

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



HUỲNH MINH PHƯỚC - 52100465

**BÁO CÁO CUỐI KÌ
MẠNG MÁY TÍNH NÂNG CAO**

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2025

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



HUỲNH MINH PHƯỚC - 52100465

BÁO CÁO CUỐI KÌ MẠNG MÁY TÍNH NÂNG CAO

Người hướng dẫn
Thầy Lê Viết Thanh

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2025

LỜI CẢM ƠN

Trước tiên, em xin gửi lời cảm ơn chân thành và lòng biết ơn sâu sắc đến thầy Lê Viết Thanh. Thầy là người đã luôn hỗ trợ và hướng dẫn tận tình cho em trong suốt quá trình nghiên cứu và hoàn thành bài nghiên cứu.

Em xin được dành lời cảm ơn chân thành cho khoa Công Nghệ Thông Tin đã cho em được tiếp cận môn mạng máy tính nâng cao mà theo em là vô cùng cần thiết.

Em đã nỗ lực và cố gắng tích lũy những kiến thức mà thầy đã truyền đạt trong suốt một học kỳ vừa qua để hoàn thành được bài báo cáo một cách hoàn thiện nhất trong khả năng của em. Nếu có xảy ra sai sót gì, em rất mong nhận được sự góp ý của thầy để em có thể hoàn thiện bản thân hơn ở những lần tiếp theo.

Em xin chân thành cảm ơn, xin chúc những điều tốt đẹp nhất sẽ luôn đồng hành cùng mọi người.

TP. Hồ Chí Minh, ngày 11 Tháng 5 năm 2025

Tác giả

(Ký tên và ghi rõ họ tên)

Phước

Huỳnh Minh Phước

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

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

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

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

TP. Hồ Chí Minh, ngày 11 tháng 5 năm 2025.

Tác giả

(Ký tên và ghi rõ họ tên)

Phước

Huỳnh Minh Phước

KIỂM TRA CUỐI KỲ

TÓM TẮT

Báo cáo trình bày quá trình triển khai một mô hình mạng dựa trên các yêu cầu cấu hình được cung cấp. Hệ thống bao gồm khu vực HQ và Branch, sử dụng các giao thức định tuyến EIGRP và OSPF cho cả IPv4 và IPv6, kết hợp với các dịch vụ mạng như DHCP, DHCPv6, NAT, VLAN, VTP, EtherChannel. Ngoài ra, các kỹ thuật bảo mật cơ bản như ACL để chặn truy cập trái phép, xác thực SSH theo VLAN, và cấu hình tunnel GRE cũng được thực hiện. Tất cả cấu hình được kiểm thử trên Cisco Packet Tracer nhằm đảm bảo tính đúng đắn và đáp ứng yêu cầu đề bài.

KIỂM TRA CUỐI KỲ

ABSTRACT

This report presents the implementation of an network model based on predefined configuration requirements. The network consists of HQ and Branch areas, utilizing EIGRP and OSPF protocols for both IPv4 and IPv6. Network services such as DHCP, DHCPv6, NAT, VLAN, VTP, and EtherChannel are configured accordingly. In addition, basic security mechanisms—including access control lists (ACLs), SSH access restrictions by VLAN, and GRE tunneling—are implemented. All configurations are tested using Cisco Packet Tracer to ensure correct functionality and full compliance with the given specifications.

MỤC LỤC

DANH MỤC HÌNH VẼ	viii
DANH MỤC BẢNG BIỂU	x
DANH MỤC CÁC CHỮ VIẾT TẮT.....	xii
CHƯƠNG 1. MỞ ĐẦU VÀ TỔNG QUAN ĐỀ TÀI.....	1
1.1 Giới thiệu đề tài.....	1
1.2 Mục tiêu thực hiện đề tài.....	1
CHƯƠNG 2. CƠ SỞ LÝ THUYẾT.....	2
2.1 Địa chỉ ipv4 và ipv6	2
2.1.1 Địa chỉ ipv4.....	2
2.1.2 Địa chỉ ipv6.....	2
2.2 Giao thức định tuyến.....	2
2.2.1 EIGRP (<i>Enhanced Interior Gateway Routing Protocol</i>).....	2
2.2.2 OSPF (<i>Open Shortest Path First</i>).....	3
2.3 Giao thức PPP (Point-to-Point Protocol)	4
2.4 GRE Tunnel (Generic Routing Encapsulation)	4
2.5 NAT và DHCP	5
2.5.1 NAT (<i>Network Address Translation</i>)	5
2.5.2 DHCP (<i>Dynamic Host Configuration Protocol</i>)	6
2.6 Chuyển mạch và EtherChannel.....	7
2.6.1 Chuyển mạch và VLAN.....	7
2.6.2 Spanning Tree Protocol (STP) và Rapid PVST+.....	7
2.6.3 EtherChannel với LACP	8

2.7 DHCPv6 và Relay Agent	8
2.7.1 <i>Stateless DHCPv6</i>	8
2.7.2 <i>Relay Agent</i>	8
CHƯƠNG 3. MÔ HÌNH ĐỀ XUẤT	9
3.1 Mô hình tổng thể (HQ và Branch)	9
3.2 Sơ đồ địa chỉ IP khu vực HQ	10
3.2.1 <i>Sơ đồ Ipv4</i>	10
3.2.2 <i>Sơ đồ Ipv6</i>	13
3.3 Sơ đồ địa chỉ IP khu vực Branch.....	16
3.3.1 <i>Sơ đồ Ipv4</i>	16
3.4 Phân bổ địa chỉ ip cho khu vực HQ	18
3.4.1 <i>Phân bổ địa chỉ ipv4</i>	18
3.4.2 <i>Phân bổ địa chỉ ipv6</i>	20
3.5 Phân bổ địa chỉ cho khu vực Branch.....	21
3.5.1 <i>Phân bổ địa chỉ ipv4</i>	21
CHƯƠNG 4. CẤU HÌNH	23
4.1 Kết nối PPP	23
4.1.1 <i>Xác thực PAP</i>	23
4.1.2 <i>Xác thực CHAP</i>	25
4.2 Tunneling GRE	27
4.3 Định tuyến.....	28
4.3.1 <i>Định tuyến ipv4</i>	28
4.3.2 <i>Định tuyến ipv6</i>	36

4.4 Chuyển mạch.....	38
4.4.1 Cấu hình VTP và VLAN.....	38
4.4.2 Cấu hình giao thức Spanning Tree	39
4.4.3 VLAN quản lý và truy cập SSH.....	40
4.4.4 Router-on-a-Stick – Kết nối giữa các VLAN.....	41
4.4.5 Cấu hình EtherChannel với LACP	42
4.5 NAT và DHCP	44
4.5.1 Cấu hình NAT	44
4.5.2 Cấu hình Port Forwarding cho HTTPS và HTTP	45
4.5.3 Cấu hình DHCP ipv4.....	46
4.5.4 Cấu hình DHCP ipv6.....	47
4.6 Các yêu khác ở ipv4.....	49
4.6.1 Chặn truy cập nội bộ từ VLAN GUEST.....	49
4.6.2 giới hạn truy cập SSH vào các switch ngoại trừ VLAN SERVERS	50
CHƯƠNG 5. KẾT LUẬN.....	52
5.1 Kết luận	52
5.2 Hướng phát triển	52
TÀI LIỆU THAM KHẢO	53

DANH MỤC HÌNH VẼ

Hình 2.1 Kỹ thuật NAT.....	5
Hình 2.2 Giao thức DHCP	6
Hình 3.1 Mô hình mạng	10
Hình 4.1 Kết quả trạng thái cổng serial trên R6 và R7	24
Hình 4.2 Kết quả ping từ R6 đến R7 sau khi thiết lập PAP.....	24
Hình 4.3 Kết quả trạng thái cổng serial trên R6 và R7	26
Hình 4.4 Kết quả trạng ping từ R7 đến R8 sau khi cấu hình CHAP	26
Hình 4.5 Bảng định tuyến tunnel giữa R6 và R8	28
Hình 4.6 Kết quả ping ip tunnel từ R6 đến R8	28
Hình 4.7 Kết quả bảng định tuyến eigrp trên R4	31
Hình 4.8 Eigrp neighbor trên router R7	32
Hình 4.9 Kết quả bảng định tuyến ospf trên R1.....	34
Hình 4.10 ospf neighbor trên router R1	34
Hình 4.11 Kết quả bảng định tuyến trên R5 và R2 sau khi redistribution	36
Hình 4.12 Kết quả bảng định tuyến ipv6 trên R5	38
Hình 4.13 Danh sách các vlan được tạo trên S1	39
Hình 4.14 Spanning tree trên switch S1	40
Hình 4.15 Kết quả tạo và gán ip vlan sub interface trên R4	42
Hình 4.16 Kết quả etherchannel trên switch S1	44
Hình 4.17 NAT trên router ACCESS.....	45
Hình 4.18 Kết quả chuyển tiếp cổng http và https	46
Hình 4.19 Kết quả cấp phát dhcp ipv4 trên máy tính vlan 10	47

Hình 4.20 Kết quả cấp phát dhcp ipv6 trên máy tính vlan 40	49
Hình 4.21 Kết quả chặn truy cập vlan guest trong nội bộ.....	50
Hình 4.22 Kết quả thực hiện giới truy cập SSH ngoại trừ vlan servers.....	51

DANH MỤC BẢNG BIỂU

Bảng 3.1 Sơ đồ ipv4 cho các vlan ở khu vực HQ	12
Bảng 3.2 Sơ đồ ipv4 cho kết nối giữa các router	13
Bảng 3.3 Sơ đồ ipv6 cho các vlan	14
Bảng 3.4 Sơ đồ ipv6 cho kết nối các router	15
Bảng 3.5 Sơ đồ ipv6 cho kết nối mạng LAN R6 và R8.....	15
Bảng 3.6 Sơ đồ ip cho các loopback ở khu vực Branch	17
Bảng 3.7 Bảng địa chỉ ipv4 khu vực HQ	19
Bảng 3.8 Bảng địa chỉ ipv6 khu vực HQ	21
Bảng 3.9 Bảng địa chỉ ipv4 khu vực Branch	22
Bảng 4.1 Lệnh cấu hình PAP trên R6 và R7.....	23
Bảng 4.2 Lệnh cấu hình CHAP trên R7 và R8	25
Bảng 4.3 Lệnh cấu hình Tunnel GRE trên R6 và R8.....	27
Bảng 4.4 Lệnh cấu hình định tuyến eigrp trên R4	29
Bảng 4.5 Lệnh cấu hình định tuyến ospf trên R3.....	32
Bảng 4.6 Lệnh cấu hình redistribution ospf eigrp trên R5	35
Bảng 4.7 Lệnh cấu hình eigrp ipv6 cho sub interface trên R4.....	37
Bảng 4.8 Lệnh cấu hình eigrp ipv6 trên r5	37
Bảng 4.9 Lệnh cấu hình ssh trên các switch	41
Bảng 4.10 Lệnh cấu hình router on a stick trên R4.....	41
Bảng 4.11 Kết nối port channel.....	42
Bảng 4.12 Lệnh cấu hình ether channel trên switch S1	43
Bảng 4.13 Lệnh cấu hình dhcp ipv4 cho vlan 10.....	47

Bảng 4.14	Lệnh cấu hình chặn truy cập nội bộ từ VLAN GUEST	49
Bảng 4.15	Lệnh cấu hình giới giới hạn truy cập SSH vào các switch	50

DANH MỤC CÁC CHỮ VIẾT TẮT

ACL	Access Control List
CHAP	Challenge Handshake Authentication Protocol
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DNS	Domain Name System
EIGRP	Enhanced Interior Gateway Routing Protocol
GRE	Generic Routing Encapsulation
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
NAT	Network Address Translation
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PPP	Point-to-Point Protocol
SSH	Secure Shell
STP	Spanning Tree Protocol
VLAN	Virtual Local Area Network
SLAAC	Stateless Address Autoconfiguration

CHƯƠNG 1. MỞ ĐẦU VÀ TỔNG QUAN ĐỀ TÀI

1.1 Giới thiệu đề tài

Trong thời đại số hóa hiện nay, hệ thống mạng máy tính đóng vai trò trọng yếu trong việc kết nối, truyền tải dữ liệu và đảm bảo sự vận hành liên tục của các tổ chức, doanh nghiệp. Một hệ thống mạng hiệu quả không chỉ giúp tối ưu hóa nguồn lực mà còn hỗ trợ quản lý, chia sẻ thông tin một cách nhanh chóng và bảo mật.

Đề tài này tập trung vào việc thiết kế và cấu hình một hệ thống mạng hoàn chỉnh cho một tổ chức gồm hai khu vực chính: Trụ sở chính (HQ) và Chi nhánh (Branch). Hệ thống bao gồm cả địa chỉ IPv4 và IPv6, các công nghệ định tuyến (EIGRP, OSPF), cấu hình kết nối WAN bằng PPP (PAP/CHAP), thiết lập NAT, DHCP, chuyển mạch (EtherChannel, STP), và phân phối địa chỉ cho các VLAN.

1.2 Mục tiêu thực hiện đề tài

- Thiết kế sơ đồ địa chỉ mạng chi tiết cho trụ sở chính và chi nhánh, bao gồm phân chia subnet, địa chỉ gateway, và IP cho các máy chủ trong từng VLAN.
- Cấu hình các router kết nối WAN bằng PPP với các phương thức xác thực PAP và CHAP.
- Cấu hình giao thức định tuyến EIGRP cho HQ, OSPF cho chi nhánh và phân phối tuyến giữa hai miền định tuyến.
- Triển khai chuyển mạch lớp 2, sử dụng Rapid PVST+ và cấu hình EtherChannel với giao thức LACP.
- Cấu hình DHCP server và NAT Overload để cấp phát địa chỉ và truy cập Internet cho toàn mạng.
- Triển khai địa chỉ IPv6 cho các kết nối liên router và các VLAN, cấu hình định tuyến EIGRP cho IPv6.
- Cấu hình DHCPv6 ở chế độ Stateless và Relay Agent để cấp phát địa chỉ IPv6 cho các host trong VLAN.

CHƯƠNG 2. CƠ SỞ LÝ THUYẾT

2.1 Địa chỉ ipv4 và ipv6

2.1.1 Địa chỉ ipv4

IPv4 là giao thức mạng được sử dụng phổ biến nhất trong các mạng hiện nay. Địa chỉ IPv4 có kích thước 32-bit, chia thành bốn octet (mỗi octet có 8-bit), tạo ra 4 tỉ địa chỉ khác nhau. Địa chỉ này thường được biểu diễn theo dạng thập phân và phân cách bằng dấu chấm (ví dụ: 192.168.1.1). Trong mỗi địa chỉ IPv4, có hai phần chính: phần mạng (network) và phần thiết bị (host).

Phần mạng xác định khu vực mạng mà thiết bị đó thuộc về, trong khi phần host xác định vị trí của thiết bị trong mạng. Quá trình chia subnet giúp tối ưu hóa việc sử dụng không gian địa chỉ, cho phép phân chia các mạng con nhỏ hơn từ một dải địa chỉ lớn, giúp quản lý mạng hiệu quả và tăng tính bảo mật. Subnetting được thực hiện thông qua việc thay đổi subnet mask hoặc prefix length.

2.1.2 Địa chỉ ipv6

IPv6 là giao thức kế nhiệm IPv4, với địa chỉ có độ dài 128-bit, đủ để cung cấp một không gian địa chỉ rộng lớn, vượt trội hơn nhiều so với IPv4. Địa chỉ IPv6 được biểu diễn dưới dạng thập lục phân, chia thành tám nhóm, mỗi nhóm có bốn ký tự, phân cách bởi dấu hai chấm (ví dụ: 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

IPv6 không chỉ cung cấp không gian địa chỉ khổng lồ mà còn hỗ trợ các tính năng mới như tính bảo mật cao hơn, hiệu suất tốt hơn, và khả năng quản lý mạng dễ dàng hơn. Một trong những tính năng quan trọng của IPv6 là Stateless Address Autoconfiguration (SLAAC), cho phép thiết bị tự động cấu hình địa chỉ của mình mà không cần sự can thiệp của máy chủ DHCP. Bên cạnh đó, IPv6 còn hỗ trợ DHCPv6 để cấp phát địa chỉ và cấu hình cho các thiết bị trong mạng.

2.2 Giao thức định tuyến

2.2.1 EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP là một giao thức định tuyến động được phát triển bởi Cisco, hoạt động theo cơ chế kết hợp giữa hai mô hình định tuyến là Distance Vector và Link State. Đây là một giao thức độc quyền (proprietary) của Cisco, tuy nhiên về sau đã được mở rộng một phần để tương thích rộng rãi hơn. EIGRP hỗ trợ cả địa chỉ IPv4 và IPv6, phù hợp cho các mạng doanh nghiệp vừa và lớn.

Điểm nổi bật nhất của EIGRP là việc sử dụng thuật toán DUAL (Diffusing Update Algorithm). Thuật toán này giúp EIGRP đạt được khả năng hội tụ nhanh sau mỗi thay đổi trong mạng, đồng thời đảm bảo các tuyến đường được lựa chọn luôn là tuyến đường khả thi và ổn định. Thay vì gửi toàn bộ bảng định tuyến định kỳ như một số giao thức định tuyến khác, EIGRP chỉ gửi các cập nhật thay đổi (partial updates), giúp tối ưu hóa băng thông và giảm tải cho thiết bị định tuyến.

Ngoài ra, EIGRP còn cung cấp một số tính năng nâng cao như:

- Phân phối lại tuyến đường (route redistribution) từ các giao thức định tuyến khác.
- Cân bằng tải theo hệ số không bằng nhau (unequal-cost load balancing), một điểm mà OSPF không hỗ trợ.
- Tự động phát hiện lỗi và tái tính toán tuyến đường nhanh chóng.

Ưu điểm của EIGRP:

- Hội tụ nhanh, ổn định.
- Tối ưu về băng thông.
- Hỗ trợ tốt các mạng phức tạp với khả năng mở rộng cao.

2.2.2 OSPF (*Open Shortest Path First*)

OSPF là một giao thức định tuyến theo trạng thái liên kết, sử dụng thuật toán Dijkstra để tính toán đường đi ngắn nhất. Giao thức này phân chia mạng thành các khu vực (area), giúp giảm thiểu kích thước bảng định tuyến và tăng tính mở rộng cho mạng lớn. Mỗi khu vực OSPF có một bộ thông tin về các liên kết trong khu vực đó, và tất cả các router trong một khu vực chia sẻ thông tin về các liên kết này để tính toán tuyến đường ngắn nhất.

OSPF được ưa chuộng trong các mạng lớn vì khả năng mở rộng và hỗ trợ các tính năng như tính toán đường đi tối ưu, bảo mật, và khả năng chịu lỗi cao. Giao thức này cũng cho phép định tuyến các mạng IPv4 và IPv6 trong cùng một hạ tầng mạng.

OSPF hỗ trợ cả IPv4 (OSPFv2) và IPv6 (OSPFv3), đồng thời tích hợp các tính năng nâng cao như:

- Bảo mật thông qua xác thực các bản tin định tuyến.
- Hỗ trợ QoS thông qua định tuyến dựa trên chính sách.
- Khả năng chịu lỗi cao nhờ vào cơ chế hội tụ nhanh và phát hiện lỗi hiệu quả.

Ưu điểm của OSPF:

- Mở rộng tốt, phù hợp cho các mạng lớn.
- Hỗ trợ đa nền tảng và hoạt động hiệu quả trên nhiều thiết bị.
- Tính ổn định và độ tin cậy cao trong môi trường mạng phức tạp.

2.3 Giao thức PPP (Point-to-Point Protocol)

PPP là giao thức liên kết dữ liệu được sử dụng để thiết lập kết nối trực tiếp giữa hai thiết bị mạng. Được phát triển để thay thế các giao thức cũ như SLIP (Serial Line Internet Protocol), PPP cung cấp một giao thức linh hoạt và mạnh mẽ, hỗ trợ nhiều phương thức xác thực như PAP (Password Authentication Protocol) và CHAP (Challenge Handshake Authentication Protocol).

PAP và CHAP giúp bảo vệ kết nối PPP bằng cách yêu cầu các thiết bị xác thực trước khi cho phép kết nối. PAP thực hiện xác thực một chiều, gửi tên người dùng và mật khẩu qua kết nối, trong khi CHAP thực hiện xác thực hai chiều và sử dụng một phương thức mã hóa mạnh mẽ để tăng cường bảo mật.

2.4 GRE Tunnel (Generic Routing Encapsulation)

GRE là giao thức đường hầm được sử dụng để đóng gói các gói tin của các giao thức mạng khác vào một gói IP duy nhất, cho phép truyền tải qua mạng trung gian. GRE không yêu cầu các giao thức mạng khác phải sử dụng cùng một giao thức mạng hoặc cấu hình IP giống nhau. Điều này giúp tạo ra một kết nối ảo giữa các mạng nội bộ qua Internet hoặc mạng WAN, giống như kết nối trực tiếp.

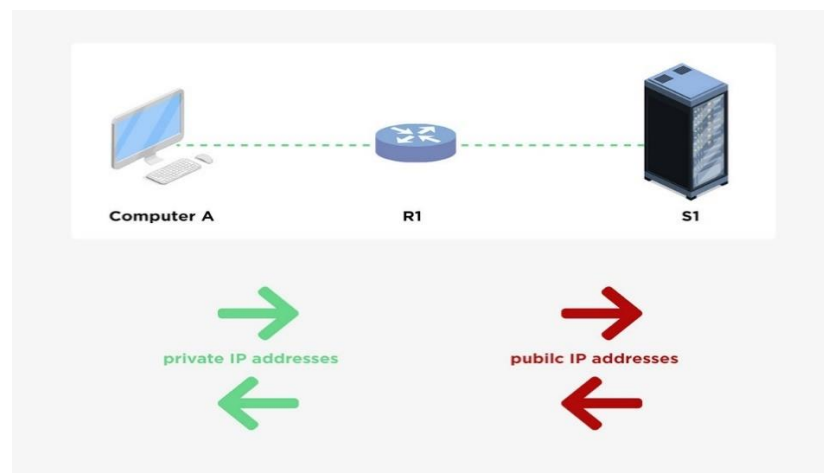
Một trong những ứng dụng phổ biến của GRE là tạo kết nối ảo giữa các mạng phân tán, đặc biệt là trong các môi trường sử dụng các giao thức định tuyến như OSPF hoặc EIGRP. Tuy nhiên, GRE không cung cấp bảo mật cho các dữ liệu được truyền tải, do đó thường được kết hợp với IPSec để mã hóa dữ liệu và bảo vệ kết nối.

2.5 NAT và DHCP

2.5.1 NAT (*Network Address Translation*)

NAT là một kỹ thuật được sử dụng trong các hệ thống mạng nhằm chuyển đổi địa chỉ IP từ không gian địa chỉ nội bộ (private IP) sang địa chỉ IP công cộng (public IP) và ngược lại. Việc này đặc biệt quan trọng trong bối cảnh số lượng địa chỉ IPv4 công cộng hạn chế, trong khi nhu cầu kết nối Internet từ nhiều thiết bị ngày càng tăng.

NAT thường được triển khai trên các thiết bị định tuyến như router hoặc firewall tại biên mạng (network edge), đóng vai trò làm cầu nối giữa mạng nội bộ và mạng Internet công cộng. Khi một gói tin từ một thiết bị trong mạng nội bộ muốn gửi ra ngoài Internet, NAT sẽ thay thế địa chỉ IP nguồn (private IP) của thiết bị đó bằng một địa chỉ IP công cộng trước khi gói tin được gửi đi. Khi gói tin phản hồi quay trở lại, NAT sẽ thực hiện ánh xạ ngược để chuyển tiếp dữ liệu đúng về thiết bị ban đầu trong mạng nội bộ.



Hình 2.1 Kỹ thuật NAT

Một biến thể phổ biến của NAT là NAT Overload, còn gọi là PAT (Port Address Translation). Kỹ thuật này cho phép nhiều thiết bị nội bộ chia sẻ cùng một

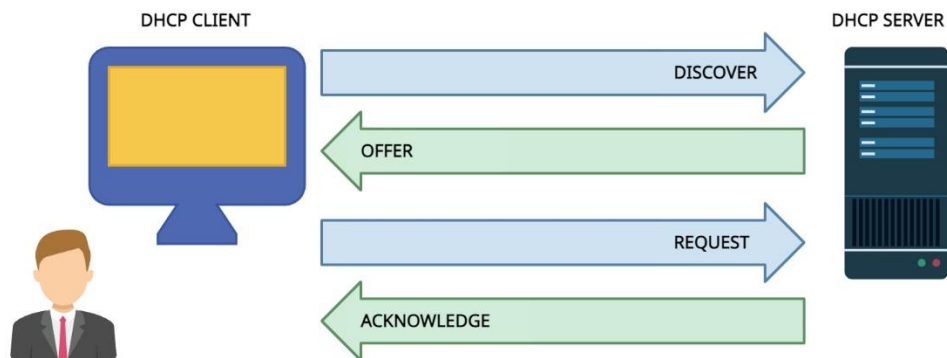
địa chỉ IP công cộng bằng cách gán thêm số hiệu cổng (port number) duy nhất cho từng kết nối. Cụ thể, bảng NAT sẽ lưu thông tin ánh xạ giữa địa chỉ IP nội bộ và cổng nội bộ với địa chỉ IP công cộng và cổng công cộng, giúp định tuyến chính xác các gói tin khi chúng quay lại.

Lợi ích của NAT:

- Tiết kiệm địa chỉ IPv4 công cộng: Cho phép hàng trăm thiết bị chia sẻ một địa chỉ IP công cộng duy nhất.
- Tăng cường bảo mật: Thiết bị trong mạng nội bộ không bị lộ trực tiếp trên Internet, giúp giảm nguy cơ bị tấn công từ bên ngoài.
- Linh hoạt triển khai: Dễ dàng mở rộng và quản lý hệ thống mạng nội bộ mà không phụ thuộc vào nhà cung cấp dịch vụ Internet.

2.5.2 DHCP (Dynamic Host Configuration Protocol)

DHCP là giao thức giúp tự động cấp phát địa chỉ IP cho các thiết bị trong mạng, thay vì yêu cầu người quản trị mạng phải cấu hình IP thủ công cho từng thiết bị.



Hình 2.2 Giao thức DHCP

Khi một thiết bị (gọi là DHCP client) vừa kết nối vào mạng và chưa có địa chỉ IP, nó sẽ gửi một gói tin yêu cầu thông tin cấu hình (DHCP Discover) dưới dạng quảng bá (broadcast) đến toàn mạng. DHCP server sẽ phản hồi bằng gói DHCP Offer, trong đó đề xuất một địa chỉ IP khả dụng cùng các thông số cấu hình khác. Quá trình

này tiếp tục với gói DHCP Request từ phía client để xác nhận địa chỉ được chọn, và kết thúc bằng gói DHCP Acknowledgment từ server để hoàn tất việc cấp phát địa chỉ.

2.6 Chuyển mạch và EtherChannel

2.6.1 Chuyển mạch và VLAN

Chuyển mạch (Switching) là quá trình sử dụng các thiết bị chuyển mạch (switch) để kết nối các thiết bị đầu cuối như máy tính, máy in, hoặc các thiết bị mạng khác trong cùng một mạng nội bộ (LAN). Switch hoạt động ở tầng 2 của mô hình OSI, sử dụng địa chỉ MAC để quyết định chuyển tiếp gói tin đến cổng đích tương ứng, nhờ đó giảm thiểu tình trạng quảng bá (broadcast) và nâng cao hiệu suất truyền dữ liệu.

Một trong những tính năng quan trọng được tích hợp trong switch là VLAN. VLAN cho phép chia nhỏ một mạng LAN vật lý thành nhiều vùng logic độc lập, trong đó mỗi VLAN hoạt động như một mạng LAN riêng biệt. Việc phân chia này dựa trên các tiêu chí như chức năng, phòng ban, hoặc cấp quyền truy cập, giúp:

- Tăng cường bảo mật, vì thiết bị ở các VLAN khác nhau không thể giao tiếp trực tiếp nếu không có sự định tuyến.
- Tối ưu hóa lưu lượng mạng, nhờ giới hạn quảng bá trong từng VLAN.

2.6.2 Spanning Tree Protocol (STP) và Rapid PVST+

Trong mạng chuyển mạch, các kết nối dự phòng giữa switch giúp tăng tính sẵn sàng, nhưng cũng có thể gây ra vòng lặp Layer 2, dẫn đến broadcast storm, nhiều bảng MAC và tắc nghẽn mạng. Để khắc phục, STP theo chuẩn IEEE 802.1D được sử dụng nhằm vô hiệu hóa các liên kết dư thừa, tạo một cây bao phủ (spanning tree), đảm bảo chỉ một đường được sử dụng tại mỗi thời điểm. Khi có sự cố, STP sẽ kích hoạt liên kết dự phòng để duy trì kết nối mạng.

Tuy nhiên, STP có thời gian hội tụ chậm. Rapid PVST+, dựa trên chuẩn IEEE 802.1w, là phiên bản cải tiến do Cisco phát triển, giúp rút ngắn thời gian hội tụ xuống chỉ vài giây, hỗ trợ cấu hình root bridge riêng cho từng VLAN, và tăng khả năng mở

rộng. Nhờ đó, Rapid PVST+ giúp mạng ổn định hơn và hiệu quả hơn trong các hệ thống nhiều VLAN.

2.6.3 EtherChannel với LACP

EtherChannel là một công nghệ mạng cho phép kết hợp nhiều liên kết vật lý giữa các thiết bị chuyên mạch (switch) thành một liên kết logic duy nhất. Việc gom nhóm này không những giúp tăng tổng băng thông giữa các thiết bị mà còn nâng cao độ tin cậy thông qua khả năng dự phòng. Trong trường hợp một trong các liên kết vật lý gặp sự cố, các liên kết còn lại trong nhóm vẫn tiếp tục hoạt động, đảm bảo duy trì kết nối mạng.

LACP là một trong những giao thức được sử dụng để thiết lập EtherChannel một cách tự động và linh hoạt. LACP cho phép hai thiết bị đàm phán và xác nhận các liên kết hợp lệ để đưa vào nhóm EtherChannel. Nhờ đó, quá trình cấu hình được đơn giản hóa, đồng thời tăng khả năng quản lý và tính ổn định cho hệ thống mạng.

2.7 DHCPv6 và Relay Agent

2.7.1 Stateless DHCPv6

Stateless DHCPv6 là một cơ chế cấp phát thông tin cấu hình trong mạng IPv6, kết hợp giữa tự động cấu hình địa chỉ SLAAC và việc cung cấp thông tin bổ sung từ máy chủ DHCPv6. Theo mô hình này, các thiết bị đầu cuối sẽ tự động cấu hình địa chỉ IP của mình dựa trên thông tin quảng bá từ router (Router Advertisement), trong khi những thông tin cấu hình khác như địa chỉ DNS hoặc tên miền sẽ được cung cấp bởi máy chủ DHCPv6.

2.7.2 Relay Agent

Relay Agent là thiết bị giúp chuyển tiếp các gói DHCPv6 giữa các mạng khác nhau. Điều này rất quan trọng khi các máy trạm và máy chủ DHCPv6 nằm trong các subnet khác nhau, Relay Agent giúp đảm bảo rằng các yêu cầu DHCPv6 từ các thiết bị ở các subnet khác nhau vẫn có thể được phục vụ đúng cách, giúp duy trì khả năng cấp phát địa chỉ cho toàn bộ mạng.

CHƯƠNG 3. MÔ HÌNH ĐỀ XUẤT

3.1 Mô hình tổng thể (HQ và Branch)

Mô hình mạng trên được chia thành hai khu vực chính: BRANCH (chi nhánh) và HQ (trụ sở chính), được kết nối thông qua thiết bị trung gian R5 và mạng lõi sử dụng GRE tunnel. Mạng này được thiết kế để mô phỏng một hệ thống mạng doanh nghiệp có tính phân chia khu vực, bảo mật, định tuyến linh hoạt và khả năng mở rộng cao.

Khu vực BRANCH bao gồm các router R1, R2 và R3. Trong đó, R1 thuộc OSPF Area 1, R3 thuộc OSPF Area 3, mỗi router đều có hai loopback interface đại diện cho các subnet nội bộ. Router R2 đóng vai trò là router trung gian để kết nối hai khu vực OSPF (Area 1 và Area 3) thông qua các liên kết point-to-point. Tất cả các tuyến đường nội bộ trong BRANCH đều được định tuyến bằng OSPF đa khu vực, đảm bảo tính tổ chức và dễ quản lý.

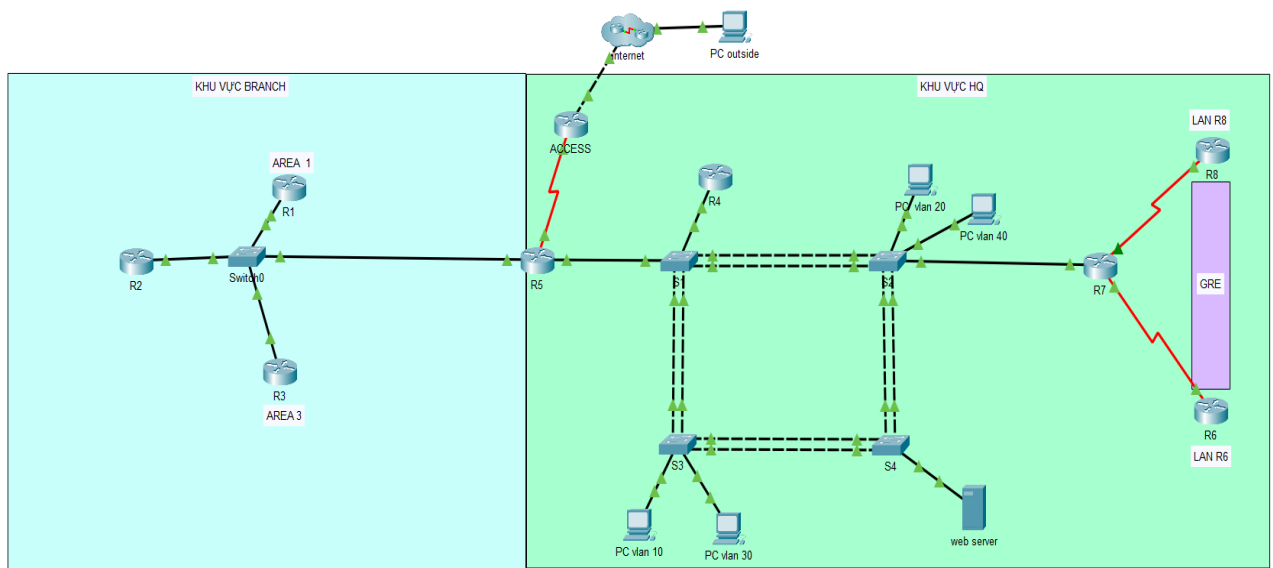
Router R5 đóng vai trò là router biên (border router), kết nối giữa chi nhánh và trụ sở chính. R5 đồng thời kết nối với mạng Internet và có nhiệm vụ redistribute giữa OSPF (ở BRANCH) và EIGRP (ở HQ), đảm bảo truyền tải định tuyến giữa hai giao thức định tuyến khác nhau. Ngoài ra, R5 cũng đóng vai trò là điểm kết nối ra Internet cho toàn hệ thống.

Khu vực HQ được tổ chức chuyên nghiệp với các thiết bị chuyển mạch (S1 đến S4) tạo thành một cấu trúc EtherChannel hình vuông, đảm bảo dự phòng và cân bằng tải. R4 là router kết nối với các switch, triển khai router-on-a-stick để phục vụ các VLAN (VLAN10, 20, 30, 40, 50, 60) thông qua giao diện subinterface (dot1Q). Đây là nơi cấu hình DHCPv6 Stateless, DNS và quản lý các địa chỉ IPv6 cho các thiết bị đầu cuối trong VLAN.

Router R7 là trung tâm kết nối giữa mạng nội bộ HQ và các mạng LAN từ xa thông qua tunnel GRE đến R6 và R8. Điều này cho phép kết nối site-to-site VPN giữa các địa điểm khác nhau như R6 (LAN R6) và R8 (LAN R8). Cấu trúc GRE này giúp

truyền tải dữ liệu giữa các site một cách an toàn qua Internet mà không ảnh hưởng đến mô hình định tuyến nội bộ.

Cuối cùng, các router R6 và R8 đại diện cho các văn phòng từ xa hoặc hệ thống mạng nội bộ khác, được kết nối đến R7 thông qua tunnel GRE. Các router này phục vụ các LAN độc lập và nhận cấu hình từ R7 như định tuyến, DHCPv6 và DNS, giúp đồng bộ hóa các mạng LAN trên toàn hệ thống doanh nghiệp.



Hình 3.1 Mô hình mạng

3.2 Sơ đồ địa chỉ IP khu vực HQ

3.2.1 Sơ đồ Ipv4

3.2.1.1 Sơ đồ ipv4 cho các vlan

Địa chỉ mạng được sử dụng: 172.27.0.0/16. Việc lựa chọn địa chỉ mạng lớp B riêng 172.27.0.0/16 cho toàn bộ khu vực trụ sở chính là hoàn toàn hợp lý trong bối cảnh triển khai mạng nội bộ cho một tổ chức quy mô trung bình đến lớn. Dải địa chỉ này cung cấp tới 65.536 địa chỉ IP (2^{16}), cho phép chia subnet linh hoạt theo từng phòng ban, đơn vị chức năng, đồng thời vẫn còn dư địa để mở rộng trong tương lai. Bên cạnh đó, việc giữ nguyên prefix /16 cho toàn vùng HQ giúp dễ dàng phân chia mạng con (subnetting) theo từng VLAN với kích thước tùy biến mà không lo thiếu địa chỉ. Tại HQ bao gồm 6 VLAN. Phân bổ địa chỉ cho từng VLAN như sau:

- VLAN 10 (UNIT1):

Yêu cầu chứa 200 host, do đó ta chọn subnet /24 (255.255.255.0), cung cấp 254 host khả dụng. Dải địa chỉ 172.27.10.0/24 được sử dụng cho VLAN này. Đây là lựa chọn tối ưu vì không quá dư thừa, chỉ thừa 54 địa chỉ, phù hợp cho các đơn vị ổn định số lượng thiết bị và không cần mở rộng nhiều. Gateway được đặt tại địa chỉ đầu tiên trong dải usable: 172.27.10.1, còn các máy chủ hoặc máy trạm được cấp địa chỉ từ 172.27.10.2 trở đi. Việc đặt gateway ở đầu dải giúp quản lý dễ dàng và nhất quán giữa các VLAN.

- VLAN 20 (UNIT2):

Có nhu cầu cao hơn với 300 host, ta chọn subnet /23 (255.255.254.0), cung cấp tới 510 host khả dụng. Mạng 172.27.20.0/23 được dùng, kết hợp địa chỉ từ 172.27.20.0 đến 172.27.21.255. Subnet này tận dụng hiệu quả không gian địa chỉ, chỉ dư khoảng 210 host, đảm bảo vẫn còn dư địa cho phát triển trong tương lai. Gateway đặt tại 172.27.20.1, còn dải IP cho máy chủ từ 172.27.20.2 trở đi.

- VLAN 30 (UNIT3):

Chỉ cần 100 host, phù hợp với subnet /25 (255.255.255.128), cung cấp 126 địa chỉ usable. Đây là lựa chọn tối ưu với mức dư không quá nhiều (26 địa chỉ), đảm bảo tiết kiệm tài nguyên IP. Dải mạng 172.27.30.0/25 được dùng, với gateway là 172.27.30.1, còn các host sử dụng các địa chỉ từ 172.27.30.2.

- VLAN 40 (GUEST):

Cần 50 host nên chọn subnet /26 (255.255.255.192), với 62 host usable. Mạng 172.27.40.0/26 là phù hợp, đảm bảo đủ không gian cho các thiết bị khách, tránh lãng phí IP. Gateway đặt tại 172.27.40.1.

- VLAN 50 (SERVERS):

Chỉ có 10 thiết bị, chọn subnet /28 (255.255.255.240), cung cấp 14 host usable, vừa đủ với mức dư tối thiểu (4 địa chỉ). Địa chỉ mạng 172.27.50.0/28 được chọn với gateway là 172.27.50.1, IP máy chủ từ 172.27.50.2 đến 172.27.50.14.

- VLAN 60 – MANAGEMENT:

Dành cho mục đích quản lý thiết bị mạng, cần khoảng 20 địa chỉ nên chọn subnet /27 (255.255.255.224), cung cấp 30 host usable. Dải 172.27.60.0/27 vừa đủ, dư 10 địa chỉ để dự phòng thiết bị quản lý hoặc nâng cấp sau này. Gateway tại 172.27.60.1.

Bảng 3.1 Sơ đồ ipv4 cho các vlan ở khu vực HQ

VLAN	TÊN VLAN	Số host yêu cầu	Slash	Địa chỉ mạng	Dải IP khả dụng	Gateway
10	UNIT1	200	/24	172.27.10.0	172.27.10.1 - 172.27.10.254	172.27.10.1
20	UNIT2	300	/23	172.27.20.0	172.27.20.1 - 172.27.21.254	172.27.20.1
30	UNIT3	100	/25	172.27.30.0	172.27.30.1 - 172.27.30.126	172.27.30.1
40	GUEST	50	/26	172.27.40.0	172.27.40.1 - 172.27.40.62	172.27.40.1
50	SERVERS	10	/28	172.27.50.0	172.27.50.1 - 172.27.50.14	172.27.50.1
60	MANAGEMENT	20	/27	172.27.60.0	172.27.60.1 - 172.27.60.30	172.27.60.1

3.2.1.2 Sơ đồ ipv4 cho các liên kết router

Địa chỉ mạng sử dụng dải IP 200.0.100.0/30 là rất thích hợp cho các kết nối point-to-point, vì chỉ cần hai địa chỉ IP usable, một cho mỗi thiết bị đầu cuối. Việc sử dụng subnet /30 giúp tối ưu hóa tài nguyên IP, đảm bảo không lãng phí địa chỉ IP trong khi vẫn đảm bảo đủ số lượng địa chỉ cho kết nối giữa hai router. Hơn nữa, việc áp dụng dải địa chỉ public như 200.0.100.0/30 trong mô phỏng và thực hành cũng giúp người học hiểu rõ hơn về các tình huống mạng thực tế khi triển khai các kết nối WAN.

Bảng 3.2 Sơ đồ ipv4 cho kết nối giữa các router

Kết nối	Địa chỉ mạng	Slash	Mask	Dải IP khả dụng	Broadcast
R7 ↔ R6	200.0.100.0	/30	255.255.255.252	200.0.100.1 - 200.0.100.2	200.0.100.3
R7 ↔ R8	200.0.100.4	/30	255.255.255.252	200.0.100.5 - 200.0.100.6	200.0.100.7
R5 ↔ ACCESS	200.0.100.8	/30	255.255.255.252	200.0.100.9 - 200.0.100.10	200.0.100.11

3.2.2 Sơ đồ Ipv6

3.2.2.1 Sơ đồ ipv6 cho các vlan

Việc phân bổ địa chỉ IPv6 cho các VLAN tại khu vực trụ sở chính (HQ) dựa trên khối mạng được cấp là 2019:ABBA:CDDC::/48, tuân theo chuẩn phân chia subnet trong IPv6. Với khối /48, ta có thể chia thành hàng nghìn subnet /64 – đây là độ dài subnet tiêu chuẩn trong mạng IPv6, hỗ trợ các cơ chế tự động cấu hình địa chỉ như SLAAC, đồng thời cung cấp không gian địa chỉ cực lớn (2^{64} địa chỉ cho mỗi subnet), đáp ứng tốt nhu cầu mở rộng lâu dài.

Từng VLAN tại HQ được gán một subnet riêng biệt từ những subnet đầu tiên trong khối /48, cụ thể theo thứ tự: VLAN 10 sử dụng subnet 2019:ABBA:CDDC:0::/64, VLAN 20 là 2019:ABBA:CDDC:1::/64, VLAN 30 là 2019:ABBA:CDDC:2::/64, tiếp theo VLAN 40 và 50 lần lượt là 2019:ABBA:CDDC:3::/64 và 2019:ABBA:CDDC:4::/64. Cách đánh số theo thứ tự tuyến tính này đảm bảo khả năng mở rộng, quản lý logic và thuận tiện trong giám sát hệ thống.

Trong mỗi subnet, gateway thường được đặt là địa chỉ đầu tiên – ví dụ, gateway cho VLAN 10 sẽ là 2019:ABBA:CDDC:0::1. Ngoài ra, mỗi gateway có thể

được cấu hình thêm địa chỉ Link-Local như FE80::1, FE80::1:1, v.v... để phục vụ cho việc định tuyến nội bộ sử dụng các giao thức như OSPFv3 hoặc EIGRP for IPv6.

Việc sử dụng cấu trúc đánh số đều đặn và theo thứ tự từ khối /48 không chỉ giúp đơn giản hóa công tác định tuyến – nhờ dễ dàng xác định mạng đích qua hậu tố subnet – mà còn giúp giảm thiểu lỗi cấu hình và tăng hiệu quả khi khắc phục sự cố. Đồng thời, đặc điểm của IPv6 cho phép gán nhiều địa chỉ (Global Unicast và Link-Local) trên cùng một interface, mang lại sự linh hoạt và khả năng tương thích cao trong vận hành mạng nội bộ.

Bảng 3.3 Sơ đồ ipv6 cho các vlan

VLAN	Subnet Prefix	Gateway IPv6	Link-local Gateway
10	2019:ABBA:CDDC:0::/64	2019:ABBA:CDDC:0::1/64	FE80::1
20	2019:ABBA:CDDC:1::/64	2019:ABBA:CDDC:1::1/64	FE80::1:1
30	2019:ABBA:CDDC:2::/64	2019:ABBA:CDDC:2::1/64	FE80::2:1
40	2019:ABBA:CDDC:3::/64	2019:ABBA:CDDC:3::1/64	FE80::3:1
50	2019:ABBA:CDDC:4::/64	2019:ABBA:CDDC:4::1/64	FE80::4:1

3.2.2.2 Sơ đồ ipv6 cho các liên kết router

Trong kiến trúc mạng của khu vực HQ, việc phân bổ địa chỉ IPv6 cho các kết nối giữa các router được thực hiện một cách tách biệt và có hệ thống nhằm đảm bảo tính phân tầng, dễ kiểm soát và hỗ trợ triển khai hiệu quả các giao thức định tuyến như OSPFv3 hoặc EIGRP for IPv6. Cụ thể, mỗi kết nối point-to-point hoặc mạng LAN chia sẻ đều được gán một subnet IPv6 riêng biệt. Kết nối ACCESS ↔ R5 sử dụng mạng 2019:ABBA:AAAA:1::/64, với địa chỉ phân bổ lần lượt là ::1 cho ACCESS và ::2 cho R5 – cách đặt địa chỉ này đơn giản, dễ ghi nhớ và thuận tiện khi cấu hình. Mạng 2019:ABBA:BBBB:1::/64 được dùng cho kết nối LAN giữa R4, R5 và R7 – đây là một ví dụ tiêu biểu của mô hình nhiều router chia sẻ cùng một mạng

lớp 2, giúp tối ưu hóa quá trình trao đổi định tuyến trong cùng một miền quảng bá. Trong khi đó, các liên kết point-to-point như R7 ↔ R6 và R7 ↔ R8 được gán lần lượt các subnet 2019:ABBA:CCCC:1::/64 và 2019:ABBA:DDDD:1::/64, đảm bảo mỗi tuyến truyền có một không gian địa chỉ riêng biệt. Cách phân chia này không chỉ nâng cao hiệu quả quản lý, giám sát kết nối mà còn giúp dễ dàng cô lập lỗi khi sự cố xảy ra và tăng tính bảo mật trong điều phối lưu lượng. Việc sử dụng các địa chỉ IPv6 được chuẩn hóa và đồng nhất cũng góp phần cải thiện tính nhất quán và khả năng mở rộng của toàn bộ hạ tầng mạng HQ.

Bảng 3.4 Sơ đồ ipv6 cho kết nối các router

Kết nối	Địa chỉ mạng
ACCESS ↔ R5	2019:ABBA:AAAA:1::/64
R4, R5, R7	2019:ABBA:BBBB:1::/64
R7 ↔ R6	2019:ABBA:CCCC:1::/64
R7 ↔ R8	2019:ABBA:DDDD:1::/64

3.2.2.3 Sơ đồ ipv6 cho mạng lan nội bộ R6, R8

Trong hệ thống mạng khu vực HQ, hai router R6 và R8 được cấu hình để phục vụ các mạng LAN nội bộ độc lập, đảm bảo phân tách rõ ràng giữa các miền quảng bá. Router R6 sử dụng dải địa chỉ IPv6 toàn cục 2019:ABBA:EEEE:1::/64 cho mạng LAN của mình, với địa chỉ được gán là 2019:ABBA:EEEE:1::1/64. Tương tự, R8 được cấu hình với địa chỉ toàn cục 2019:ABBA:FFFF:1::/64 và sử dụng địa chỉ cụ thể 2019:ABBA:FFFF:1::1/64 trên interface kết nối mạng LAN.

Bảng 3.5 Sơ đồ ipv6 cho kết nối mạng LAN R6 và R8

Thiết bị	Địa chỉ mạng
R6	2019:ABBA:EEEE:1::/64
R8	2019:ABBA:FFFF:1::/64

Việc tách biệt hai mạng LAN này không chỉ giúp đảm bảo tính bảo mật và kiểm soát lưu lượng tốt hơn mà còn hỗ trợ triển khai các chính sách định tuyến, phân quyền truy cập và cấu hình firewall ở từng phân đoạn mạng. Cách chia tách này đồng thời phù hợp với nguyên tắc phân vùng chức năng trong các hệ thống mạng doanh nghiệp lớn, dễ dàng cho việc giám sát và bảo trì.

3.3 Sơ đồ địa chỉ IP khu vực Branch

3.3.1 Sơ đồ Ipv4

Việc lựa chọn địa chỉ mạng riêng lớp A 10.28.0.0/16 cho khu vực chi nhánh là hoàn toàn hợp lý và phù hợp với mô hình mạng phân cấp. Dải địa chỉ này đảm bảo sự tách biệt hoàn toàn với trụ sở chính HQ, vốn đang sử dụng 172.27.0.0/16, từ đó giúp việc định tuyến, phân vùng mạng và quản lý IP giữa các khu vực được rõ ràng và hiệu quả. Với khả năng cung cấp lên tới 65.536 địa chỉ IP (2^{16}), dải 10.28.0.0/16 cho phép chi nhánh thoải mái chia subnet phục vụ nhiều mục đích như loopback interface, các mạng LAN nội bộ, hoặc các vùng DMZ riêng biệt nếu cần thiết mở rộng trong tương lai. Ở khu vực Branch sẽ chia ip cho các loopback:

- R1 – Loopback 0:

Giao diện cần 500 địa chỉ IP, vì vậy subnet /23 (255.255.254.0) là phù hợp khi cung cấp 510 địa chỉ khả dụng. Địa chỉ mạng được chọn là 10.28.10.0/23, với dải usable từ 10.28.10.1 đến 10.28.11.254. Subnet này không chỉ đủ mà còn dư 10 địa chỉ – phù hợp cho mở rộng nhẹ về sau. Việc dùng /23 thay vì /22 giúp tránh lãng phí không gian địa chỉ.

- R1 – Loopback 1:

Cần 300 địa chỉ, cũng dùng /23 để đồng bộ với Lo0. Địa chỉ mạng 10.28.12.0/23, usable từ 10.28.12.1 đến 10.28.13.254. Số dư là 210 địa chỉ – hợp lý cho các tình huống cần mở rộng. Việc giữ cùng prefix với Lo0 cũng giúp cấu hình nhất quán, dễ quản lý.

- R2 – Loopback 0:

Với nhu cầu 100 host, subnet /25 (255.255.255.128) là hợp lý khi cung cấp 126 địa chỉ usable. Mạng 10.28.20.0/25, usable từ 10.28.20.1 đến 10.28.20.126. Subnet này đủ dùng và tiết kiệm, không tạo ra sự lãng phí tài nguyên.

- R3 – Loopback 0:

Cần 200 host, lựa chọn /24 (255.255.255.0) là tối ưu. Subnet 10.28.30.0/24 cung cấp 254 địa chỉ usable – đủ dùng và phổ biến trong thực tế. Đây là lựa chọn cho các mạng trung bình, dễ định tuyến và dễ áp dụng chính sách bảo mật.

- R3 – Loopback 1:

Giống như R2.Lo0, giao diện này cần 100 host nên tiếp tục sử dụng /25, với mạng là 10.28.31.0/25, usable từ 10.28.31.1 đến 10.28.31.126. Việc tái sử dụng cách chia subnet giúp thống nhất cấu hình và đơn giản hóa quá trình bảo trì mạng.

Bảng 3.6 Sơ đồ ip cho các loopback ở khu vực Branch

Router	Interface	Số host yêu cầu	Slash	Network Address	Dải IP khả dụng
R1	Lo0	500	/23	10.28.10.0	10.28.10.1 – 10.28.11.254
	Lo1	300	/23	10.28.12.0	10.28.12.1 – 10.28.13.254
R2	Lo0	100	/25	10.28.20.0	10.28.20.1 – 10.28.20.126
R3	Lo0	200	/24	10.28.30.0	10.28.30.1 – 10.28.30.254
	Lo1	100	/25	10.28.31.0	10.28.31.1 – 10.28.31.126

3.4 Phân bổ địa chỉ ip cho khu vực HQ

3.4.1 Phân bổ địa chỉ ipv4

Tại khu vực HQ, các thiết bị mạng được cấu hình với địa chỉ IP cụ thể theo từng giao diện nhằm đảm bảo kết nối nội bộ hiệu quả và liên thông với các khu vực khác. Router R4 đóng vai trò định tuyến nội bộ giữa các VLAN và được cấu hình các subinterface trên cổng G0/0 gồm: G0/0.10 (172.27.10.1/24), G0/0.20 (172.27.20.1/23), G0/0.30 (172.27.30.1/25), G0/0.40 (172.27.40.1/26), G0/0.50 (172.27.50.1/28), và G0/0.60 (172.27.60.1/27). Trong đó, subinterface G0/0.60 đóng vai trò là cổng mặc định cho VLAN 60, phục vụ kết nối quản lý và trao đổi bảng định tuyến giữa các router và switch trong HQ.

Router R5 sử dụng giao diện G0/1 với địa chỉ 172.27.60.6/27 để kết nối vào VLAN 60, đặt default gateway là 172.27.60.1. Ngoài ra, R5 còn có giao diện serial S0/3/0 với địa chỉ 200.0.100.9/30 dùng để kết nối đến thiết bị mạng bên ngoài khu vực HQ (thiết bị ACCESS có địa chỉ 200.0.100.10/30).

Router R7 có hai giao diện serial: S0/3/0 (200.0.100.1/30) kết nối đến R6 (200.0.100.2/30), và S0/3/1 (200.0.100.5/30) kết nối đến R8 (200.0.100.6/30). Giao diện G0/0 của R7 sử dụng địa chỉ 172.27.60.7/27 và cũng thuộc VLAN 60, cho phép R7 trao đổi thông tin định tuyến với R4 và R5.

R6 và R8 được kết nối với nhau thông qua một đường hầm GRE cấu hình trên Tunnel0 với địa chỉ lần lượt là 10.10.10.1/30 và 10.10.10.2/30. R6 cũng sử dụng cổng serial S0/3/0 với địa chỉ 200.0.100.2/30 để kết nối đến R7, trong khi R8 dùng S0/3/1 với địa chỉ 200.0.100.6/30 để nối với R7.

Hệ thống switch quản lý gồm S1 đến S4 đều thuộc VLAN 60 và được gán các địa chỉ IP từ 172.27.60.2 đến 172.27.60.5, sử dụng default gateway là 172.27.60.1. Nhờ đó, các switch có thể quản lý tập trung và liên kết với các router R4, R5, R7 thông qua cùng một dải địa chỉ mạng.

Toàn bộ các thiết bị router trong HQ không cần cấu hình default gateway cho các giao diện kết nối nội bộ, vì quá trình định tuyến được xử lý tự động thông qua các giao thức định tuyến động.

Bảng 3.7 Bảng địa chỉ ipv4 khu vực HQ

No.	Device	Interface	IP Address	Subnet Mask (Prefix)	Default Gateway
1	R4	G0/0.10	172.27.10.1	255.255.255.0 (/24)	N/A
		G0/0.20	172.27.20.1	255.255.254.0 (/23)	N/A
		G0/0.30	172.27.30.1	255.255.255.128 (/25)	N/A
		G0/0.40	172.27.40.1	255.255.255.192 (/26)	N/A
		G0/0.50	172.27.50.1	255.255.255.240 (/28)	N/A
		G0/0.60	172.27.60.1	255.255.255.224 (/27)	N/A
2	R5	G0/1	172.27.60.6	255.255.255.224 (/27)	N/A
		S0/3/0	200.0.100.9	255.255.255.252 (/30)	N/A
3	R7	G0/0	172.27.60.7	255.255.255.224 (/27)	N/A
		S0/3/0	200.0.100.1	255.255.255.252 (/30)	N/A
		S0/3/1	200.0.100.5	255.255.255.252 (/30)	N/A
4	S1	VLAN 60	172.27.60.2	255.255.255.224 (/27)	172.27.60.1

5	S2	VLAN 60	172.27.60.3	255.255.255.224 (/27)	172.27.60.1
6	S3	VLAN 60	172.27.60.4	255.255.255.224 (/27)	172.27.60.1
7	S4	VLAN 60	172.27.60.5	255.255.255.224 (/27)	172.27.60.1
8	R6	Tunnel0	10.10.10.1	255.255.255.252 (/30)	N/A
		S0/3/0	200.0.100.2	255.255.255.252 (/30)	N/A
9	R8	Tunnel0	10.10.10.2	255.255.255.252 (/30)	N/A
		S0/3/1	200.0.100.6	255.255.255.252 (/30)	N/A
10	ACCESS	S0/3/0	200.0.100.10	255.255.255.252 (/30)	N/A
11	Server	Fa0/0	172.27.50.10	255.255.255.240 (/28)	172.27.50.1

3.4.2 Phân bổ địa chỉ ipv6

Trong cấu hình IPv6 cho mạng HQ, các thiết bị chủ yếu sử dụng địa chỉ IPv6 tĩnh được chỉ định cho từng interface. Cổng ACCESS có địa chỉ IPv6 2019:ABBA:AAAA:1::1/64 với địa chỉ liên kết FE80::1:1. Router R5 cấu hình trên interface Se0/3/0 với địa chỉ 2019:ABBA:AAAA:1::2/64 và FE80::1:2 (link-local), đồng thời sử dụng Gig0/1 với địa chỉ 2019:ABBA:BBBB:1::2/64 và FE80::2:2 (link-local). Router R4 cấu hình trên Gig0/0.60 với địa chỉ IPv6 2019:ABBA:BBBB:1::1/64 và FE80::2:4 (link-local). Router R7 có địa chỉ trên Gig0/0 là 2019:ABBA:BBBB:1::3/64 và FE80::2:3 (link-local), và cũng được cấu hình trên các interface Se0/3/0 và Se0/3/1 với các địa chỉ 2019:ABBA:CCCC:1::1/64 (FE80::3:1) và 2019:ABBA:DDDD:1::1/64 (FE80::4:1). Router R6 có địa chỉ trên Se0/3/0 là

2019:ABBA:CCCC:1::2/64 và FE80::3:2 (link-local), trong khi trên Gig0/0, nó được cấu hình với địa chỉ 2019:ABBA:EEEE:1::1/64 và FE80::5:1 (link-local). Cuối cùng, router R8 được cấu hình trên interface Se0/3/1 với địa chỉ 2019:ABBA:DDDD:1::2/64 (FE80::4:2) và trên Gig0/0 với địa chỉ 2019:ABBA:FFFF:1::1/64 (FE80::5:2). Tất cả các router này không cần default gateway vì chúng giao tiếp với nhau qua các đường truyền trực tiếp.

Bảng 3.8 Bảng địa chỉ ipv6 khu vực HQ

No.	Device	Interface	Global IPv6 Address	Link-Local IPv6
1	R4	Gig0/0	2019:ABBA:BBBB:1::1/64	FE80::2:4
2	R5	Se0/3/0	2019:ABBA:AAAA:1::2/64	FE80::1:2
		Gig0/1	2019:ABBA:BBBB:1::2/64	FE80::2:2
3	R6	Se0/3/0	2019:ABBA:CCCC:1::2/64	FE80::3:2
		Gig0/0 (LAN)	2019:ABBA:EEEE:1::1/64	FE80::5:1
4	R7	Gig0/0	2019:ABBA:BBBB:1::3/64	FE80::2:3
		Se0/3/0	2019:ABBA:CCCC:1::1/64	FE80::3:1
		Se0/3/1	2019:ABBA:DDDD:1::1/64	FE80::4:1
5	R8	Se0/3/1	2019:ABBA:DDDD:1::2/64	FE80::4:2
		Gig0/0 (LAN)	2019:ABBA:FFFF:1::1/64	FE80::5:2
6	ACCESS	Se0/3/0	2019:ABBA:AAAA:1::1/64	FE80::1:1

3.5 Phân bổ địa chỉ cho khu vực Branch

3.5.1 Phân bổ địa chỉ ipv4

Tại khu vực Branch, các router R1, R2, và R3 có địa chỉ IP được phân bổ cho các giao diện kết nối với HQ. R1 có giao diện G0/0 với địa chỉ 10.28.1.1/24, kết nối đến HQ. Các giao diện Loopback0 và Loopback1 của R1 được cấp địa chỉ

10.28.10.1/23 và 10.28.12.1/23, phục vụ cho các kết nối ảo và hỗ trợ định tuyến giữa các phân đoạn mạng. R2 có giao diện G0/0 với địa chỉ 10.28.1.2/24, kết nối đến HQ. Giao diện Loopback0 của R2 có địa chỉ 10.28.20.1/25 để cung cấp kết nối ảo cho các yêu cầu định tuyến. R3 có giao diện G0/0 với địa chỉ 10.28.1.3/24, kết nối đến HQ. Giao diện Loopback0 và Loopback1 của R3 được cấp địa chỉ 10.28.30.1/24 và 10.28.31.1/25, phục vụ cho các kết nối định tuyến ảo trong mạng. Tương tự như các router trong HQ, các thiết bị trong Branch cũng không cần default gateway cho các giao diện LAN do đã có định tuyến nội bộ được cấu hình rõ ràng giữa các router. Các router kết nối giữa Branch và HQ sẽ xử lý việc chuyển tiếp các gói tin tới các đích chính xác.

Bảng 3.9 Bảng địa chỉ ipv4 khu vực Branch

No.	Device	Interface	IP Address	Subnet Mask/Prefix	Default Gateway
1	R1	G0/0	10.28.1.1	255.255.255.0 (/24)	N/A
		Loopback0	10.28.10.1	255.255.254.0 (/23)	N/A
		Loopback1	10.28.12.1	255.255.254.0 (/23)	N/A
2	R2	G0/0	10.28.1.2	255.255.255.0 (/24)	N/A
		Loopback0	10.28.20.1	255.255.255.128 (/25)	N/A
3	R3	G0/0	10.28.1.3	255.255.255.0 (/24)	N/A
		Loopback0	10.28.30.1	255.255.255.0 (/24)	N/A
		Loopback1	10.28.31.1	255.255.255.128 (/25)	N/A

CHƯƠNG 4. CẤU HÌNH

4.1 Kết nối PPP

4.1.1 Xác thực PAP

Trong mô hình mạng, giao thức xác thực PAP được sử dụng để bảo vệ kết nối giữa hai router R7 và R6 thông qua đường nối vật lý Serial. Để cấu hình kết nối PPP với PAP, đầu tiên, các router phải được cấu hình để sử dụng giao thức đóng gói PPP thay vì HDLC mặc định. Cấu hình bắt đầu bằng việc khai báo thông tin người dùng trên mỗi router, bao gồm tên người dùng (username) và mật khẩu (password), đảm bảo hai bên xác thực lẫn nhau một cách chính xác.

Bảng 4.1 Lệnh cấu hình PAP trên R6 và R7

R6	R7
enable	enable
configure terminal	configure terminal
username admin password cisco	username admin01 password cisco
interface serial0/3/0	interface serial0/3/0
encapsulation ppp	encapsulation ppp
ppp authentication pap	ppp authentication pap
ppp pap sent-username admin01 password cisco	ppp pap sent-username admin password cisco
no shutdown	no shutdown

Trên router R6, người dùng có tên admin và mật khẩu cisco được tạo ra. Giao diện Serial Se0/3/0 được cấu hình để sử dụng PPP, đồng thời bật cơ chế xác thực PAP bằng lệnh `ppp authentication pap`. Tiếp theo, lệnh `ppp pap sent-username admin01 password cisco` cho phép R6 gửi tên người dùng và mật khẩu khi thực hiện xác thực ngược lại với R7.

Tương tự, trên router R7, một người dùng có tên admin01 và mật khẩu cisco được cấu hình. Trên giao diện Serial Se0/3/0, PPP được bật kèm theo xác thực PAP. R7 sử dụng lệnh `ppp pap sent-username admin password cisco` để xác thực với thông tin mà R6 yêu cầu.

Sau khi cấu hình, để kiểm tra trạng thái kết nối, người dùng có thể sử dụng các lệnh sau:

- `show interface serial0/3/0`: Kiểm tra trạng thái vật lý và giao thức (Status và Protocol phải ở trạng thái "up").

<pre> R7>en R7#show int se0/3/0 Serial0/3/0 is up, line protocol is up (connected) Hardware is HD64570 Internet address is 200.0.100.1/30 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation PPP, loopback not set, keepalive set (10 sec) LCP Open Open: IPCP, CDPCP, IPV6CP Last input never, output never, output hang never Last clearing of "show interface" counters never Input queue: 0/75/0 (size/max/drops); Total output drops: 0 Queueing strategy: weighted fair Output queue: 0/1000/64/0 (size/max total/threshold/drops) Conversations 0/0/256 (active/max active/max total) Reserved Conversations 0/0 (allocated/max allocated) Available Bandwidth 1158 kilobits/sec 5 minute input rate 163 bits/sec, 0 packets/sec 5 minute output rate 178 bits/sec, 0 packets/sec 172 packets input, 10556 bytes, 0 no buffer Received 0 broadcasts, 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort 148 packets output, 9171 bytes, 0 underruns 0 output errors, 0 collisions, 0 interface resets 0 output buffer failures, 0 output buffers swapped out 0 carrier transitions DCD=up DSR=up DTR=up RTS=up CTS=up </pre>	<pre> R6>en R6#show int se0/3/0 Serial0/3/0 is up, line protocol is up (connected) Hardware is HD64570 Internet address is 200.0.100.2/30 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation PPP, loopback not set, keepalive set (10 sec) LCP Open Open: IPCP, CDPCP, IPV6CP Last input never, output never, output hang never Last clearing of "show interface" counters never Input queue: 0/75/0 (size/max/drops); Total output drops: 0 Queueing strategy: weighted fair Output queue: 0/1000/64/0 (size/max total/threshold/drops) Conversations 0/0/256 (active/max active/max total) Reserved Conversations 0/0 (allocated/max allocated) Available Bandwidth 1158 kilobits/sec 5 minute input rate 170 bits/sec, 0 packets/sec 5 minute output rate 150 bits/sec, 0 packets/sec 157 packets input, 9776 bytes, 0 no buffer Received 0 broadcasts, 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort 125 packets output, 7834 bytes, 0 underruns 0 output errors, 0 collisions, 0 interface resets 0 output buffer failures, 0 output buffers swapped out 0 carrier transitions DCD=up DSR=up DTR=up RTS=up CTS=up </pre>
---	--

Hình 4.1 Kết quả trạng thái cổng serial trên R6 và R7

- `show ip interface brief`: Kiểm tra toàn bộ địa chỉ IP và trạng thái của các interface.
- `ping <địa chỉ IP đích>`: Kiểm tra khả năng liên lạc giữa hai router, xác nhận rằng kết nối PPP đã thiết lập thành công. Ta thực hiện ping địa chỉ ip đã cấu hình từ router R6 đến R7 và kiểm tra kết quả:

```

R6#ping 200.0.100.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.0.100.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/14 ms

```

Hình 4.2 Kết quả ping từ R6 đến R7 sau khi thiết lập PAP

4.1.2 Xác thực CHAP

Đối với kết nối giữa R7 và R8, giao thức xác thực CHAP được sử dụng nhằm tăng cường tính bảo mật trong quá trình xác thực. Khác với PAP, CHAP sử dụng cơ chế thách thức-ngắt quãng (challenge handshake), điều này giúp bảo vệ mật khẩu trong quá trình xác thực, vì mật khẩu không được truyền qua mạng dưới dạng rõ ràng. CHAP yêu cầu một quá trình xác thực lặp đi lặp lại trong suốt phiên làm việc, làm cho nó an toàn hơn so với PAP.

Trên R7, một người dùng có tên R8 và mật khẩu cisco được tạo ra. Tại giao diện Se0/3/1, giao thức đóng gói PPP được cấu hình, cùng với xác thực CHAP thông qua lệnh `ppp authentication chap`. Khác với PAP, khi cấu hình CHAP, không cần chỉ định tên người dùng để gửi đi, vì CHAP sẽ tự động sử dụng tên máy chủ (hostname) của router làm tên người dùng để thực hiện xác thực. Do đó, tên máy chủ của R7 phải khớp với tên người dùng đã cấu hình trên R8.

Tương tự, trên R8, người dùng R7 với mật khẩu cisco được khai báo, đảm bảo rằng quá trình xác thực sẽ diễn ra chính xác và an toàn giữa hai router. Giao diện Se0/3/1 của R8 được cấu hình với PPP và xác thực CHAP, giống như trên R7.

Bảng 4.2 Lệnh cấu hình CHAP trên R7 và R8

R7	R8
<code>enable</code>	<code>enable</code>
<code>configure terminal</code>	<code>configure terminal</code>
<code>username R8 secret cisco</code>	<code>username R7 secret cisco</code>
<code>interface serial0/3/1</code>	<code>interface serial0/3/1</code>
<code>encapsulation ppp</code>	<code>encapsulation ppp</code>
<code>ppp authentication chap</code>	<code>ppp authentication chap</code>
<code>no shutdown</code>	<code>no shutdown</code>

Sau khi hoàn tất việc cấu hình, các lệnh kiểm tra sau có thể được sử dụng để xác minh kết nối:

- `show interface serial0/3/1`: Lệnh này giúp kiểm tra tình trạng vật lý và giao thức trên cả hai router. Status và Protocol phải ở trạng thái "up" để xác nhận kết nối thành công.

```
R7#show interface serial0/3/1
Serial0/3/1 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 200.0.100.5/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Open
Open: IPCP, CDPCP, IPV6CP
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
  Conversations 0/0/256 (active/max active/max total)
  Reserved Conversations 0/0 (allocated/max allocated)
  Available Bandwidth 1158 kilobits/sec
5 minute input rate 228 bits/sec, 0 packets/sec
5 minute output rate 215 bits/sec, 0 packets/sec
489 packets input, 30896 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
466 packets output, 29753 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up

R8>show interface serial0/3/1
Serial0/3/1 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 200.0.100.6/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Open
Open: IPCP, CDPCP, IPV6CP
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
  Conversations 0/0/256 (active/max active/max total)
  Reserved Conversations 0/0 (allocated/max allocated)
  Available Bandwidth 1158 kilobits/sec
5 minute input rate 215 bits/sec, 0 packets/sec
5 minute output rate 229 bits/sec, 0 packets/sec
492 packets input, 31305 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
452 packets output, 28801 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

Hình 4.3 Kết quả trạng thái cổng serial trên R6 và R7

- `show ip interface brief`: Lệnh này cung cấp thông tin về địa chỉ IP và trạng thái kết nối của các giao diện.
- `ping <địa chỉ IP đích>`: Lệnh ping xác nhận rằng dữ liệu có thể truyền qua kết nối PPP đã xác thực CHAP một cách chính xác. Ta thực hiện ping địa chỉ ip đã cấu hình từ router R6 đến R7 và kiểm tra kết quả:

```
R7#ping 200.0.100.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.0.100.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/14/19 ms
```

Hình 4.4 Kết quả trạng ping từ R7 đến R8 sau khi cấu hình CHAP

Khi cấu hình PPP với CHAP, có một số lưu ý quan trọng cần nhớ. Đầu tiên, giao thức đóng gói PPP phải được bật trên cả hai đầu kết nối để hỗ trợ CHAP. Tiếp theo, thông tin người dùng và mật khẩu cần phải khớp giữa hai router. Cuối cùng, với CHAP, tên máy chủ (hostname) của router phải khớp với tên người dùng mà đối tác đã định nghĩa, đảm bảo quá trình xác thực diễn ra chính xác và an toàn.

4.2 Tunneling GRE

Trong mô hình mạng, GRE được triển khai nhằm tạo kết nối ảo giữa hai router R6 và R8, cho phép truyền dữ liệu giữa các mạng riêng qua một mạng công cộng (WAN). GRE hỗ trợ đóng gói nhiều loại giao thức lớp mạng, do đó rất phù hợp trong các tình huống cần truyền tải dữ liệu giữa hai điểm đầu xa trong mô hình mạng phức tạp.

Để thiết lập đường hầm GRE, địa chỉ mạng riêng 10.10.10.0/30 được sử dụng. R6 được gán địa chỉ IP 10.10.10.1/30 trên Tunnel0, còn R8 có địa chỉ 10.10.10.2/30.

Trên R6, giao diện Serial0/3/0 được cấu hình địa chỉ IP 200.0.100.2/30 làm địa chỉ nguồn vật lý, đảm bảo khả năng kết nối tới R8 qua mạng WAN. Sau đó, giao diện Tunnel0 được kích hoạt, gán IP 10.10.10.1/30, đồng thời chỉ định địa chỉ nguồn là Serial0/3/0 và địa chỉ đích là 200.0.100.6, tức địa chỉ serial của R8.

Trên R8, quá trình cấu hình tương tự được thực hiện. Giao diện Serial0/3/1 mang địa chỉ 200.0.100.6/30, và giao diện Tunnel0 được cấu hình IP 10.10.10.2/30. Địa chỉ nguồn tunnel là Serial0/3/1, còn địa chỉ đích là 200.0.100.2 – tức Serial của R6.

Việc cấu hình này cho phép tạo một đường hầm ảo giữa R6 và R8, từ đó các gói dữ liệu có thể được truyền qua tunnel như thể hai thiết bị nằm trong cùng một mạng nội bộ.

Bảng 4.3 Lệnh cấu hình Tunnel GRE trên R6 và R8

R6	R8
hostname R6	hostname R8
interface Serial0/3/0	interface Serial0/3/1
ip address 200.0.100.2 255.255.255.252	ip address 200.0.100.6 255.255.255.252
no shutdown	no shutdown
interface Tunnel0	interface Tunnel0
ip address 10.10.10.1 255.255.255.252	ip address 10.10.10.2 255.255.255.252

tunnel source Serial0/3/0	tunnel source Serial0/3/1
tunnel destination 200.0.100.6	tunnel destination 200.0.100.2
no shutdown	no shutdown

Để kiểm tra kết nối GRE sau khi cấu hình, có thể sử dụng lệnh:

- `show ip route | include 10.10.10`: Xác minh xem tuyến đường đến mạng tunnel đã được tạo thành công và có thể sử dụng để truyền dữ liệu.

```
R6>en
R6#show ip route | include 10.10.10.
C      10.10.10.0/30 is directly connected, Tunnel0
L      10.10.10.1/32 is directly connected, Tunnel0

R8#show ip route | include 10.10.10
C      10.10.10.0/30 is directly connected, Tunnel0
L      10.10.10.2/32 is directly connected, Tunnel0
```

Hình 4.5 Bảng định tuyến tunnel giữa R6 và R8

- `ping <địa chỉ IP đích>`: Thực hiện ping địa chỉ thiết lập tunnel giữa 2 router R6 và R8 để kiểm tra:

```
R6#ping 10.10.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/5/13 ms
```

Hình 4.6 Kết quả ping ip tunnel từ R6 đến R8

4.3 Định tuyến

4.3.1 Định tuyến ipv4

4.3.1.1 Định tuyến EIGRP tại khu vực HQ

Trong mạng HQ, các router như R4, R5, R6, R7, R8 sẽ chia sẻ các tuyến đường với nhau qua EIGRP. Tuy nhiên, R5 là router trung tâm, vì sau này nó sẽ thực hiện redistribute thông tin định tuyến và đóng vai trò chính trong việc chia sẻ và quản lý các thông tin định tuyến giữa các router khác trong mạng.

R4 chịu trách nhiệm chính cho việc cấu hình và quản lý các VLAN trong mạng. Các VLAN, chẳng hạn như VLAN 60, sẽ được cấu hình trên các sub-interface của R4, ví dụ như GigabitEthernet0/0.60 cho VLAN 60. R4 sẽ sử dụng các lệnh network để chia sẻ các thông tin định tuyến về các VLAN R4 quản lý với các router khác. R4, R5, R7 được gán ip của vlan 60 để giao tiếp và chia sẻ bảng định tuyến. R5, R7 sẽ chia sẻ thông tin của mình và lấy thông tin của tất cả vlan trên sub interface của R4 thông qua vlan 60.

Bảng 4.4 Lệnh cấu hình định tuyến eigrp trên R4

R4
router eigrp 100
network 172.27.60.0 0.0.0.31
network 172.27.10.0 0.0.0.255
network 172.27.20.0 0.0.1.255
network 172.27.30.0 0.0.0.127
network 172.27.40.0 0.0.0.63
network 172.27.50.0 0.0.0.15
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface GigabitEthernet0/0.60
end

Ta sẽ thực hiện phân tích cấu hình mẫu trên R4 như bảng 4.4 Đầu tiên, tiến trình EIGRP được kích hoạt bằng câu lệnh router eigrp 100, với AS (Autonomous System) số 100 được thống nhất sử dụng trên toàn bộ hệ thống mạng. Tiếp theo, các mạng con nội bộ thuộc khu vực HQ được khai báo thông qua các lệnh network, bao gồm:

- 172.27.60.0 0.0.0.31: VLAN 60
- 172.27.10.0 0.0.0.255: VLAN 10
- 172.27.20.0 0.0.1.255: VLAN 20

- 172.27.30.0 0.0.0.127: VLAN 30
- 172.27.40.0 0.0.0.63: VLAN 40
- 172.27.50.0 0.0.0.15: VLAN 50

Các địa chỉ này đều nằm trong dải địa chỉ nội bộ của HQ (172.27.0.0/16), phản ánh các phân đoạn mạng được gán cho các VLAN khác nhau. Để đảm bảo an toàn và tối ưu, lệnh `passive-interface default` được áp dụng để tắt gửi gói hello trên tất cả các cổng. Tuy nhiên, hai giao diện quan trọng được kích hoạt EIGRP để thiết lập mối quan hệ hàng xóm là `GigabitEthernet0/0` và `GigabitEthernet0/0.60` dùng để giao tiếp với các router khác trong khu vực HQ.

Thiết lập `passive-interface` trong EIGRP giúp kiểm soát lưu lượng định tuyến và tăng cường bảo mật bằng cách ngăn router gửi/nhận gói Hello trên các giao diện không cần thiết, như cổng kết nối đến switch hoặc người dùng. Lệnh `passive-interface default` áp dụng cho tất cả các cổng, trong khi `no passive-interface` được dùng để bật EIGRP trên các cổng cần thiết, thường là các kết nối giữa các router, đảm bảo việc trao đổi thông tin định tuyến chính xác và hiệu quả.

Đối với các router khác như R5, R6, R7 và R8, ngoài việc cấu hình EIGRP với cùng AS 100 và khai báo toàn bộ các mạng nội bộ giống R4 (các mạng thuộc dải 172.27.0.0/16), thì mỗi router đều bổ sung thêm các đường mạng kết nối liên-router và các mạng truyền dẫn ngoài HQ, cụ thể như sau:

- R5: Bổ sung các đường mạng kết nối đến các router khác thông qua các liên kết như `GigabitEthernet0/0`, `GigabitEthernet0/1`, `Serial0/3/0`, đồng thời thực hiện `redistribute ospf 1` để chia sẻ thông tin định tuyến từ OSPF sang EIGRP – đây là điểm đặc biệt giúp R5 hoạt động như một router biên giữa hai giao thức định tuyến.
- R6: Bổ sung mạng 10.10.10.0/30 cho GRE Tunnel giữa R6 và R8, và mạng 200.0.100.0/30 cho kết nối đến router R7 qua đường WAN. Giao diện `Tunnel0` và `Serial0/3/0` được mở để truyền EIGRP.

- R7: Ngoài các mạng nội bộ, R7 bổ sung hai mạng WAN là 200.0.100.0/30 (nối R6–R7) và 200.0.100.4/30 (nối R7–R8), đồng thời mở các cổng Serial và Gigabit để EIGRP hoạt động trên các liên kết này.
- R8: Bổ sung các mạng giống R6, bao gồm 10.10.10.0/30 (tunnel với R6) và 200.0.100.4/30 (kết nối với R7). Cấu hình Tunnel0 tại R8 tương ứng với Tunnel tại R6, giúp đảm bảo đường truyền ảo hoạt động và được quảng bá qua EIGRP.

Tóm lại, tất cả các router đều thống nhất sử dụng AS 100 và quảng bá toàn bộ mạng nội bộ HQ. Tuy nhiên, để đảm bảo kết nối liên vùng và truyền tải thông tin định tuyến đầy đủ, các router ngoại vi như R5–R8 được bổ sung thêm các mạng WAN và tunnel phù hợp với vai trò kết nối liên router và các thiết bị đầu cuối ở khu vực ngoài HQ. Sau khi thực hiện xong ta có sẽ thực hiện lệnh `show ip route eigrp` trên các router để kiểm tra kết quả bảng định tuyến. Dưới đây là kết quả định tuyến eigrp trên R4:

```
R4#
R4#sh ip route ei
R4#sh ip route eigrp
    10.0.0.0/8 is variably subnetted, 7 subnets, 3 masks
D       10.10.10.0/30 [90/27394560] via 172.27.60.7, 02:07:46, GigabitEthernet0/0.60
D EX    10.28.1.0/24 [170/284160] via 172.27.60.6, 02:07:46, GigabitEthernet0/0.60
D EX    10.28.10.1/32 [170/284160] via 172.27.60.6, 02:06:55, GigabitEthernet0/0.60
D EX    10.28.12.1/32 [170/284160] via 172.27.60.6, 02:06:55, GigabitEthernet0/0.60
D EX    10.28.20.1/32 [170/284160] via 172.27.60.6, 02:06:55, GigabitEthernet0/0.60
D EX    10.28.30.1/32 [170/284160] via 172.27.60.6, 02:06:55, GigabitEthernet0/0.60
D EX    10.28.31.1/32 [170/284160] via 172.27.60.6, 02:06:55, GigabitEthernet0/0.60
    200.0.100.0/30 is subnetted, 3 subnets
D       200.0.100.0 [90/2172416] via 172.27.60.7, 02:07:46, GigabitEthernet0/0.60
D       200.0.100.4 [90/2172416] via 172.27.60.7, 02:07:46, GigabitEthernet0/0.60
D       200.0.100.8 [90/2172416] via 172.27.60.6, 02:07:46, GigabitEthernet0/0.60
D*EX 0.0.0.0/0 [170/6780416] via 172.27.60.6, 02:07:46, GigabitEthernet0/0.60
```

Hình 4.7 Kết quả bảng định tuyến eigrp trên R4

Ta có thể thực hiện kiểm tra `neighbor` trên R7 để xem tất cả router được định tuyến eigrp thành công chưa vì R7 nối với tất cả các router trong khu vực HQ. Có thể thấy là nó đã thiết lập láng giềng thành công với R6, R8, R4, R5 thông qua danh sách ip:

```

R7>en
R7#sh ip eig
R7#sh ip eigrp ne
IP-EIGRP neighbors for process 100
H   Address           Interface      Hold Uptime      SRTT   RTO   Q   Seq
   (sec)              (ms)          Cnt   Num
0   200.0.100.2        Se0/3/0       14    00:14:16  40     1000  0   33
1   200.0.100.6        Se0/3/1       10    00:14:16  40     1000  0   33
2   172.27.60.1        Gig0/0        13    00:14:07  40     1000  0   24
3   172.27.60.6        Gig0/0        13    00:14:07  40     1000  0   51

R7#

```

Hình 4.8 Eigrp neighbor trên router R7

4.3.1.2 Định tuyến OSPF tại khu vực Branch

Tại khu vực Branch, OSPF được triển khai dưới dạng OSPF đa khu vực (Multi-Area OSPF) để tối ưu hóa quá trình trao đổi thông tin định tuyến. Các router R1, R2 và R3 được cấu hình để kết nối với Area 0 (Backbone Area) và các khu vực khác như Area 1 và Area 3, giúp giảm tải cho backbone và phân chia mạng theo từng khu vực chức năng.

Bảng 4.5 Lệnh cấu hình định tuyến ospf trên R3

R3
interface Loopback0
ip address 10.28.30.1 255.255.255.0
interface Loopback1
ip address 10.28.31.1 255.255.255.128
router ospf 1
router-id 3.3.3.3
network 10.28.1.3 0.0.0.0 area 0
network 10.28.30.0 0.0.0.255 area 3
network 10.28.31.0 0.0.0.127 area 3

passive-interface default

no passive-interface GigabitEthernet0/0

Trên router R1, các interface Loopback0 và Loopback1 được đưa vào Area 1, trong khi interface kết nối tới mạng trung tâm (10.28.1.1) thuộc Area 0. Việc chia tách này giúp cô lập các mạng con, cải thiện khả năng hội tụ và khả năng mở rộng. Câu lệnh `passive-interface default` giúp chặn gửi nhận OSPF Hello trên tất cả các interface, chỉ cho phép các interface cần thiết (như GigabitEthernet0/0) hoạt động định tuyến nhờ `no passive-interface`.

Router R2 được cấu hình với Area 0 và Area 3. Interface Loopback0 (10.28.20.1/25) thuộc Area 3, trong khi liên kết với backbone là Area 0. Điều này biến R2 thành Area Border Router (ABR) giữa Area 0 và Area 3.

Router R3 được cấu hình tham gia định tuyến OSPF với hai khu vực: Area 0 (backbone) và Area 3. Trong cấu hình, R3 sử dụng hai địa chỉ loopback là 10.28.30.1/24 và 10.28.31.1/25 để mô phỏng các mạng nội bộ và được quảng bá vào Area 3 thông qua các lệnh `network`. Lệnh `router-id 3.3.3.3` được sử dụng để định danh R3 trong tiến trình OSPF. Để tăng tính bảo mật và tránh gửi các gói tin Hello không cần thiết, lệnh `passive-interface default` được áp dụng để mặc định tắt chế độ gửi Hello trên tất cả các cổng. Sau đó, cổng GigabitEthernet0/0 – cổng kết nối thực tế giữa các router – được kích hoạt trở lại bằng lệnh `no passive-interface` nhằm đảm bảo thiết lập láng giềng OSPF thành công.

Tương tự R3, các router R1 và R2 cũng được cấu hình OSPF theo mô hình đa khu vực. Tuy nhiên, thay vì sử dụng các mạng loopback thuộc dải 10.28.30.0/24 và 10.28.31.0/25 như R3, thì R1 sử dụng các mạng nội bộ 10.28.10.0/23 và 10.28.12.0/23 thuộc Area 1; còn R2 sử dụng mạng loopback 10.28.20.0/25 trong Area 3.

Các router này đều tuân theo cùng một nguyên tắc cấu hình OSPF nhưng khác nhau về địa chỉ mạng, khu vực OSPF tham gia và router ID cụ thể. Dùng lệnh `show ip route ospf` để kiểm tra bảng định tuyến.

```

R1>en
R1#sh ip route ospf
R1#sh ip route ospf
10.0.0.0/8 is variably subnetted, 10 subnets, 4 masks
O E2 10.10.10.0 [110/20] via 10.28.1.4, 00:01:18, GigabitEthernet0/0
O IA 10.28.20.1 [110/2] via 10.28.1.2, 00:01:18, GigabitEthernet0/0
O IA 10.28.30.1 [110/2] via 10.28.1.3, 00:01:18, GigabitEthernet0/0
O IA 10.28.31.1 [110/2] via 10.28.1.3, 00:01:18, GigabitEthernet0/0
172.27.0.0/16 is variably subnetted, 6 subnets, 6 masks
O E2 172.27.10.0 [110/20] via 10.28.1.4, 00:01:18, GigabitEthernet0/0
O E2 172.27.20.0 [110/20] via 10.28.1.4, 00:01:18, GigabitEthernet0/0
O E2 172.27.30.0 [110/20] via 10.28.1.4, 00:01:18, GigabitEthernet0/0
O E2 172.27.40.0 [110/20] via 10.28.1.4, 00:01:18, GigabitEthernet0/0
O E2 172.27.50.0 [110/20] via 10.28.1.4, 00:01:18, GigabitEthernet0/0
O E2 172.27.60.0 [110/20] via 10.28.1.4, 00:01:18, GigabitEthernet0/0
200.0.100.0/30 is subnetted, 3 subnets
O E2 200.0.100.0 [110/20] via 10.28.1.4, 00:01:18, GigabitEthernet0/0
O E2 200.0.100.4 [110/20] via 10.28.1.4, 00:01:18, GigabitEthernet0/0
O E2 200.0.100.8 [110/20] via 10.28.1.4, 00:01:18, GigabitEthernet0/0
O*E2 0.0.0.0/0 [110/1] via 10.28.1.4, 00:01:18, GigabitEthernet0/0

```

Hình 4.9 Kết quả bảng định tuyến ospf trên R1

Sau khi cấu hình xong có thể kiểm tra ospf neighbor trên R1 để xem có thấy các router khác đã được thiết lập láng giềng:

```

R1#
R1#sh ip
R1#sh ip os
R1#sh ip ospf ne
R1#sh ip ospf neighbor

```

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	1	FULL/BDR	00:00:37	10.28.1.3	GigabitEthernet0/0
2.2.2.2	1	2WAY/DROTHER	00:00:37	10.28.1.2	GigabitEthernet0/0
5.5.5.5	1	FULL/DR	00:00:37	10.28.1.4	GigabitEthernet0/0

```

R1#
R1#
R1#
R1#

```

Hình 4.10 ospf neighbor trên router R1

4.3.1.3 Định tuyến mặc định từ router R5 đến Access

Ở phần này thực hiện lệnh `ip route 0.0.0.0 0.0.0.0 200.0.100.10`. Lệnh này định nghĩa rằng mọi gói tin không biết đích sẽ được chuyển tiếp đến địa chỉ IP 200.0.100.10 – tức router ACCESS. Tuyến mặc định này sau đó sẽ được phân phối (redistribute) vào các giao thức định tuyến đang chạy trên R5 như OSPF và EIGRP, để các router khác trong hệ thống cũng biết cách đi ra ngoài mạng.

4.3.1.4 Redistribution giữa OSPF và EIGRP trên R5

Trong mô hình mạng này, router R5 đóng vai trò trung gian giữa hai miền định tuyến sử dụng hai giao thức khác nhau: EIGRP trong khu vực nội bộ và OSPF trong phần mạng kết nối ra bên ngoài. Để đảm bảo các thiết bị trong cả hai miền định tuyến có thể học và sử dụng thông tin định tuyến lẫn nhau, cần triển khai kỹ thuật redistribution – tái phân phối định tuyến giữa hai giao thức trên cùng một router.

Bảng 4.6 Lệnh cấu hình redistribution ospf eigrp trên R5

router eigrp 100	router ospf 1
network 172.27.60.0 0.0.0.31	router-id 5.5.5.5
network 172.27.10.0 0.0.0.255	network 10.28.1.4 0.0.0.0 area 0
network 172.27.20.0 0.0.1.255	redistribute eigrp 100 subnets
network 172.27.30.0 0.0.0.127	default-information originate
network 172.27.40.0 0.0.0.63	passive-interface default
network 172.27.50.0 0.0.0.15	no passive-interface GigabitEthernet0/0
redistribute ospf 1 metric 10000 100 255 1 1500	no passive-interface GigabitEthernet0/1
redistribute static	no passive-interface Serial0/3/0
passive-interface default	end

— Redistribute từ EIGRP sang OSPF:

Trên R5, tiến trình OSPF được khởi tạo với router-id là 5.5.5.5. R5 đưa mạng kết nối về backbone (10.28.1.4) vào OSPF Area 0 thông qua lệnh network 10.28.1.4 0.0.0.0 area 0. Để chia sẻ các route học được từ tiến trình EIGRP, lệnh redistribute eigrp 100 subnets được sử dụng. Tùy chọn subnets đảm bảo rằng các subnet có độ dài khác nhau đều được tái phân phối, thay vì chỉ các route classful.

Bên cạnh đó, tuyến mặc định đã được cấu hình trên R5 (ip route 0.0.0.0 0.0.0.0 200.0.100.10) sẽ được quảng bá vào OSPF bằng lệnh default-information originate.

Điều này cho phép các router khác trong OSPF biết đường đi ra Internet thông qua R5. Để kiểm soát việc gửi bản tin OSPF Hello, R5 cấu hình passive-interface default để tắt chế độ gửi nhận OSPF trên tất cả các interface, và chỉ mở lại trên những cổng cần thiết như GigabitEthernet0/0, GigabitEthernet0/1 và Serial0/3/0.

— Redistribute từ OSPF sang EIGRP:

Ở chiều ngược lại, trong tiến trình EIGRP (AS 100), R5 đưa các mạng nội bộ như 172.27.10.0/24, 172.27.20.0/23, ..., 172.27.60.0/27 vào định tuyến bằng các lệnh network. Để chia sẻ các route học được từ OSPF, lệnh redistribute ospf 1 metric 10000 100 255 1 1500 được sử dụng. Lệnh này yêu cầu bắt buộc cung cấp các thông số metric vì OSPF không sử dụng các thành phần metric tương tự như EIGRP.

```
R5>en
R5#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, Ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 200.0.100.10 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 8 subnets, 3 masks
D 10.10.10.0/30 [90/27394560] via 172.27.60.7, 02:06:30, GigabitEthernet0/1
C 10.28.1.0/24 is directly connected, GigabitEthernet0/0
L 10.28.1.4/32 is directly connected, GigabitEthernet0/0
O IA 10.28.10.1/32 [110/2] via 10.28.1.1, 02:05:49, GigabitEthernet0/0
O IA 10.28.12.1/32 [110/2] via 10.28.1.1, 02:05:49, GigabitEthernet0/0
O IA 10.28.20.1/32 [110/2] via 10.28.1.2, 02:05:49, GigabitEthernet0/0
O IA 10.28.30.1/32 [110/2] via 10.28.1.3, 02:05:49, GigabitEthernet0/0
O IA 10.28.31.1/32 [110/2] via 10.28.1.3, 02:05:49, GigabitEthernet0/0
172.27.0.0/16 is variably subnetted, 7 subnets, 7 masks
D 172.27.10.0/24 [90/30720] via 172.27.60.1, 02:06:30, GigabitEthernet0/1
D 172.27.20.0/23 [90/30720] via 172.27.60.1, 02:06:30, GigabitEthernet0/1
D 172.27.30.0/25 [90/30720] via 172.27.60.1, 02:06:30, GigabitEthernet0/1
D 172.27.40.0/26 [90/30720] via 172.27.60.1, 02:06:30, GigabitEthernet0/1
D 172.27.50.0/28 [90/30720] via 172.27.60.1, 02:06:30, GigabitEthernet0/1
C 172.27.60.0/27 is directly connected, GigabitEthernet0/1
L 172.27.60.6/32 is directly connected, GigabitEthernet0/1
200.0.100.0/24 is variably subnetted, 4 subnets, 2 masks
D 200.0.100.0/30 [90/2172416] via 172.27.60.7, 02:06:30, GigabitEthernet0/1
D 200.0.100.4/30 [90/2172416] via 172.27.60.7, 02:06:30, GigabitEthernet0/1
C 200.0.100.8/30 is directly connected, Serial0/3/0
L 200.0.100.9/32 is directly connected, Serial0/3/0
S* 0.0.0.0/0 [1/0] via 200.0.100.10

R2>en
R2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, Ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 10.28.1.4 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 9 subnets, 4 masks
O E2 10.10.10.0/30 [110/20] via 10.28.1.4, 02:07:39, GigabitEthernet0/0
C 10.28.1.0/24 is directly connected, GigabitEthernet0/0
L 10.28.1.2/32 is directly connected, GigabitEthernet0/0
O IA 10.28.10.1/32 [110/2] via 10.28.1.1, 02:07:39, GigabitEthernet0/0
O IA 10.28.12.1/32 [110/2] via 10.28.1.1, 02:07:39, GigabitEthernet0/0
C 10.28.20.0/25 is directly connected, Loopback0
L 10.28.20.1/32 is directly connected, Loopback0
O IA 10.28.30.1/32 [110/2] via 10.28.1.3, 02:07:39, GigabitEthernet0/0
O IA 10.28.31.1/32 [110/2] via 10.28.1.3, 02:07:39, GigabitEthernet0/0
172.27.0.0/16 is variably subnetted, 6 subnets, 6 masks
O E2 172.27.10.0/24 [110/20] via 10.28.1.4, 02:07:39, GigabitEthernet0/0
O E2 172.27.20.0/23 [110/20] via 10.28.1.4, 02:07:39, GigabitEthernet0/0
O E2 172.27.30.0/25 [110/20] via 10.28.1.4, 02:07:39, GigabitEthernet0/0
O E2 172.27.40.0/26 [110/20] via 10.28.1.4, 02:07:39, GigabitEthernet0/0
O E2 172.27.50.0/28 [110/20] via 10.28.1.4, 02:07:39, GigabitEthernet0/0
O E2 172.27.60.0/27 [110/20] via 10.28.1.4, 02:07:39, GigabitEthernet0/0
200.0.100.0/30 is subnetted, 3 subnets
O E2 200.0.100.0/30 [110/20] via 10.28.1.4, 02:07:39, GigabitEthernet0/0
O E2 200.0.100.4/30 [110/20] via 10.28.1.4, 02:07:39, GigabitEthernet0/0
O E2 200.0.100.8/30 [110/20] via 10.28.1.4, 02:07:39, GigabitEthernet0/0
O*E2 0.0.0.0/0 [110/1] via 10.28.1.4, 02:07:39, GigabitEthernet0/0
```

Hình 4.11 Kết quả bảng định tuyến trên R5 và R2 sau khi redistribution

Khi thực hiện cấu hình lệnh xong ta có thể kiểm tra bảng định tuyến trên R5 bằng lệnh show ip route và kiểm tra bảng định tuyến của một router bất kỳ xem R5 có phân phối được thông tin định tuyến giữa 2 giao thức hay không. Sau đây là kết quả bảng định tuyến trên R5 và R2 để cho thấy kết quả hoạt động của R5 cũng như thông tin định tuyến mà các Router của 2 khu vực chia sẻ được với nhau như hình 4.9

4.3.2 Định tuyến ipv6

4.3.2.1 Định tuyến EIGRP tại khu vực HQ

Trong mạng HQ, giao thức định tuyến EIGRP for IPv6 được triển khai để thiết lập quá trình trao đổi thông tin định tuyến giữa các router R4 đến R8. Các bước cấu hình định tuyến IPv6 bao gồm:

Kích hoạt định tuyến IPv6 toàn cục

Trên tất cả các router trong mạng HQ (R4, R5, R6, R7, R8), ta kích hoạt chức năng định tuyến IPv6 toàn cục bằng lệnh: `ipv6 unicast-routing`

Cấu hình IPv6 và EIGRP trên các sub-interface R4:

Router R4 chịu trách nhiệm định tuyến giữa các VLAN trong mạng nội bộ, nên được gán các địa chỉ IPv6 theo từng VLAN cụ thể thông qua các sub-interface:

Bảng 4.7 Lệnh cấu hình `eigrp ipv6` cho sub interface trên R4

R4
<code>interface Gig0/0.10</code>
<code>encapsulation dot1Q 10</code>
<code>ipv6 address 2019:ABBA:CDDC:0::1/64</code>
<code>ipv6 address FE80::1 link-local</code>
<code>ipv6 enable</code>
<code>ipv6 eigrp 10</code>

Các sub-interface VLAN 20 đến 50 cấu hình tương tự, chỉ thay đổi địa chỉ mạng. Điều này cho phép các PC trong các VLAN khác nhau giao tiếp với nhau qua địa chỉ IPv6 và tham gia vào quá trình định tuyến với EIGRP.

Cấu hình EIGRP IPv6 trên các router trong HQ:

Trên từng router trong site HQ, cấu hình `ipv6 router eigrp 10` với router-id tương ứng, và kích hoạt EIGRP trên các interface tham gia định tuyến:

Bảng 4.8 Lệnh cấu hình `eigrp ipv6` trên r5

R5
<code>ipv6 router eigrp 10</code>
<code>eigrp router-id 5.5.5.5</code>

interface Se0/3/0
ipv6 eigrp 10
interface Gig0/1
ipv6 eigrp 10

Router R4, R6, R7, R8: mỗi router đều cấu hình router-id khác nhau và kích hoạt EIGRP trên các interface liên kết (Gigabit hoặc Serial) tham gia định tuyến trong mạng HQ.

Định tuyến mặc định đến site ACCESS:

Trên router R5, cấu hình một tuyến mặc định đến site Access sử dụng địa chỉ IPv6 đích là ::/0, với next-hop là router Access: ipv6 route ::/0 2019:ABBA:AAAA:1::1. Tuyến này được redistribute (phân phối) vào giao thức EIGRP để các router trong site HQ biết cách gửi gói tin đến bên ngoài: ipv6 router eigrp 10, redistribute static.

```

R5#
R5#sh ipv
R5#sh ipv6 route
IPv6 Routing Table - 13 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S    ::/0 [1/0]
    via 2019:ABBA:AAAA:1::1
C    2019:ABBA:AAAA:1::/64 [0/0]
    via Serial0/3/0, directly connected
L    2019:ABBA:AAAA:1::2/128 [0/0]
    via Serial0/3/0, receive
C    2019:ABBA:BBBB:1::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L    2019:ABBA:BBBB:1::2/128 [0/0]
    via GigabitEthernet0/1, receive
D    2019:ABBA:CCCC:1::/64 [90/2172416]
    via FE80::2:3, GigabitEthernet0/1
D    2019:ABBA:CDDC::/64 [90/30720]
    via FE80::2:4, GigabitEthernet0/1
D    2019:ABBA:CDDC:1::/64 [90/30720]
    via FE80::2:4, GigabitEthernet0/1
D    2019:ABBA:CDDC:2::/64 [90/30720]
    via FE80::2:4, GigabitEthernet0/1
D    2019:ABBA:CDDC:3::/64 [90/30720]
    via FE80::2:4, GigabitEthernet0/1
D    2019:ABBA:CDDC:4::/64 [90/30720]
    via FE80::2:4, GigabitEthernet0/1
D    2019:ABBA:DDDD:1::/64 [90/2172416]
    via FE80::2:3, GigabitEthernet0/1
L    FF00::/8 [0/0]
    via Null0, receive

```

Hình 4.12 Kết quả bảng định tuyến ipv6 trên R5

Sau khi thực hiện xong cấu hình định tuyến ipv6 trên khu vực HQ ta dùng lệnh show ip route để kiểm tra bảng định tuyến của router bất kì để xác nhận kết quả thực hiện. Hình 4.9 trên là kết quả thực hiện thành công trên R5.

4.4 Chuyển mạch

4.4.1 Cấu hình VTP và VLAN

Để quản lý thống nhất cơ sở dữ liệu VLAN tại khu vực HQ, hệ thống sử dụng giao thức VTP với vtp domain là tdtu và vtp password là tdtuvn. Switch S1 được cấu hình ở chế độ VTP server thông qua lệnh vtp mode server để tạo và phân phối VLAN, còn các switch còn lại (S2, S3, S4) được cấu hình là VTP client thông qua lệnh vtp mode client, giúp tự động đồng bộ VLAN từ server mà không cần cấu hình thủ công.

Trên VTP Server S1, các VLAN sau được tạo ra để phục vụ cho các đơn vị và mục đích riêng biệt:

- VLAN 10 – UNIT1
- VLAN 20 – UNIT2
- VLAN 30 – UNIT3
- VLAN 40 – GUEST
- VLAN 50 – SERVERS
- VLAN 60 – MANAGEMENT

```
S1>en
Password:
S1#sh vlan br
```

VLAN	Name	Status	Ports
1	default	active	Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10	UNIT1	active	
20	UNIT2	active	
30	UNIT3	active	
40	GUEST	active	
50	SERVERS	active	
60	MANAGEMENT	active	Fa0/1
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
S1#
S1#
```

Hình 4.13 Danh sách các vlan được tạo trên S1

4.4.2 Cấu hình giao thức *Spanning Tree*

Hệ thống chuyển mạch trong mạng được cấu hình sử dụng Rapid PVST+ một biến thể nâng cao của giao thức STP truyền thống, cho phép thời gian hội tụ nhanh hơn khi có sự thay đổi topology như link down hoặc thiết bị bị ngắt kết nối. Rapid

PVST+ hoạt động riêng biệt trên từng VLAN, từ đó đảm bảo tính linh hoạt và hiệu quả trong kiểm soát vòng lặp mạng.

Cấu hình để kích hoạt chế độ Rapid PVST+ trên toàn bộ hệ thống switch: spanning-tree mode rapid-pvst

Để kiểm soát đường đi ưu tiên và hướng lưu lượng theo thiết kế, các Root Bridge được phân công như sau:

- Switch S1 được thiết lập là Root Bridge cho VLAN 10, 20, 30, là các VLAN dành cho đơn vị (UNIT), với giá trị priority là 4096 – thấp hơn giá trị mặc định (32768), giúp S1 được ưu tiên làm gốc với lệnh spanning-tree vlan 10,20,30 priority 4096
- Switch S2 được chọn làm Root Bridge cho VLAN 40, 50, 60, đại diện cho các VLAN khách, server và quản lý. Priority cũng được thiết lập là 4096 với lệnh spanning-tree vlan 40,50,60 priority 4096.

```
S1#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
            Address    0006.2A86.7175
            Cost        12
            Port        27 (Port-channel1)
            Hello Time   2 sec    Max Age 20 sec    Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
            Address    0060.4785.744B
            Hello Time   2 sec    Max Age 20 sec    Forward Delay 15 sec
            Aging Time   20

Interface    Role Sts Cost      Prio.Nbr Type
-----
Fa0/6        Desg FWD 19        128.6    P2p
Po1          Root FWD 12        128.27   Shr
Po2          Desg FWD 12        128.28   Shr

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    4106
            Address    0060.4785.744B
            This bridge is the root
            Hello Time   2 sec    Max Age 20 sec    Forward Delay 15 sec

  Bridge ID  Priority    4106 (priority 4096 sys-id-ext 10)
            Address    0060.4785.744B
            Hello Time   2 sec    Max Age 20 sec    Forward Delay 15 sec
            Aging Time   20

Interface    Role Sts Cost      Prio.Nbr Type
-----
Fa0/6        Desg FWD 19        128.6    P2p
Po1          Desg FWD 12        128.27   Shr
Po2          Desg FWD 12        128.28   Shr

VLAN0020
  Spanning tree enabled protocol rstp
  Root ID    Priority    4116
            Address    0006.2A86.7175
            Cost        12
            Port        27 (Port-channel1)
            Hello Time   2 sec    Max Age 20 sec    Forward Delay 15 sec

  Bridge ID  Priority    4116 (priority 4096 sys-id-ext 11)
            Address    0060.4785.744B
            Hello Time   2 sec    Max Age 20 sec    Forward Delay 15 sec
            Aging Time   20

Interface    Role Sts Cost      Prio.Nbr Type
-----
Fa0/6        Desg FWD 19        128.6    P2p
Po1          Root FWD 12        128.27   Shr
Po2          Desg FWD 12        128.28   Shr
```

Hình 4.14 Spanning tree trên switch S1

Sau khi cấu hình có thể dùng lệnh show spanning-tree trên switch để kiểm chứng thông tin cấu hình.

4.4.3 VLAN quản lý và truy cập SSH

Để hỗ trợ quản trị tập trung và an toàn, tất cả các switch đều được gán địa chỉ IP trong VLAN 60 (vùng quản lý) với subnet /27 là 172.27.60.0/27

Mỗi switch sử dụng default-gateway là 172.27.60.1 để có thể kết nối ra ngoài, đồng thời cho phép truy cập SSH từ xa. Các bước cấu hình SSH gồm:

Bảng 4.9 Lệnh cấu hình ssh trên các switch

SW
ip domain-name tdtu.vn
crypto key generate rsa modulus 1024
username admin privilege 15 secret cisco
line vty 0 4
login local
transport input ssh

Việc cấu hình SSH giúp bảo mật phiên làm việc từ xa, tránh truy cập trái phép và nâng cao tính bảo mật hệ thống mạng.

4.4.4 Router-on-a-Stick – Kết nối giữa các VLAN

Để các VLAN có thể liên lạc với nhau, hệ thống triển khai mô hình Router-on-a-Stick thông qua router R4. Cổng kết nối giữa R4 và switch SW1 (FastEthernet0/6) được cấu hình ở chế độ trunk, cho phép truyền dữ liệu của nhiều VLAN.

Việc chỉ định .60 là native VLAN đảm bảo tương thích với cấu hình trunk trên switch, nơi VLAN 60 cũng được khai báo là native. Trên cổng switch S1 nối đến router R4 cũng sẽ được thiết lập đường native vlan 60 và cho phép những vlan giao tiếp thông qua cổng này. Trên R4, mỗi subinterface tương ứng với một VLAN:

Bảng 4.10 Lệnh cấu hình router on a stick trên R4

R4

interface Gig0/0.10
encapsulation dot1Q 10
ip address 172.27.10.1 255.255.255.0
...
interface Gig0/0.60
encapsulation dot1Q 60 native
ip address 172.27.60.1 255.255.255.224

Kiểm tra vlan được gán bằng lệnh show ip int br trên R4 :

```

R4#sh ip int br
Interface                IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0       unassigned      YES manual  up              up
GigabitEthernet0/0.10    172.27.10.1     YES manual  up              up
GigabitEthernet0/0.20    172.27.20.1     YES manual  up              up
GigabitEthernet0/0.30    172.27.30.1     YES manual  up              up
GigabitEthernet0/0.40    172.27.40.1     YES manual  up              up
GigabitEthernet0/0.50    172.27.50.1     YES manual  up              up
GigabitEthernet0/0.60    172.27.60.1     YES manual  up              up
GigabitEthernet0/1       unassigned      YES unset   administratively down down
GigabitEthernet0/2       unassigned      YES unset   administratively down down
Serial0/3/0              unassigned      YES unset   administratively down down
Serial0/3/1              unassigned      YES unset   administratively down down
Vlan1                    unassigned      YES unset   administratively down down
R4#

```

Hình 4.15 Kết quả tạo và gán ip vlan sub interface trên R4

4.4.5 Cấu hình EtherChannel với LACP

Nhằm tăng băng thông và tính dự phòng, các kết nối giữa các switch được cấu hình EtherChannel sử dụng giao thức LACP. Giao thức này cho phép các switch thương lượng việc gộp các cổng vật lý thành một kênh logic duy nhất gọi là Port-Channel. Các kết nối cụ thể như sau:

Bảng 4.11 Kết nối port channel

Cặp Switch	Cổng S1/S3/S2/S4	Channel Group
S1 ↔ S2	Fa0/2, Fa0/3	1
S1 ↔ S3	Fa0/4, Fa0/5	2

S2 ↔ S4	Fa0/4, Fa0/5	3
S3 ↔ S4	Fa0/1, Fa0/2	4

Dưới đây là ví dụ về lệnh cấu hình trên switch S1:

Bảng 4.12 Lệnh cấu hình ether channel trên switch S1

S2
interface range fa0/2 - 3
channel-group 1 mode active
interface port-channel 1
switchport mode trunk
interface range fa0/4 - 5
channel-group 2 mode active
interface port-channel 2
switchport mode trunk

Trong đó:

- Câu lệnh channel-group <số> mode active dùng để thêm các cổng vào nhóm EtherChannel với chế độ active, nghĩa là sử dụng LACP để thương lượng.
- Cấu hình switchport mode trunk trên các port-channel giúp truyền nhiều VLAN giữa các switch mà không bị chặn.
- Tất cả các port-channel đều hoạt động trunking 802.1Q, đảm bảo các VLAN như VLAN 10, 20, 30... đều có thể đi qua toàn bộ hệ thống switch.

Tương tự, các switch khác cũng được cấu hình tương ứng. Toàn bộ port-channel được đặt ở chế độ trunk, cho phép truyền tất cả VLAN giữa các switch, đảm

bảo tất cả các đường kết nối song song giữa switch đều được cấu hình EtherChannel chuẩn.

Sau khi thực hiện cấu hình xong có thể dùng lệnh `show etherchannel summary` để kiểm tra thông tin port cũng như giao thức được sử dụng để kết hợp kênh. Dưới đây là kết quả mẫu trên switch S1 sau khi cấu hình:

```
S1#show etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3        S - Layer2
        U - in use        f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)        LACP        Fa0/2(P) Fa0/3(P)
2      Po2(SU)        LACP        Fa0/4(P) Fa0/5(P)
```

Hình 4.16 Kết quả etherchannel trên switch S1

4.5 NAT và DHCP

4.5.1 Cấu hình NAT

NAT là một kỹ thuật quan trọng giúp chuyển đổi địa chỉ IP trong mạng nội bộ (private) sang địa chỉ IP công cộng khi kết nối với Internet. Để áp dụng NAT trên router Access, cần thực hiện các bước sau:

Xác định giao diện inside và outside: GigabitEthernet0/0 (IP công cộng 203.0.113.254) là giao diện outside, nơi kết nối với ISP. Serial0/3/0 (IP 200.0.100.10) là giao diện inside, kết nối với mạng nội bộ và chi nhánh. Và thực hiện ip nat inside và outside lần lượt cho gi0/0 và se0/3/0.

Tạo Access-List: Để cho phép NAT cho các dải địa chỉ IP trong mạng nội bộ (HQ và Branch), chúng ta sử dụng Access-List. Trong trường hợp này, Access-List 1 sẽ cho phép dải địa chỉ IP 172.27.0.0/16 và 10.28.0.0/16.

Áp dụng NAT Overload (PAT): Sau khi tạo Access-List, chúng ta cấu hình NAT Overload để tất cả các thiết bị trong mạng nội bộ có thể chia sẻ một địa chỉ IP công cộng khi truy cập Internet. Điều này được thực hiện qua câu lệnh sau: ip nat inside source list 1 interface GigabitEthernet0/0 overload

Cấu hình route mặc định: Cuối cùng, cấu hình route mặc định giúp router Access chuyển tiếp các gói tin không xác định đến ISP bằng lệnh ip route 0.0.0.0 0.0.0.0 203.0.113.1.

Quá trình cấu hình trên ISP bao gồm việc thiết lập giao diện GigabitEthernet0/0 với địa chỉ IP 203.0.113.1/24 để kết nối với router Access. Sau đó, cấu hình route mặc định ip route 0.0.0.0 0.0.0.0 203.0.113.254 để chuyển tiếp gói tin đến Access. Loopback0 nhằm đảm bảo các gói tin tới DNS server được chuyển tiếp đúng cách. Sau khi cấu hình dùng lệnh show run để kiểm tra trên interface đã cấu hình.

```
interface Serial0/3/0
ip address 200.0.100.10 255.255.255.252
ip nat inside
ipv6 address FE80::1:1 link-local
ipv6 address 2019:ABBA:AAAA:1::1/64
clock rate 2000000

interface GigabitEthernet0/0
ip address 203.0.113.254 255.255.255.0
ip nat outside
duplex auto
speed auto

ip nat inside source list 1 interface GigabitEthernet0/0 overload
ip nat inside source static tcp 172.27.60.10 80 203.0.113.254 80
ip nat inside source static tcp 172.27.60.10 443 203.0.113.254 443
ip nat inside source static tcp 172.27.50.10 80 203.0.113.254 80
ip nat inside source static tcp 172.27.50.10 443 203.0.113.254 443
ip classless
ip route 0.0.0.0 0.0.0.0 200.0.100.1
ip route 0.0.0.0 0.0.0.0 200.0.100.9
ip route 172.27.0.0 255.255.0.0 200.0.100.9
ip route 172.28.0.0 255.255.0.0 200.0.100.9
ip route 0.0.0.0 0.0.0.0 203.0.113.1
!
ip flow-export version 9
!
access-list 1 permit 172.27.0.0 0.0.255.255
access-list 1 permit 10.28.0.0 0.0.255.255
```

Hình 4.17 NAT trên router ACCESS

4.5.2 Cấu hình Port Forwarding cho HTTPS và HTTP

Chuyển tiếp cổng cho phép các yêu cầu từ bên ngoài (Internet) tới một địa chỉ IP công cộng được chuyển tiếp tới một địa chỉ IP nội bộ. Đối với trường hợp này, chúng ta cấu hình chuyển tiếp cổng HTTP (port 80) và HTTPS (port 443) từ địa chỉ

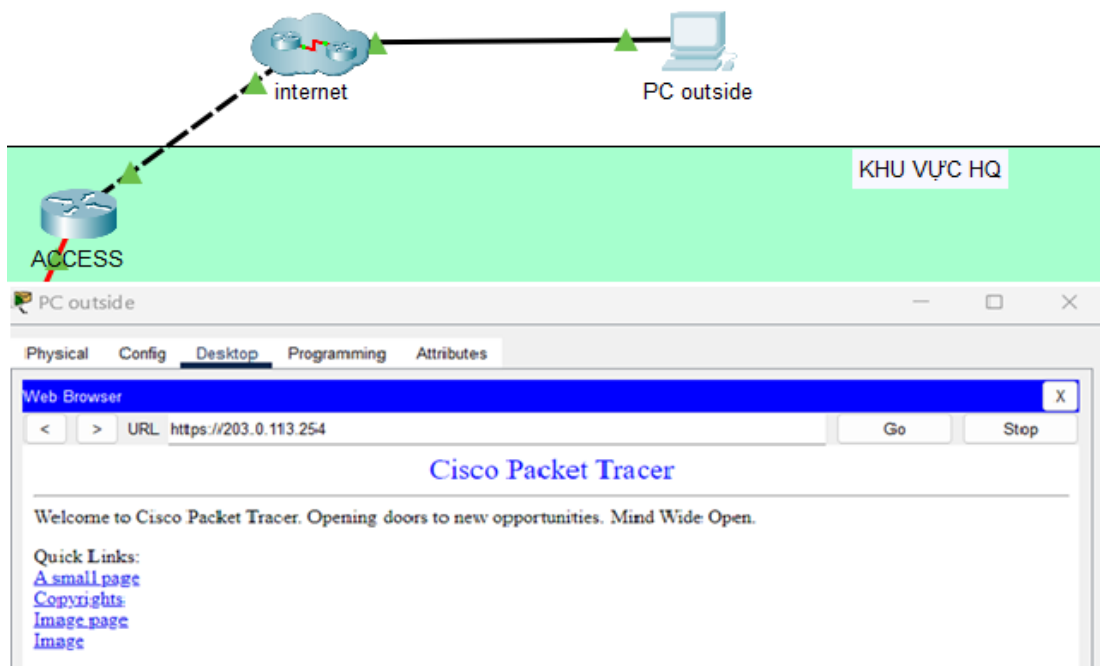
IP công cộng của router Access (203.0.113.254) đến một máy chủ trong mạng nội bộ (IP 172.27.50.10). Cấu hình chuyển tiếp cổng bằng 2 dòng sau trên router Access:

```
ip nat inside source static tcp 172.27.50.10 80 203.0.113.254 80
```

```
ip nat inside source static tcp 172.27.50.10 443 203.0.113.254 443
```

Với cấu hình này, khi người dùng bên ngoài truy cập <http://203.0.113.254> hoặc <https://203.0.113.254>, yêu cầu sẽ được chuyển tiếp tới máy chủ nội bộ có địa chỉ 172.27.50.10 thông qua các cổng HTTP và HTTPS.

Ta sẽ thực hiện kiểm tra bằng cách tạo 1 đường mạng và 1 PC nội bộ khác nối đến internet và tiến hành truy cập vào web browser trên PC và nhập địa chỉ IP trên Router ACCESS và nó chuyển tiếp đến web của server ở vlan 50 với kết quả như sau:



Hình 4.18 Kết quả chuyển tiếp cổng http và https

4.5.3 Cấu hình DHCP ipv4

Router R4 cung cấp dịch vụ DHCP cho các VLAN trong mạng. DHCP giúp tự động cấp phát địa chỉ IP cho các thiết bị trong mạng, giảm thiểu việc cấu hình thủ công và đảm bảo tính hiệu quả trong việc quản lý các thiết bị kết nối. Các địa chỉ IP

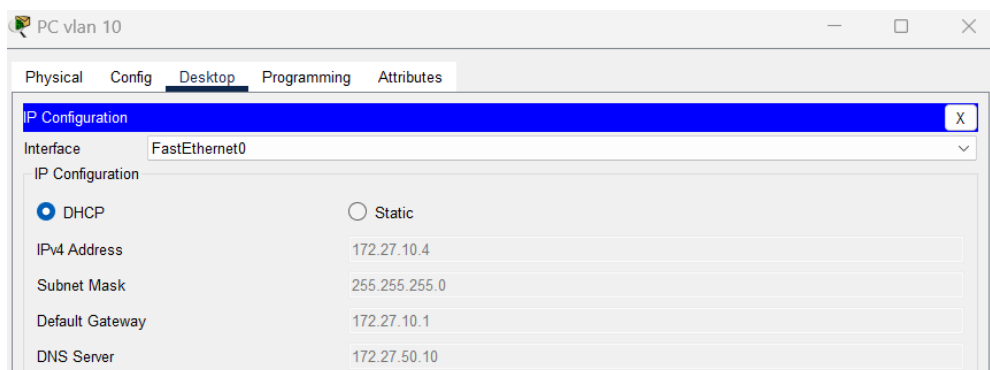
cấp phát cho các thiết bị trong các VLAN khác nhau sẽ nằm trong các pool riêng biệt. Quá trình thực hiện như sau:

Bảng 4.13 Lệnh cấu hình dhcp ipv4 cho vlan 10

Vlan 10
ip dhcp pool VLAN10
network 172.27.10.0 255.255.255.0
default-router 172.27.10.1
dns-server 172.27.50.10

Loại trừ địa chỉ IP: Các địa chỉ IP được loại trừ khỏi phạm vi cấp phát DHCP, nhằm đảm bảo các địa chỉ này không được cấp phát tự động cho các thiết bị, chẳng hạn như địa chỉ gateway (172.27.10.1, 172.27.20.1, 172.27.30.1, 172.27.40.1) bằng lệnh `ip dhcp excluded-address`

Cấu hình pool DHCP cho các VLAN: Cấu hình này giúp cấp phát địa chỉ IP cho các thiết bị trong các VLAN khác nhau. Ví dụ ở vlan như sau: VLAN 10 cấp phát địa chỉ IP trong dải 172.27.10.0/24, gateway là 172.27.10.1, và DNS server là 172.27.50.10.



Hình 4.19 Kết quả cấp phát dhcp ipv4 trên máy tính vlan 10

Sau khi thực hiện xong có thể kiểm tra ip config trên các PC của từng vlan có được cấp phát đúng yêu cầu cấu hình.

4.5.4 Cấu hình DHCP ipv6

Trong mô hình mạng tại site HQ, DHCPv6 được cấu hình theo cơ chế Stateless để cung cấp các thông tin bổ sung như DNS server và domain-name cho các thiết bị đầu cuối trong các VLAN 10, 20, 30 và 40. Do thiết bị R7 không hỗ trợ chức năng IPv6 DHCP relay agent, nên toàn bộ quá trình cấu hình DHCPv6 được thực hiện tập trung trên router R4 – nơi các subinterface tương ứng với từng VLAN được định nghĩa.

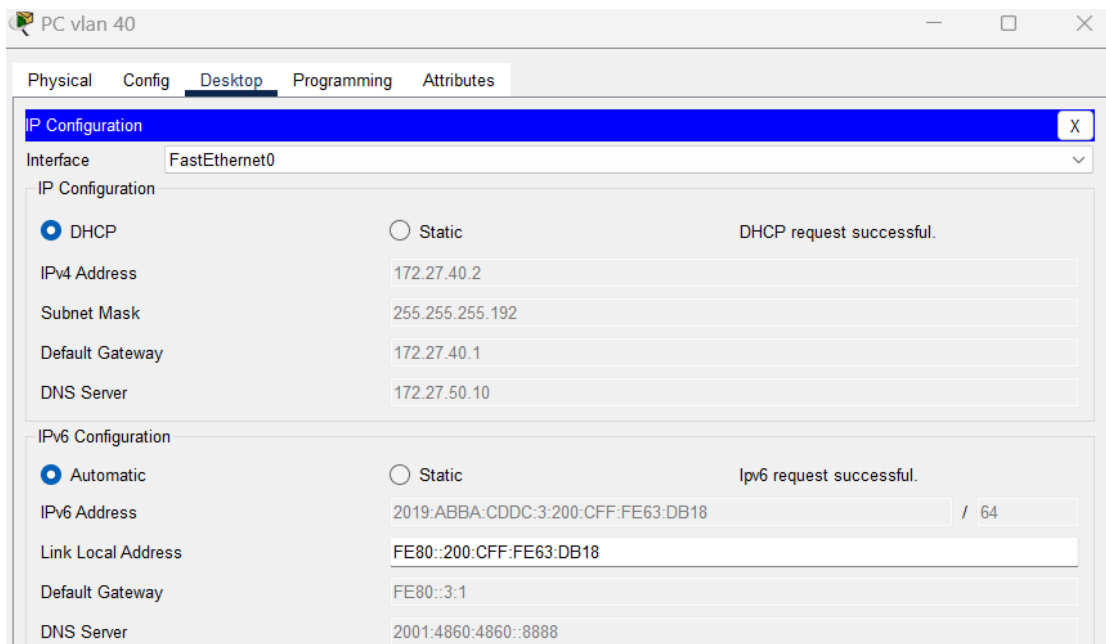
Trên router R4, các pool DHCPv6 được tạo với cú pháp `ipv6 dhcp pool <tên_pool>`, trong đó khai báo các tham số như DNS server (2001:4860:4860::8888) và domain name (tdtu.com). Sau đó, trên mỗi subinterface (Gig0/0.10, Gig0/0.20, v.v...), lệnh `ipv6 nd other-config-flag` được bật để báo hiệu cho các thiết bị đầu cuối rằng cần truy vấn DHCPv6 để nhận thông tin bổ sung. Cuối cùng, lệnh `ipv6 dhcp server <tên_pool>` gán pool tương ứng với từng interface.

Một số yếu tố cần lưu ý trong quá trình cấu hình DHCPv6 Stateless gồm:

- Không cấp phát địa chỉ IP (thiết bị sẽ tự sinh địa chỉ từ prefix Router Advertisement).
- Chỉ cung cấp các tham số bổ sung như DNS và domain name.
- Phải bật cờ `other-config-flag` trên interface để thiết bị nhận biết cần dùng DHCPv6.
- Do relay-agent ipv6 không được hỗ trợ, nên cần gom cấu hình DHCPv6 về một router có khả năng xử lý đầy đủ – trong trường hợp này là R4 thay vì yêu cầu là thực hiện trên R7.

Việc tập trung cấu hình tại router R4 giúp đảm bảo hiệu quả truyền thông và quản lý thống nhất việc cấp phát thông tin mạng cho toàn bộ hệ thống VLAN trong site HQ.

Sau khi cấu hình xong, thực hiện kiểm tra kết quả cấp phát DHCP bằng cách vào Desktop trên máy tính thuộc VLAN 40, chọn IP Configuration và bấm vào nút DHCP Request. Nếu cấu hình đúng, máy tính sẽ nhận được địa chỉ IP, subnet mask, default gateway và DNS server từ DHCP server.



Hình 4.20 Kết quả cấp phát dhcp ipv6 trên máy tính vlan 40

4.6 Các yêu khác ở ipv4

4.6.1 Chặn truy cập nội bộ từ VLAN GUEST







Đối với yêu cầu đầu tiên, một ACL mở rộng mang tên BLOCK_GUEST_ACCESS được tạo trên router R4 nhằm chặn toàn bộ lưu lượng từ VLAN 40 truy cập vào dải địa chỉ mạng nội bộ của HQ (172.27.0.0/16) và Branch (10.28.0.0/16). Đồng thời, ACL này vẫn cho phép các gói tin DHCP cần thiết (discover và offer) cũng như cho phép tất cả lưu lượng khác từ VLAN GUEST đi ra Internet. ACL được gắn vào subinterface GigabitEthernet0/0.40 ở chiều in. Thực hiện thông qua các lệnh sau:

Bảng 4.14 Lệnh cấu hình chặn truy cập nội bộ từ VLAN GUEST

R4	
ip access-list extended BLOCK_GUEST_ACCESS	interface GigabitEthernet0/0.40
deny ip 172.27.40.0 0.0.0.63 172.27.0.0 0.0.255.255	ip access-group BLOCK_GUEST_ACCESS in

deny ip 172.27.40.0 0.0.0.63 10.28.0.0 0.0.255.255	
permit udp 172.27.40.0 0.0.0.63 any eq bootpc	
permit udp any any eq bootps	
permit ip 172.27.40.0 0.0.0.63 any	

Sau khi áp dụng, kiểm thử cho thấy VLAN 40 không thể ping đến các VLAN nội bộ như vlan 10 và router R3 ở chi nhánh nhưng vẫn truy cập Internet và web bình thường – đúng với mục tiêu yêu cầu.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC vl...	PC vlan 10	ICMP		0.000	N	0	(edit)	
	Failed	PC vl...	R3	ICMP		0.000	N	1	(edit)	
	Successful	PC vl...	internet	ICMP		0.000	N	2	(edit)	

Hình 4.21 Kết quả chặn truy cập vlan guest trong nội bộ

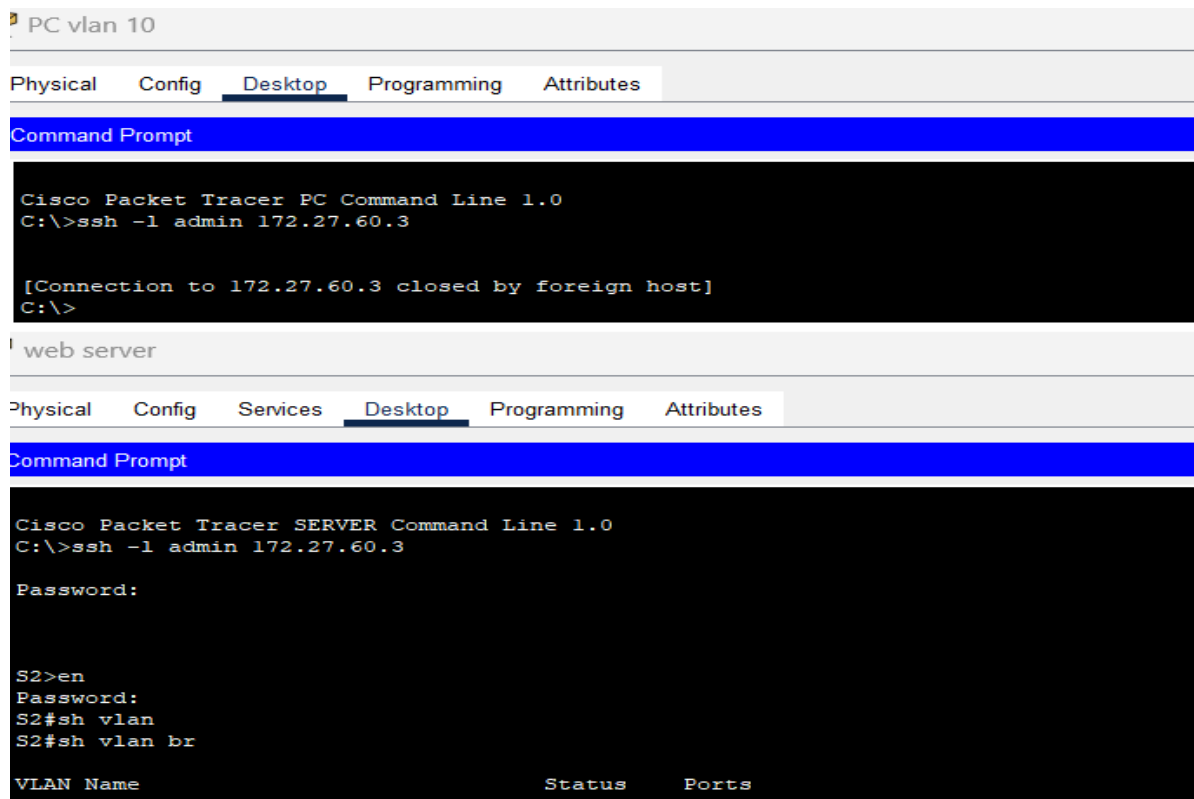
4.6.2 giới hạn truy cập SSH vào các switch ngoại trừ VLAN SERVERS

Với yêu cầu thứ hai, để đảm bảo tính bảo mật và giới hạn quyền truy cập từ xa vào hệ thống mạng, chỉ các thiết bị thuộc VLAN SERVERS (dải địa chỉ 172.27.50.0/28) mới được phép thực hiện kết nối SSH đến các switch trong hệ thống mạng nội bộ (bao gồm S1, S2, S3 và S4). Để thực hiện điều này, một danh sách kiểm soát truy cập dạng chuẩn có tên SSH_ONLY_SERVERS được tạo ra trên từng switch. ACL này cho phép lưu lượng đến từ VLAN 50 và ngăn chặn tất cả các kết nối từ các VLAN khác.

Bảng 4.15 Lệnh cấu hình giới hạn truy cập SSH vào các switch

Tạo ACL (SSH_ONLY_SERVERS)	Áp dụng vào line vty trên switch
ip access-list standard SSH_ONLY_SERVERS	line vty 0 4

permit 172.27.50.0 0.0.0.15	access-class SSH_ONLY_SERVERS in
deny any	transport input ssh



Hình 4.22 Kết quả thực hiện giới truy cập SSH ngoại trừ vlan servers

ACL được áp dụng trực tiếp vào line vty 0 4, là đường điều khiển từ xa qua SSH của switch, bằng lệnh access-class. Đồng thời, để tăng cường bảo mật, chỉ cho phép giao thức SSH được sử dụng với lệnh transport input ssh, từ chối các giao thức điều khiển từ xa không an toàn như Telnet.

Quá trình kiểm thử xác nhận rằng khi thực hiện kết nối SSH từ một thiết bị thuộc VLAN 50 bằng lệnh ssh -l admin <ip-switch>, kết nối được thiết lập thành công. Trong khi đó, các thiết bị từ các VLAN khác không thể truy cập SSH vào switch, đảm bảo rằng chỉ những người dùng có thẩm quyền mới được truy cập từ xa vào thiết bị mạng. Hình 4.15 là kết quả thực hiện ssh từ vlan 10 và vlan 50 cho thành cấu hình thực hiện thành công.

CHƯƠNG 5. KẾT LUẬN

5.1 Kết luận

Qua quá trình triển khai mô hình mạng cho khu vực HQ và Branch, đề tài đã thực hiện đầy đủ các yêu cầu về thiết lập địa chỉ IP (IPv4 và IPv6), cấu hình định tuyến (EIGRP, OSPF, và định tuyến tĩnh), định tuyến qua Tunnel GRE, cấu hình các dịch vụ mạng như NAT, DHCP, DHCPv6 và VLAN nội bộ. Ngoài ra, đề tài cũng đã chú trọng đến các yếu tố bảo mật cơ bản thông qua việc áp dụng Access Control List (ACL) để phân quyền truy cập mạng, như chặn VLAN GUEST truy cập các vùng mạng nội bộ và chỉ cho phép VLAN SERVERS truy cập SSH đến các switch.

Hệ thống sau khi cấu hình được kiểm thử kỹ lưỡng, đảm bảo khả năng kết nối ổn định giữa các thiết bị và khả năng truy cập Internet bình thường. Các cơ chế phân vùng truy cập được triển khai hợp lý, vừa đáp ứng yêu cầu bảo mật, vừa đảm bảo tính linh hoạt trong quản lý.

5.2 Hướng phát triển

Do giới hạn của phần mềm Packet Tracer, đề tài chưa thể triển khai một số tính năng nâng cao. Tuy nhiên, trong tương lai có thể phát triển theo các hướng sau:

- Chuyển sang môi trường thật (GNS3, thiết bị thực): để triển khai được các chức năng như DHCPv6 relay, xác thực 802.1X, hoặc các giao thức nâng cao hơn.
- Bổ sung các biện pháp bảo mật mở rộng: như cấu hình Port Security trên switch, sử dụng Access Port/Dynamic Port, hoặc giới hạn MAC address theo port.
- Tăng cường giám sát và quản lý: thông qua giao thức SNMP hoặc sử dụng syslog, tuy Packet Tracer chưa hỗ trợ đầy đủ nhưng có thể mô phỏng một phần.
- Tích hợp mô hình với các dịch vụ khác: như Web Server, Email Server để phục vụ cho bài toán tổng thể hơn (Packet Tracer có thể mô phỏng mức cơ bản).

TÀI LIỆU THAM KHẢO

Tiếng Việt

VNExperts. (n.d.). Cấu hình NAT trên Router Cisco. VNExperts.
<https://vnexperts.vn/cau-hinh-nat-tren-router-cisco.html>

Tiếng Anh

Lakhwani, R. (2020). Redistribution Between EIGRP and OSPF. NetworkLessons.
<https://networklessons.com/ip-routing/redistribution-between-eigrp-and-ospf>

Study-CCNA. (n.d.). Link Aggregation Control Protocol (LACP). Study-CCNA.
<https://study-ccna.com/link-aggregation-control-protocol-lACP/>

Michael, T. (2021). SLAAC/Stateless DHCP vs SLAAC/RDNSS. ToluMichael.
<https://tolumichael.com/slaacstateless-dhcp-vs-slaacrdnss/>

ComputerNetworkingNotes. (n.d.). EIGRP Configuration: Step-by-Step Guide. ComputerNetworkingNotes.
<https://www.computernetworkingnotes.com/ccna-study-guide/eigrp-configuration-step-by-step-guide.html>

NetworkLessons. (n.d.). OSPF Multi-Area Configuration. NetworkLessons.
<https://networklessons.com/ospf/ospf-multi-area-configuration>