

BỘ GIÁO DỤC VÀ ĐÀO TẠO BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
TRƯỜNG ĐẠI HỌC THỦY LỢI



Dương Ngô Quyền

THIẾT KẾ VÀ MÔ PHỎNG MẠNG DOANH NGHIỆP QUY
MÔ TRUNG BÌNH

ĐỒ ÁN TỐT NGHIỆP

HÀ NỘI, NĂM 2025

BỘ GIÁO DỤC VÀ ĐÀO TẠO BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
TRƯỜNG ĐẠI HỌC THỦY LỢI

DƯƠNG NGÔ QUYỀN

**THIẾT KẾ VÀ MÔ PHÒNG MẠNG DOANH NGHIỆP QUY
MÔ TRUNG BÌNH**

Ngành: Công nghệ thông tin

Mã số: 7480201

NGƯỜI HƯỚNG DẪN: TS. Võ Tá Hoàng

HÀ NỘI, NĂM 2025



CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

NHIỆM VỤ ĐỒ ÁN TỐT NGHIỆP

Họ tên sinh viên: DƯƠNG NGÔ QUYỀN

Lớp: 63CNTT2

Khoa: Công nghệ thông tin

Hệ đào tạo: Đại học chính quy

Ngành: Công Nghệ Thông Tin

1- TÊN ĐỀ TÀI:

THIẾT KẾ VÀ MÔ PHÒNG MẠNG DOANH NGHIỆP QUY MÔ TRUNG BÌNH

2- CÁC TÀI LIỆU CƠ BẢN:

- [1] Cisco Networking Academy - CCNA Guide
- [2] Tài liệu SCADA & IoT trong công nghiệp
- [3] Sách "Mạng máy tính" - Andrew Tanenbaum
- [4] Hướng dẫn sử dụng EVE-NG của eve-ng.net
- [1] Cisco Networking Academy - CCNA Guide

3 - NỘI DUNG CÁC PHẦN THUYẾT MINH VÀ TÍNH TOÁN:

Nội dung các phần	Tỷ lệ %
Chương 1: Tổng quan cơ sở lý thuyết	20%
Chương 2: Phân tích yêu cầu hệ thống	40%
Chương 3: Thiết kế và triển khai hệ thống	40%

4. GIÁO VIÊN HƯỚNG DẪN TỪNG PHẦN

Phần	Họ và tên giáo viên hướng dẫn
Chương 1: Tổng quan cơ sở lý thuyết	TS. Võ Tá Hoàng
Chương 2: Phân tích yêu cầu hệ thống	TS. Võ Tá Hoàng
Chương 3: Thiết kế và triển khai hệ thống	TS. Võ Tá Hoàng

5. NGÀY GIAO NHIỆM VỤ ĐỒ ÁN TỐT NGHIỆP

Ngày....tháng.... năm 2025

Trưởng Bộ môn
(Ký và ghi rõ Họ tên)

Giáo viên hướng dẫn chính
(Ký và ghi rõ Họ tên)

TS. Võ Tá Hoàng

Nhiệm vụ Đồ án tốt nghiệp đã được Hội đồng thi tốt nghiệp của Khoa thông qua.

Ngày.tháng.năm 2025

Chủ tịch Hội đồng
(Ký và ghi rõ Họ tên)

Sinh viên đã hoàn thành và nộp bản Đồ án tốt nghiệp cho Hội đồng thi ngày 07 tháng 07 năm 2025

Sinh viên làm Đồ án tốt nghiệp
(Ký và ghi rõ Họ tên)

Dương Ngô Quyền



TRƯỜNG ĐẠI HỌC THỦY LỢI
KHOA CÔNG NGHỆ THÔNG TIN

BẢN TÓM TẮT ĐỀ CƯƠNG ĐỒ ÁN TỐT NGHIỆP

TÊN ĐỀ TÀI: THIẾT KẾ VÀ MÔ PHỎNG MẠNG DOANH NGHIỆP QUY MÔ TRUNG BÌNH

Sinh viên thực hiện: Dương Ngô Quyền

Lớp: 63CNTT2

Mã sinh viên: 2151060264

Số điện thoại: 0399920307

Email: duongngoquyen2003@gmail.com

Giáo viên hướng dẫn: TS. Võ Tá Hoàng

TÓM TẮT ĐỀ TÀI

Mạng máy tính là một phần không thể thiếu trong các doanh nghiệp hiện đại, giúp tối ưu hóa quy trình làm việc, tăng cường bảo mật và nâng cao hiệu suất vận hành. Đề tài này tập trung vào nghiên cứu, thiết kế và mô phỏng một hệ thống mạng cho doanh nghiệp quy mô trung bình, đảm bảo các yếu tố về hiệu suất, bảo mật và khả năng mở rộng.

Dự án sẽ triển khai một mô hình mạng doanh nghiệp với các thành phần chính bao gồm:

- Bộ định tuyến (Router), thiết bị chuyển mạch (Switch), kết nối WAN và tường lửa để phát triển toàn bộ kiến trúc mạng.
- ACL (Danh sách kiểm soát truy cập) để tăng cường bảo mật, hạn chế truy cập trái phép.
- Triển khai VLAN và định tuyến liên VLAN để tối ưu hóa phân đoạn mạng và quản lý lưu lượng.
- Thiết lập các giao thức mạng quan trọng như DHCP và DNS để tự động hóa cấp phát IP và đảm bảo kết nối hiệu quả.

CÁC MỤC TIÊU CHÍNH

- Hiểu rõ nhu cầu của mạng doanh nghiệp quy mô trung bình
- Xây dựng một hệ thống mạng doanh nghiệp quy mô trung bình có khả năng mở rộng và bảo mật cao
- Thực hiện triển khai các công nghệ như Vlan, định tuyến liên Vlan và firewall,...

- Đánh giá và tối ưu hiệu suất mạng doanh nghiệp

KẾT QUẢ DỰ KIẾN

- ✓ Một mô hình mạng doanh nghiệp quy mô trung bình hoàn chỉnh
- ✓ Cải thiện bảo mật nhờ ACL và Firewall
- ✓ Cấu hình và kiểm thử thành công trên môi trường giả lập
- ✓ Làm chủ lý thuyết và có khả năng ứng dụng vào thực tế

TIẾN ĐỘ THỰC HIỆN

TT	Thời gian	Nội dung công việc	Kết quả dự kiến đạt được
1	Tuần 1	<p>Khảo sát yêu cầu mạng doanh nghiệp</p> <ul style="list-style-type: none">• Thực hiện khảo sát toàn diện về nhu cầu mạng của doanh nghiệp.• Nghiên cứu và áp dụng các phương pháp phân tích yêu cầu mạng tốt nhất.• Đánh giá hiệu suất mạng hiện tại (nếu có) và xác định rủi ro tiềm ẩn.• Lập kế hoạch quản lý rủi ro để giải quyết các vấn đề phát sinh.	Xác định mô hình mạng, số lượng thiết bị, yêu cầu bảo mật

2	Tuần 2	<p>Lập sơ đồ thiết kế mạng (VLAN, IP, kiểu topology)</p> <ul style="list-style-type: none"> • Thiết kế kiến trúc mạng bao gồm VLAN, phân bổ địa chỉ IP và topology tối ưu. • Sử dụng các công cụ thiết kế mạng và phần mềm mô phỏng để kiểm tra và xác nhận thiết kế trước khi triển khai. • So sánh các phương pháp thiết kế mạng khác nhau và biện minh cho lựa chọn. • Lập kế hoạch khả năng mở rộng và dự phòng để đảm bảo mạng có thể phát triển và bền vững. 	Bản vẽ sơ đồ mạng, phân chia subnet
3	Tuần 3	Thiết lập giao thức DHCP và DNS với các cấu hình nâng cao	Mạng LAN hoạt động, cấp phát IP tự động
4	Tuần 4	<p>Triển khai VLAN và thiết lập Firewall</p> <ul style="list-style-type: none"> • Triển khai VLAN để phân đoạn mạng, tăng cường bảo mật và quản lý. • Cấu hình firewall và triển khai các biện pháp bảo mật tiên tiến như hệ thống phát hiện xâm nhập (IDS) và kiểm soát truy cập. 	Mạng bảo vệ tốt hạn chế truy cập trái phép
5	Tuần 5-7	<p>Kiểm thử, đánh giá hiệu suất mạng. Điều chỉnh QoS, tối ưu băng thông, giám tắc nghẽn mạng.</p> <ul style="list-style-type: none"> • Thực hiện kiểm tra tải và kiểm tra xâm nhập để đánh giá hiệu suất và an 	Báo cáo hiệu suất và tối ưu hệ thống

		<p>toàn mạng.</p> <ul style="list-style-type: none"> Sử dụng các công cụ giám sát và phân tích mạng để thu thập dữ liệu và xác định khu vực cần cải thiện. Phân tích kết quả kiểm tra và đề xuất tối ưu hóa để nâng cao hiệu suất 	
6	Tuần 8-10	Hoàn thiện báo cáo đồ án và tài liệu hướng dẫn triển khai	Báo cáo hoàn chỉnh tài liệu hướng dẫn sử dụng

TÀI LIỆU THAM KHẢO

- [1] Cisco Networking Academy - CCNA Guide
- [2] Tài liệu SCADA & IoT trong công nghiệp
- [3] Sách "Mạng máy tính" - Andrew Tanenbaum
- [4] Hướng dẫn sử dụng EVE-NG của eve-ng.net

LỜI CAM ĐOAN

Em xin cam đoan đây là Đồ án tốt nghiệp/ Khóa luận tốt nghiệp của bản thân tác giả. Các kết quả trong Đồ án tốt nghiệp/Khóa luận tốt nghiệp này là trung thực, và không sao chép từ bất kỳ một nguồn nào và dưới bất kỳ hình thức nào. Việc tham khảo các nguồn tài liệu (nếu có) đã được thực hiện trích dẫn và ghi nguồn tài liệu tham khảo đúng quy định.

Tác giả ĐATN/KLTN

Chữ ký

Dương Ngô Quyền

LỜI CẢM ƠN

Để hoàn thành đồ án tốt nghiệp này, em xin gửi lời cảm ơn chân thành và sâu sắc nhất đến thầy giáo, **TS. Võ Tá Hoàng**. Trong suốt quá trình thực hiện đề tài, thầy đã tận tình hướng dẫn, chỉ bảo, cung cấp những kiến thức chuyên môn quý báu và định hướng cho em những hướng đi đúng đắn. Sự nhiệt tình và tâm huyết của thầy là nguồn động viên to lớn giúp em vượt qua những khó khăn và hoàn thành tốt nhiệm vụ của mình.

Em cũng xin trân trọng cảm ơn các thầy cô trong Khoa Công nghệ Thông tin, Trường Đại học Thủy Lợi đã trang bị cho em những kiến thức nền tảng vững chắc trong suốt những năm học vừa qua. Đây là hành trang vô cùng quan trọng để em có thể tự tin thực hiện đề tài này và bước vào con đường sự nghiệp sau này.

Cuối cùng, em xin gửi lời cảm ơn đến gia đình và bạn bè đã luôn ở bên cạnh, động viên và tạo mọi điều kiện thuận lợi để em có thể tập trung học tập và nghiên cứu.

Mặc dù đã có nhiều cố gắng, song do kiến thức và kinh nghiệm còn hạn chế, đồ án chắc chắn không thể tránh khỏi những thiếu sót. Em rất mong nhận được những ý kiến đóng góp quý báu từ các thầy cô và các bạn để đồ án được hoàn thiện hơn.

Em xin chân thành cảm ơn!

Mục Lục

DANH MỤC CÁC HÌNH ẢNH.....	V
DANH MỤC CÁC BẢNG BIỂU.....	VI
DANH MỤC CÁC TỪ VIẾT TẮT VÀ GIẢI THÍCH THUẬT NGỮ.....	VII
MỞ ĐẦU.....	1
CHƯƠNG 1: TỔNG QUAN ĐỀ TÀI VÀ CƠ SỞ LÝ THUYẾT.....	4
1.1. Tổng quan về Mạng Doanh nghiệp (Enterprise Network).....	4
1.1.1. Định nghĩa, Vai trò và các Thành phần Cốt lõi.....	4
1.1.2. Mô hình Thiết kế Mạng Phân cấp của Cisco (Hierarchical Network Design).....	4
1.2. Các Công nghệ Nền tảng trong Thiết kế Mạng.....	5
1.2.1. Phân đoạn Mạng với VLAN và Định tuyến liên VLAN.....	5
1.2.2. Đảm bảo Tính sẵn sàng cao với FHRP.....	6
1.2.3 Spanning Tree Protocol (STP).....	7
1.2.4. Các Dịch vụ Mạng Cốt lõi (DHCP & DNS).....	8
1.3. Các Nguyên tắc và Công nghệ Bảo mật Mạng.....	9
1.3.1. Bảo mật Vành đai với Firewall Cisco ASA.....	9
1.3.2. Kiểm soát Truy cập với Access Control List (ACL).....	10
1.4. Công cụ Mô phỏng EVE-NG (Emulated Virtual Environment - Next Generation).....	11
CHƯƠNG 2: PHÂN TÍCH YÊU CẦU VÀ THIẾT KẾ HỆ THỐNG MẠNG.....	12
2.1. Phân tích Yêu cầu Hệ thống (Requirements Analysis).....	12
2.1.1. Yêu cầu Chức năng.....	12
2.1.2. Yêu cầu Phi chức năng.....	12
2.2. Thiết kế Kiến trúc Tổng thể (High-Level Design).....	13
2.2.1. Sơ đồ Topo Logic.....	13
2.2.2. Sơ đồ Topo Vật lý.....	14
2.3. Lựa chọn thiết bị.....	14
2.4. Quy hoạch Không gian Địa chỉ IP và VLAN (IP Addressing and VLAN Scheme).....	15
2.4.1. Lựa chọn Dải địa chỉ và Phương pháp Chia mạng con.....	15
2.5. Thiết kế Chính sách Bảo mật.....	17
CHƯƠNG 3: MÔ PHỎNG HỆ THỐNG BẰNG CÔNG CỤ EVE-NG.....	20
3.1. Cấu hình Hạ tầng Chuyển mạch Lớp 2.....	20
3.1.1. Cấu hình VLAN và Trunking.....	20
3.1.2. Cấu hình Spanning Tree Protocol.....	35
3.2. Cấu hình Định tuyến và Dự phòng Lớp 3.....	37
3.2.1. Cấu hình Giao diện ảo chuyển mạch (SVI) và Định tuyến OSPF.....	37
3.2.2. Cấu hình HSRP.....	41
3.3. Cấu hình Dịch vụ Mạng.....	45
3.3.1. Cấu hình DHCP Server và DHCP Relay.....	45
3.4. Cấu hình Firewall Cisco ASA.....	50
3.4.1. Cấu hình Giao diện, Vùng và Cấp độ An ninh.....	50
3.4.2. Cấu hình NAT (Object-based).....	51
3.4.3. Cấu hình Access Control List (ACL).....	51
3.5. Cấu hình Giám sát Mạng.....	52

3.5.1. Cấu hình Syslog	52
3.6 KIỂM THỬ VÀ ĐÁNH GIÁ	52
3.6.1. Xây dựng các Kịch bản Kiểm tra	52
3.6.2. Thực thi và Phân tích Kết quả	54
3.6.3. Đánh giá Tổng thể	55
KẾT LUẬN	57
TÀI LIỆU THAM KHẢO	60

DANH MỤC CÁC HÌNH ẢNH

2. 1	Sơ đồ mạng tổng quát.....	13
3. 1	Ảnh kết quả tạo Vlan trên sw47	21
3. 2	Kết quả tạo các đường trunk	24
3. 3	Kết quả tạo vlan của SWit	27
3. 4	Kết quả tạo vlan của SWsale	29
3. 5	Kết quả tạo vlan của SWmarketing	31
3. 6	Kết quả tạo vlan của SWtaichinh	33
3. 7	Kết quả tạo vlan của SWgiamdoc	35
3. 8	Kết quả tạo SVI trên SWL3-5	38
3. 9	Kết quả cấu hình SVI trên SWL3-45	39
3. 10	Kết quả cấu hình OSPF trên SWL3-5	40
3. 11	Kết quả cấu hình OSPF trên SWL3-45	41
3. 12	Sơ đồ HSRP (SWL3-5 chính)	41
3. 13	Kết quả cấu hình HSRP trên SWL3-5	43
3. 14	Kết quả cấu hình HSRP trên SWL3-45	45
3. 15	Kết quả cấu hình chặn cấp phát các ip của SWL3-5	46
3. 16	Kết quả tạo pool trên SWL3-5	48
3. 17	Kết quả cấu hình DHCP Relay của SWL3-5	49
3. 18	Kết quả cấu hình DHCP Relay của SWL3-45	50
3. 19	Lệnh ping từ VPC đến vlan sale	53
3. 20	Lệnh ping từ VPC đến vùng DMZ	53
3. 21	Kiểm tra trạng thái của HSRP trên SWL3-5	53
3. 22	Kiểm tra trạng thái của HSRP trên SWL3-45 khi SWL3-5 hoạt động	54
3. 23	Trạng thái HSRP của SWL3-45 khi SWL3-5 tắt	54
3. 24	Kết quả của câu lệnh show standby brief trên SWL3-45	55
3. 25	Kết quả ping trace 10.10.0.1	55

DANH MỤC CÁC BẢNG BIỂU

Table 1	Bảng 2.4.1 Quy hoạch chi tiết địa chỉ IP và VLAN	Error! Bookmark not defined.
Table 2	Các địa chỉ ip khác	Error! Bookmark not defined.
Table 3	Truy cập giữa các Vlan	Error! Bookmark not defined.

DANH MỤC CÁC TỪ VIẾT TẮT VÀ GIẢI THÍCH THUẬT NGỮ

Viết tắt	Tên đầy đủ	Giải thích
ACL	Access Control List	Danh sách kiểm soát truy cập, dùng để lọc gói tin.
AP	Access Point	Điểm truy cập không dây.
ARP	Address Resolution Protocol	Giao thức phân giải địa chỉ.
ASA	Adaptive Security Appliance	Thiết bị an ninh thích ứng của Cisco, một loại tường lửa.
DAI	Dynamic ARP Inspection	Kiểm tra ARP động, một tính năng bảo mật Lớp 2.
DHCP	Dynamic Host Configuration Protocol	Giao thức cấu hình máy chủ động.
DMZ	Demilitarized Zone	Vùng phi quân sự, một vùng mạng đệm an ninh.
DNS	Domain Name System	Hệ thống phân giải tên miền.
EIGRP	Enhanced Interior Gateway Routing Protocol	Giao thức định tuyến công nội bộ tăng cường.
EVE-NG	Emulated Virtual Environment - Next Generation	Môi trường ảo hóa giả lập thế hệ mới.
FHRP	First Hop Redundancy Protocol	Giao thức dự phòng chặng đầu tiên.
GLBP	Gateway Load Balancing Protocol	Giao thức cân bằng tải cổng kết nối.
HSRP	Hot Standby Router Protocol	Giao thức router dự phòng nóng.
STP	Spanning Tree Protocol	Giao thức ngăn chặn các vòng lặp
LAN	Local Area Network	Mạng máy tính cục bộ.
MAC	Media Access Control	Địa chỉ kiểm soát truy cập phương tiện.
NAT	Network Address Translation	Dịch địa chỉ mạng.
NMS	Network Management Station	Trạm quản lý mạng.

Viết tắt	Tên đầy đủ	Giải thích
OSPF	Open Shortest Path First	Giao thức tìm đường đi ngắn nhất đầu tiên.
PAgP	Port Aggregation Protocol	Giao thức tổng hợp cổng.
PAT	Port Address Translation	Dịch địa chỉ cổng.
PC	Personal Computer	Máy tính cá nhân.
QoS	Quality of Service	Chất lượng dịch vụ.
SME	Small and Medium-sized Enterprise	Doanh nghiệp vừa và nhỏ.
SNMP	Simple Network Management Protocol	Giao thức quản lý mạng đơn giản.
SVI	Switched Virtual Interface	Giao diện ảo chuyển mạch.
TCP	Transmission Control Protocol	Giao thức điều khiển truyền vận.
UDP	User Datagram Protocol	Giao thức gói dữ liệu người dùng.
VLAN	Virtual Local Area Network	Mạng LAN ảo.
VLSM	Variable Length Subnet Mask	Mặt nạ mạng con có chiều dài thay đổi.
VPN	Virtual Private Network	Mạng riêng ảo.
VRRP	Virtual Router Redundancy Protocol	Giao thức dự phòng router ảo.
WAN	Wide Area Network	Mạng diện rộng.

MỞ ĐẦU

1. Bối cảnh và Tính cấp thiết của Đề tài

Trong kỷ nguyên số hóa, hạ tầng mạng máy tính đã trở thành xương sống không thể thiếu cho mọi hoạt động của doanh nghiệp. Đối với các doanh nghiệp có quy mô trung bình (SMEs), một hệ thống mạng được thiết kế tối ưu không chỉ là công cụ hỗ trợ vận hành mà còn là yếu tố quyết định đến lợi thế cạnh tranh. Sự phụ thuộc ngày càng tăng vào các ứng dụng nội bộ, trao đổi dữ liệu và dịch vụ đám mây đòi hỏi một hạ tầng mạng phải đảm bảo đồng thời ba yếu tố cốt lõi: hiệu năng cao, bảo mật vững chắc và tính sẵn sàng liên tục.

Một thiết kế mạng yếu kém có thể dẫn đến những hậu quả nghiêm trọng như tắc nghẽn lưu lượng, thời gian chết (downtime) kéo dài, thất thoát dữ liệu nhạy cảm và ảnh hưởng trực tiếp đến hiệu quả kinh doanh. Tuy nhiên, một thực tế đáng chú ý là các tài liệu và nghiên cứu hiện có về thiết kế mạng thường tập trung vào hai thái cực: hoặc là các giải pháp cho doanh nghiệp quy mô rất lớn với ngân sách khổng lồ, hoặc là các mô hình đơn giản cho văn phòng nhỏ. Phân khúc doanh nghiệp quy mô trung bình, với số lượng người dùng khoảng từ 200 đến 500, lại có những yêu cầu đặc thù nhưng chưa được phân tích một cách bài bản và chi tiết. Các thách thức về phân chia phòng ban logic, cấu hình dự phòng, bảo mật đa lớp và tối ưu hóa tài nguyên trong bối cảnh ngân sách hạn chế là những vấn đề mà các doanh nghiệp này thường xuyên đối mặt.

Để giải quyết khoảng trống này, đề án "Thiết kế, Mô phỏng và Đánh giá Hiệu năng Hệ thống Mạng Doanh nghiệp Quy mô Trung bình" được thực hiện. Đề tài áp dụng một phương pháp luận khoa học, kết hợp giữa nghiên cứu lý thuyết và thực nghiệm giả lập. Nền tảng giả lập EVE-NG (Emulated Virtual Environment - Next Generation) được lựa chọn làm công cụ chính, cho phép xây dựng một môi trường mạng ảo hóa nhưng chạy hệ điều hành thật của các thiết bị. Cách tiếp cận này mang lại ưu điểm vượt trội: cho phép kiểm thử các kịch bản thực tế, đánh giá hiệu năng, phân tích luồng dữ liệu và xác thực các chính sách bảo mật một cách chính xác trước khi đưa vào triển khai trong môi trường sản xuất, từ đó giảm thiểu rủi ro và chi phí.

2. Mục tiêu Nghiên cứu

Xây dựng một mô hình mạng doanh nghiệp quy mô trung bình hoàn chỉnh: Mô hình này phải có khả năng mở rộng và bảo mật cao, dựa trên kiến trúc phân lớp và các công nghệ tiên tiến, đáp ứng đầy đủ các yêu cầu về chức năng và phi chức năng của một tổ chức hiện đại.

Triển khai chi tiết các công nghệ mạng cốt lõi: Thực hiện cấu hình và kiểm chứng hoạt động của các công nghệ nền tảng, bao gồm phân đoạn mạng bằng VLAN, định tuyến liên VLAN, kiểm soát truy cập bằng ACL, đảm bảo tính sẵn sàng cao với giao thức HSRP, cấp phát IP tự động qua DHCP, phân giải tên miền với DNS và bảo vệ vành đai mạng bằng Firewall.

Thực hiện các kịch bản kiểm thử và đánh giá một cách khoa học: Xây dựng và thực thi các kịch bản kiểm thử để xác minh tính đúng đắn của thiết kế, đo lường hiệu năng thực tế, phân tích khả năng chịu lỗi và mức độ bảo mật của hệ thống.

Đề xuất một mô hình tham khảo có giá trị thực tiễn: Kết quả của đề án không chỉ dừng lại ở mức độ học thuật mà còn hướng tới việc cung cấp một mô hình mẫu, có thể được áp dụng hoặc tùy chỉnh cho các doanh nghiệp có nhu cầu tương tự, đồng thời đưa ra các định hướng phát triển trong tương lai.

3. Đối tượng và Phạm vi Nghiên cứu

- ✧ **Đối tượng nghiên cứu:** Đối tượng chính của đề án là hệ thống mạng của một doanh nghiệp quy mô trung bình, giả định có nhiều phòng ban chức năng (như IT, Sale, Marketing, Tài chính, Ban Giám đốc) và số lượng người dùng trong khoảng từ 200 đến 500.
- ✧ **Phạm vi nghiên cứu:** Đề án tập trung vào việc thiết kế, mô phỏng và đánh giá các khía cạnh kỹ thuật của hệ thống mạng. Phạm vi công nghệ bao gồm:
 - **Hạ tầng mạng:** Router, Switch Layer 2, Switch Layer 3, Firewall Cisco ASA.
 - **Công nghệ chuyển mạch:** VLAN, Trunking, Spanning Tree Protocol (STP).
 - **Công nghệ định tuyến:** Định tuyến liên VLAN, định tuyến động (OSPF).
 - **Công nghệ dự phòng:** Giao thức dự phòng chặng đầu (HSRP)
 - **Dịch vụ mạng:** DHCP Server, DHCP Relay, DNS Server.
 - **Công nghệ bảo mật:** ACL (Standard, Extended), NAT (Static, Dynamic PAT)
 - **Nền tảng thực hiện:** Toàn bộ hệ thống được xây dựng và kiểm thử trên môi trường giả lập EVE-NG.

4. Phương pháp Nghiên cứu

- ✧ **Phương pháp nghiên cứu lý thuyết:** Tổng hợp, phân tích và hệ thống hóa các kiến thức từ giáo trình, tài liệu kỹ thuật của các nhà cung cấp (ví dụ: Cisco), các bài báo khoa học, và các tiêu chuẩn công nghiệp (ví dụ: RFC, IEEE). Phương pháp này được sử dụng chủ yếu trong Chương 1 để xây dựng nền tảng lý luận vững chắc cho các quyết định thiết kế.
- ✧ **Phương pháp thực nghiệm (mô phỏng):** Sử dụng phần mềm giả lập mạng chuyên dụng EVE-NG để xây dựng mô hình mạng ảo hóa. Phương pháp này cho phép triển khai các cấu hình thực tế, tạo ra các kịch bản lỗi, và thực hiện các phép đo đặc, kiểm thử một cách trực quan và chính xác. Việc lựa chọn EVE-NG thay vì các công cụ mô phỏng đơn giản hơn như Packet Tracer là một quyết định có chủ đích nhằm đảm bảo tính hợp lệ và độ tin cậy của các kết quả thực nghiệm, do EVE-NG chạy hệ điều hành thực của thiết bị.
- ✧ **Phương pháp phân tích và đánh giá:** Dựa trên các kết quả thu được từ quá trình kiểm thử, tiến hành phân tích, so sánh và đánh giá hiệu quả của các giải pháp đã triển khai so với các yêu cầu ban đầu. Từ đó, rút ra các kết luận về ưu, nhược điểm của mô hình và đề xuất các hướng cải tiến.

5. Cấu trúc Đồ án

- ✧ **Chương 1: TỔNG QUAN ĐỀ TÀI VÀ CƠ SỞ LÝ THUYẾT:** Trình bày cơ sở lý thuyết chuyên sâu về mạng doanh nghiệp, kiến trúc mạng phân cấp, và các công nghệ nền tảng như VLAN, ACL, HSRP, DHCP, DNS cùng với giới thiệu về công cụ giả lập EVE-NG.
- ✧ **Chương 2: PHÂN TÍCH YÊU CẦU VÀ THIẾT KẾ HỆ THỐNG MẠNG:** Đi sâu vào phân tích các yêu cầu của hệ thống, từ đó đề xuất một kiến trúc thiết kế tổng thể, bao gồm quy hoạch địa chỉ IP, phân chia VLAN và xây dựng các chính sách bảo mật.
- ✧ **Chương 3: MÔ PHỎNG HỆ THỐNG BẰNG CÔNG CỤ EVE-NG:** Mô tả chi tiết quá trình triển khai hệ thống trên môi trường EVE-NG, cung cấp các cấu hình cụ thể cho từng thiết bị mạng và dịch vụ. Kiểm thử giả định các tình huống. Kết luận, đánh giá

CHƯƠNG 1: TỔNG QUAN ĐỀ TÀI VÀ CƠ SỞ LÝ THUYẾT

1.1. Tổng quan về Mạng Doanh nghiệp (Enterprise Network)

1.1.1. Định nghĩa, Vai trò và các Thành phần Cốt lõi

Mạng doanh nghiệp (Enterprise Network) là một hệ thống hạ tầng truyền thông toàn diện, được thiết kế và triển khai trong phạm vi nội bộ của một tổ chức hoặc doanh nghiệp. Mục tiêu chính của nó là kết nối các tài nguyên công nghệ thông tin đa dạng như máy tính người dùng, máy chủ, máy in, thiết bị lưu trữ và các thiết bị mạng khác. Thông qua hệ thống này, người dùng và các phòng ban có thể chia sẻ tài nguyên, truy cập dữ liệu, giao tiếp nội bộ và kết nối với Internet một cách hiệu quả, bảo mật và ổn định. Đây chính là hạ tầng kỹ thuật số xương sống, tạo điều kiện cho mọi quy trình vận hành và kinh doanh của tổ chức diễn ra một cách thông suốt.

Một mạng doanh nghiệp điển hình được cấu thành từ nhiều thiết bị phần cứng chuyên dụng, mỗi loại thực hiện một chức năng riêng biệt :

- **Router (Bộ định tuyến):** Hoạt động ở Lớp 3 (Lớp Mạng) của mô hình OSI, router có chức năng chính là kết nối các mạng logic khác nhau (ví dụ các subnet) và quyết định đường đi tốt nhất cho các gói tin dựa trên địa chỉ IP đích. Trong mạng doanh nghiệp, router đóng vai trò là cổng kết nối ra Internet (WAN), kết nối các chi nhánh và thực hiện các chức năng định tuyến phức tạp.
- **Switch (Thiết bị chuyển mạch):** Là thiết bị trung tâm của mạng cục bộ (LAN).
- **Switch Layer 2:** Hoạt động ở Lớp 2 (Lớp Liên kết dữ liệu), chuyển tiếp các khung dữ liệu (frame) dựa trên địa chỉ MAC của thiết bị. Nó tạo ra các miền xung đột (collision domain) riêng biệt cho mỗi cổng, giúp tăng hiệu suất mạng so với hub. Tuy nhiên, tất cả các cổng mặc định thuộc cùng một miền quảng bá (broadcast domain).
- **Switch Layer 3 (Multilayer Switch):** Là một thiết bị lai ghép, kết hợp chức năng của switch Lớp 2 và router Lớp 3. Nó có thể thực hiện chuyển mạch ở Lớp 2 dựa trên địa chỉ MAC và định tuyến ở Lớp 3 dựa trên địa chỉ IP với tốc độ rất cao nhờ sử dụng các mạch tích hợp chuyên dụng (ASIC). Thiết bị này rất lý tưởng cho việc định tuyến giữa các VLAN trong mạng nội bộ, nơi yêu cầu thông lượng lớn và độ trễ thấp.[11]
- **Firewall (Tường lửa):** Là thiết bị bảo mật, thường được đặt ở vành đai mạng (giữa mạng nội bộ và Internet) để kiểm soát luồng lưu lượng ra vào. Firewall hoạt động dựa trên các chính sách bảo mật (security policies) đã được định nghĩa trước để cho phép hoặc từ chối các gói tin, bảo vệ hệ thống khỏi các truy cập trái phép và các mối đe dọa từ bên ngoài.
- **Thiết bị đầu cuối (End Devices):** Bao gồm máy tính cá nhân (PC), máy tính xách tay, máy chủ, máy in, điện thoại IP, và các thiết bị IoT. Đây là những điểm khởi tạo và tiếp nhận dữ liệu trong mạng.

1.1.2. Mô hình Thiết kế Mạng Phân cấp của Cisco (Hierarchical Network Design)

- **Lớp Truy cập (Access Layer):** Đây là lớp rìa của mạng, nơi các thiết bị người dùng cuối như máy tính, máy in, và điểm truy cập không dây (Access Point) kết nối trực tiếp vào hệ thống.
 - **Chức năng chính:** Cung cấp kết nối mạng cho các thiết bị đầu cuối và thực thi các chính sách bảo mật ban đầu tại cổng.
 - **Công nghệ đặc trưng:** Chuyển mạch Lớp 2, bảo mật cổng (Port Security) để giới hạn số lượng thiết bị trên một cổng, cấp nguồn qua Ethernet (PoE) cho các thiết bị như điện thoại IP và AP, phân loại và đánh dấu gói tin cho Chất lượng Dịch vụ (QoS), và phân chia người dùng vào các VLAN.
- **Lớp Phân phối (Distribution Layer):** Lớp này đóng vai trò là cầu nối thông minh giữa lớp Truy cập và lớp Lõi, tổng hợp lưu lượng từ nhiều switch truy cập và thực thi các chính sách của mạng.
 - **Chức năng chính:** Định tuyến, lọc gói tin, và kiểm soát luồng truy cập. Đây là ranh giới giữa các miền quảng bá và là nơi các chính sách bảo mật (như ACL) được áp dụng để kiểm soát giao tiếp giữa các VLAN.
 - **Công nghệ đặc trưng:** Chuyển mạch Lớp 3, định tuyến giữa các VLAN (Inter-VLAN Routing), áp dụng các danh sách kiểm soát truy cập (ACL), tổng hợp các liên kết (Link Aggregation/EtherChannel), và triển khai các giao thức dự phòng gateway (FHRP).
- **Lớp lõi (Core Layer):** Lớp Lõi được ví như xương sống tốc độ cao của toàn bộ mạng doanh nghiệp, chịu trách nhiệm vận chuyển một lượng lớn dữ liệu một cách nhanh chóng và đáng tin cậy.
 - **Chức năng chính:** Chuyển mạch gói tin ở tốc độ cao nhất có thể. Lớp này phải đảm bảo tính sẵn sàng và hiệu suất tối đa.
 - **Thiết kế:** Lớp Lõi cần được giữ đơn giản nhất có thể, tránh các xử lý phức tạp làm chậm quá trình chuyển mạch như áp dụng ACL hay định tuyến phức tạp. Tính dự phòng cao là yêu cầu bắt buộc ở lớp này.

1.2. Các Công nghệ Nền tảng trong Thiết kế Mạng

1.2.1. Phân đoạn Mạng với VLAN và Định tuyến liên VLAN

- ✧ **Khái niệm VLAN:** Mạng LAN ảo (Virtual LAN - VLAN) là một công nghệ cho phép một switch vật lý được chia thành nhiều switch ảo độc lập. Về mặt kỹ thuật, mỗi VLAN là một miền quảng bá (broadcast domain) riêng biệt. Các thiết bị trong cùng một VLAN có thể giao tiếp với nhau như thể chúng đang ở trong cùng một mạng LAN vật lý, ngay cả khi chúng được kết nối vào các switch khác nhau. Việc phân chia này dựa trên logic thay vì vị trí vật lý.
- ✧ **Lợi ích của VLAN:**
 - ✓ **Tăng cường Bảo mật:** Bằng cách cô lập lưu lượng giữa các phòng ban (ví dụ: Kế toán, Nhân sự, Kỹ thuật), VLAN ngăn chặn người dùng ở một phòng ban nghe lén hoặc truy cập trái phép vào tài nguyên của phòng ban khác. Traffic giữa các VLAN phải đi qua một thiết bị Lớp 3, nơi các chính sách bảo mật có thể được áp dụng.

- ✓ **Cải thiện Hiệu suất:** Các gói tin quảng bá (broadcast), vốn tiêu tốn tài nguyên của mọi thiết bị trong mạng, sẽ chỉ được lan truyền trong phạm vi VLAN của nó. Việc chia nhỏ mạng thành nhiều VLAN giúp giảm kích thước của các miền quảng bá, từ đó giảm lưu lượng không cần thiết và tối ưu hóa băng thông hệ thống.
- ✓ **Tăng tính Linh hoạt và Đơn giản hóa Quản lý:** Quản trị viên có thể nhóm các máy tính theo chức năng hoặc dự án thay vì vị trí vật lý. Khi một người dùng di chuyển văn phòng, chỉ cần cấu hình lại cổng switch thuộc về VLAN tương ứng mà không cần thay đổi dây cáp vật lý.
- ✧ **Định tuyến liên VLAN (Inter-VLAN Routing):** Theo mặc định, các thiết bị ở các VLAN khác nhau không thể giao tiếp với nhau vì chúng thuộc các miền quảng bá và các mạng con (subnet) khác nhau. Để cho phép sự giao tiếp có kiểm soát này, cần phải có một thiết bị Lớp 3 (như router hoặc switch L3) để thực hiện định tuyến giữa các VLAN. Có hai phương pháp chính để thực hiện điều này:
 - ✓ **Router-on-a-Stick:** Đây là một giải pháp sử dụng một router ngoài với một giao diện vật lý duy nhất được kết nối với switch thông qua một cổng trunk. Trên router, các giao diện con (sub-interfaces) được tạo ra, mỗi giao diện con được gán cho một VLAN và có một địa chỉ IP làm gateway cho VLAN đó. Mọi traffic giữa các VLAN phải đi lên router qua đường trunk, được định tuyến, và sau đó đi xuống switch trở lại. Mặc dù dễ triển khai, phương pháp này có thể trở thành một điểm nghẽn cổ chai về hiệu năng vì tất cả lưu lượng liên VLAN đều phải đi qua một liên kết vật lý duy nhất.[2]
 - ✓ **Switch đa lớp (Layer 3 Switch):** Đây là giải pháp hiệu quả hơn và có khả năng mở rộng tốt hơn. Switch Lớp 3 có thể thực hiện cả chức năng chuyển mạch Lớp 2 và định tuyến Lớp 3 ở tốc độ dây (wire-speed) bằng phần cứng chuyên dụng (ASIC). Thay vì sử dụng router ngoài, các giao diện ảo chuyển mạch (Switched Virtual Interfaces - SVIs) được tạo ra trên chính switch. Mỗi SVI được gán một địa chỉ IP và hoạt động như một gateway cho một VLAN tương ứng. Việc định tuyến giữa các VLAN diễn ra ngay bên trong switch, mang lại hiệu suất cao hơn nhiều so với Router-on-a-Stick. Đối với một mạng doanh nghiệp quy mô trung bình với yêu cầu cao về hiệu năng, việc sử dụng Switch Lớp 3 tại lớp Phân phối là lựa chọn thiết kế vượt trội.[2]

1.2.2. Đảm bảo Tính sẵn sàng cao với FHRP

- ✧ **Vấn đề Điểm lỗi duy nhất (Single Point of Failure):** Trong một mạng LAN điển hình, tất cả các thiết bị đầu cuối đều được cấu hình với một địa chỉ IP của default gateway. Gateway này thường là địa chỉ IP của một router hoặc một SVI trên switch Lớp 3. Nếu thiết bị vật lý đóng vai trò gateway này gặp sự cố (hỏng hóc, mất nguồn, lỗi phần mềm), toàn bộ các máy trạm trong mạng LAN đó sẽ mất kết nối ra các mạng bên ngoài (như các VLAN khác hoặc Internet). Điều này tạo ra một điểm lỗi duy nhất, đi ngược lại yêu cầu về tính sẵn sàng cao của mạng doanh nghiệp.
- ✧ **Giải pháp FHRP:** Các Giao thức Dự phòng Chặng đầu tiên (First Hop Redundancy Protocols - FHRP) là một nhóm các giao thức được thiết kế để giải quyết vấn đề này. Chúng cho phép hai hoặc nhiều router/switch L3 vật lý cùng

hoạt động để tạo ra một gateway ảo duy nhất. Gateway ảo này có địa chỉ IP ảo (Virtual IP - VIP) và địa chỉ MAC ảo riêng. Các máy tính trong mạng sẽ được cấu hình để sử dụng địa chỉ IP ảo này làm default gateway của chúng.[8]

- ✧ **Cơ chế hoạt động của HSRP:** Giao thức Router Dự phòng Nóng (Hot Standby Router Protocol - HSRP) là một giao thức độc quyền của Cisco và là một trong những FHRP phổ biến nhất.[8]
- ✧ **Vai trò Active/Standby:** Trong một nhóm HSRP, một router được bầu chọn làm **Active** và chịu trách nhiệm chính trong việc chuyển tiếp lưu lượng cho gateway ảo. Router này sẽ trả lời các yêu cầu ARP cho địa chỉ IP ảo bằng địa chỉ MAC ảo. Một router khác sẽ ở trạng thái **Standby**, theo dõi router Active và sẵn sàng tiếp quản ngay lập tức nếu router Active gặp sự cố. Các router còn lại trong nhóm (nếu có) sẽ ở trạng thái Listen.[10]
- ✧ **Quy trình bầu chọn:** Việc bầu chọn router Active dựa trên giá trị **priority** được cấu hình (từ 0-255, mặc định là 100). Router có priority cao nhất sẽ trở thành Active. Trong trường hợp priority bằng nhau, router có địa chỉ IP thực cao nhất trên giao diện tham gia HSRP sẽ thắng cử.[10]
- ✧ **Cơ chế Preemption:** Mặc định, nếu một router có priority cao hơn tham gia vào mạng sau khi quá trình bầu chọn đã kết thúc, nó sẽ không tự động giành quyền Active. Tính năng **preemption** (giành quyền) phải được kích hoạt một cách tường minh (standby preempt). Khi được kích hoạt, một router có priority cao hơn (ví dụ, router cũ vừa được sửa chữa và khởi động lại) sẽ có thể giành lại vai trò Active từ router đang hoạt động có priority thấp hơn, đảm bảo router mạnh nhất hoặc được ưu tiên nhất luôn làm nhiệm vụ chính.[10]
- ✧ **So sánh các giao thức FHRP:**
 - **HSRP (Hot Standby Router Protocol):** Độc quyền của Cisco. Sử dụng mô hình Active/Standby.[14]
 - **VRRP (Virtual Router Redundancy Protocol):** Là một tiêu chuẩn mở của IETF (RFC 5798), cho phép hoạt động trong môi trường đa nhà cung cấp. Sử dụng mô hình Master/Backup, tương tự Active/Standby.[15]
 - **GLBP (Gateway Load Balancing Protocol):** Độc quyền của Cisco. Vượt trội hơn HSRP và VRRP ở chỗ nó cung cấp khả năng cân bằng tải thực sự. Thay vì chỉ có một router Active, GLBP cho phép nhiều router trong nhóm cùng lúc chuyển tiếp traffic. Một router được bầu làm Active Virtual Gateway (AVG) có trách nhiệm gán địa chỉ MAC ảo cho các router khác, được gọi là Active Virtual Forwarders (AVF). Các máy trạm vẫn dùng một IP ảo duy nhất, nhưng khi chúng gửi yêu cầu ARP, AVG sẽ trả lời bằng các địa chỉ MAC ảo khác nhau, qua đó phân phối tải trên nhiều gateway.[15]
- **Trong khuôn khổ đề án này, do môi trường giả lập hoàn toàn sử dụng các image của Cisco, việc lựa chọn HSRP là hợp lý và phổ biến.**

1.2.3 Spanning Tree Protocol (STP)

- ✧ **Spanning Tree Protocol (STP)** là một giao thức mạng Layer 2 (lớp liên kết dữ liệu) được sử dụng để ngăn chặn các vòng lặp (loops) trong mạng cục bộ (LAN)

có chứa các đường dẫn dự phòng. Mục tiêu chính của STP là tạo ra một cấu trúc mạng logic không có vòng lặp, đảm bảo hiệu suất và độ ổn định của mạng.

✧ **Các phiên bản STP:**

- **RSTP (Rapid Spanning Tree Protocol - IEEE 802.1w):** Cải thiện đáng kể thời gian hội tụ bằng cách giới thiệu các vai trò cổng và trạng thái mới, cho phép các cổng chuyển sang trạng thái Forwarding nhanh hơn.
- **PVST+ (Per-VLAN Spanning Tree Plus - Cisco Proprietary):** Chạy một phiên bản STP riêng biệt cho mỗi VLAN, cho phép cân bằng tải traffic trên các đường dẫn dự phòng.
- **MSTP (Multiple Spanning Tree Protocol - IEEE 802.1s):** Cho phép nhóm các VLAN vào các thể hiện (instance) STP khác nhau, tối ưu hóa việc sử dụng tài nguyên và khả năng mở rộng trong các mạng lớn.

✧ **Lợi ích của STP:**

- Ngăn chặn vòng lặp: Chức năng chính và quan trọng nhất, giúp mạng hoạt động ổn định.
- Cung cấp tính dự phòng: Mặc dù chặn một số đường dẫn, STP vẫn duy trì khả năng phục hồi khi có sự cố, tự động kích hoạt các đường dẫn dự phòng.
- Ngăn chặn bão Broadcast: Tránh tình trạng tắc nghẽn mạng do gói tin broadcast bị lặp vô hạn.
- Tăng cường hiệu suất mạng: Bằng cách loại bỏ các đường dẫn dư thừa, STP giúp tối ưu hóa băng thông và cải thiện tốc độ truyền tải dữ liệu.

1.2.4. Các Dịch vụ Mạng Cốt lõi (DHCP & DNS)

- ✧ **DHCP (Dynamic Host Configuration Protocol):** DHCP là giao thức cho phép cấp phát địa chỉ IP và các thông tin cấu hình mạng khác (như subnet mask, default gateway, DNS server) một cách tự động cho các thiết bị client. Điều này giúp giảm đáng kể công sức quản trị so với việc cấu hình IP tĩnh cho từng máy. Trên các thiết bị Cisco IOS, một router hoặc switch Lớp 3 có thể được cấu hình để hoạt động như một máy chủ DHCP. Nó có thể tạo ra nhiều vùng cấp phát (DHCP pools) khác nhau, mỗi pool tương ứng với một mạng con (VLAN) riêng biệt. [16]
- ✧ **DHCP Relay Agent:** Khi máy chủ DHCP và các máy client nằm ở các miền quảng bá (VLAN) khác nhau, các gói tin DHCPDISCOVER dạng broadcast từ client sẽ không thể đến được máy chủ DHCP vì router không chuyển tiếp broadcast. Để giải quyết vấn đề này, ta sử dụng tính năng DHCP Relay Agent. Giao diện router/switch L3 (SVI) phía client sẽ được cấu hình với lệnh `ip helper-address <địa_chỉ_DHCP_server>`. Khi giao diện này nhận được một gói DHCP broadcast, nó sẽ chuyển gói tin đó thành một gói unicast và gửi đến địa chỉ của DHCP server đã được chỉ định. Quan trọng hơn, router sẽ chèn địa chỉ IP của chính giao diện nhận broadcast đó vào trường giaddr (Gateway IP Address) trong

gói tin DHCP. Dựa vào trường giaddr này, máy chủ DHCP biết được client thuộc mạng con nào và sẽ cấp phát một địa chỉ IP từ pool tương ứng. [17]

- ✧ **DNS (Domain Name System):** DNS là hệ thống phân giải tên miền thành địa chỉ IP và ngược lại. Thay vì phải nhớ các địa chỉ IP phức tạp, người dùng chỉ cần nhớ các tên miền dễ đọc (ví dụ: www.google.com).

1.3. Các Nguyên tắc và Công nghệ Bảo mật Mạng

1.3.1. Bảo mật Vành đai với Firewall Cisco ASA

- ✧ **Khái niệm Vùng bảo mật và Cấp độ an ninh:** Tường lửa Cisco ASA (Adaptive Security Appliance) sử dụng một mô hình bảo mật dựa trên các vùng (zones) và cấp độ an ninh (security levels). Mỗi giao diện của ASA được gán một tên (ví dụ: inside, outside, dmz) và một cấp độ an ninh là một con số từ 0 đến 100.[18]
 - inside: Thường là mạng nội bộ, mạng đáng tin cậy nhất, được gán cấp độ an ninh cao nhất là **100**.
 - outside: Thường là mạng Internet, mạng không đáng tin cậy nhất, được gán cấp độ an ninh thấp nhất là **0**.
 - dmz (Demilitarized Zone): Vùng phi quân sự, nơi đặt các máy chủ cần truy cập từ Internet (như web server, mail server). Vùng này có mức độ tin cậy trung gian, thường được gán một cấp độ an ninh ở giữa, ví dụ **50**.[18]
- ❖ Quy tắc mặc định của ASA là: Traffic được phép đi từ giao diện có cấp độ an ninh cao hơn đến giao diện có cấp độ an ninh thấp hơn. Traffic từ cấp độ thấp hơn đến cao hơn bị chặn. Ví dụ, traffic từ inside (100) có thể đi ra dmz (50) và outside (0). Traffic từ dmz (50) có thể đi ra outside (0) nhưng không thể tự ý đi vào inside (100).[18]
- ✧ **Dịch địa chỉ mạng (NAT) trên ASA:** NAT là một chức năng cốt lõi của firewall, cho phép che giấu không gian địa chỉ IP private nội bộ và cho phép nhiều thiết bị dùng chung một hoặc một vài địa chỉ IP public. ASA hỗ trợ hai loại NAT chính[19]:
 - **Auto NAT (Object NAT):** Cấu hình NAT được thực hiện bên trong một đối tượng mạng (network object). Đây là cách cấu hình đơn giản và phổ biến cho các kịch bản NAT thông thường.[19]
 - **Manual NAT (Twice NAT):** Cấu hình NAT được thực hiện như các dòng lệnh riêng biệt, cho phép kiểm soát chi tiết hơn, có thể dịch cả địa chỉ nguồn và đích cùng lúc.[19]
- ✧ **Các loại NAT phổ biến bao gồm:**
 - ◆ **Static NAT:** Ánh xạ một-một giữa một địa chỉ IP private và một địa chỉ IP public. Thường dùng để "public" một máy chủ trong DMZ ra Internet.[19]
 - ◆ **Dynamic PAT (Port Address Translation):** Ánh xạ nhiều-một, cho phép nhiều địa chỉ IP private cùng sử dụng một địa chỉ IP public duy nhất bằng cách sử dụng các số hiệu cổng khác nhau để phân biệt các phiên kết nối. Đây là phương pháp phổ biến nhất để cho phép người dùng nội bộ truy cập Internet.[19]

- ◆ **Sự tương tác giữa ACL và Security Level:** Đây là một điểm cực kỳ quan trọng và thường gây nhầm lẫn. Quy tắc mặc định "cao-xuống-thấp" của security level là một quy tắc *ngầm định*. Khi một quản trị viên áp dụng một ACL tường minh vào một giao diện (ví dụ, access-group DMZ_IN in interface dmz để cho phép một dịch vụ nào đó từ DMZ vào inside), quy tắc ngầm định này sẽ bị **vô hiệu hóa** trên giao diện đó. Điều này có nghĩa là, sau khi áp dụng ACL, chỉ những gì được permit trong ACL đó mới được phép đi qua. Tất cả các traffic khác, bao gồm cả traffic vốn được phép trước đây (như từ DMZ ra Internet), sẽ bị chặn bởi quy tắc deny all ngầm định ở cuối mỗi ACL. Do đó, người quản trị phải định nghĩa lại một cách tường minh toàn bộ chính sách cho giao diện đó, bao gồm cả việc cho phép traffic ra Internet. Không nhận thức được điều này là một lỗi cấu hình phổ biến có thể gây ra sự cố mất kết nối khó chẩn đoán.[20]

1.3.2. Kiểm soát Truy cập với Access Control List (ACL)

- ✧ **Khái niệm:** ACL là một danh sách các câu lệnh điều kiện (Access Control Entries - ACEs) được áp dụng tuần tự cho các gói tin đi qua một giao diện mạng. Mỗi câu lệnh xác định hành động là cho phép (permit) hay từ chối (deny) gói tin dựa trên các tiêu chí nhất định. ACL hoạt động như một cơ chế tường lửa cơ bản ở Lớp 3 và Lớp 4.
- ✧ **Phân loại ACL:**
 - **Standard ACL (Dải số 1-99 và 1300-1999):** Chỉ lọc gói tin dựa trên địa chỉ IP nguồn. Do tính đơn giản, chúng có khả năng xử lý nhanh nhưng kém linh hoạt trong việc kiểm soát truy cập.
 - **Extended ACL (Dải số 100-199 và 2000-2699):** Cung cấp khả năng kiểm soát chi tiết hơn nhiều. Chúng có thể lọc dựa trên địa chỉ IP nguồn và đích, giao thức Lớp 4 (TCP, UDP, ICMP,...), và số cổng nguồn/đích (ví dụ: cho phép truy cập web đến cổng 80 nhưng chặn truy cập FTP đến cổng 21).
 - **Reflexive ACL:** Là một dạng ACL động, cho phép traffic trả về của một phiên kết nối được khởi tạo từ bên trong mạng. Nó hoạt động bằng cách tạo ra các mục nhập tạm thời trong một ACL riêng khi có traffic đi ra, và sau đó kiểm tra traffic đi vào dựa trên các mục nhập tạm thời này. Đây là một dạng stateful firewall cơ bản.[21]
 - **Time-based ACL:** Cho phép các quy tắc trong ACL chỉ có hiệu lực trong một khoảng thời gian nhất định trong ngày hoặc trong tuần. Điều này rất hữu ích để áp dụng các chính sách truy cập khác nhau giữa giờ làm việc và ngoài giờ làm việc.[22]
- ✧ **Nguyên tắc Đặt ACL (ACL Placement):** Việc đặt ACL ở đâu và theo hướng nào (in hay out) có ảnh hưởng lớn đến hiệu suất và an ninh mạng. Có một nguyên tắc chung được công nhận rộng rãi :[23]
 - **Extended ACL:** Nên được đặt càng gần **nguồn** của luồng dữ liệu cần lọc càng tốt. Lý do là Extended ACL có thể lọc rất cụ thể (dựa trên nguồn, đích, cổng). Việc đặt nó gần nguồn sẽ giúp chặn traffic không mong muốn ngay lập tức, tránh cho nó đi vào mạng và tiêu tốn tài nguyên bằng thông một cách vô ích.

- **Standard ACL:** Nên được đặt càng gần **đích** của luồng dữ liệu càng tốt. Vì Standard ACL chỉ lọc theo địa chỉ nguồn, nếu đặt nó gần nguồn, nó có thể vô tình chặn cả những lưu lượng hợp lệ từ nguồn đó đi đến các đích khác mà ta không muốn chặn.

1.4. Công cụ Mô phỏng EVE-NG (Emulated Virtual Environment - Next Generation)

Để kiểm chứng một thiết kế mạng phức tạp một cách khoa học mà không cần đầu tư vào hệ thống phần cứng vật lý đắt đỏ, việc sử dụng các công cụ giả lập là một giải pháp tối ưu. Trong khuôn khổ đề án này, EVE-NG được lựa chọn làm nền tảng chính.

- ✧ **Phân biệt Emulator và Simulator:** Cần phân biệt rõ EVE-NG là một **emulator** (trình giả lập), khác với các **simulator** (trình mô phỏng) như Cisco Packet Tracer.
 - ◆ **Simulator:** Mô phỏng lại các chức năng và hành vi của thiết bị mạng bằng cách viết lại một phần mã nguồn. Chúng thường nhẹ, dễ sử dụng nhưng bị giới hạn về tính năng và không phải lúc nào cũng phản ánh chính xác hoạt động của thiết bị thật. Các lệnh có thể bị thiếu hoặc hoạt động không đúng như trên thiết bị vật lý.
 - ◆ **Emulator:** Chạy trực tiếp image hệ điều hành gốc từ nhà sản xuất (ví dụ: Cisco IOS, IOS-XE, ASA, Juniper JunOS) bên trong một máy ảo. Do đó, các lệnh, tính năng, quy trình xử lý gói tin và hành vi của thiết bị ảo trong EVE-NG gần như giống hệt với thiết bị vật lý. Điều này mang lại độ chính xác và tin cậy cao hơn nhiều cho các kết quả kiểm thử, làm cho các kết luận rút ra từ môi trường giả lập có giá trị khoa học và thực tiễn cao.
- ✧ **Lợi ích trong Nghiên cứu và Đào tạo:** Việc lựa chọn EVE-NG không chỉ là một quyết định về công cụ, mà là một quyết định về phương pháp luận nghiên cứu, khẳng định tính hợp lệ và độ tin cậy của các kết quả thực nghiệm trong đề án. Các lợi ích chính bao gồm :
 - ◆ **Tiết kiệm chi phí:** Loại bỏ nhu cầu mua sắm và bảo trì thiết bị vật lý.
 - ◆ **Tính linh hoạt:** Dễ dàng xây dựng, thay đổi và phá hủy các topo mạng phức tạp chỉ với vài cú nhấp chuột.
 - ◆ **Kiểm chứng trước khi triển khai:** Cho phép kiểm tra kỹ lưỡng các cấu hình, chính sách bảo mật và kịch bản lỗi trước khi áp dụng vào mạng thực tế, giảm thiểu rủi ro và thời gian chết.
 - ◆ **Hỗ trợ học tập và nghiên cứu:** Là một công cụ vô giá cho sinh viên và kỹ sư mạng để thực hành, nghiên cứu các công nghệ mới và chuẩn bị cho các kỳ thi chứng chỉ quốc tế như CCNA, CCNP.

CHƯƠNG 2: PHÂN TÍCH YÊU CẦU VÀ THIẾT KẾ HỆ THỐNG MẠNG

2.1. Phân tích Yêu cầu Hệ thống (Requirements Analysis)

2.1.1. Yêu cầu Chức năng

Đây là các yêu cầu về những gì hệ thống mạng phải làm để phục vụ hoạt động của doanh nghiệp.

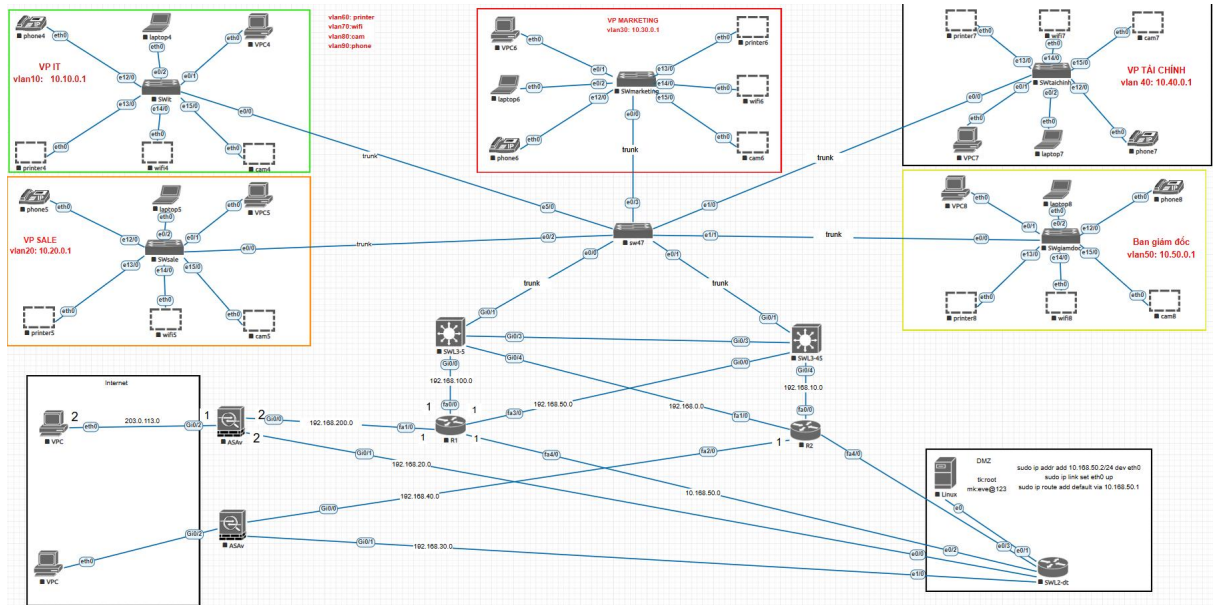
- ✧ **Quy mô người dùng:** Hệ thống phải được thiết kế để hỗ trợ hoạt động ổn định cho một doanh nghiệp quy mô trung bình với số lượng người dùng và thiết bị trong khoảng từ 200 đến 500.
- ✧ **Phân chia phòng ban:** Mạng phải được phân đoạn logic để phục vụ các phòng ban chức năng riêng biệt, đảm bảo sự tách biệt về mặt hoạt động và quản lý. Các phòng ban chính bao gồm: Phòng Công nghệ Thông tin (IT), Phòng Kinh doanh (Sale), Phòng Marketing, Phòng Tài chính, và Ban Giám đốc. Các thiết bị bao gồm: printer, wifi, camera, phone.
- ✧ **Kết nối Internet:** Cung cấp kết nối Internet ổn định, có kiểm soát cho tất cả nhân viên.
- ✧ **Dịch vụ nội bộ:** Cho phép người dùng truy cập các máy chủ dịch vụ nội bộ (ví dụ: Web Server, File Server, Database Server) được đặt trong một vùng mạng riêng (DMZ hoặc Server Farm) theo các chính sách phân quyền đã được định nghĩa.
- ✧ **Cấp phát địa chỉ động:** Hệ thống phải có khả năng tự động cấp phát địa chỉ IP cho các thiết bị người dùng cuối (máy tính, điện thoại IP) thông qua giao thức DHCP để đơn giản hóa việc quản lý và giảm thiểu lỗi cấu hình thủ công.
- ✧ **Phân giải tên miền:** Cung cấp dịch vụ DNS để phân giải tên miền nội bộ (ví dụ: server.noidia.corp) và các tên miền công cộng trên Internet, giúp người dùng truy cập tài nguyên một cách thuận tiện.

2.1.2. Yêu cầu Phi chức năng

- ✧ **Hiệu năng (Performance):** Đảm bảo thông lượng cao và độ trễ thấp cho các luồng dữ liệu quan trọng, đặc biệt là giữa các máy trạm và máy chủ nội bộ, cũng như kết nối giữa các lớp mạng.
- ✧ **Bảo mật (Security):**
 1. Thực thi chính sách kiểm soát truy cập chặt chẽ giữa các VLAN, chỉ cho phép các luồng giao tiếp cần thiết cho hoạt động kinh doanh.
 2. Bảo vệ vành đai mạng, ngăn chặn các truy cập trái phép và các mối đe dọa từ Internet.
- ✧ **Tính sẵn sàng (Availability):** Giảm thiểu tối đa thời gian chết (downtime) bằng cách loại bỏ các điểm lỗi duy nhất (single points of failure) tại các thành phần mạng cốt lõi như gateway và các liên kết giữa các switch.

- ✧ **Khả năng mở rộng (Scalability):** Thiết kế phải có tính module, cho phép dễ dàng tăng số lượng người dùng hoặc thêm các phòng ban, chi nhánh mới trong tương lai mà không cần phải thiết kế lại toàn bộ hệ thống.

2.2. Thiết kế Kiến trúc Tổng thể (High-Level Design)



2. 1 Sơ đồ mạng tổng quát

2.2.1. Sơ đồ Topo Logic

Sơ đồ topo logic (Hình 2.1) mô tả cấu trúc logic của mạng, bao gồm các VLAN, các mạng con (subnet), các vùng bảo mật và các luồng giao tiếp chính.

- ✧ **Hệ thống sẽ được chia thành:**

- ✓ 5 VLAN chính cho các phòng ban: IT(VLAN10), SALE(VLAN20), MARKETING(VLAN30), TAICHINH(VLAN40), GIAMDOC(VLAN50).
- ✓ 4 VLAN cho các các thiết bị: PRINTER (VLAN 60), WIFI (VLAN 70), CAMERA (VLAN 80), PHONE (VLAN 90).
- ✓ Ngoài ra, một vùng DMZ (VLAN 100) được tạo ra để chứa các máy chủ có thể cần truy cập từ bên ngoài.

- ✧ **Các vùng bảo mật:** Tường lửa ASA sẽ phân chia mạng thành ba vùng chính dựa trên mức độ tin cậy:
- ✧ **INSIDE:** Vùng mạng nội bộ, có mức độ tin cậy cao nhất (security-level 100), bao gồm tất cả các VLAN của nhân viên (10, 20, 30, 40, 50).
- ✧ **OUTSIDE:** Vùng mạng không tin cậy, kết nối ra Internet (security-level 0).
- ✧ **DMZ:** Vùng đệm, nơi đặt các máy chủ dịch vụ (security-level 50).
- ✧ **Gateway ảo:** Giao thức HSRP sẽ được triển khai trên cặp Switch Layer 3 ở lớp Phân phối để tạo ra một địa chỉ IP gateway ảo (Virtual IP) cho mỗi VLAN, đảm bảo tính dự phòng cho gateway.

- ✧ **Định tuyến:** Giao thức định tuyến động OSPF sẽ được sử dụng để trao đổi thông tin định tuyến giữa các switch phân phối và tường lửa, đảm bảo tính linh hoạt và tự động cập nhật đường đi khi có sự thay đổi trong mạng. Lựa chọn OSPF thay vì EIGRP là do OSPF là một chuẩn mở, mang lại sự linh hoạt nếu doanh nghiệp muốn tích hợp thiết bị từ các nhà cung cấp khác trong tương lai, thể hiện một tầm nhìn thiết kế dài hạn và tuân thủ chuẩn công nghiệp.

2.2.2. Sơ đồ Topo Vật lý

- ✧ **Lớp Lõi/Vành đai (Core/Edge):** Sử dụng một cặp Firewall Cisco ASA v làm thiết bị trung tâm. Cặp firewall này chịu trách nhiệm kết nối ra hai nhà cung cấp dịch vụ Internet (ISP) khác nhau, thực thi chính sách bảo mật vành đai và định tuyến ra bên ngoài.
- ✧ **Lớp Phân phối (Distribution):** Sử dụng một cặp Switch Layer 3 (ví dụ: Cisco IOL L3) hoạt động song song. Mỗi switch phân phối kết nối lên cả hai firewall và kết nối xuống tất cả các switch truy cập. Cặp switch này sẽ được cấu hình HSRP để cung cấp gateway dự phòng và OSPF để trao đổi định tuyến.
- ✧ **Lớp Truy cập (Access):** Sử dụng các Switch Layer 2 (ví dụ: Cisco IOL L2) để kết nối trực tiếp với các thiết bị đầu cuối (máy ảo PC, server, IP phone). Mỗi switch truy cập sẽ có hai liên kết lên, mỗi liên kết nối đến một switch phân phối khác nhau, tạo thành một đường đi dự phòng.
- ✧ **Máy chủ và Client:** Sử dụng các máy ảo (VPCS, máy ảo Windows/Linux) để giả lập các máy chủ (DNS, DHCP, Web) và các máy trạm người dùng trong từng phòng ban.

2.3. Lựa chọn thiết bị

- ✧ SwitchL2: Cisco Layer 2 Switch (IOS)
 - ✓ Chạy được trên máy yếu, không cần cấu hình mạnh
 - ✓ Dễ dàng tích hợp với phần mềm giả lập
 - ✓ Hỗ trợ VLAN, STP, Port-security, Trunking, Etherchannel...
- ✧ SwitchL3: Cisco Layer 3 Switch (IOS)
 - ✓ Routing đầy đủ
 - ✓ Mô phỏng đa chức năng
 - ✓ Tương thích cao với EVE-NG
- ✧ Router: Cisco 7200 Series Router
 - ✓ Hiệu năng cao
 - ✓ Đa giao thức định tuyến
 - ✓ Tương thích cao
- ✧ Firewall: Cisco ASA v 9.15.2
 - ✓ Triển khai linh hoạt
 - ✓ Đầy đủ tính năng

- ✓ Tương thích cao
- ✓ Bảo mật mạnh mẽ
- ✧ Máy chủ: Linux-ubuntu-server
- ✓ Chi phí thấp
- ✓ Ổn định và độ sẵn sàng cao
- ✓ Bảo mật tốt
- ✓ Hệ quản lý gói mạnh mẽ
- ✓ Tương thích tốt
- ✓ Hiệu năng cao và tiết kiệm tài nguyên

2.4. Quy hoạch Không gian Địa chỉ IP và VLAN (IP Addressing and VLAN Scheme)

2.4.1. Lựa chọn Dải địa chỉ và Phương pháp Chia mạng con

- ✧ Lựa chọn dải địa chỉ: 10.0.0.0
- ✧ Phương pháp Chia mạng con: Để đơn giản hóa việc quản lý và phù hợp với quy mô của từng phòng ban trong mô hình này, phương pháp chia mạng con có chiều dài cố định với subnet mask là /24 (255.255.255.0) được sử dụng cho mỗi VLAN. Mỗi mạng con /24 cung cấp 254 địa chỉ host, đủ cho nhu cầu của mỗi phòng ban trong doanh nghiệp quy mô trung bình và dễ dàng cho việc mở rộng sau này.

Bảng 2.1: Quy hoạch chi tiết địa chỉ IP và VLAN

Tên VLAN	VLAN ID	Mạng con (Subnet/Mask)	Dải IP Cấp phát (DHCP)	Địa chỉ Gateway (Thực)	Địa chỉ Gateway (HSRP VIP)	Ghi chú
IT	10	10.10.0.0 /24	10.10.0.0.4–10.10.0.254	SW5: 10.10.0.2 SW4: 10.10.0.3	10.10.0.1	Phòng Công nghệ thông tin
SALE	20	10.20.0.0 /24	10.20.0.4–10.20.0.254	SW5: 10.20.0.2 SW4: 10.20.0.3	10.20.0.1	Phòng sale

Tên VLAN	VLAN ID	Mạng con (Subnet/Mask)	Dải IP Cấp phát (DHCP)	Địa chỉ Gate way (Thực)	Địa chỉ Gate way (HSRP VIP)	Ghi chú
				5: 10.20.0.3		
MARKETING	30	10.30.0.0/24	10.30.0.4–10.30.0.254	SW5: 10.30.0.2 SW4 5: 10.30.0.3	10.30.0.1	Phòng marketing
TÀI CHÍNH	40	10.40.0.0/24	10.40.0.4–10.40.0.254	SW5: 10.40.0.2 SW4 5: 10.40.0.3	10.40.0.1	tài chính
GIÁM ĐỐC	50	10.50.0.0/24	10.50.0.4–10.50.0.254	SW5: 10.50.0.2 SW4 5: 10.50.0.3	10.50.0.1	Giám đốc
PRINTER	60	10.60.0.0/24	10.60.0.4–10.60.0.254	SW5: 10.60.0.2 SW4 5: 10.60.0.3	10.60.0.1	Thiết bị máy in
WIFI	70	10.70.0.0/24	10.70.0.4–10.70.0.254	SW5: 10.70.0.2	10.70.0.1	Thiết bị wifi

Tên VLAN	VLAN ID	Mạng con (Subnet/Mask)	Dải IP Cấp phát (DHCP)	Địa chỉ Gateway (Thực)	Địa chỉ Gateway (HSRP VIP)	Ghi chú
				SW45: 10.70.0.3		
CAMERA	80	10.80.0.0/24	10.80.0.4–10.80.0.254	SW5: 10.80.0.2 SW45: 10.80.0.3	10.80.0.1	Thiết bị camera
PHONE	90	10.90.0.0/24	10.90.0.4–10.90.0.254	SW5: 10.90.0.2 SW45: 10.90.0.3	10.90.0.1	Điện thoại bàn
DMZ	100	10.168.50.0/24	10.168.50.1–10.168.50.2	N/a	N/A	Vùng chứa Server Public

Bảng 1 Quy hoạch chi tiết địa chỉ IP và VLAN

Địa chỉ mạng	Kết nối
192.168.200.0/24	R1 và ASAv
192.168.100.0/24	R1 và SW13-5
10.168.50.0/24	R1 và vùng DMZ
192.168.50.0/24	R1 và SW13-45
203.0.113.0/24	ASA và pc ngoài internet
192.168.20.0/24	ASA và vùng DMZ

Bảng 2 Các địa chỉ ip khác

2.5. Thiết kế Chính sách Bảo mật

Từ Đến \	IT	SALE	MKT	TC	GD	DMZ (100)	INTER NET
VP IT (10)	Permit All	Permit All	Permit All	Permit All	Permit All	Permit All	Permit All
VP SALE (20)	Deny All	Permit All	Permit All	Deny All	Deny All	Permit TCP 80, 443	Permit TCP 80, 443
VP MARKETING (30)	Deny All	Permit All	Permit All	Deny All	Deny All	Permit TCP 80, 443	Permit TCP 80, 443
VP TÀI CHÍNH (40)	Deny All	Deny All	Deny All	Permit All	Deny All	Deny All	Permit TCP 80, 443
VP GIÁM ĐỐC (50)	Permit All	Permit All	Permit All	Permit All	Permit All	Permit All	Permit All
PRINTER	Permit All	Permit All	Permit All	Permit All	Permit All	Permit All	Deny All
WIFI	Deny all	Deny all	Deny all	Deny all	Deny all	Permit All	Deny all
CAM	Deny all	Deny all	Deny all	Deny all	Deny all	Permit all	Deny all
PHONE	Permit All	Permit All	Permit All	Permit All	Permit All	Permit All	Deny all
DMZ (100)	Deny All	Deny All	Deny All	Deny	Deny	Permit All	Permit All

Từ \ Đến	IT	SALE	MKT	TC	GD	DMZ (100)	INTER NET
				All	All		
INTE RNE T	Deny All	Deny All	Deny All	De ny All	Den y All	Permit TCP 80, 443, 53	Deny All

Bảng 3 Đường đi các VLAN

✧ **Diễn giải ma trận:**

- ✓ **Phòng IT (VLAN 10) và Ban Giám đốc (VLAN 50):** Có quyền truy cập không hạn chế đến tất cả các phòng ban khác và Internet để thực hiện nhiệm vụ quản trị và giám sát.
- ✓ **Phòng Sale (VLAN 20) và Marketing (VLAN 30):** Được phép giao tiếp với nhau nhưng bị chặn truy cập vào các phòng ban nhạy cảm như Tài chính, IT, Ban Giám đốc. Chỉ được phép truy cập các dịch vụ web (HTTP/HTTPS) trên Internet và trong DMZ.
- ✓ **Phòng Tài chính (VLAN 40):** Bị cô lập hoàn toàn với các phòng ban khác (trừ IT và Ban Giám đốc) để đảm bảo an toàn cho dữ liệu tài chính. Chỉ được phép truy cập web ra Internet.
- ✓ **DMZ (VLAN 100):** Hoàn toàn bị cô lập, không được phép chủ động kết nối vào bất kỳ VLAN nội bộ nào. Chỉ có thể trả lời các kết nối được khởi tạo từ bên trong hoặc các kết nối được cho phép từ Internet.
- ✓ **Internet:** Chỉ được phép truy cập vào các dịch vụ đã được public trong DMZ (Web, DNS). Mọi nỗ lực truy cập vào mạng nội bộ (VLAN 10-50) đều bị chặn.
- ✓ Các chính sách này sẽ được thực thi bằng cách sử dụng Extended ACL trên các giao diện SVI của switch phân phối và trên các giao diện của firewall ASA.
- ✓ Các thiết bị tùy vào chức năng của mình mà permit và deny các phòng ban cho phù hợp với chức năng của mình.

CHƯƠNG 3: MÔ PHỎNG HỆ THỐNG BẰNG CÔNG CỤ EVE-NG

3.1. Cấu hình Hạ tầng Chuyển mạch Lớp 2

3.1.1. Cấu hình VLAN và Trunking

Trên SwitchL2 (SW47-server):

Bash

! Đổi tên switch

Switch>

Switch>en

Switch#conf t

Switch(config)#hostname SW47

! Cài đặt vtp

SW47(config)#vtp mode server

SW47(config)#vtp domain thu

! Tạo VLAN cho các phòng ban

SW47(config)# vlan 10

SW47(config-vlan)# name it

SW47(config-vlan)# exit

SW47(config)# vlan 20

SW47(config-vlan)# name sale

SW47(config-vlan)# exit

SW47(config)# vlan 30

SW47(config-vlan)# name marketing

SW47(config-vlan)# exit

SW47(config)# vlan 40

SW47(config-vlan)# name taichinh

SW47(config-vlan)# exit

SW47(config)# vlan 50

SW47(config-vlan)# name giamdoc

```
SW47(config-vlan)# exit
```

! Tạo vlan cho các thiết bị riêng (printer, wifi, camera, phone)

```
SW47(config)# vlan 60
```

```
SW47(config-vlan)# name printer
```

```
SW47(config-vlan)# exit
```

```
SW47(config)# vlan 70
```

```
SW47(config-vlan)# name wifi
```

```
SW47(config-vlan)# exit
```

```
SW47(config)# vlan 80
```

```
SW47(config-vlan)# name cam
```

```
SW47(config-vlan)# exit
```

```
SW47(config)# vlan 90
```

```
SW47(config-vlan)# name phone
```

```
SW47(config-vlan)# exit
```

➤ **Xác minh**

Bash

```
SW47# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Et1/2, Et1/3, Et2/0, Et2/1 Et2/2, Et2/3, Et3/0, Et3/1 Et3/2, Et3/3, Et4/0, Et4/1 Et4/2, Et4/3, Et5/1, Et5/2 Et5/3, Et6/0, Et6/1, Et6/2 Et6/3, Et7/0, Et7/1, Et7/2 Et7/3, Et8/0, Et8/1, Et8/2 Et8/3, Et9/0, Et9/1, Et9/2 Et9/3
10	it	active	
20	sale	active	
30	marketing	active	
40	taichinh	active	
50	giamdoc	active	
60	printer	active	
70	wifi	active	
80	cam	active	

3. 1 Ảnh kết quả tạo Vlan trên sw47

! Tạo đường trunk cho sw47

```
SW47(config)#int e5/0
```

```
SW47(config-if)#sw
```

```
SW47(config-if)#switchport t
```

```
SW47(config-if)#switchport trunk e
```

```
SW47(config-if)#switchport trunk encapsulation d
```

```
SW47(config-if)#switchport trunk encapsulation dot1q
```

```
SW47(config-if)#sw
```

```
SW47(config-if)#switchport mode trunk
```

```
SW47(config)#int e0/2
```

```
SW47(config-if)#sw
```

```
SW47(config-if)#switchport t
```

```
SW47(config-if)#switchport trunk e
```

```
SW47(config-if)#switchport trunk encapsulation d
```

```
SW47(config-if)#switchport trunk encapsulation dot1q
```

```
SW47(config-if)#sw
```

```
SW47(config-if)#switchport mode trunk
```

```
SW47(config-if)#
```

```
SW47(config)#int e0/0
```

```
SW47(config-if)#sw
```

```
SW47(config-if)#switchport t
```

```
SW47(config-if)#switchport trunk e
```

```
SW47(config-if)#switchport trunk encapsulation d
```

```
SW47(config-if)#switchport trunk encapsulation dot1q
```

```
SW47(config-if)#sw
```

```
SW47(config-if)#switchport mode trunk
SW47(config-if)#
SW47(config)#int e0/1
SW47(config-if)#sw
SW47(config-if)#switchport t
SW47(config-if)#switchport trunk e
SW47(config-if)#switchport trunk encapsulation d
SW47(config-if)#switchport trunk encapsulation dot1q
SW47(config-if)#sw
SW47(config-if)#switchport mode trunk
SW47(config-if)#
SW47(config)#int e1/1
SW47(config-if)#sw
SW47(config-if)#switchport t
SW47(config-if)#switchport trunk e
SW47(config-if)#switchport trunk encapsulation d
SW47(config-if)#switchport trunk encapsulation dot1q
SW47(config-if)#sw
SW47(config-if)#switchport mode trunk
SW47(config-if)#
SW47(config)#int e1/0
SW47(config-if)#sw
SW47(config-if)#switchport t
SW47(config-if)#switchport trunk e
SW47(config-if)#switchport trunk encapsulation d
SW47(config-if)#switchport trunk encapsulation dot1q
SW47(config-if)#sw
SW47(config-if)#switchport mode trunk
```

```

SW47(config-if)#
SW47(config)#int e0/3
SW47(config-if)#sw
SW47(config-if)#switchport t
SW47(config-if)#switchport trunk e
SW47(config-if)#switchport trunk encapsulation d
SW47(config-if)#switchport trunk encapsulation dot1q
SW47(config-if)#sw
SW47(config-if)#switchport mode trunk
SW47(config-if)#

```

➤ Xác minh

```
SW47# show interfaces trunk
```

```

Port      Mode      Encapsulation  Status      Native vlan
Et0/0     on        802.1q         trunking    1
Et0/1     on        802.1q         trunking    1
Et0/2     on        802.1q         trunking    1
Et0/3     on        802.1q         trunking    1
Et1/0     on        802.1q         trunking    1
Et1/1     on        802.1q         trunking    1
Et5/0     on        802.1q         trunking    1

Port      Vlans allowed on trunk
Et0/0     1-4094
Et0/1     1-4094
Et0/2     1-4094
Et0/3     1-4094
Et1/0     1-4094
Et1/1     1-4094
Et5/0     1-4094

```

3. 2 Kết quả tạo các đường trunk

! Cấu hình và chia cổng cho các vlan trên switch_client

- chia vlan it:vlan 10--int e0/1-e11/3

Gateway: 10.10.0.1

- chia vlan sale:vlan 20

Gateway: 10.20.0.1

- chia vlan marketing:vlan 30

Gateway: 10.30.0.1

- chia vlan taichinh:vlan40

Gateway: 10.40.0.1

- chia vlan giamdoc:vlan 50

Gateway: 10.50.0.1

- chia vlan printer: cổng e13/0-3

Gateway: 10.60.0.1

- chia vlan wifi: cổng e14/0-3

Gateway: 10.70.0.1

- chia vlan cam: cổng e15/0-3

Gateway: 10.80.0.1

- chia vlan phone: cổng e12/0-3

Gateway: 10.90.0.1

1. Cấu hình cho SWit

Switch>

Switch>en

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hos

Switch(config)#hostname SWit // đổi tên sw

SWit(config)#int e0/0 //cấu hình đường trunk ra switch-server

SWit(config-if)#sw

SWit(config-if)#switchport t

SWit(config-if)#switchport trunk e

SWit(config-if)#switchport trunk encapsulation d

SWit(config-if)#switchport trunk encapsulation dot1q

SWit(config-if)#sw

SWit(config-if)#switchport mode trunk

```

SWit(config-if)#
SWit(config-if)#exit
SWit(config)#
SWit(config)#vtp mode client // cấu hình vtp
Setting device to VTP Client mode for VLANs.
SWit(config)#vtp domain tlu
Domain name already set to tlu.
SWit(config)#in
SWit(config)#int range e0/1-e11/3    // gán cổng cho vlan 10
SWit(config-if-range)#sw
SWit(config-if-range)#switchport mode access
SWit(config-if-range)#sw
SWit(config-if-range)#switchport access vlan 10
SWit(config)#int range e12/0-3 // gán cổng cho vlan 90
SWit(config-if-range)#sw
SWit(config-if-range)#switchport mode access
SWit(config-if-range)#sw
SWit(config-if-range)#switchport access vlan 90
SWit(config-if-range)#int range e13/0-3 // gán cổng cho vlan 60
SWit(config-if-range)#sw
SWit(config-if-range)#switchport mode access
SWit(config-if-range)#sw
SWit(config-if-range)#switchport access vlan 60
SWit(config-if-range)#int range e14/0-3 // gán cổng cho vlan 70
SWit(config-if-range)#sw
SWit(config-if-range)#switchport mode access
SWit(config-if-range)#sw
SWit(config-if-range)#switchport access vlan 70

```

```
SWit(config-if-range)#int range sw
```

```
SWit(config-if-range)#int range e15/0-3 //gán cổng cho vlan 80
```

```
SWit(config-if-range)#sw
```

```
SWit(config-if-range)#switchport mode access
```

```
SWit(config-if-range)#sw
```

```
SWit(config-if-range)#switchport access vlan 80
```

➤ Xác minh:

```
SWit#show vlan
```

```
10   it                               active   Et0/1, Et0/2, Et0/3, Et1/0
                                           Et1/1, Et1/2, Et1/3
20   sale                             active
30   marketing                        active
40   taichinh                         active
50   giamdoc                          active
60   printer                         active   Et13/0, Et13/1, Et13/2, Et13/3
70   wifi                             active   Et14/0, Et14/1, Et14/2, Et14/3
80   cam                             active   Et15/0, Et15/1, Et15/2, Et15/3
90   phone                           active   Et12/0, Et12/1, Et12/2, Et12/3
```

3. 3 Kết quả tạo vlan của SWit

2. Cấu hình cho SWsale

```
Switch>
```

```
Switch>en
```

```
Switch#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)#hos
```

```
Switch(config)#hostname SWsale // đổi tên sw
```

```
SWsale(config)#int e0/0 //cấu hình đường trunk ra switch-server
```

```
SWsale(config-if)#sw
```

```
SWsale(config-if)#switchport t
```

```
SWsale(config-if)#switchport trunk e
```

```
SWsale(config-if)#switchport trunk encapsulation d
```

```
SWsale(config-if)#switchport trunk encapsulation dot1q
```

```

SWsale(config-if)#sw
SWsale(config-if)#switchport mode trunk
SWsale(config-if)#
SWsale(config-if)#exit
SWsale(config)#
SWsale(config)#vtp mode client // cấu hình vtp
Setting device to VTP Client mode for VLANs.
SWsale(config)#vtp domain tlu
Domain name already set to tlu.
SWsale(config)#in
SWsale(config)#int range e0/1-e11/3 // gán cổng cho vlan
SWsale(config-if-range)#sw
SWsale(config-if-range)#switchport mode access
SWsale(config-if-range)#sw
SWsale(config-if-range)#switchport access vlan 20
SWsale(config)#int range e12/0-3 // gán cổng cho vlan 90
SWsale(config-if-range)#sw
SWsale(config-if-range)#switchport mode access
SWsale(config-if-range)#sw
SWsale(config-if-range)#switchport access vlan 90
SWsale(config-if-range)#int range e13/0-3 // gán cổng cho vlan 60
SWsale(config-if-range)#sw
SWsale(config-if-range)#switchport mode access
SWsale(config-if-range)#sw
SWsale(config-if-range)#switchport access vlan 60
SWsale(config-if-range)#int range e14/0-3 // gán cổng cho vlan 70
SWsale(config-if-range)#sw
SWsale(config-if-range)#switchport mode access

```

```

SWsale(config-if-range)#sw
SWsale(config-if-range)#switchport access vlan 70
SWsale(config-if-range)#int range sw
SWsale(config-if-range)#int range e15/0-3 //gán cổng cho vlan 80
SWsale(config-if-range)#sw
SWsale(config-if-range)#switchport mode access
SWsale(config-if-range)#sw
SWsale(config-if-range)#switchport access vlan 80

```

➤ **Xác minh**

SWsale#show vlan

```

10   it                active      Et11/0, Et11/1, Et11/2, Et11/3
20   sale              active      Et0/1, Et0/2, Et0/3, Et1/0
                                   Et1/1, Et1/2, Et1/3
30   marketing         active
40   taichinh          active
50   giamdoc           active
60   printer          active      Et13/0, Et13/1, Et13/2, Et13/3
70   wifi              active      Et14/0, Et14/1, Et14/2, Et14/3
80   cam               active      Et15/0, Et15/1, Et15/2, Et15/3
90   phone             active      Et12/0, Et12/1, Et12/2, Et12/3
--More--

```

3. 4 Kết quả tạo vlan của SWsale

3. Cấu hình cho SWmarketing

Switch>

Switch>en

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hos

Switch(config)#hostname SWmaketing // đổi tên sw

SWmaketing(config)#int e0/0 //cấu hình đường trunk ra switch-server

SWmaketing(config-if)#sw

SWmaketing(config-if)#switchport t

```

SWmarketing(config-if)#switchport trunk e
SWmarketing(config-if)#switchport trunk encapsulation d
SWmarketing(config-if)#switchport trunk encapsulation dot1q
SWmarketing(config-if)#sw
SWmarketing(config-if)#switchport mode trunk
SWmarketing(config-if)#
SWmarketing(config-if)#exit
SWmarketing(config)#
SWmarketing(config)#vtp mode client // cấu hình vtp
Setting device to VTP Client mode for VLANs.
SWmarketing(config)#vtp domain tlu
Domain name already set to tlu.
SWmarketing(config)#in
SWmarketing(config)#int range e0/1-e11/3 // gán cổng cho vlan 30
SWmarketing(config-if-range)#sw
SWmarketing(config-if-range)#switchport mode access
SWmarketing(config-if-range)#sw
SWmarketing(config-if-range)#switchport access vlan 30
SWmarketing(config)#int range e12/0-3 // gán cổng cho vlan 90
SWmarketing(config-if-range)#sw
SWmarketing(config-if-range)#switchport mode access
SWmarketing(config-if-range)#sw
SWmarketing(config-if-range)#switchport access vlan 90
SWmarketing(config-if-range)#int range e13/0-3 // gán cổng cho vlan 60
SWmarketing(config-if-range)#sw
SWmarketing(config-if-range)#switchport mode access
SWmarketing(config-if-range)#sw
SWmarketing(config-if-range)#switchport access vlan 60

```

SWmarketing(config-if-range)#int range e14/0-3 // gán cổng cho vlan 70

SWmarketing(config-if-range)#sw

SWmarketing(config-if-range)#switchport mode access

SWmarketing(config-if-range)#sw

SWmarketing(config-if-range)#switchport access vlan 70

SWmarketing(config-if-range)#int range sw

SWmarketing(config-if-range)#int range e15/0-3 //gán cổng cho vlan 80

SWmarketing(config-if-range)#sw

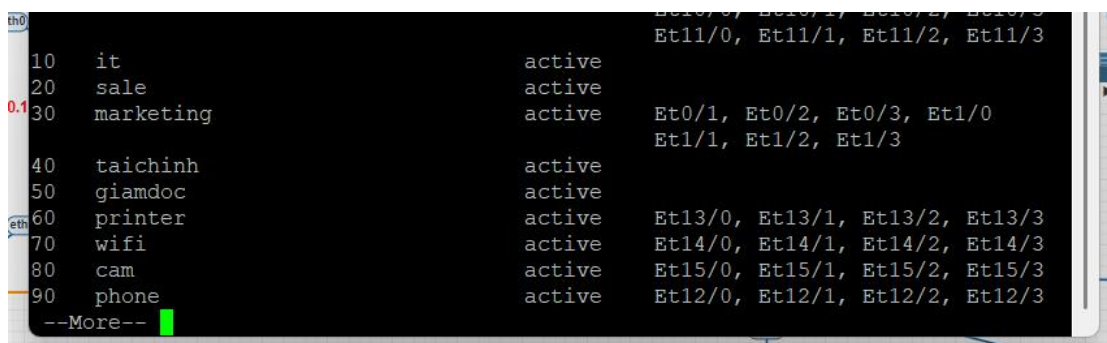
SWmarketing(config-if-range)#switchport mode access

SWmarketing(config-if-range)#sw

SWmarketing(config-if-range)#switchport access vlan 80

➤ **Xác minh**

SWmarketing#show vlan



10	it	active	Et11/0, Et11/1, Et11/2, Et11/3
20	sale	active	
30	marketing	active	Et0/1, Et0/2, Et0/3, Et1/0 Et1/1, Et1/2, Et1/3
40	taichinh	active	
50	giamdac	active	
60	printer	active	Et13/0, Et13/1, Et13/2, Et13/3
70	wifi	active	Et14/0, Et14/1, Et14/2, Et14/3
80	cam	active	Et15/0, Et15/1, Et15/2, Et15/3
90	phone	active	Et12/0, Et12/1, Et12/2, Et12/3
--More--			

3. 5 Kết quả tạo vlan của SWmarketing

4. Cấu hình cho SWtaichinh

Switch>

Switch>en

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hos

Switch(config)#hostname SWtaichinh // đổi tên sw

```

SWtaichinh(config)#int e0/0 //cấu hình đường trunk ra switch-server
SWtaichinh(config-if)#sw
SWtaichinh(config-if)#switchport t
SWtaichinh(config-if)#switchport trunk e
SWtaichinh(config-if)#switchport trunk encapsulation d
SWtaichinh(config-if)#switchport trunk encapsulation dot1q
SWtaichinh(config-if)#sw
SWtaichinh(config-if)#switchport mode trunk
SWtaichinh(config-if)#
SWtaichinh(config-if)#exit
SWtaichinh(config)#
SWtaichinh(config)#vtp mode client // cấu hình vtp
Setting device to VTP Client mode for VLANs.
SWtaichinh(config)#vtp domain tlu
Domain name already set to tlu.
SWtaichinh(config)#in
SWtaichinh(config)#int range e0/1-e11/3 // gán cổng cho vlan 40
SWtaichinh(config-if-range)#sw
SWtaichinh(config-if-range)#switchport mode access
SWtaichinh(config-if-range)#sw
SWtaichinh(config-if-range)#switchport access vlan 40
SWtaichinh(config)#int range e12/0-3 // gán cổng cho vlan 90
SWtaichinh(config-if-range)#sw
SWtaichinh(config-if-range)#switchport mode access
SWtaichinh(config-if-range)#sw
SWtaichinh(config-if-range)#switchport access vlan 90
SWtaichinh(config-if-range)#int range e13/0-3 // gán cổng cho vlan 60
SWtaichinh(config-if-range)#sw

```



```

SWtaichinh(config-if-range)#switchport mode access
SWtaichinh(config-if-range)#sw
SWtaichinh(config-if-range)#switchport access vlan 60
SWtaichinh(config-if-range)#int range e14/0-3 // gán cổng cho vlan 70
SWtaichinh(config-if-range)#sw
SWtaichinh(config-if-range)#switchport mode access
SWtaichinh(config-if-range)#sw
SWtaichinh(config-if-range)#switchport access vlan 70
SWtaichinh(config-if-range)#int range sw
SWtaichinh(config-if-range)#int range e15/0-3 //gán cổng cho vlan 80
SWtaichinh(config-if-range)#sw
SWtaichinh(config-if-range)#switchport mode access
SWtaichinh(config-if-range)#sw
SWtaichinh(config-if-range)#switchport access vlan 80

```

➤ **Xác minh**

SWtaichinh#show vlan

			Et8/0, Et8/1, Et8/2, Et8/3
			Et9/0, Et9/1, Et9/2, Et9/3
			Et10/0, Et10/1, Et10/2, Et10/3
			Et11/0, Et11/1, Et11/2, Et11/3
10	it	active	
20	sale	active	
30	marketing	active	
40	taichinh	active	Et0/1, Et0/2, Et0/3, Et1/0
			Et1/1, Et1/2, Et1/3
50	giamdoc	active	
60	printer	active	Et13/0, Et13/1, Et13/2, Et13/3
70	wifi	active	Et14/0, Et14/1, Et14/2, Et14/3
80	cam	active	Et15/0, Et15/1, Et15/2, Et15/3
90	phone	active	Et12/0, Et12/1, Et12/2, Et12/3

3. 6 Kết quả tạo vlan của SWtaichinh

5. Cấu hình cho SWgiamdoc

Switch>

Switch>en

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)#hos
```

```
Switch(config)#hostname SWgiamdoc // đổi tên sw
```

```
SWgiamdoc(config)#int e0/0 //cấu hình đường trunk ra switch-server
```

```
SWgiamdoc(config-if)#sw
```

```
SWgiamdoc(config-if)#switchport t
```

```
SWgiamdoc(config-if)#switchport trunk e
```

```
SWgiamdoc(config-if)#switchport trunk encapsulation d
```

```
SWgiamdoc(config-if)#switchport trunk encapsulation dot1q
```

```
SWgiamdoc(config-if)#sw
```

```
SWgiamdoc(config-if)#switchport mode trunk
```

```
SWgiamdoc(config-if)#
```

```
SWgiamdoc(config-if)#exit
```

```
SWgiamdoc(config)#
```

```
SWgiamdoc(config)#vtp mode client // cấu hình vtp
```

Setting device to VTP Client mode for VLANs.

```
SWgiamdoc(config)#vtp domain tlu
```

Domain name already set to tlu.

```
SWgiamdoc(config)#in
```

```
SWgiamdoc(config)#int range e0/1-e11/3 // gán cổng cho vlan 50
```

```
SWgiamdoc(config-if-range)#sw
```

```
SWgiamdoc(config-if-range)#switchport mode access
```

```
SWgiamdoc(config-if-range)#sw
```

```
SWgiamdoc(config-if-range)#switchport access vlan 50
```

```
SWgiamdoc(config)#int range e12/0-3 // gán cổng cho vlan 90
```

```
SWgiamdoc(config-if-range)#sw
```

```
SWgiamdoc(config-if-range)#switchport mode access
```

```
SWgiamdoc(config-if-range)#sw
```

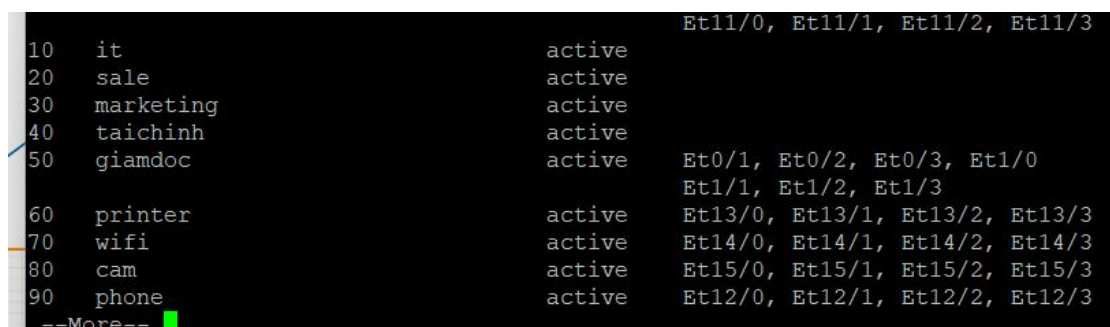
```

SWgiamdoc(config-if-range)#switchport access vlan 90
SWit(config-if-range)#int range e13/0-3 // gán cổng cho vlan 60
SWgiamdoc(config-if-range)#sw
SWgiamdoc(config-if-range)#switchport mode access
SWgiamdoc(config-if-range)#sw
SWgiamdoc(config-if-range)#switchport access vlan 60
SWgiamdoc(config-if-range)#int range e14/0-3 // gán cổng cho vlan 70
SWgiamdoc(config-if-range)#sw
SWgiamdoc(config-if-range)#switchport mode access
SWgiamdoc(config-if-range)#sw
SWgiamdoc(config-if-range)#switchport access vlan 70
SWgiamdoc(config-if-range)#int range sw
SWgiamdoc(config-if-range)#int range e15/0-3 //gán cổng cho vlan 80
SWgiamdoc(config-if-range)#sw
SWgiamdoc(config-if-range)#switchport mode access
SWgiamdoc(config-if-range)#sw
SWgiamdoc(config-if-range)#switchport access vlan 80

```

➤ **Xác minh**

SWgiamdoc#show vlan



VLAN ID	Name	Status	Interfaces
10	it	active	Et11/0, Et11/1, Et11/2, Et11/3
20	sale	active	
30	marketing	active	
40	taichinh	active	
50	giamdoc	active	Et0/1, Et0/2, Et0/3, Et1/0, Et1/1, Et1/2, Et1/3
60	printer	active	Et13/0, Et13/1, Et13/2, Et13/3
70	wifi	active	Et14/0, Et14/1, Et14/2, Et14/3
80	cam	active	Et15/0, Et15/1, Et15/2, Et15/3
90	phone	active	Et12/0, Et12/1, Et12/2, Et12/3

3. 7 Kết quả tạo vlan của SWgiamdoc

3.1.2. Cấu hình Spanning Tree Protocol

- Cho phép cổng lên trạng thái forwarding ngay (không chờ 30 giây) – dùng cho thiết bị cuối

- Nếu có thiết bị gửi BPDU (vd: mini-switch), công sẽ “auto shutdown” để ngăn loop

! Trên các Switch Access

1. SWit

```
SWit#  
SWit#conf t  
SWit(config)#span  
SWit(config)#spanning-tree mode rapid-pvst  
SWit(config)#int range e0/1-e15/3  
SWit(config-if-range)#spanning-tree portfast  
SWit(config-if-range)#spanning-tree bpduguard enable
```

2. SWsale

```
SWsale#  
SWsale#conf t  
SWsale(config)#spanning-tree mode rapid-pvst  
SWsale(config)#int range e0/1-e15/3  
SWsale(config-if-range)#spanning-tree portfast  
SWsale(config-if-range)#spanning-tree bpduguard enable
```

3. SWmarketing

```
SWmarketing#  
SWmarketing#conf t  
SWmarketing(config)#spanning-tree mode rapid-pvst  
SWmarketing(config)#int range e0/1-e15/3  
SWmarketing(config-if-range)#spanning-tree portfast  
SWmarketing(config-if-range)#spanning-tree bpduguard enable
```

4. SWtaichinh

```
SWtaichinh#  
SWtaichinh#conf t  
SWtaichinh(config)#spanning-tree mode rapid-pvst  
SWtaichinh(config)#int range e0/1-e15/3  
SWtaichinh(config-if-range)#spanning-tree portfast  
SWtaichinh(config-if-range)#spanning-tree bpduguard enable
```

5. SWgiamdoc

```
SWgiamdoc#  
SWgiamdoc#conf t  
SWgiamdoc(config)#spanning-tree mode rapid-pvst  
SWgiamdoc(config)#int range e0/1-e15/3  
SWgiamdoc(config-if-range)#spanning-tree portfast  
SWgiamdoc(config-if-range)#spanning-tree bpduguard en  
SWgiamdoc(config-if-range)#spanning-tree bpduguard enable
```

3.2. Cấu hình Định tuyến và Dự phòng Lớp 3

3.2.1. Cấu hình Giao diện ảo chuyển mạch (SVI) và Định tuyến OSPF

Trên SWL3-5 và SWL3-45

Bash

! Kích hoạt định tuyến IP

SWL3-5(config)# ip routing

! Cấu hình SVI cho SWL3-5 (VLAN 10,20,30,...)

SWL3-5(config)#int g0/1.10

SWL3-5(config-subif)#encapsulation dot1Q 10

SWL3-5(config-subif)#ip add 10.10.0.2 255.255.255.0

SWL3-5(config-subif)#int g0/1.20

SWL3-5(config-subif)#encapsulation dot1Q 20

SWL3-5(config-subif)#ip add 10.20.0.2 255.255.255.0

SWL3-5(config-subif)#int g0/1.30

SWL3-5(config-subif)#encapsulation dot1Q 30

SWL3-5(config-subif)#ip add 10.30.0.2 255.255.255.0

SWL3-5(config-subif)#int g0/1.40

SWL3-5(config-subif)#encapsulation dot1Q 40

SWL3-5(config-subif)#ip add 10.40.0.2 255.255.255.0

SWL3-5(config-subif)#int g0/1.50

SWL3-5(config-subif)#encapsulation dot1Q 50

SWL3-5(config-subif)#ip add 10.50.0.2 255.255.255.0

SWL3-5(config-subif)#int g0/1.60

SWL3-5(config-subif)#encapsulation dot1Q 60

SWL3-5(config-subif)#ip add 10.60.0.2 255.255.255.0

```

SW13-5(config-subif)#int g0/1.70
SW13-5(config-subif)#encapsulation dot1Q 70
SW13-5(config-subif)#ip add 10.70.0.2 255.255.255.0
SW13-5(config-subif)#int g0/1.80
SW13-5(config-subif)#encapsulation dot1Q 80
SW13-5(config-subif)#ip add 10.80.0.2 255.255.255.0
SW13-5(config-subif)#int g0/1.90
SW13-5(config-subif)#encapsulation dot1Q 90
SW13-5(config-subif)#ip add 10.90.0.2 255.255.255.0

```

```

L 10.0.1.1/32 is directly connected, GigabitEthernet0/3
C 10.10.0.0/24 is directly connected, GigabitEthernet0/1.10
L 10.10.0.2/32 is directly connected, GigabitEthernet0/1.10
C 10.20.0.0/24 is directly connected, GigabitEthernet0/1.20
L 10.20.0.2/32 is directly connected, GigabitEthernet0/1.20
C 10.30.0.0/24 is directly connected, GigabitEthernet0/1.30
L 10.30.0.2/32 is directly connected, GigabitEthernet0/1.30
C 10.40.0.0/24 is directly connected, GigabitEthernet0/1.40
L 10.40.0.2/32 is directly connected, GigabitEthernet0/1.40
C 10.50.0.0/24 is directly connected, GigabitEthernet0/1.50
L 10.50.0.2/32 is directly connected, GigabitEthernet0/1.50
C 10.60.0.0/24 is directly connected, GigabitEthernet0/1.60
L 10.60.0.2/32 is directly connected, GigabitEthernet0/1.60
C 10.70.0.0/24 is directly connected, GigabitEthernet0/1.70
L 10.70.0.2/32 is directly connected, GigabitEthernet0/1.70
C 10.80.0.0/24 is directly connected, GigabitEthernet0/1.80

```

3. 8 Kết quả tạo SVI trên SW13-5

! Cấu hình SVI cho SW13-45 (VLAN 10,20,30,...)

```

SW13-45(config)#int g0/1.10
SW13-45(config-subif)#encapsulation dot1Q 10
SW13-45(config-subif)#ip add 10.10.0.3 255.255.255.0
SW13-45(config-subif)#int g0/1.20
SW13-45(config-subif)#encapsulation dot1Q 20
SW13-45(config-subif)#ip add 10.20.0.3 255.255.255.0
SW13-45(config-subif)#int g0/1.30
SW13-45(config-subif)#encapsulation dot1Q 30

```

```

SW13-45(config-subif)#ip add 10.30.0.3 255.255.255.0
SW13-45(config-subif)#int g0/1.40
SW13-45(config-subif)#encapsulation dot1Q 40
SW13-45(config-subif)#ip add 10.40.0.3 255.255.255.0
SW13-45(config-subif)#int g0/1.50
SW13-45(config-subif)#encapsulation dot1Q 50
SW13-45(config-subif)#ip add 10.50.0.3 255.255.255.0
SW13-45(config-subif)#int g0/1.60
SW13-45(config-subif)#encapsulation dot1Q 60
SW13-45(config-subif)#ip add 10.60.0.2 255.255.255.0
SW13-45(config-subif)#int g0/1.70
SW13-45(config-subif)#encapsulation dot1Q 70
SW13-45(config-subif)#ip add 10.70.0.3 255.255.255.0
SW13-45(config-subif)#int g0/1.80
SW13-45(config-subif)#encapsulation dot1Q 80
SW13-45(config-subif)#ip add 10.80.0.3 255.255.255.0
SW13-45(config-subif)#int g0/1.90
SW13-45(config-subif)#encapsulation dot1Q 90
SW13-45(config-subif)#ip add 10.90.0.3 255.255.255.0

```

```

10.30.0.2/32 is directly connected, GigabitEthernet0/1.30
10.40.0.0/24 is directly connected, GigabitEthernet0/1.40
10.40.0.2/32 is directly connected, GigabitEthernet0/1.40
10.50.0.0/24 is directly connected, GigabitEthernet0/1.50
10.50.0.2/32 is directly connected, GigabitEthernet0/1.50
10.60.0.0/24 is directly connected, GigabitEthernet0/1.60
10.60.0.2/32 is directly connected, GigabitEthernet0/1.60
10.70.0.0/24 is directly connected, GigabitEthernet0/1.70
10.70.0.2/32 is directly connected, GigabitEthernet0/1.70
10.80.0.0/24 is directly connected, GigabitEthernet0/1.80
10.80.0.2/32 is directly connected, GigabitEthernet0/1.80
10.90.0.0/24 is directly connected, GigabitEthernet0/1.90
10.90.0.2/32 is directly connected, GigabitEthernet0/1.90

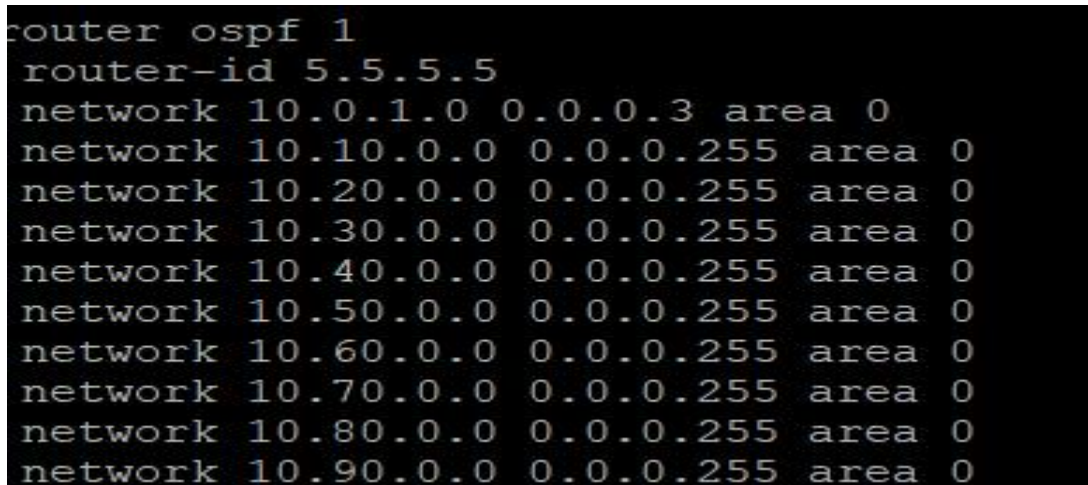
```

3. 9 Kết quả cấu hình SVI trên SW13-45

! Cấu hình OSPF

❖ SWL3-5

```
SWL3-5(config)#router ospf 1
SWL3-5(config-router)#router-id 5.5.5.5
SWL3-5(config-router)#net 10.10.0.0 0.0.0.255 area 0
SWL3-5(config-router)#net 10.20.0.0 0.0.0.255 area 0
SWL3-5(config-router)#net 10.30.0.0 0.0.0.255 area 0
SWL3-5(config-router)#net 10.40.0.0 0.0.0.255 area 0
SWL3-5(config-router)#net 10.50.0.0 0.0.0.255 area 0
SWL3-5(config-router)#net 10.60.0.0 0.0.0.255 area 0
SWL3-5(config-router)#net 10.70.0.0 0.0.0.255 area 0
SWL3-5(config-router)#net 10.80.0.0 0.0.0.255 area 0
SWL3-5(config-router)#net 10.90.0.0 0.0.0.255 area 0
```



```
router ospf 1
router-id 5.5.5.5
network 10.0.1.0 0.0.0.3 area 0
network 10.10.0.0 0.0.0.255 area 0
network 10.20.0.0 0.0.0.255 area 0
network 10.30.0.0 0.0.0.255 area 0
network 10.40.0.0 0.0.0.255 area 0
network 10.50.0.0 0.0.0.255 area 0
network 10.60.0.0 0.0.0.255 area 0
network 10.70.0.0 0.0.0.255 area 0
network 10.80.0.0 0.0.0.255 area 0
network 10.90.0.0 0.0.0.255 area 0
```

3. 10 Kết quả cấu hình OSPF trên SWL3-5

❖ SWL3-45

```
SWL3-45(config)#router ospf 1
SWL3-45(config-router)#router-id 4.5.4.5
SWL3-45(config-router)#net 10.10.0.0 0.0.0.255 area 0
SWL3-45(config-router)#net 10.20.0.0 0.0.0.255 area 0
SWL3-45(config-router)#net 10.30.0.0 0.0.0.255 area 0
SWL3-45(config-router)#net 10.40.0.0 0.0.0.255 area 0
SWL3-45(config-router)#net 10.50.0.0 0.0.0.255 area 0
SWL3-45(config-router)#net 10.60.0.0 0.0.0.255 area 0
SWL3-45(config-router)#net 10.70.0.0 0.0.0.255 area 0
SWL3-45(config-router)#net 10.80.0.0 0.0.0.255 area 0
SWL3-45(config-router)#net 10.90.0.0 0.0.0.255 area 0
```



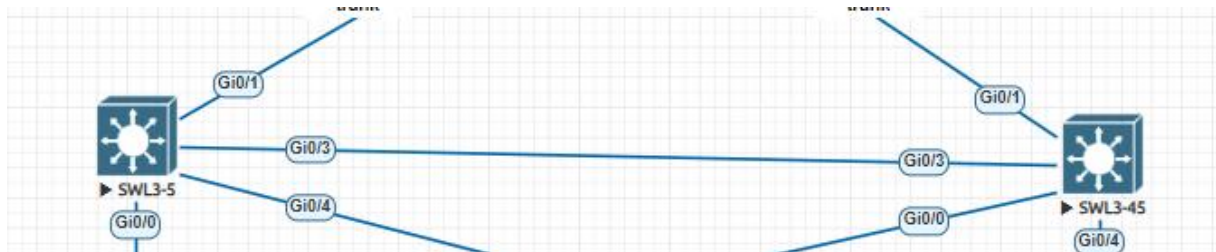
```
SW13-5(config-router)#net 10.0.1.0 0.0.0.255 area 0
SW13-45(config-router)#net 192.168.100.0 0.0.0.255 area 0
SW13-45(config-router)#net 192.168.50.0 0.0.0.255 area 0
SW13-45(config-router)#net 192.168.0.0 0.0.0.255 area 0
```

```
router ospf 1
router-id 4.5.4.5
network 10.0.1.0 0.0.0.3 area 0
network 10.10.0.0 0.0.0.255 area 0
network 10.20.0.0 0.0.0.255 area 0
network 10.30.0.0 0.0.0.255 area 0
network 10.40.0.0 0.0.0.255 area 0
network 10.50.0.0 0.0.0.255 area 0
network 10.60.0.0 0.0.0.255 area 0
network 10.70.0.0 0.0.0.255 area 0
```

3. 11 Kết quả cấu hình OSPF trên SWL3-45

3.2.2. Cấu hình HSRP

HSRP được cấu hình để cung cấp một gateway ảo, dự phòng.



3. 12 Sơ đồ HSRP (SWL3-5 chính)

! SWL3-5 (Active chính)

```
SW13-5(config)#int g0/1.10
SW13-5(config-subif)#standby 10 ip 10.10.0.1
SW13-5(config-subif)#standby 10 priority 110
SW13-5(config-subif)#standby 10 preempt
SW13-5(config)#int g0/1.20
SW13-5(config-subif)#standby 20 ip 10.20.0.1
SW13-5(config-subif)#standby 20 priority 110
```

SW13-5(config-subif)#standby 20 preempt
SW13-5(config)#int g0/1.30
SW13-5(config-subif)#standby 30 ip 10.30.0.1
SW13-5(config-subif)#standby 30 priority 110
SW13-5(config-subif)#standby 30 preempt
SW13-5(config)#int g0/1.40
SW13-5(config-subif)#standby 40 ip 10.40.0.1
SW13-5(config-subif)#standby 40 priority 110
SW13-5(config-subif)#standby 40 preempt
SW13-5(config)#int g0/1.50
SW13-5(config-subif)#standby 50 ip 10.50.0.1
SW13-5(config-subif)#standby 50 priority 110
SW13-5(config-subif)#standby 50 preempt
SW13-5(config)#int g0/1.60
SW13-5(config-subif)#standby 60 ip 10.60.0.1
SW13-5(config-subif)#standby 60 priority 110
SW13-5(config-subif)#standby 60 preempt
SW13-5(config)#int g0/1.70
SW13-5(config-subif)#standby 70 ip 10.70.0.1
SW13-5(config-subif)#standby 70 priority 110
SW13-5(config-subif)#standby 70 preempt
SW13-5(config)#int g0/1.80
SW13-5(config-subif)#standby 80 ip 10.80.0.1
SW13-5(config-subif)#standby 80 priority 110
SW13-5(config-subif)#standby 80 preempt
SW13-5(config)#int g0/1.90
SW13-5(config-subif)#standby 90 ip 10.90.0.1
SW13-5(config-subif)#standby 90 priority 110

SW13-5(config-subif)#standby 90 preempt

Xác minh:

Bash

SW13-5# show standby brief

```
SW13-5#show standby brief
                P indicates configured to preempt.
                |
Interface      Grp  Pri P State      Active      Standby      Virtual IP
Gi0/1.10       10   110 P Active local        unknown      10.10.0.1
Gi0/1.20       20   110 P Active local        unknown      10.20.0.1
Gi0/1.30       30   110 P Active local        unknown      10.30.0.1
Gi0/1.40       40   110 P Active local        unknown      10.40.0.1
Gi0/1.50       50   110 P Active local        unknown      10.50.0.1
Gi0/1.60       60   110 P Active local        unknown      10.60.0.1
Gi0/1.70       70   110 P Active local        unknown      10.70.0.1
Gi0/1.80       80   110 P Active local        unknown      10.80.0.1
Gi0/1.90       90   110 P Active local        unknown      10.90.0.1
```

3. 13 Kết quả cấu hình HSRP trên SW13-5

!SW13-45 (Standby):

Bash

SW13-45(config)#int g0/1.10

SW13-45(config-subif)#standby 10 ip 10.10.0.1

SW13-45(config-subif)#standby 10 priority 90

SW13-45(config-subif)#standby 10 preempt

SW13-45(config)#int g0/1.20

SW13-45(config-subif)#standby 20 ip 10.20.0.1

SW13-45(config-subif)#standby 20 priority 90

SW13-45(config-subif)#standby 20 preempt

SW13-45(config)#int g0/1.30

SW13-45(config-subif)#standby 30 ip 10.30.0.1

SW13-45(config-subif)#standby 30 priority 90

SW13-45(config-subif)#standby 30 preempt

SW13-45(config)#int g0/1.40

SW13-45(config-subif)#standby 40 ip 10.40.0.1

SW13-45(config-subif)#standby 40 priority 90

```
SW13-45(config-subif)#standby 40 preempt
SW13-45(config)#int g0/1.50
SW13-45(config-subif)#standby 50 ip 10.50.0.1
SW13-45(config-subif)#standby 50 priority 90
SW13-45(config-subif)#standby 50 preempt
SW13-45(config)#int g0/1.60
SW13-45(config-subif)#standby 60 ip 10.60.0.1
SW13-45(config-subif)#standby 60 priority 90
SW13-45(config-subif)#standby 60 preempt
SW13-45(config)#int g0/1.70
SW13-45(config-subif)#standby 70 ip 10.70.0.1
SW13-45(config-subif)#standby 70 priority 90
SW13-45(config-subif)#standby 70 preempt
SW13-45(config)#int g0/1.80
SW13-45(config-subif)#standby 80 ip 10.80.0.1
SW13-45(config-subif)#standby 80 priority 90
SW13-45(config-subif)#standby 80 preempt
SW13-45(config)#int g0/1.90
SW13-45(config-subif)#standby 90 ip 10.90.0.1
SW13-45(config-subif)#standby 90 priority 90
SW13-45(config-subif)#standby 90 preempt
```

Xác minh:

```
Bash
SW13-45# show standby brief
```

```
SWL3-45#show standby brief
          P indicates configured to preempt.
          |
Interface   Grp  Pri  P State   Active        Standby        Virtual IP
Gi0/1.10    10   90   P Active  local         unknown       10.10.0.1
Gi0/1.20    20   90   P Active  local         unknown       10.20.0.1
Gi0/1.30    30   90   P Active  local         unknown       10.30.0.1
Gi0/1.40    40   90   P Active  local         unknown       10.40.0.1
Gi0/1.50    50   90   P Active  local         unknown       10.50.0.1
Gi0/1.60    60   90   P Active  local         unknown       10.60.0.1
Gi0/1.70    70   90   P Active  local         unknown       10.70.0.1
Gi0/1.80    80   90   P Active  local         unknown       10.80.0.1
```

3. 14 Kết quả cấu hình HSRP trên SWL3-45

Giải thích:

standby 10 ip 10.10.0.1: Thiết lập HSRP group 10 với địa chỉ IP ảo là 10.10.0.1

standby 10 priority 110: Đặt priority cho SWL3-5 cao hơn (110 > 90) để nó được bầu làm Active.

standby 10 preempt: Cho phép router có priority cao hơn giành lại quyền Active.

3.3. Cấu hình Dịch vụ Mạng

3.3.1. Cấu hình DHCP Server và DHCP Relay

Trên DHCP Server (SWL3-5 và SWL3-45):

Bash

! Loại trừ các địa chỉ gateway

```
SWL3-5(config)# ip dhcp excluded-address 10.10.0.1 10.10.0.3
```

```
SWL3-5(config)# ip dhcp excluded-address 10.20.0.1 10.20.0.3
```

```
SWL3-5(config)# ip dhcp excluded-address 10.30.0.1 10.30.0.3
```

```
SWL3-5(config)# ip dhcp excluded-address 10.40.0.1 10.40.0.3
```

```
SWL3-5(config)# ip dhcp excluded-address 10.50.0.1 10.50.0.3
```

```
SWL3-5(config)# ip dhcp excluded-address 10.60.0.1 10.60.0.3
```

```
SWL3-5(config)# ip dhcp excluded-address 10.70.0.1 10.70.0.3
```

```
SWL3-5(config)# ip dhcp excluded-address 10.80.0.1 10.80.0.3
```

```
SWL3-5(config)# ip dhcp excluded-address 10.90.0.1 10.90.0.3
```

```

!
ng ip dhcp excluded-address 10.10.0.1 10.10.0.3
gi ip dhcp excluded-address 10.60.0.1 10.60.0.3
ip dhcp excluded-address 10.70.0.1 10.70.0.3
ly ip dhcp excluded-address 10.80.0.1 10.80.0.3
ip dhcp excluded-address 10.90.0.1 10.90.0.3
ip dhcp excluded-address 10.20.0.1 10.20.0.3
ia ip dhcp excluded-address 10.30.0.1 10.30.0.3
ip dhcp excluded-address 10.40.0.1 10.40.0.3
a ip dhcp excluded-address 10.50.0.1 10.50.0.3
!

```

3. 15 Kết quả cấu hình chặn cấp phát các ip của SWL3-5

! Tạo pool cho các vlan

```

SWL3-5(config)#ip dhcp pool it
SWL3-5(dhcp-config)#network 10.10.0.0 255.255.255.0
SWL3-5(dhcp-config)#default-router 10.10.0.1
SWL3-5(dhcp-config)#dns-server 8.8.8.8
SWL3-5(config)#ip dhcp pool sale
SWL3-5(dhcp-config)#network 10.20.0.0 255.255.255.0
SWL3-5(dhcp-config)#default-router 10.20.0.1
SWL3-5(dhcp-config)#dns-server 8.8.8.8
SWL3-5(dhcp-config)#ip dhcp pool marketing
SWL3-5(dhcp-config)#network 10.30.0.0 255.255.255.0
SWL3-5(dhcp-config)#default-router 10.30.0.1
SWL3-5(dhcp-config)#dns-server 8.8.8.8
SWL3-5(dhcp-config)#ip dhcp pool taichinh
SWL3-5(dhcp-config)#network 10.40.0.0 255.255.255.0
SWL3-5(dhcp-config)#default-router 10.40.0.0 255.255.255.0
SWL3-5(dhcp-config)#dns-server 8.8.8.8
SWL3-5(dhcp-config)#ip dhcp pool giamdoc
SWL3-5(dhcp-config)#network 10.50.0.0 255.255.255.0
SWL3-5(dhcp-config)#default-router 10.50.0.1

```

```
SWL3-5(dhcp-config)#dns-server 8.8.8.8
SWL3-5(dhcp-config)#ip dhcp pool printer
SWL3-5(dhcp-config)#network 10.60.0.0 255.255.255.0
SWL3-5(dhcp-config)#default-router 10.60.0.1
SWL3-5(dhcp-config)#dns-server 8.8.8.8
SWL3-5(dhcp-config)#ip dhcp pool wifi
SWL3-5(dhcp-config)#network 10.70.0.0 255.255.255.0
SWL3-5(dhcp-config)#default-router 10.70.0.1
SWL3-5(dhcp-config)#dns-server 8.8.8.8
SWL3-5(dhcp-config)#ip dhcp pool cam
SWL3-5(dhcp-config)#network 10.80.0.0 255.255.255.0
SWL3-5(dhcp-config)#default-router 10.80.0.1
SWL3-5(dhcp-config)#dns-server 8.8.8.8
SWL3-5(dhcp-config)#ip dhcp pool phone
SWL3-5(dhcp-config)#network 10.90.0.0 255.255.255.0
SWL3-5(dhcp-config)#default-router 10.90.0.1
SWL3-5(dhcp-config)#dns-server 8.8.8.8
```

```

!
ip dhcp pool taichinh
 network 10.40.0.0 255.255.255.0
 default-router 10.40.0.1
 dns-server 8.8.8.8
!
ip dhcp pool giamdoc
 network 10.50.0.0 255.255.255.0
 default-router 10.50.0.1
 dns-server 8.8.8.8
!
ip dhcp pool printer
 network 10.60.0.0 255.255.255.0
 default-router 10.60.0.1
 dns-server 8.8.8.8
!
ip dhcp pool wifi
 network 10.70.0.0 255.255.255.0
 default-router 10.70.0.1
 dns-server 8.8.8.8

```

3. 16 Kết quả tạo pool trên SWL3-5

Trên các SVI của Switch Phân phối (SWL3-5 và SWL3-45):

Bash

! Cấu hình DHCP Relay trên SVI

SWL3-5(config-subif)#int g0/1.10

SWL3-5(config-subif)#ip helper-address 10.10.0.2

SWL3-5(config-subif)#int g0/1.20

SWL3-5(config-subif)#ip helper-address 10.20.0.2

SWL3-5(config-subif)#int g0/1.30

SWL3-5(config-subif)#ip helper-address 10.30.0.2

SWL3-5(config-subif)#int g0/1.40

SWL3-5(config-subif)#ip helper-address 10.40.0.2

SWL3-5(config-subif)#int g0/1.50

SWL3-5(config-subif)#ip helper-address 10.50.0.2

SWL3-5(config-subif)#int g0/1.60

SWL3-5(config-subif)#ip helper-address 10.60.0.2

SWL3-5(config-subif)#int g0/1.70

SWL3-5(config-subif)#ip helper-address 10.70.0.2

SWL3-5(config-subif)#int g0/1.80

SWL3-5(config-subif)#ip helper-address 10.80.0.2

SWL3-5(config-subif)#int g0/1.90

SWL3-5(config-subif)#ip helper-address 10.90.0.2

```
interface GigabitEthernet0/1.20
 encapsulation dot1Q 20
 ip address 10.20.0.2 255.255.255.0
 ip helper-address 10.20.0.2
 standby 20 ip 10.20.0.1
 standby 20 priority 110
 standby 20 preempt
!
interface GigabitEthernet0/1.30
 encapsulation dot1Q 30
 ip address 10.30.0.2 255.255.255.0
 ip helper-address 10.30.0.2
 standby 30 ip 10.30.0.1
 standby 30 priority 110
 standby 30 preempt
!
interface GigabitEthernet0/1.40
 encapsulation dot1Q 40
 ip address 10.40.0.2 255.255.255.0
 ip helper-address 10.40.0.2
 standby 40 ip 10.40.0.1
--More--
```

3. 17 Kết quả cấu hình DHCP Relay của SWL3-5

! Cấu hình DHCP Relay trên SVI trên SWL3-45

SWL3-45(config)#int g0/1.10

SWL3-45(config-subif)#ip help

SWL3-45(config-subif)#ip helper-address 10.10.0.3

SWL3-45(config-subif)#int g0/1.20

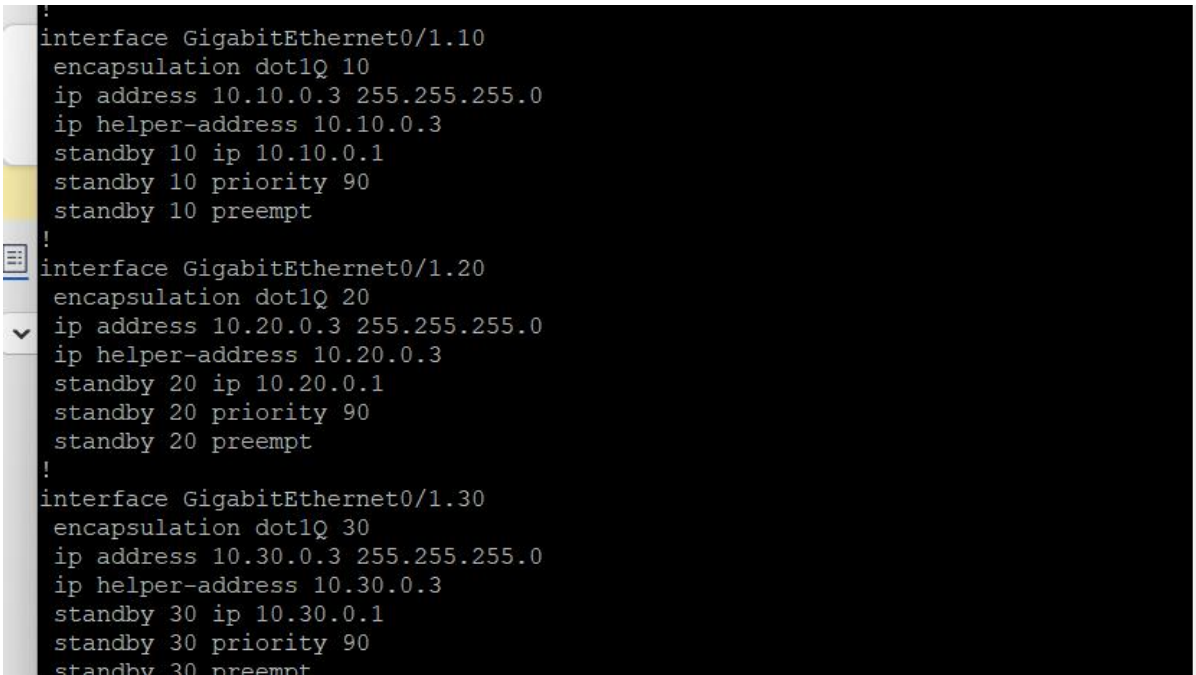
SWL3-45(config-subif)#ip helper-address 10.20.0.3

SWL3-45(config-subif)#int g0/1.30

```

SWL3-45(config-subif)#ip helper-address 10.30.0.3
SWL3-45(config-subif)#int g0/1.40
SWL3-45(config-subif)#ip helper-address 10.40.0.3
SWL3-45(config-subif)#int g0/1.50
SWL3-45(config-subif)#ip helper-address 10.50.0.3
SWL3-45(config-subif)#int g0/1.60
SWL3-45(config-subif)#ip helper-address 10.60.0.3
SWL3-45(config-subif)#int g0/1.70
SWL3-45(config-subif)#ip helper-address 10.70.0.3
SWL3-45(config-subif)#int g0/1.80
SWL3-45(config-subif)#ip helper-address 10.80.0.3
SWL3-45(config-subif)#int g0/1.90
SWL3-45(config-subif)#ip helper-address 10.90.0.3

```



```

!
interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 10.10.0.3 255.255.255.0
 ip helper-address 10.10.0.3
 standby 10 ip 10.10.0.1
 standby 10 priority 90
 standby 10 preempt
!
interface GigabitEthernet0/1.20
 encapsulation dot1Q 20
 ip address 10.20.0.3 255.255.255.0
 ip helper-address 10.20.0.3
 standby 20 ip 10.20.0.1
 standby 20 priority 90
 standby 20 preempt
!
interface GigabitEthernet0/1.30
 encapsulation dot1Q 30
 ip address 10.30.0.3 255.255.255.0
 ip helper-address 10.30.0.3
 standby 30 ip 10.30.0.1
 standby 30 priority 90
 standby 30 preempt
!

```

3. 18 Kết quả cấu hình DHCP Relay của SWL3-45

3.4. Cấu hình Firewall Cisco ASA

3.4.1. Cấu hình Giao diện, Vùng và Cấp độ An ninh

Bash

```
ciscoasa(config)# int g0/0
```

```
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# ip add 192.168.200.2
ciscoasa(config-if)# security-level 100
```

```
ciscoasa(config-if)# int g0/1
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# ip add 192.168.20.2
ciscoasa(config-if)# security-level 50
```

```
ciscoasa(config-if)# int g0/2
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip add 203.0.113.1
ciscoasa(config-if)# security-level 0
```

3.4.2. Cấu hình NAT (Object-based)

Sử dụng Object NAT để đơn giản hóa cấu hình.

Bash

! Tạo network object cho mạng nội bộ

```
ASA(config)# object network INTERNAL_NETS
```

```
ASA(config-network-object)# subnet 10.10.0.0 255.255.0.0
```

! Cấu hình Dynamic PAT cho mạng nội bộ ra Internet

```
ASA(config-network-object)# nat (inside,outside) dynamic interface
```

! Tạo network object cho Web Server trong DMZ

```
ASA(config)# object network WEB_SERVER_PRIVATE
```

```
ASA(config-network-object)# host <diachiip>
```

3.4.3. Cấu hình Access Control List (ACL)

ACL được áp dụng để thực thi ma trận chính sách truy cập đã thiết kế.

Bash

! ACL cho phép traffic từ Internet vào Web Server trong DMZ

```
ASA(config)# access-list OUTSIDE_IN extended permit tcp any host <diachiip> eq
www
```

```
ASA(config)# access-list OUTSIDE_IN extended permit tcp any host <diachiip> eq https
```

```
ASA(config)# access-group OUTSIDE_IN in interface outside
```

! ACL cho phép một số traffic từ DMZ vào Inside (ví dụ: truy cập DB)

! QUAN TRỌNG: Phải permit cả traffic từ DMZ ra Internet, nếu không sẽ bị chặn

```
ASA(config)# access-list DMZ_IN extended permit tcp host <DMZ_server_ip> host <DB_server_ip> eq 1433
```

```
ASA(config)# access-list DMZ_IN extended permit ip any any! Cho phép DMZ ra Internet
```

```
ASA(config)# access-group DMZ_IN in interface dmz
```

3.5. Cấu hình Giám sát Mạng

3.5.1. Cấu hình Syslog

Trên một thiết bị Cisco IOS (Router/Switch):

Bash

```
SWL3-5(config)#logging host 192.168.100.2
```

```
SWL3-5(config)#service timestamps log datetime msec
```

3.6 KIỂM THỬ VÀ ĐÁNH GIÁ

3.6.1. Xây dựng các Kịch bản Kiểm tra

Kịch bản 1: Kiểm tra kết nối và phân quyền truy cập liên VLAN.

Mục tiêu: Xác minh rằng các chính sách truy cập giữa các VLAN được thực thi đúng như trong Ma trận Chính sách (Bảng 2.2).

Phương pháp: Sử dụng các lệnh ping và telnet từ một máy trạm trong một VLAN đến các máy trạm/máy chủ trong các VLAN khác.

Từ một PC trong VP_IT (VLAN 10), ping đến một PC trong VP_TAI_CHINH (VLAN 40). Kết quả mong đợi: Thành công.

```
VPCS> ping 10.40.0.4
84 bytes from 10.40.0.4 icmp_seq=1 ttl=63 time=7.050 ms
84 bytes from 10.40.0.4 icmp_seq=2 ttl=63 time=3.069 ms
84 bytes from 10.40.0.4 icmp_seq=3 ttl=63 time=2.772 ms
84 bytes from 10.40.0.4 icmp_seq=4 ttl=63 time=3.562 ms
84 bytes from 10.40.0.4 icmp_seq=5 ttl=63 time=3.202 ms
```

3. 19 Lệnh ping từ VPC đến vlan sale

Từ một PC trong VP SALE (VLAN 20), telnet đến cổng 80 của Web Server trong DMZ (VLAN 100). Kết quả mong đợi: Thành công.

```
VPCS> ping 10.168.50.2
84 bytes from 10.168.50.2 icmp_seq=1 ttl=62 time=46.658 ms
84 bytes from 10.168.50.2 icmp_seq=2 ttl=62 time=19.105 ms
84 bytes from 10.168.50.2 icmp_seq=3 ttl=62 time=22.894 ms
84 bytes from 10.168.50.2 icmp_seq=4 ttl=62 time=22.299 ms
84 bytes from 10.168.50.2 icmp_seq=5 ttl=62 time=21.934 ms
```

3. 20 Lệnh ping từ VPC đến vùng DMZ

Kịch bản 2: Kiểm tra tính năng chuyển đổi dự phòng của HSRP (Failover).

Mục tiêu: Xác minh rằng khi switch phân phối Active gặp sự cố, switch Standby sẽ tiếp quản vai trò và duy trì kết nối cho người dùng.

Phương pháp: Tắt nguồn (hoặc tắt giao diện SVI) trên switch phân phối đang ở trạng thái Active. Quan sát sự thay đổi trạng thái HSRP và kiểm tra kết nối từ một máy trạm ra ngoài.

Lệnh kiểm tra: show standby brief trên cả hai switch phân phối, traceroute từ một PC đến một địa chỉ ngoài VLAN của nó.

```
SWL3-5#show standby brief
P indicates configured to preempt.
|
Interface    Grp  Pri P State  Active        Standby        Virtual IP
Gi0/1.10     10   110 P Active local        10.10.0.3      10.10.0.1
Gi0/1.20     20   110 P Active local        10.20.0.3      10.20.0.1
Gi0/1.30     30   110 P Active local        10.30.0.3      10.30.0.1
Gi0/1.40     40   110 P Active local        10.40.0.3      10.40.0.1
Gi0/1.50     50   110 P Active local        10.50.0.3      10.50.0.1
Gi0/1.60     60   110   Active local        10.60.0.3      10.60.0.1
Gi0/1.70     70   110 P Active local        10.70.0.3      10.70.0.1
Gi0/1.80     80   110 P Active local        10.80.0.3      10.80.0.1
Gi0/1.90     90   110 P Active local        10.90.0.3      10.90.0.1
```

3. 21 Kiểm tra trạng thái của HSRP trên SWL3-5

```
SWL3-45#show standby brief
P indicates configured to preempt.
|
Interface    Grp  Pri P State    Active        Standby        Virtual IP
Gi0/1.10     10   90  P Standby  10.10.0.2     local          10.10.0.1
Gi0/1.20     20   90  P Standby  10.20.0.2     local          10.20.0.1
Gi0/1.30     30   90  P Standby  10.30.0.2     local          10.30.0.1
Gi0/1.40     40   90  P Standby  10.40.0.2     local          10.40.0.1
Gi0/1.50     50   90  P Standby  10.50.0.2     local          10.50.0.1
Gi0/1.60     60   90  P Standby  10.60.0.2     local          10.60.0.1
Gi0/1.70     70   90  P Standby  10.70.0.2     local          10.70.0.1
Gi0/1.80     80   90  P Standby  10.80.0.2     local          10.80.0.1
Gi0/1.90     90   90  P Standby  10.90.0.2     local          10.90.0.1
SWL3-45#
```

3. 22 Kiểm tra trạng thái của HSRP trên SWL3-45 khi SWL3-5 hoạt động

```
SWL3-45#show standby brief
P indicates configured to preempt.
|
Interface    Grp  Pri P State    Active        Standby        Virtual IP
Gi0/1.10     10   90  P Active   local          unknown        10.10.0.1
Gi0/1.20     20   90  P Active   local          unknown        10.20.0.1
Gi0/1.30     30   90  P Active   local          unknown        10.30.0.1
Gi0/1.40     40   90  P Active   local          unknown        10.40.0.1
Gi0/1.50     50   90  P Active   local          unknown        10.50.0.1
Gi0/1.60     60   90  P Active   local          unknown        10.60.0.1
Gi0/1.70     70   90  P Active   local          unknown        10.70.0.1
Gi0/1.80     80   90  P Active   local          unknown        10.80.0.1
Gi0/1.90     90   90  P Active   local          unknown        10.90.0.1
SWL3-45#
```

3. 23 Trạng thái HSRP của SWL3-45 khi SWL3-5 tắt

Kịch bản 3: Kiểm tra chính sách Firewall ASA.

Mục tiêu: Xác minh các quy tắc NAT và ACL trên firewall hoạt động chính xác.

Phương pháp:

Từ một máy ảo giả lập bên ngoài Internet, thử truy cập vào địa chỉ IP public của Web Server trong DMZ. Kết quả mong đợi: Thành công.

Từ Internet, thử truy cập vào một địa chỉ IP nội bộ bất kỳ. Kết quả mong đợi: Thất bại.

Từ một máy chủ trong DMZ, thử ping đến một máy chủ trong vùng inside. Kết quả mong đợi: Thất bại.

3.6.2. Thực thi và Phân tích Kết quả

Ví dụ phân tích Kịch bản 2 (HSRP Failover):

Trạng thái ban đầu:

* Phân tích: SWL3-5 đang là Active cho tất cả các VLAN do có priority cao hơn (110 > 90).

Thực hiện sự cố: Tắt SWL3-5

Trạng thái sau sự cố:

Trên SWL3-45, log hệ thống hiển thị:

SWL3-45# show standby brief

```
SWL3-45#show standby brief
P indicates configured to preempt.
|
Interface    Grp  Pri P State  Active      Standby      Virtual IP
Gi0/1.10     10   90  P Active local      unknown     10.10.0.1
Gi0/1.20     20   90  P Active local      unknown     10.20.0.1
Gi0/1.30     30   90  P Active local      unknown     10.30.0.1
Gi0/1.40     40   90  P Active local      unknown     10.40.0.1
Gi0/1.50     50   90  P Active local      unknown     10.50.0.1
Gi0/1.60     60   90  P Active local      unknown     10.60.0.1
Gi0/1.70     70   90  P Active local      unknown     10.70.0.1
Gi0/1.80     80   90  P Active local      unknown     10.80.0.1
Gi0/1.90     90   90  P Active local      unknown     10.90.0.1
SWL3-45#
```

3. 24 Kết quả của câu lệnh show standby brief trên SWL3-45

VPC > trace 10.10.0.1

```
VPCS> trace 10.10.0.1
Trace to 10.10.0.1, 8 hops max, press Ctrl+C to stop
 1  *10.10.0.3  3.431 ms (ICMP type:3, code:3, Destination port unreachable)
*
```

3. 25 Kết quả ping trace 10.10.0.1

* Phân tích: Ngay sau khi SWL3-5 gặp sự cố, SWL3-45 đã chuyển sang trạng thái Active. Lệnh trace từ VPC xác nhận rằng lưu lượng giờ đây được định tuyến qua gateway 10.10.0.3 (địa chỉ IP của SWL3-45). Kết nối của người dùng được duy trì liên tục.

3.6.3. Đánh giá Tổng thể

Về Hiệu năng: Việc sử dụng Switch Layer 3 cho định tuyến liên VLAN cho các liên kết trunk đã tạo ra một "xương sống" mạng nội bộ có thông lượng cao. Trong quá trình kiểm thử, không ghi nhận hiện tượng nghẽn mạng hay độ trễ bất thường. Các luồng

traffic giữa các VLAN được xử lý ở tốc độ phần cứng, đáp ứng tốt yêu cầu của một doanh nghiệp quy mô trung bình.

Về Tính sẵn sàng: Hệ thống đã chứng tỏ khả năng chịu lỗi cao. Sự kết hợp giữa HSRP (cho gateway) đã loại bỏ các điểm lỗi duy nhất tại lớp phân phối và lớp truy cập. Đặc biệt, việc triển khai HSRP cho thấy một thiết kế dự phòng thông minh, có khả năng phản ứng với các sự cố gián tiếp, đảm bảo thời gian chết được giảm thiểu tối đa và quá trình chuyển đổi dự phòng diễn ra một cách minh bạch đối với người dùng cuối.

Về Mức độ An toàn: Hệ thống đã triển khai một chiến lược bảo mật đa lớp hiệu quả:

Lớp vành đai: Firewall ASA với các vùng bảo mật và chính sách NAT/ACL chặt chẽ đã cô lập hiệu quả mạng nội bộ khỏi các mối đe dọa từ Internet và kiểm soát chặt chẽ luồng truy cập vào vùng DMZ.

Lớp phân phối: Các ACL trên SVI đã thực thi thành công việc phân quyền truy cập giữa các phòng ban, ngăn chặn sự di chuyển ngang trái phép trong mạng nội bộ.

KẾT LUẬN

✧ Tổng kết Kết quả Đạt được

1. Xây dựng thành công một mô hình mạng hoàn chỉnh, có khả năng mở rộng và bảo mật cao: Đồ án đã thiết kế và triển khai một kiến trúc mạng phân cấp 3 lớp (Core/Distribution/Access) theo chuẩn công nghiệp. Việc sử dụng VLAN để phân đoạn mạng, Switch Layer 3 để định tuyến hiệu năng cao, và các cơ chế dự phòng như HSRP đã tạo ra một nền tảng vững chắc, đáp ứng được các yêu cầu về hiệu năng, tính sẵn sàng và khả năng mở rộng của một doanh nghiệp đang phát triển.
2. **Triển khai chi tiết và thành công các công nghệ mạng cốt lõi:** Các công nghệ nền tảng đã được cấu hình và kiểm chứng hoạt động một cách chính xác. Cụ thể:
 - **VLAN và Inter-VLAN Routing:** Đã phân chia thành công mạng thành các VLAN riêng biệt cho từng phòng ban, các thiết bị và cấu hình định tuyến liên VLAN hiệu quả bằng SVI trên Switch Layer 3.
 - **Tính sẵn sàng cao (High Availability):** Đã triển khai thành công HSRP kết hợp Interface Tracking, đảm bảo gateway luôn sẵn sàng và có khả năng chuyển đổi dự phòng thông minh.
 - **Bảo mật đa lớp:** Đã thiết lập thành công các chính sách bảo mật từ vành đai vào trong. Firewall ASA kiểm soát chặt chẽ traffic ra vào Internet và vùng DMZ. ACL trên SVI phân quyền truy cập giữa các phòng ban. Dịch vụ mạng: Đã cấu hình thành công DHCP Server cấp phát IP động cho các VLAN khác nhau thông qua DHCP Relay.
 - **Thực hiện kiểm thử và đánh giá khoa học:** Các kịch bản kiểm thử được xây dựng và thực thi đã xác minh tính đúng đắn của toàn bộ thiết kế. Kết quả cho thấy hệ thống hoạt động ổn định, các cơ chế dự phòng chuyển đổi liền mạch và các chính sách bảo mật được thực thi hiệu quả, đúng như mong đợi.
 - **Đề xuất một mô hình tham khảo có giá trị thực tiễn:** Mô hình được xây dựng trong đồ án không chỉ là một bài tập lý thuyết mà còn là một thiết kế mẫu, tuân thủ các thực tiễn tốt nhất (best practices). Nó có thể được sử dụng làm tài liệu tham khảo, tùy chỉnh và áp dụng cho các doanh nghiệp có quy mô và nhu cầu tương tự.

✧ Tự đánh giá

■ Ưu điểm

- ◆ Thiết kế toàn diện và tuân thủ chuẩn: Mô hình mạng được xây dựng dựa trên kiến trúc phân cấp đã được kiểm chứng, kết hợp hài hòa giữa các công nghệ để giải quyết các bài toán cụ thể về hiệu năng, bảo mật và độ sẵn sàng.
- ◆ Tư duy thiết kế có hệ thống: Đồ án đã thể hiện được mối liên kết nhân quả giữa các quyết định thiết kế. Ví dụ, việc dùng VLAN dẫn đến nhu cầu định tuyến, và việc định tuyến lại dẫn đến nhu cầu dùng ACL để kiểm soát. Tương tự, nhu cầu dự phòng được giải quyết bằng một hệ thống gồm HSRP và EtherChannel, chứ không phải các tính năng riêng lẻ.

- ◆ **Chú trọng bảo mật theo chiều sâu:** An ninh mạng được xem xét ở nhiều lớp, từ vành đai (Firewall), đến lớp phân phối (ACL) tạo ra một hệ thống phòng thủ vững chắc.
- ◆ **Tính thực tiễn và khả năng áp dụng:** Việc sử dụng công cụ giả lập EVE-NG với các hệ điều hành thật của thiết bị đảm bảo rằng các cấu hình và kết quả kiểm thử có độ chính xác cao, có thể được áp dụng trực tiếp vào môi trường thực tế.

■ **Nhược điểm**

- ◆ **Chưa tích hợp mạng không dây (Wireless LAN):** Mạng không dây là một phần không thể thiếu trong các doanh nghiệp hiện đại. Mô hình hiện tại mới chỉ tập trung vào mạng có dây.
- ◆ **Thiếu giải pháp truy cập từ xa (Remote Access):** Nhu cầu làm việc từ xa ngày càng tăng, đòi hỏi phải có các giải pháp truy cập an toàn vào mạng nội bộ như VPN.
- ◆ **Chưa triển khai IPv6:** Hệ thống vẫn đang hoạt động hoàn toàn trên nền tảng IPv4. Trong bối cảnh địa chỉ IPv4 đang cạn kiệt, việc sẵn sàng cho IPv6 là một yêu cầu quan trọng.
- ◆ **Chưa có chính sách Chất lượng Dịch vụ (QoS):** Hệ thống chưa có cơ chế ưu tiên cho các loại traffic nhạy cảm với độ trễ như thoại (VoIP) hay hội nghị truyền hình (Video Conference), có thể ảnh hưởng đến trải nghiệm người dùng khi mạng có tải cao.
- ◆ **Chưa triển khai STP** để tăng khả năng dự phòng đường truyền nhưng do kinh phí hạn hẹp và quy mô trung bình nên chưa cần thiết cấu hình
- ◆ **Chưa có dự phòng cho sw47** nhưng sw47 có thể thay thế dễ dàng khi bị hỏng nên khi sw47 trục trặc chúng ta có thể thay thế ngay thiết bị mới

✧ **Hướng Phát triển Tương lai**

- ◆ **Tích hợp mạng không dây (Wireless LAN):** Triển khai các điểm truy cập (Access Points) và một bộ điều khiển mạng không dây (Wireless LAN Controller - WLC). Thiết kế các SSID riêng biệt cho nhân viên và khách, trong đó SSID của nhân viên được xác thực qua máy chủ RADIUS (sử dụng chuẩn 802.1X) để tăng cường bảo mật, còn SSID của khách được đặt trong một VLAN riêng và bị cô lập hoàn toàn với mạng nội bộ.
- ◆ **Triển khai giải pháp truy cập từ xa an toàn (VPN):** Cấu hình VPN trên firewall ASA để cho phép nhân viên làm việc từ xa có thể kết nối an toàn vào mạng nội bộ. Có thể triển khai cả hai loại: IPsec Site-to-Site VPN để kết nối các chi nhánh và SSL/TLS Remote Access VPN (ví dụ: Cisco AnyConnect) cho người dùng cá nhân.

- ◆ **Xây dựng hệ thống hoạt động song song với IPv6 (Dual-stack):** Cấu hình song song cả địa chỉ IPv4 và IPv6 trên tất cả các giao diện của router, switch L3 và máy chủ. Triển khai định tuyến cho IPv6 (ví dụ: OSPFv3) và các dịch vụ mạng tương ứng (DHCPv6, SLAAC). Việc này giúp doanh nghiệp sẵn sàng cho quá trình chuyển đổi sang IPv6 một cách liền mạch. HSRP cho IPv6 cũng cần được triển khai để đảm bảo tính dự phòng.
- ◆ **Triển khai Chất lượng Dịch vụ (QoS):** Phân tích các loại traffic trong mạng, sau đó xây dựng và áp dụng các chính sách QoS. Sử dụng các cơ chế như phân loại (classification), đánh dấu (marking), xếp hàng (queuing), và kiểm soát tắc nghẽn (congestion avoidance) để ưu tiên băng thông và giảm độ trễ cho các ứng dụng quan trọng như VoIP và Video Conference, đảm bảo chất lượng dịch vụ ngay cả khi mạng bận rộn.

TÀI LIỆU THAM KHẢO

- [1] Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks (5th ed.). Prentice Hall.
- [2] Cisco Networking Academy. (2020). CCNA 200-301 Official Cert Guide, Volume 1 & 2. Cisco Press.
- [3] Cisco. (2023). Cisco ASA Series General Operations CLI Configuration Guide.
- [4] Cisco. (2023). IP Routing: HSRP Configuration Guide, Cisco IOS XE.
- [5] Internet Engineering Task Force. (2010). RFC 5798: Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6.
- [6] EVE-NG Ltd. (2024). EVE-NG Documentation. Retrieved from <https://www.eve-ng.net/index.php/documentation/>
- [7] Pluralsight. (2021). Access Control List (ACL) Concepts.
- [8] NetworkLessons. (n.d.). HSRP (Hot Standby Routing Protocol).
- [9] PracticalNetworking.net. (n.d.). Cisco ASA NAT.
- [10] Zytrax, Inc. (n.d.). BIND for the Small LAN - Views.
- [11] Why do we prefer using SW layer 3 than Router in Inter-Vlan Routing?
- [12] Inter-VLAN Routing: Ultimate Configuration Guide for Cisco
- [13] Hot Standby Router Protocol (HSRP) | NetworkAcademy.io
- [14] The Ultimate Comparison Guide - FHRP Shootout: HSRP vs. VRRP vs. GLBP
- [15] 30 Days Coding
- [16] Configure DHCP Server Cisco | ManageEngine
- [17] DHCP Relay Agent - IOS | Network Command Reference
- [18] ASA security levels explained | CCNA Security#
- [19] Your Ultimate NAT Configuration Guide for Cisco ASA
- [20] ASA Implicit Rule “Permit all traffic to less secure networks” ACL « DANIEL KUCHENSKI
- [21] Reflexive Access List
- [22] Time based Access-List - GeeksforGeeks
- [23] ACL placement? - Cisco Community