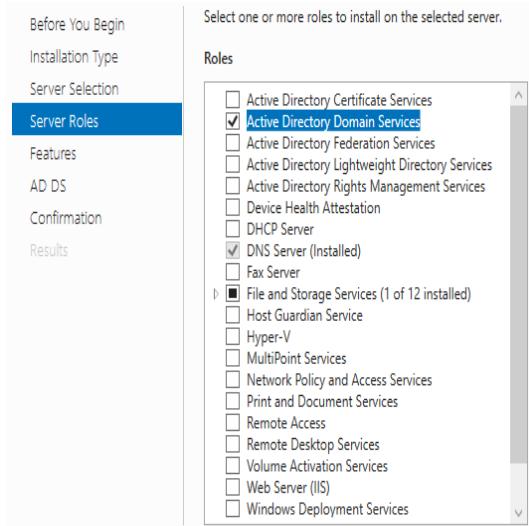


Hình 5.30 Add User vào Group

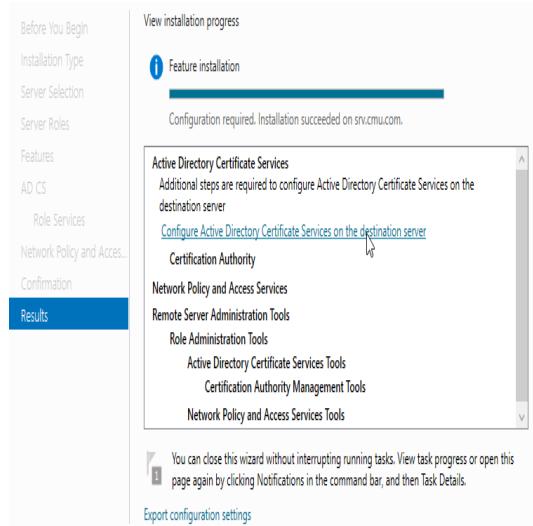


Hình 5.31 Chọn Groups

e) Cấu hình xác thực RADIUS

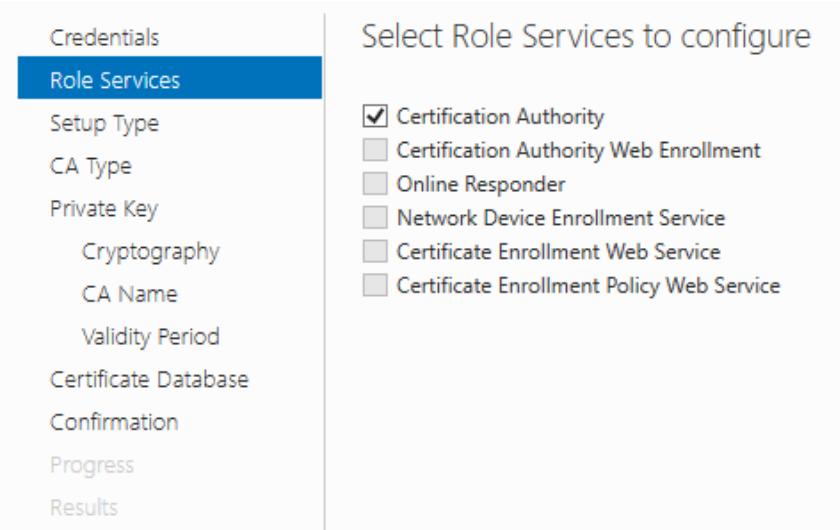


Hình 5.32 Chọn Server Roles



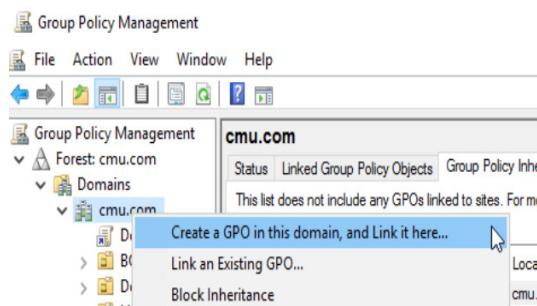
Hình 5.33 Cấu hình

- Chọn dịch vụ Active Directory Domain Services và Network Policy and Access Service.
- Cấu hình Active Directory Certificate Services.
- Chọn Roles Services là Certification Authority.

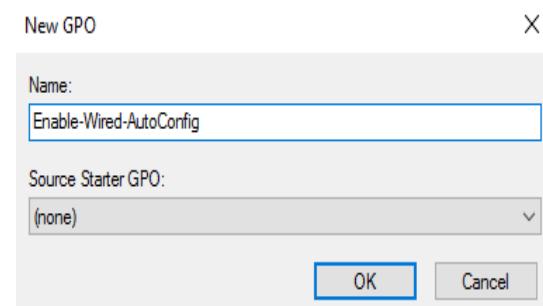


Hình 5.34 Chọn Certification Authority

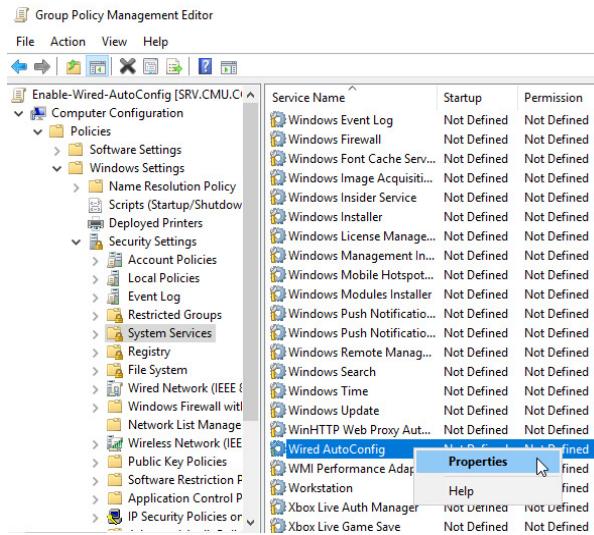
- Tạo Policy cho phép bật Wired AutoConfig Services:
 - Nhấp chuột phải vào cmu.com -> Chọn Create a GPO.
 - Tạo và cấu hình policy cho phép bật Wired AutoConfig Services.



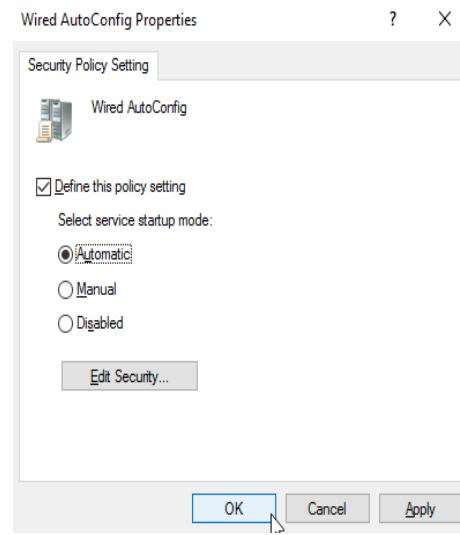
Hình 5.35 Tạo Policy



Hình 5.36 Nhập tên

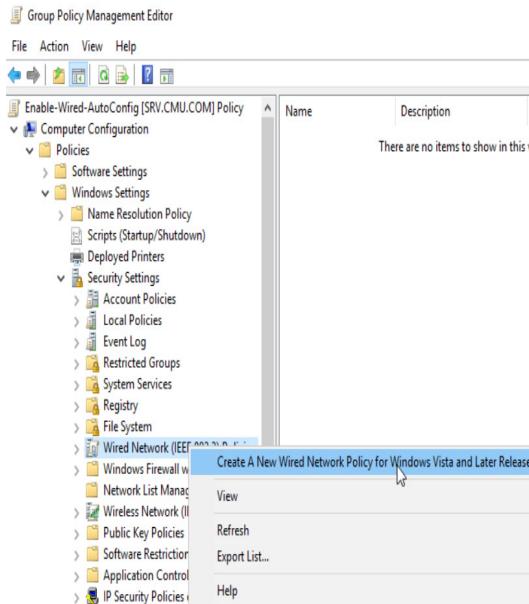


Hình 5.37 Chọn Properties

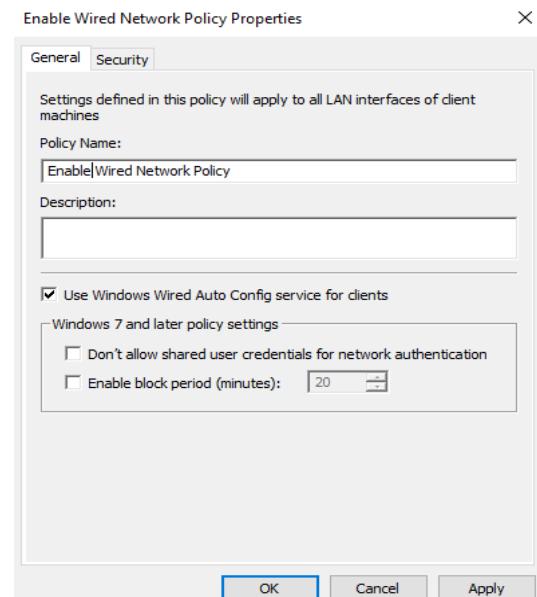


Hình 5.38 Chọn OK

- Tạo Policy cho phép bật IEEE 802.1X:

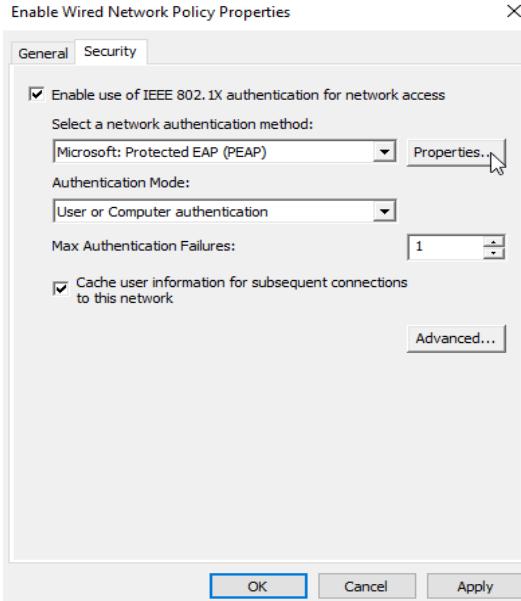


Hình 5.39 Tao Policy

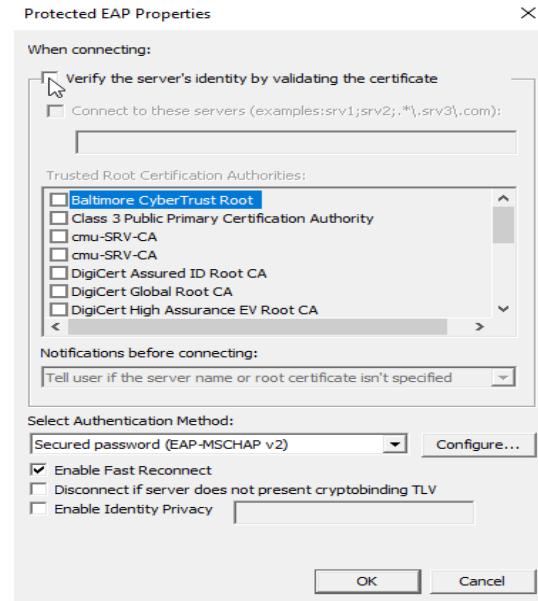


Hình 5.40 Nhập tên

- Tạo Policy -> Nhập Policy Name.
- Chọn Security -> Properties -> Bỏ chọn Verify the server's identity.

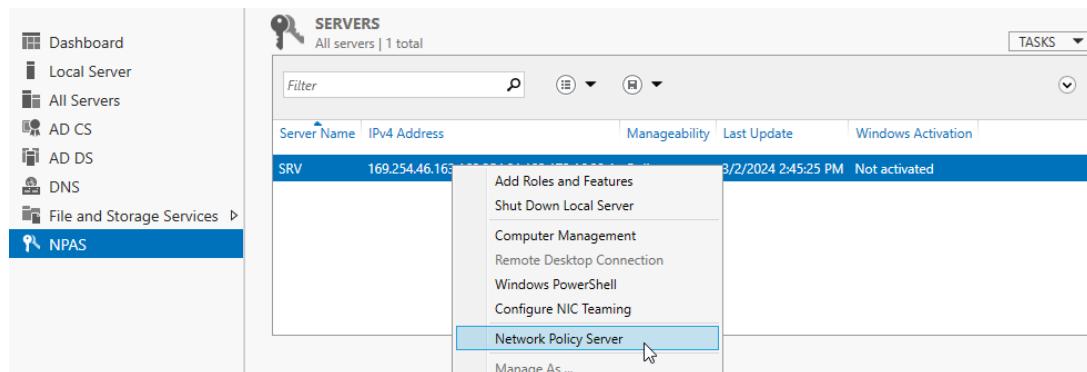


Hình 5.41 Chọn Properties



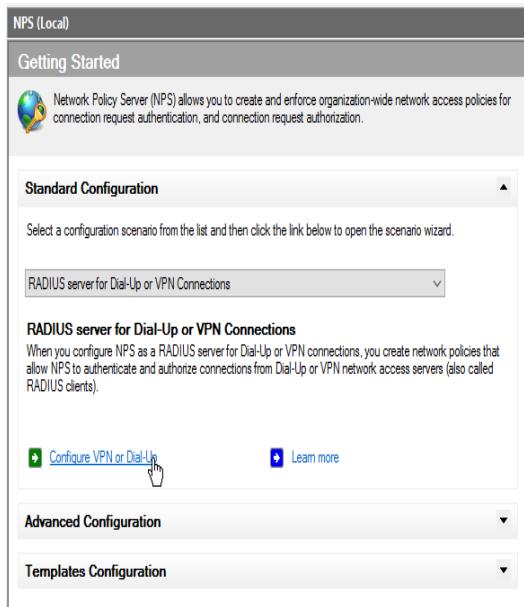
Hình 5.42 Nhấn để bỏ chọn

- Cấu hình Radius Server theo chuẩn 802.1X:

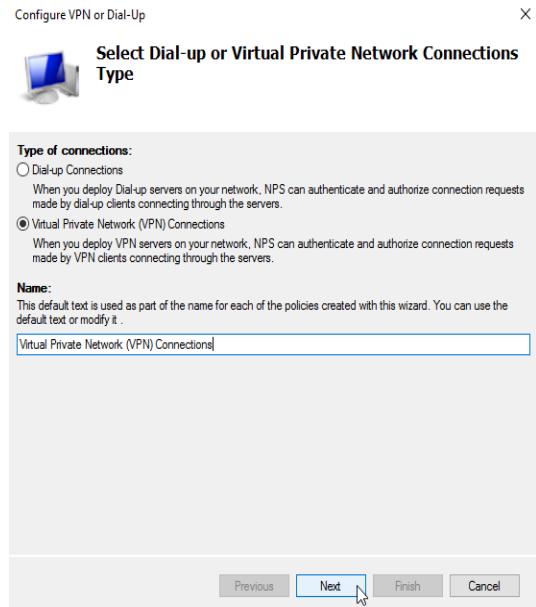


Hình 5.43 Chọn Network Policy Server

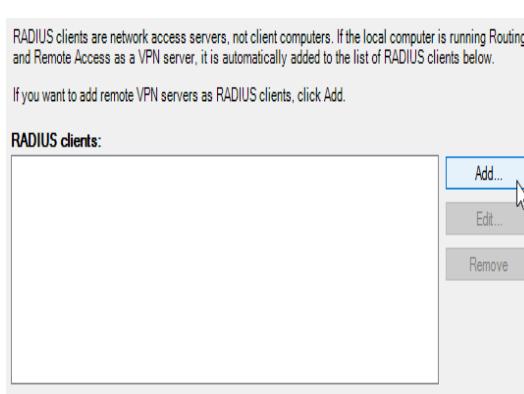
- Thêm RADIUS clients là các switch Nexus trong hệ thống mạng.
- Nhập tên của các thiết bị sao cho dễ quản lý và IP tương ứng và Shared Secret là Admin1@123:



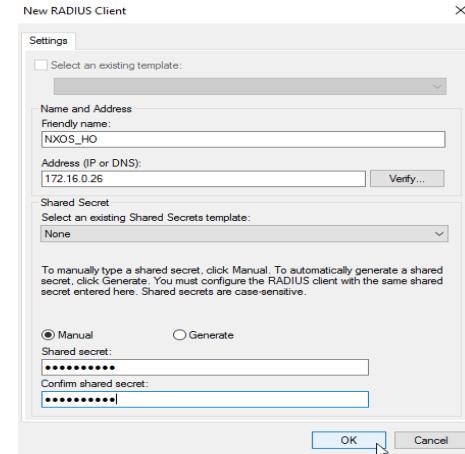
Hình 5.44 Chọn Configure VPN



Hình 5.45 Chọn VPN



Hình 5.46 Chọn Add

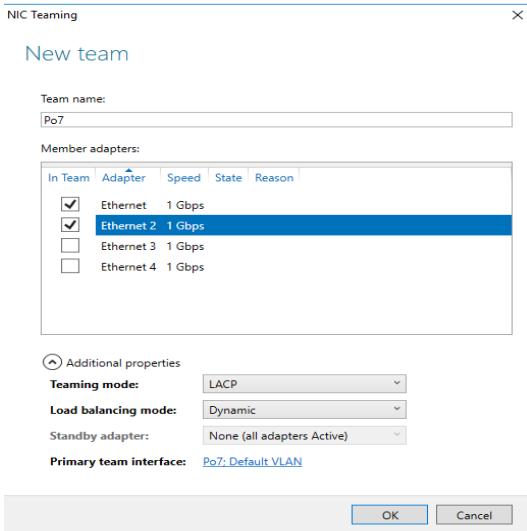


Hình 5.47 Cấu hình RADIUS client

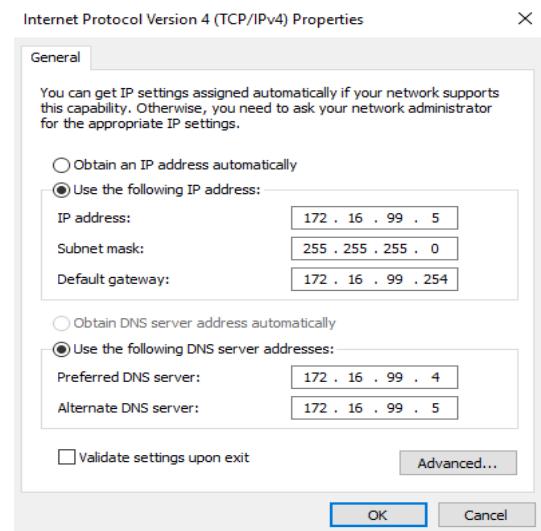
5.2.2 Cấu hình server DNS_Mail_DHCP

a) Cấu hình NIC Teaming

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



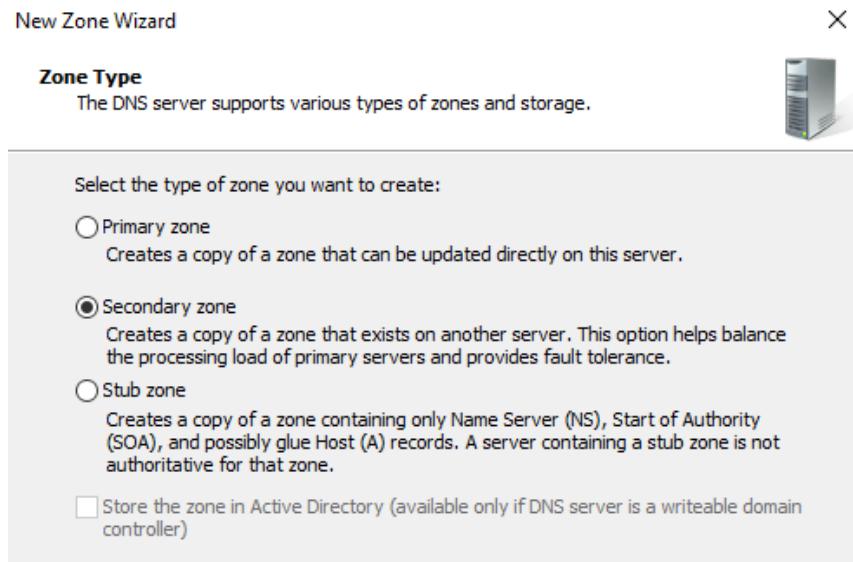
Hình 5.48 Cấu hình NIC Teaming



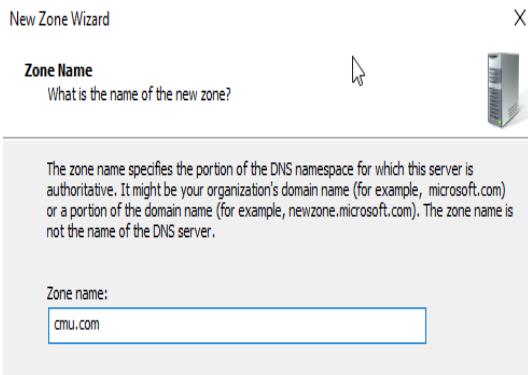
Hình 5.49 Điền địa chỉ IPv4

b) Cấu hình dịch vụ DNS Alternate Server

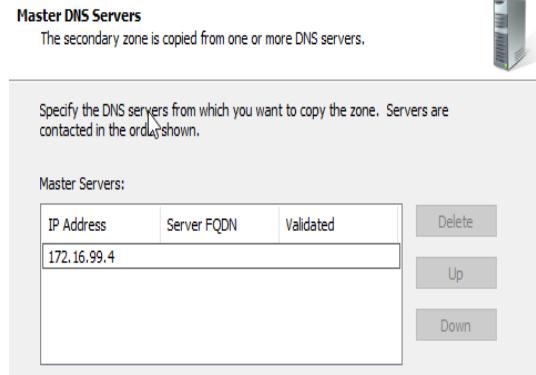
- Vào DNS Manager -> Tạo New Zone -> Chọn Zone Type là Secondary zone.
- Nhập Zone name là cmu.com và nhập địa chỉ IP của Master Servers.



Hình 5.50 Chọn Zone Type

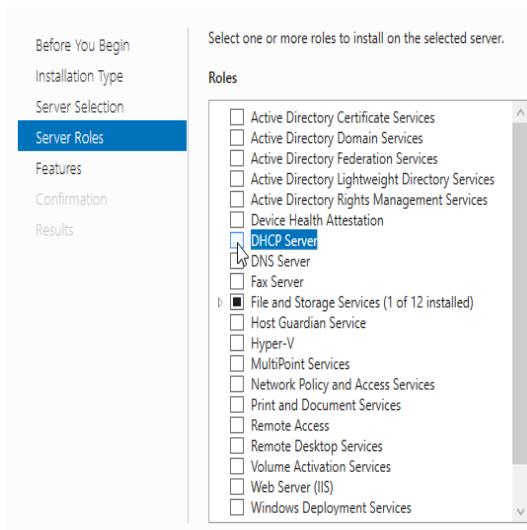


Hình 5.51 Nhập Zone Name

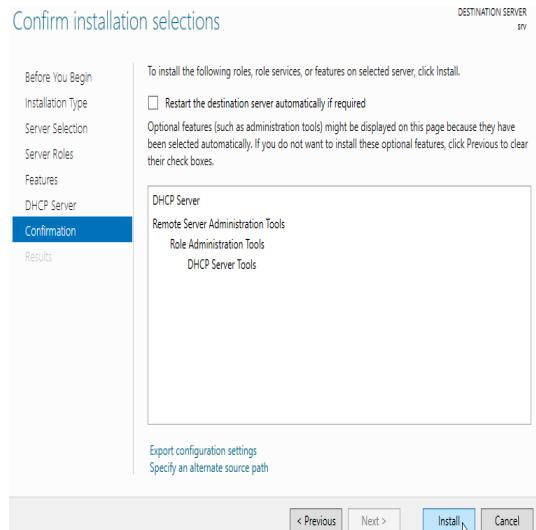


Hình 5.52 Nhập địa chỉ IP

c) Cấu hình dịch vụ DHCP Server

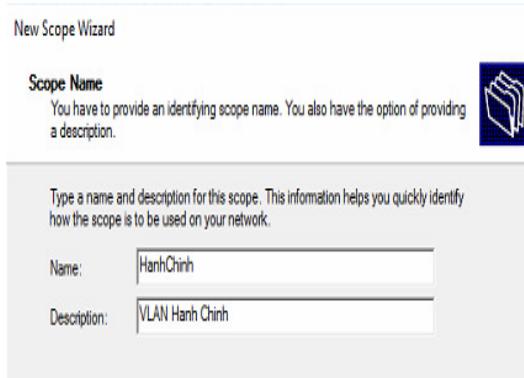


Hình 5.53 Thêm dịch vụ DHCP

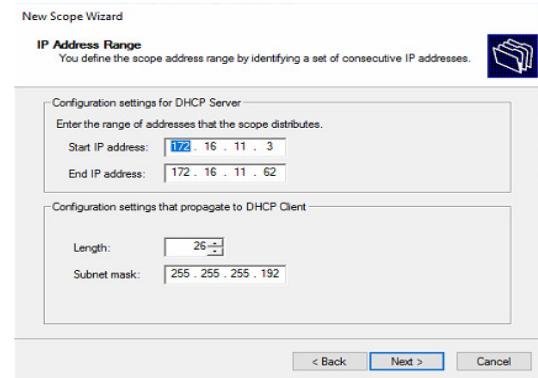


Hình 5.54 Install DHCP Server

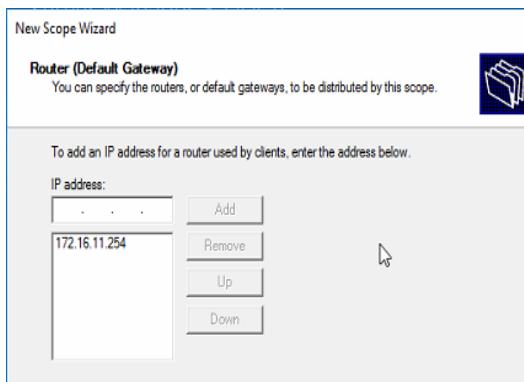
- Tạo Scope Name cho các VLAN.
- Nhập dải địa chỉ IP của VLAN.
- Nhập địa chỉ gateway.
- Nhập domain name và địa chỉ IP của DNS Server.



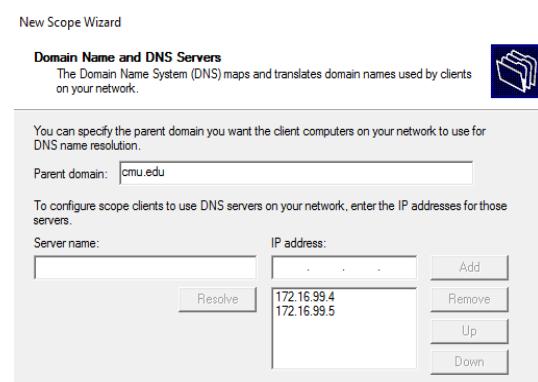
Hình 5.55 Tạo Scope Name cho VLAN



Hình 5.56 Nhập dải địa chỉ IP VLAN



Hình 5.57 Nhập địa chỉ gateway

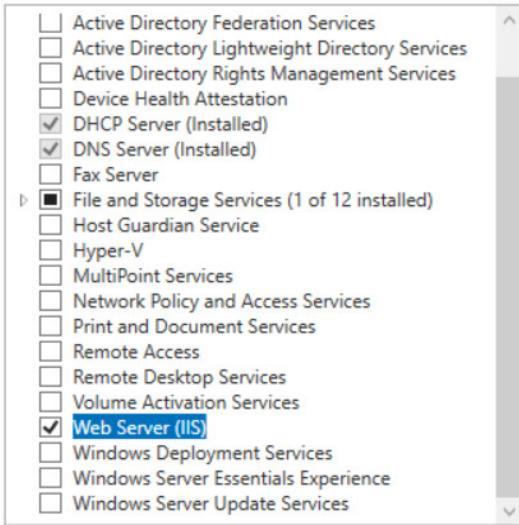


Hình 5.58 Nhập domain name, địa chỉ IP

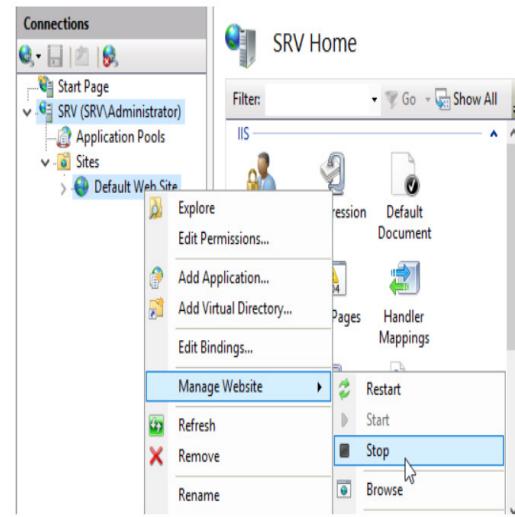
- Làm tương tự với những VLAN còn lại.

d) Cấu hình Web server

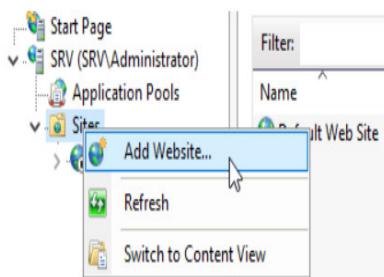
- Thêm dịch vụ IIS cho Server.
- Tắt trang web mặc định của web server.
- Thêm source Web vào các ổ đĩa của Server. Sau đó gán vào đường dẫn của website mới.



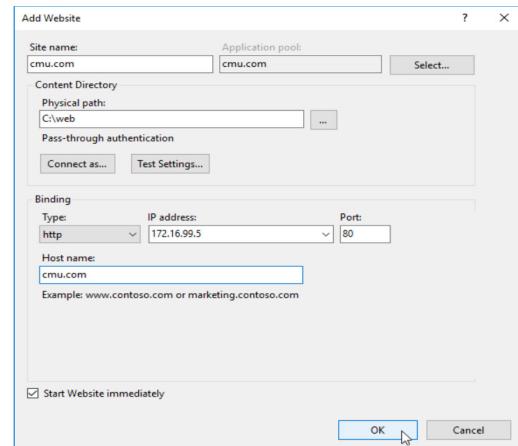
Hình 5.59 Thêm dịch vụ IIS



Hình 5.60 Tắt trang web mặc định



Hình 5.61 Chọn Add Website

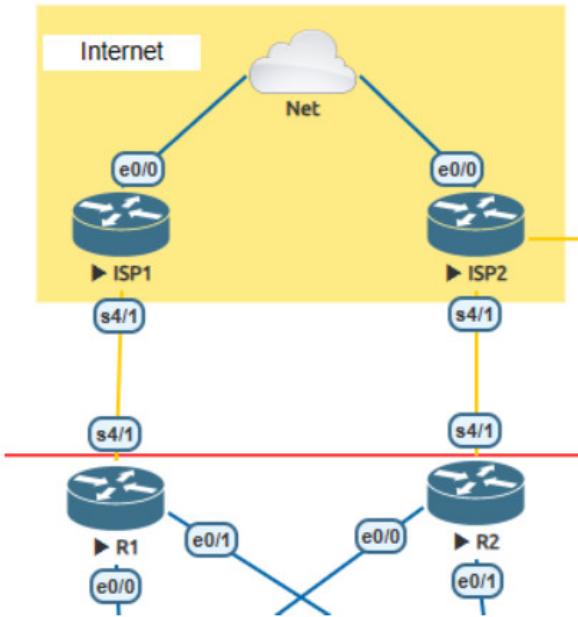


Hình 5.62 Gán các đường dẫn Website

5.3 Demo hệ thống

5.3.1 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 5.63 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 5.64 Hai Router sau khi được kết nối với ISP

5.3.2 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 5.65 Kết quả kiểm tra giao thức NAT

5.3.3 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 5.66 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.

5.3.4 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 5.67 Kiểm tra kết nối giữa các VLAN

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

5.3.5 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 5.68 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 5.69 Xem Interface NVE 1

Interface	VNI	Multicast-group	State	Mode	Type	[BD/VRF]	Flags
nvel1	10011	239.1.1.11	Up	DP	L2	[11]	
nvel1	10012	239.1.1.12	Up	DP	L2	[12]	
nvel1	10013	239.1.1.13	Up	DP	L2	[13]	
nvel1	10014	239.1.1.14	Up	DP	L2	[14]	
nvel1	10015	239.1.1.15	Up	DP	L2	[15]	
nvel1	10016	239.1.1.16	Up	DP	L2	[16]	
nvel1	10017	239.1.1.17	Up	DP	L2	[17]	
nvel1	10018	239.1.1.18	Up	DP	L2	[18]	
nvel1	10019	239.1.1.19	Up	DP	L2	[19]	
nvel1	10020	239.1.1.20	Up	DP	L2	[20]	
nvel1	10021	239.1.1.21	Up	DP	L2	[21]	
nvel1	10022	239.1.1.22	Up	DP	L2	[22]	
nvel1	10023	239.1.1.23	Up	DP	L2	[23]	
nvel1	10099	239.1.1.99	Up	DP	L2	[99]	

Hình 5.70 Xem NVE VNI

5.3.6 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 5.71 Kiểm tra giao thức dự phòng gateway HSRP tại NXOS3

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

```

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 5.72 Kiểm tra giao thức dự phòng gateway HSRP tại NXOS4

5.3.7 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 5.73 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 5.74 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 5.75 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           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: 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 5.76 Kiểm tra Port-channel 4 trên Sw_DC1

5.3.8 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 5.77 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

```

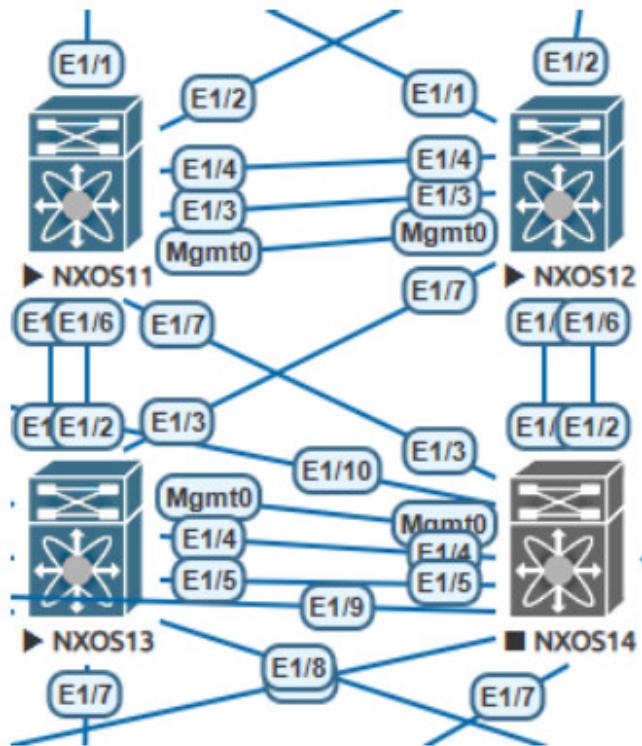
Hình 5.78 VPC domain 2 trên switch NXOS3

vPC status					Active vlans
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 5.79 VPC Status

5.3.9 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
```

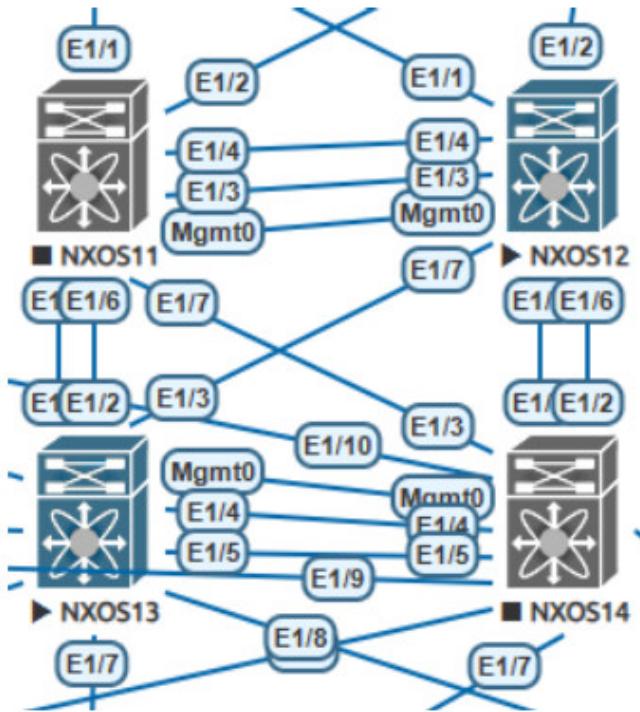
```
NgoaiNgu> show ip
```

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 5.80 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
```

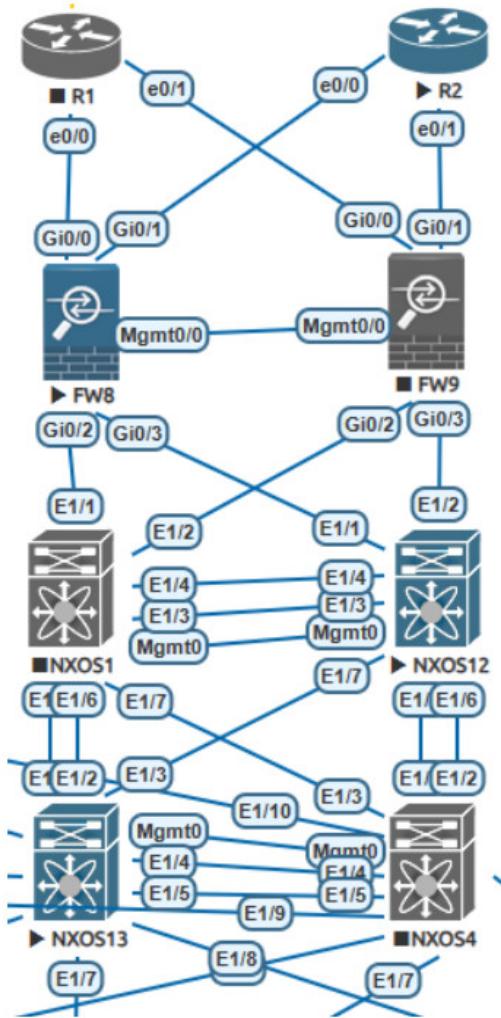
```
TCNH> show ip
```

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 5.81 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 5.82 Hệ thống vẫn hoạt động bình thường nhờ các thiết bị redundant

CHƯƠNG 4 - TỔNG KẾT

4.4 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.

4.5 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 VXLAN 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.

4.6 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 (Soft-

ware 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 về VXLAN bao gồm việc áp dụng các kỹ thuật liên quan như EVPN (Ethernet Virtual Private Network), QoS (Quality of Service), Dynamic Load Balancing được thực hiện để tối ưu hiệu suất và đảm bảo tính tin cậy của hệ thống.

TÀI LIỆU THAM KHẢO

- Sequeira, A. J. (2013). *Interconnecting Cisco Network Devices*. Cisco Press.
- Somit Maloo, F. A. (2020). *CCNP and CCIE Data Center Core DCCOR 350-601 Official Cert Guide*. Cisco Press.
- Stallings, W. (2021). *Data and Computer Communication*. Prentice Hall.
- Systems, C. (2021). *Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 10.1(x)*. Cisco Systems.