BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG

BÁO CÁO CUỐI KÌ MẠNG MÁY TÍNH NÂNG CAO

Xây dựng mô hình mạng cho tổ chức có chi nhánh

Người hướng dẫn: GV. LÊ VIẾT THANH
Người thực hiện: NGUYỄN PHƯỚC LỘC – 52200283
Nhóm: 11
Khóa: 26

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2025

LỜI CẢM ƠN

Trước tiên, em xin gửi lời cảm ơn chân thành đến thầy Lê Viết Thanh đã luôn tận tình chỉ bảo, hướng dẫn và giúp đỡ em trong suốt quá trình thực hiện đề tài báo cáo. Sự giúp đỡ và những chỉ dẫn quý báu của thầy đã giúp em hoàn thành bài báo cáo này một cách tốt nhất.

Em cũng xin cảm ơn Trường đại học Tôn Đức Thắng đã tạo điều kiện cho em có cơ hội tiếp cận và tìm hiểu sâu hơn. Đây là cơ hội quý giá giúp em phát triển kiến thức và kỹ năng trong quá trình học tập và nghiên cứu.

Em hy vọng rằng những kiến thức và kinh nghiệm thu được từ quá trình thực hiện đề tài sẽ là nền tảng hữu ích cho những nghiên cứu và công việc sau này.

ĐỒ ÁN ĐƯỢC HOÀN THÀNH TẠI
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG

Tôi xin cam đoan đây là sản phẩm đồ án của riêng tôi và được sự hướng dẫn 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 đồ 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 đồ 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)
Nguyễn Phước Lộc

TÓM TẮT

Báo cáo mô tả quá trình thiết kế và cấu hình hệ thống mạng cho tổ chức với hai khu vực chính: trụ sở (HQ) và chi nhánh. Mạng được cấu hình cho cả IPv4 và IPv6, đảm bảo kết nối nội bộ và khả năng truy cập Internet.

Trong IPv4, cấu hình bao gồm các giao thức định tuyến EIGRP và OSPF, kết nối PPP, thiết lập đường hầm GRE, chuyển mạch với VTP và Rapid PVST+, cùng các cấu hình bảo mật như SSH và ACL. NAT Overload và DHCP được sử dụng để cung cấp kết nối Internet và cấp phát địa chỉ IP.

IPv6 được triển khai với hệ thống địa chỉ, EIGRPv6, và DHCPv6 Stateless kết hợp relay agent cho các VLAN. Địa chỉ link-local được cấu hình tĩnh cho các giao diện.

Chương Q&A cung cấp bảng phân bổ địa chỉ IP cho các thiết bị và hướng dẫn cấu hình mạng. Báo cáo hoàn thiện yêu cầu kỹ thuật của đề bài và đề xuất các giải pháp tối ưu hóa cho hệ thống mạng trong tương lai.

MỤC LỤC

DANH SÁCH HÌNH VẼ

DANH SÁCH BẢNG

DANH SÁCH CHỮ VIẾT TẮT

ACL: Access Control List

CHAP: Challenge Handshake Authentication Protocol

DHCP: Dynamic Host Configuration Protocol

EIGRP: Enhanced Interior Gateway Routing Protocol

GRE: Generic Routing Encapsulation

HQ: Headquarters

IPv4: Internet Protocol version 4

IPv6: Internet Protocol version 6

LACP: Link Aggregation Control Protocol

OSPF: Open Shortest Path First

PPP: Point-to-Point Protocol

SSH: Secure Shell

CHƯƠNG 1 - GIỚI THIỆU

1.1 Giới thiệu

Đề tài này tập trung vào việc triển khai và cấu hình một hệ thống mạng mô phỏng, kết hợp các công nghệ và thành phần mạng phổ biến như định tuyến tĩnh, định tuyến động, VLAN, NAT, DHCP, Access Control List (ACL), PPP, GRE Tunnel và IPv6. Báo cáo chi tiết quá trình xây dựng mô hình mạng, cấu hình các thiết bị mạng, và kiểm tra kết nối, đồng thời phân tích hoạt động của hệ thống. Thông qua đó, người thực hiện sẽ nắm vững nguyên lý hoạt động của các giao thức và dịch vụ mạng cơ bản, từ đó trang bị những kiến thức cần thiết cho công việc trong lĩnh vực quản trị mạng và bảo mật hệ thống thông tin trong tương lai.

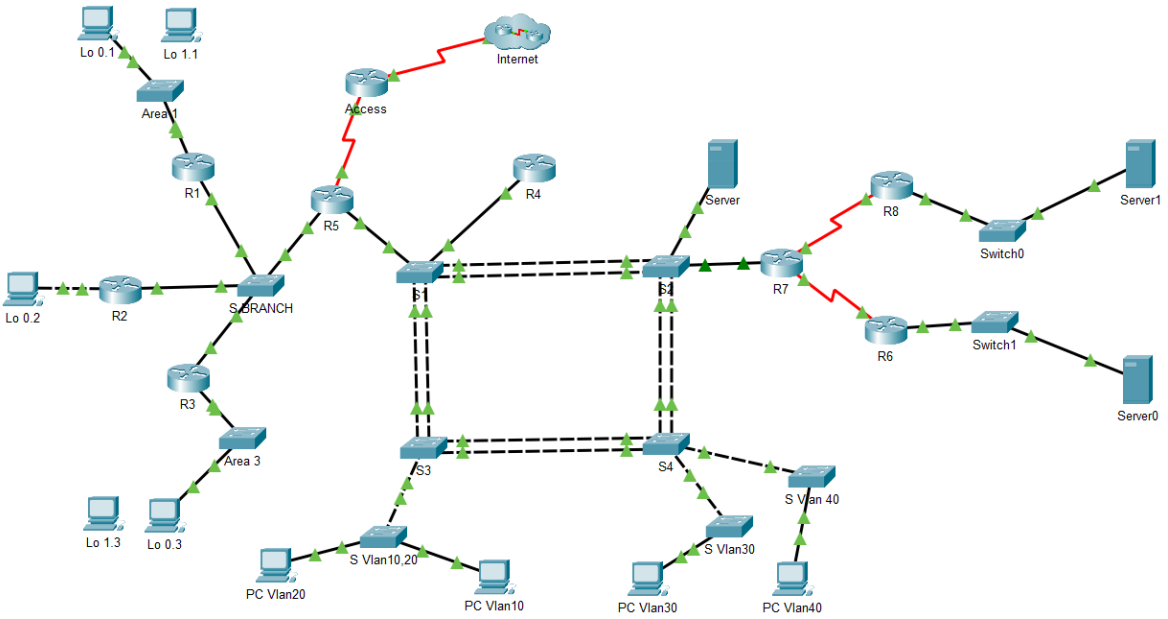
1.2 Mục tiêu bài làm

Bài báo cáo này tập trung vào việc xây dựng một mô hình mạng tích hợp đầy đủ các công nghệ và dịch vụ mạng cơ bản, như định tuyến, phân chia VLAN, NAT, DHCP, ACL, kết nối GRE và PPP, nhằm đáp ứng các yêu cầu cơ bản và nâng cao trong thiết kế, triển khai và quản trị mạng.

Mục tiêu chính là giúp sinh viên củng cố và mở rộng kiến thức về địa chỉ IPv4 và IPv6, đồng thời hiểu rõ cơ chế hoạt động của các giao thức định tuyến tĩnh và động như OSPF, RIP và EIGRP. Ngoài ra, báo cáo còn tập trung vào việc áp dụng các kỹ thuật NAT để chuyển đổi địa chỉ IP trong mạng nội bộ sang địa chỉ công cộng, cũng như triển khai dịch vụ DHCP để tự động cấp phát địa chỉ IP cho các thiết bị đầu cuối.

Bên cạnh đó, mô hình mạng này còn tích hợp các kỹ thuật kiểm soát truy cập qua danh sách điều khiển (Access Control List – ACL), thiết lập đường hầm GRE để kết nối các mạng riêng qua hạ tầng công cộng, và triển khai giao thức PPP nhằm gia tăng tính bảo mật và ổn định cho kết nối điểm-điểm. Cuối cùng, mô hình sẽ được kiểm thử thông qua các công cụ dòng lệnh như ping và traceroute, giúp đánh giá tính chính xác và hiệu quả của hệ thống sau khi triển khai.

1.3 Mô tả mô hình



Hình 1.1: Mô hình mạng

Sơ đồ mạng được chia thành hai khu vực chính: BRANCH và HQ.

- **Khu vực HQ:**
  - Bao gồm các Router R4, R6, R7, R8, và các Switch S1, S2, S3, S4.
  - Với switch S1 làm VTP Server, các switch còn lại là VTP client, các vlan được thiết lập VLAN 10 (UNIT1), VLAN 20 (UNIT2), VLAN 30 (UNIT3),VLAN 40 (GUEST), VLAN 50 (SERVERS), và VLAN 60(Management).
  - Khu vực HQ sử dụng giao thức định tuyến động EIGRP và các vlan được định tuyến trên R4 theo phương pháp router-on-a-stick.
- **Khu vực Branch:**
  - Bao gồm các Router R1, R2, R3, và Switch S5. Khu vực Branch sử dụng giao thức định tuyến động OSPF.
- **Kết nối điểm-điểm**
  - Trên R5, cấu hình default route đến router ACCESS và phân phối nó đến HQ và Branch thông qua EIGRP và OSPF.

– Kết nối giữa router R7 và R6 sử dụng xác thực PAP và kết nối giữa router R7 và R8 sử dụng xác thực CHAP.

CHƯƠNG 2 - PHÂN TÍCH YÊU CẦU

2.1 Phân tích yêu cầu

Đề tài yêu cầu xây dựng một hệ thống mạng mô phỏng, đảm bảo đầy đủ các chức năng cơ bản, đáp ứng các yêu cầu về tính kết nối, bảo mật và hiệu quả trong việc truyền dữ liệu giữa các khu vực mạng khác nhau. Mô hình mạng sẽ được chia thành hai khu vực chính: HQ (trụ sở chính) và Branch (chi nhánh).

Trong mỗi khu vực, mạng sẽ được phân chia thành nhiều VLAN khác nhau, tương ứng với các đơn vị hoặc nhóm người dùng như Management, Guest, Unit1, Unit2... nhằm mục đích hỗ trợ quản lý và kiểm soát truy cập hiệu quả.

Ngoài ra, hệ thống yêu cầu triển khai các dịch vụ và giao thức như:

- **Định tuyến động OSPF** để đảm bảo tính khả dụng và hiệu quả của mạng.
- **Định tuyến tĩnh** để kiểm soát các tuyến đường cố định.
- **Cấu hình DHCP** để cấp phát địa chỉ IP động cho các thiết bị trong mạng.
- **NAT** (Network Address Translation) cho phép truy cập Internet từ mạng nội bộ.
- **Access Control List (ACL)** để kiểm soát lưu lượng mạng và hạn chế truy cập không hợp lệ.
- **PPP (Point-to-Point Protocol)** để triển khai kết nối điểm-điểm.

Đặc biệt, hệ thống yêu cầu hỗ trợ **địa chỉ IPv6**, thể hiện sự chuyển đổi và cập nhật sang hệ thống địa chỉ mới.

Cuối cùng, việc **kiểm thử toàn bộ các dịch vụ và giao thức** đã cấu hình là rất quan trọng để đảm bảo tính ổn định và khả năng kết nối của mạng, phân tách truy cập theo VLAN, truyền dữ liệu qua **GRE tunnel**, và đảm bảo hệ thống hoạt động ổn định trên toàn bộ mạng.

2.2 Cơ sở lý thuyết

2.2.1 NAT

NAT là một kỹ thuật cho phép thay đổi thông tin địa chỉ IP (và/hoặc port) trong header của gói tin khi nó đi qua một router hoặc firewall.

- NAT Overload (Port Address Translation - PAT): Là một dạng NAT động phổ biến nhất, cho phép nhiều thiết bị sử dụng địa chỉ IP private trong mạng nội bộ chia sẻ một hoặc một vài địa chỉ IP public để truy cập Internet. PAT thực hiện điều này bằng cách ánh xạ các cặp (địa chỉ IP private, port nguồn private) sang (địa chỉ IP public, port nguồn public duy nhất cho mỗi session).
- Static NAT (Port Forwarding): Là một dạng NAT tĩnh, ánh xạ một địa chỉ IP public và một port public cụ thể tới một địa chỉ IP private và một port private cụ thể của một server nội bộ. Điều này cho phép các thiết bị từ bên ngoài Internet truy cập vào các dịch vụ được cung cấp bởi server đó.

2.2.2 Tunneling GRE

GRE là một giao thức tunneling được phát triển bởi Cisco, cho phép đóng gói một loạt các loại gói tin giao thức lớp mạng bên trong các gói tin IP ảo. GRE tạo ra một liên kết logic điểm-điểm ảo giữa hai router qua một mạng IP trung gian (ví dụ: Internet). Nó thường được sử dụng để truyền tải các giao thức không thể định tuyến trực tiếp qua mạng trung gian hoặc để tạo các mạng riêng ảo đơn giản.

2.2.3 EtherChannel

EtherChannel là một công nghệ gộp liên kết cho phép kết hợp nhiều cổng Ethernet vật lý thành một liên kết logic duy nhất, giúp tăng băng thông và cung cấp khả năng dự phòng.

2.2.4 Giao thức Kết nối Điểm-điểm (Point-to-Point Protocol - PPP)

PPP là một giao thức lớp liên kết dữ liệu được sử dụng để thiết lập kết nối trực tiếp giữa hai điểm mạng. Nó cung cấp cơ chế đóng gói dữ liệu, quản lý liên kết (Link Control Protocol - LCP) và đàm phán các giao thức lớp mạng (Network Control Protocol - NCP) như IPCP cho IPv4.

- Password Authentication Protocol (PAP): Là một cơ chế xác thực đơn giản trong PPP, trong đó client gửi username và password dưới dạng clear-text (không mã hóa) cho server để xác thực. Do tính bảo mật thấp, PAP ít được khuyến khích sử dụng.

- Challenge Handshake Authentication Protocol (CHAP): Là một cơ chế xác thực mạnh hơn PAP. CHAP sử dụng phương pháp "bắt tay ba bước" (three-way handshake) và không truyền password trực tiếp qua mạng. Server gửi một "challenge" (thách thức) cho client, client tính toán "response" (phản hồi) dựa trên challenge và một secret (mật khẩu chia sẻ) đã biết, sau đó gửi lại cho server. Server cũng thực hiện tính toán tương tự để xác minh.

2.2.5 EIGRP

EIGRP là một giao thức định tuyến vector khoảng cách nâng cao (advanced distance-vector) độc quyền của Cisco (sau này đã được mở một phần). EIGRP sử dụng thuật toán DUAL (Diffusing Update Algorithm) để đảm bảo các đường đi không bị lặp (loop-free) và cho phép hội tụ nhanh chóng khi có sự thay đổi trong mạng.

2.2.6 Giao thức OSPF

OSPF là một giao thức định tuyến trạng thái liên kết (link-state) mã nguồn mở, được sử dụng rộng rãi làm giao thức định tuyến nội miền (IGP). OSPF xây dựng một cơ sở dữ liệu trạng thái liên kết (LSDB) toàn diện về topo mạng và sử dụng thuật toán Dijkstra (Shortest Path First - SPF) để tính toán các đường đi tốt nhất.

2.3 Quy hoạch địa chỉ mạng IPv4

Để đáp ứng nhu cầu địa chỉ cho toàn bộ hệ thống, khu vực HQ được cấp phát dải mạng 10.0.0.0/16 và khu vực Chi nhánh sử dụng dải mạng 172.16.0.0/16.

Trong đó, ở khu vực HQ với dải mạng 10.0.0.0/16 được chia thành các mạng con như trong bảng 2.1.

Đối với VLAN 20 UNIT2 yêu cầu 300 hosts, một mạng con với subnet mask /23 được cấp phát. Mặt nạ mạng này cung cấp $2^{(32-23)} - 2 = 510$ địa chỉ host hợp lệ, đáp ứng đủ yêu cầu và là lựa chọn tối ưu nhất theo nguyên tắc VLSM. Quá trình tương tự được áp dụng cho các VLAN còn lại.

Ở chi nhánh với dãi mạng gốc là 172.16.0.0/16, các mạng con được dùng chi tiết ở trong bảng 2.2

Các giao diện kết nối điểm-điểm trên các router được phân bổ địa chỉ theo bảng 2.3

Bảng 2.1: Phân bổ địa chỉ IPv4 cho các VLAN tại HQ

VLAN ID	Tên VLAN	Số host	Địa chỉ mạng / Prefix	Broadcast	Dải IP sử dụng
10	UNIT1	200	10.0.0.0/24	10.0.0.255	10.0.0.1 – 10.0.0.254
20	UNIT2	300	10.0.2.0/23	10.0.3.255	10.0.2.1 – 10.0.3.254
30	UNIT3	100	10.0.4.0/25	10.0.4.127	10.0.4.1 – 10.0.4.126
40	GUEST	50	10.0.4.128/26	10.0.4.191	10.0.4.129 – 10.0.4.190
50	SERVERS	10	10.0.4.192/28	10.0.4.207	10.0.4.193 – 10.0.4.206
60	Management	20	10.0.4.208/27	10.0.4.239	10.0.4.209 – 10.0.4.238

Bảng 2.2: Phân bổ địa chỉ IPv4 tại Branch

Device	Interface	Số host	Địa chỉ mạng / Prefix	Gateway	Dải IP sử dụng
R1	lo0	500	172.16.0.0/23 (510 host)	172.16.0.1	172.16.0.2 - 172.16.1.254
R1	lo1	300	172.16.2.0/23 (510 host)	172.16.2.1	172.16.2.2 - 172.16.3.254
R2	lo0	100	172.16.4.0/25 (126 host)	172.16.4.1	172.16.4.2 - 172.16.4.126
R3	lo0	200	172.16.5.0/24 (254 host)	172.16.5.1	172.16.5.1 - 172.16.5.254
R3	lo1	100	172.16.6.0/25 (126 host)	172.16.6.1	172.16.6.2 - 172.16.6.126

Bảng 2.3: Phân bổ địa chỉ IPv4 cho các kết nối điểm-điểm

Device	Interface	Địa chỉ ip
R7	Serial0/1/1	200.0.100.1/30
R6	Serial0/1/0	200.0.100.2/30
R7	Serial0/1/0	200.0.100.5/30
R8	Serial0/1/0	200.0.100.6/30
R5	Serial0/1/0	200.0.100.9/30
ACCESS	Serial0/1/0	200.0.100.10/30

2.4 Cấu hình địa chỉ mạng IPv6

Hệ thống mạng không chỉ triển khai giao thức IPv4 mà còn được thiết kế để hỗ trợ đầy đủ giao thức IPv6, đảm bảo tính sẵn sàng cho tương lai và khả năng tương tác trong môi trường mạng hiện đại. Quá trình cấu hình địa chỉ IPv6 được thực hiện theo các yêu cầu cụ thể của đề bài, bao gồm việc sử dụng các khối địa chỉ được cấp phát, phân bổ cho các VLAN và các liên kết điểm-điểm, đồng thời cấu hình địa chỉ link-local tĩnh.

2.4.1 Phân bổ Địa chỉ Global Unicast cho các VLAN tại Trụ sở chính (HQ)

Sử dụng năm subnet đầu tiên của mạng **2019:ABBA:CDDC:/48** để phân bổ cho các VLAN 10, 20, 30, 40, và 50. Địa chỉ gateway mặc định sẽ sử dụng địa chỉ IP đầu tiên trong mỗi subnet, trong khi địa chỉ link-local được cấu hình theo định dạng **FE80::tên thiết bị:ID Vlan**. Địa chỉ link-local được sử dụng để giao tiếp giữa các thiết bị nằm trên cùng một liên kết và thiết lập quan hệ láng giềng trong các giao thức định tuyến như OSPFv3, EIGRP. Các giao thức này thường ưu tiên sử dụng địa chỉ link-local để gửi bản tin Hello và trao đổi thông tin định tuyến, thay vì sử dụng địa chỉ toàn cục.

Bảng 2.4: Phân bổ địa chỉ IPv6 cho VLAN

VLAN ID	Địa chỉ mạng	Gateway	link-local
10	2019:ABBA:CDDC:0::/64	2019:ABBA:CDDC:0::1/64	FE80::4:10
20	2019:ABBA:CDDC:1::/64	2019:ABBA:CDDC:1::1/64	FE80::4:20
30	2019:ABBA:CDDC:2::/64	2019:ABBA:CDDC:2::1/64	FE80::4:30
40	2019:ABBA:CDDC:3::/64	2019:ABBA:CDDC:3::1/64	FE80::4:40
50	2019:ABBA:CDDC:4::/64	2019:ABBA:CDDC:4::1/64	FE80::4:50

2.4.2 Phân bổ Địa chỉ Global Unicast cho các Kết nối Router

Đối với các liên kết điểm-điểm giữa các router trong cả khu vực HQ và Branch, cũng như kết nối ra router ACCESS và các mạng LAN mô phỏng tại Chi nhánh, địa chỉ IPv6 Global Unicast được cấp phát dựa trên thông tin cung cấp trong đề bài.

Bảng 2.5: Phân bổ địa chỉ IPv6 cho VLAN

Device	**Interface**	**Địa chỉ mạng**	**link-local**
R5	Serial0/1/0	2019:ABBA:AAAA:1::1/64	FE80::5:1
Access	Serial0/1/0	2019:ABBA:AAAA:1::2/64	FE80::ACC:1
R5	Serial0/1/1	2019:ABBA:BBBB:1::1/64	FE80::5:2
R4	Gigabit0/0/0	2019:ABBA:BBBB:1::2/64	FE80::4:1
R7	Gigabit0/0/0	2019:ABBA:BBBB:1::3/64	FE80::7:1
R7	Serial0/1/1	2019:ABBA:CCCC:1::1/64	FE80::7:3
R7	Serial0/1/0	2019:ABBA:DDDD:1::3/64	FE80::7:2
R6	Serial0/1/0	2019:ABBA:CCCC:1::2/64	FE80::6:1
R6	Gigabit0/0/0	2019:ABBA:EEEE:1::1/64	FE80::6:2
R8	Serial0/1/0	2019:ABBA:DDDD:1::2/64	FE80::8:1
R8	Gigabit0/0/0	2019:ABBA:FFFF:1::1/64	FE80::8:2

CHƯƠNG 3 - TRIỂN KHAI CẤU HÌNH MÔ HÌNH MẠNG

3.1 Cấu hình mạng

3.1.1 Cấu hình VTP, EtherChannel, Rapid PVST+

Bảng 3.6: Bảng cấu hình cơ bản cho các Switch S1-S4

S1	**S2**	**S3**	**S4**
hostname S1 vtp mode server vtp domain TDTU vtp password cisco	hostname S2 vtp mode client vtp domain TDTU vtp password cisco	hostname S3 vtp mode client vtp domain TDTU vtp password cisco	hostname S4 vtp mode client vtp domain TDTU vtp password cisco
int range f0/1 - 2 channel-group 1 mode active switchport mode trunk	int range f0/1 - 2 channel-group 1 mode active switchport mode trunk	int range f0/1 - 2 channel-group 1 mode active switchport mode trunk	int range f0/1 - 2 channel-group 1 mode active switchport mode trunk
int range f0/3 - 4 channel-group 2 mode active switchport mode trunk	int range f0/3 - 4 channel-group 2 mode active switchport mode trunk	int range f0/3 - 4 channel-group 2 mode active switchport mode trunk	int range f0/3 - 4 channel-group 2 mode active switchport mode trunk

3.1.2 Cấu hình định tuyến động OSPF và EIGRP

Ở trụ sở chính dùng giao thức EIGRP để định tuyến và ở chi nhánh dùng OSPF để định tuyến.

Định tuyến EIGRP

Các router R4, R5, R6, R7, R8 tham gia định tuyến EIGRP trong đó R5 sẽ phân phối default route ra ngoài đến các router còn lại trong vùng.

Bảng 3.7: Cấu hình định tuyến EIGRP trên R4, R5, R7

R4	**R5**	**R7**
router eigrp 1	router eigrp 1	router eigrp 1
network 10.0.0.0 0.0.0.255	network 200.0.100.8 0.0.0.3	network 200.0.100.4 0.0.0.3
network 10.0.2.0 0.0.1.255	network 10.0.4.0 0.0.0.7	network 200.0.100.0 0.0.0.3
network 10.0.3.0 0.0.0.127	passive-interface default	passive-interface default
network 10.0.3.128 0.0.0.63	no passive-interface GigabitEther-net0/0/1	no passive-interface Serial0/1/0
network 10.0.0.3.192 0.0.0.31	no passive-interface Serial0/1/0	no passive-interface Serial0/1/1
network 10.0.0.3.224 0.0.0.15	redistribute static metric 10000 100 255 1 1500	no passive-interface GigabitEther-net0/0/0
network 10.0.0.4.0 0.0.0.7		
passive-interface default		
no passive-interface GigabitEther-net0/0/0		

Bảng 3.8: Cấu hình định tuyến EIGRP trên R8 và R6

R8	**R6**
router eigrp 1	router eigrp 1
network 200.0.100.4 0.0.0.3	network 200.0.100.0 0.0.0.3
network 10.0.4.192 0.0.0.63	network 10.0.4.128 0.0.0.63
passive-interface default	passive-interface default
no passive-interface Se-rial0/1/0	no passive-interface Se-rial0/1/0

Định tuyến OSPF

Ở chi nhánh, các router R1, R2, R3 và R5 sử dụng giao thức OSPF để định tuyến, trong đó R5 phân phối default route ra ngoài đến các router còn lại trong vùng.

Bảng 3.9: Cấu hình định tuyến OSPF trên R1 và R2

R1	**R2**

`router ospf 1`
`log-adjacency-changes`
`network 172.16.0.0 0.0.1.255 area 0`
`network 172.16.2.0 0.0.1.255 area 0`
`network 172.16.7.0 0.0.0.7 area 0`
	`router ospf 1`
	`log-adjacency-changes`
	`network 172.16.4.0 0.0.0.127 area 0`
	`network 172.16.7.0 0.0.0.7 area 0`

Bảng 3.10: Cấu hình định tuyến OSPF trên R3 và R5

R3	**R5**

`router ospf 1`
`log-adjacency-changes`
`network 172.16.5.0 0.0.0.255 area 0`
`network 172.16.6.0 0.0.0.127 area 0`
`network 172.16.7.0 0.0.0.7 area 0`
	`router ospf 1`
	`log-adjacency-changes`
	`network 172.16.7.0 0.0.0.7 area 0`
	`default-information origi-nate`

3.1.3 Định tuyến Vlan

Router R4 được cấu hình định tuyến vlan trên các giao diện phụ ảo tương ứng với các vlan.

Bảng 3.11: Cấu hình định tuyến Vlan trên R4

R4	
interface GigabitEthernet0/0/0	
no shutdown	
interface GigabitEthernet0/0/0.10	interface GigabitEthernet0/0/0.40
encapsulation dot1Q 10	encapsulation dot1Q 40
ip address 10.0.2.1 255.0.0.0	ip address 10.0.3.129 255.255.255.192
interface GigabitEthernet0/0/0.20	interface GigabitEthernet0/0/0.50
encapsulation dot1Q 20	encapsulation dot1Q 50
ip address 10.0.0.1 255.255.254.0	ip address 10.0.3.225 255.255.255.240
interface GigabitEthernet0/0/0.30	interface GigabitEthernet0/0/0.60
encapsulation dot1Q 30	encapsulation dot1Q 60
ip address 10.0.3.1 255.255.255.128	ip address 10.0.3.193 255.255.255.224

3.1.4 Kết nối PPP và GRE Tunnel

Kết nối PPP

Bảng 3.12: Cấu hình PPP(pap) giữa R6 và R7

R6	**R7**
username R7 password 0 cisco	username R6 password 0 cisco
interface Serial0/1/0	interface Serial0/1/1
ip address 200.0.100.2 255.255.255.252	ip address 200.0.100.1 255.255.255.252
encapsulation ppp	encapsulation ppp
ppp authentication pap	ppp authentication pap
ppp pap sent-username R6 password 0 cisco	ppp pap sent-username R7 password 0 cisco

Bảng 3.13: Cấu hình PPP(chap) giữa R8 và R7

R8	**R7**
`interface Serial0/1/0`	`interface Serial0/1/0`
`ip address 200.0.100.6 255.255.255.252`	`ip address 200.0.100.5 255.255.255.252`
`encapsulation ppp`	`encapsulation ppp`
`ppp authentication chap`	`ppp authentication chap`
`username R8 password 0 cisco`	

GRE Tunnel

Bảng 3.14: Cấu hình GRE Tunnel giữa R6 và R8

R6	**R8**
`interface Tunnel0`	`interface Tunnel0`
`ip address 10.0.4.10 255.255.255.252`	`ip address 10.0.4.9 255.255.255.252`
`tunnel source Serial0/1/0`	`tunnel source Serial0/1/0`
`tunnel destination 200.0.100.6`	`tunnel destination 200.0.100.2`
`tunnel mode gre ip`	`tunnel mode gre ip`
`no shut down`	`no shut down`

3.1.5 Cấu hình NAT, ACL và DHCP

Cấu hình NAT

Cấu hình NAT overload trên ACCESS, biên dịch địa chỉ IP nội bộ sang địa chỉ IP public. Cấu hình chuyển tiếp cổng (static NAT) để cho phép các máy chủ từ Internet truy cập dịch vụ HTTP và HTTPS.

Bảng 3.15: Cấu hình NAT overload trên router Access

ACCESS	
interface Serial0/1/0 ip address 200.0.100.10 255.255.255.252 ip nat inside access-list 1 permit 10.0.0.0 0.0.255.255 ip nat inside source static tcp 10.0.3.231 443 200.0.100.13 443 ip nat inside source list 1 interface Serial0/1/1 overload	interface Serial0/1/1 ip address 200.0.100.13 255.255.255.252 ip nat outside access-list 1 permit 172.16.0.0 0.0.255.255 ip nat inside source static tcp 10.0.3.231 80 200.0.100.13 80

Bảng 3.16: Cấu hình chuyển tiếp cổng trên ACCESS

ACCESS	
ip nat inside source static tcp 10.0.3.231 443 200.0.100.13 443	ip nat inside source static tcp 10.0.3.231 80 200.0.100.13 80

Cấu hình ACL

Tạo ACL trên R4 không cho phép người dùng trong VLAN GUEST truy cập vào toàn bộ mạng của HQ và chi nhánh nhưng vẫn có thể sử dụng Internet.

Bảng 3.17: Cấu hình ACL trên R4

R4	
access-list 140 deny ip 10.0.3.128 0.0.0.63 10.0.0.0 0.0.255.255 access-list 140 deny ip 10.0.3.128 0.0.0.63 172.16.0.0 0.0.255.255	access-list 140 permit ip any any interface GigabitEthernet0/0/0.40 ip access-group 140 in

Tạo ACL chỉ cho phép VLAN SERVERS có thể SSH vào các switch.

Bảng 3.18: Cấu hình ACL trên các switch

S1, S2, S3, S4	
access-list 50 permit 10.0.3.224 0.0.0.15	login local
line vty 0 4	transport input ssh
access-class 50 in	

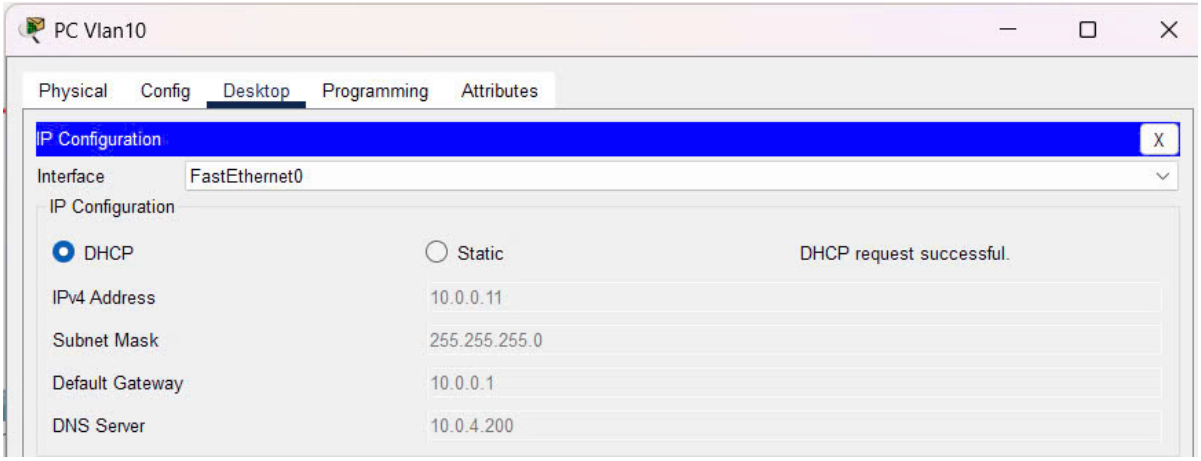
Cấu hình DHCP

Tạo các DHCP pool trên router R4 cho các vlan 10, 20, 30, 40, với các dải địa chỉ dựa trên bảng 2.1 trong đề bài.

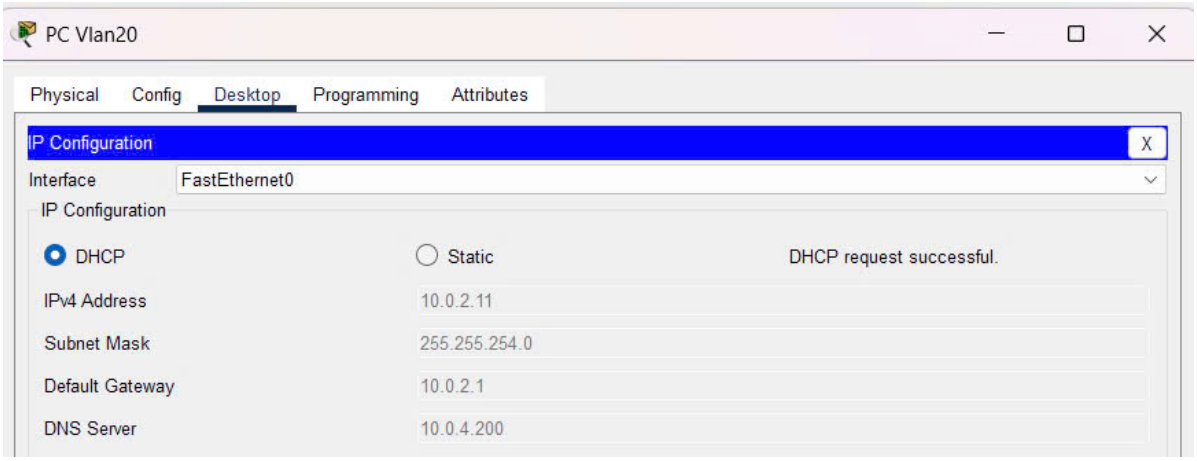
Bảng 3.19: Cấu hình DHCP trên R4

R4	
ip dhcp pool VLAN10	ip dhcp pool VLAN30
network 10.0.2.0 255.255.255.0	network 10.0.3.0 255.255.255.128
default-router 10.0.2.1	default-router 10.0.3.1
ip dhcp pool VLAN20	ip dhcp pool VLAN40
network 10.0.0.0 255.255.254.0	network 10.0.3.128 255.255.255.192
default-router 10.0.0.1	default-router 10.0.3.129

Trên các host của vlan 10, 20, 30, 40 chuyển sang giao thức DHCP để kiểm tra cấu hình :

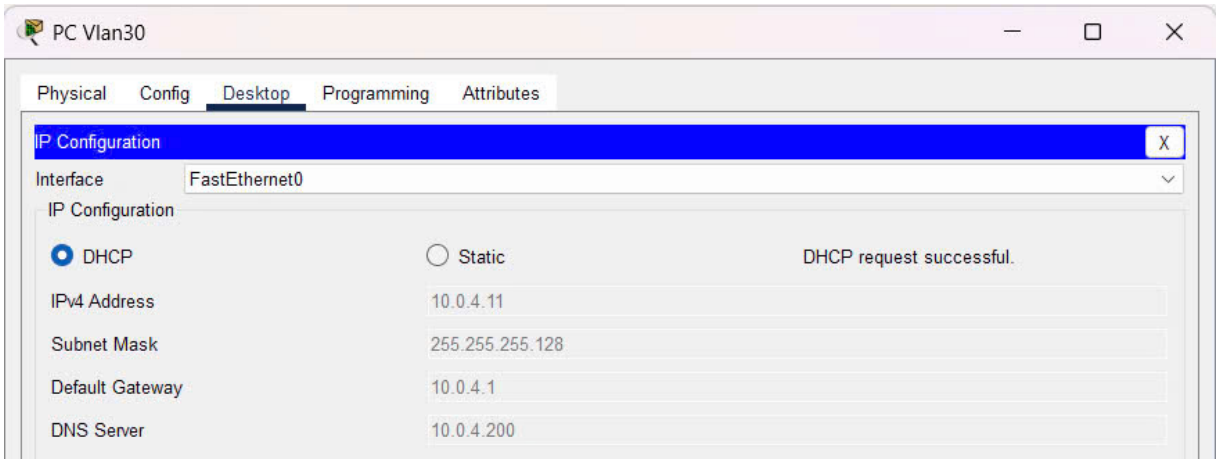


(a) Vlan10

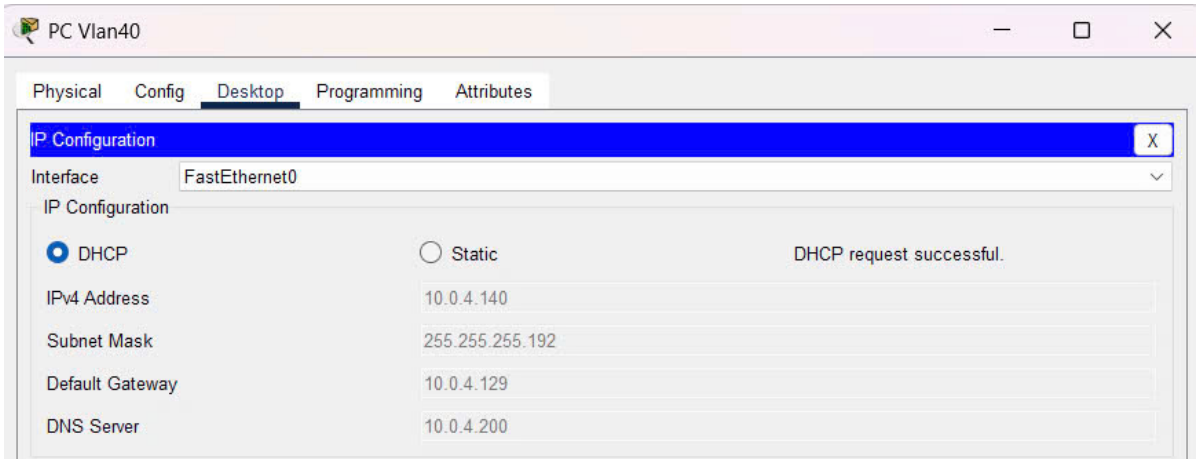


(b) Vlan20

Hình 3.2: PC thuộc vlan 10 và 20



(a) Vlan30



(b) Vlan40

Hình 3.3: PC thuộc vlan 30 và 40

3.1.6 Cấu hình Ipv6

Cấu hình địa chỉ IPv6 và định tuyến EIGRP IPv6

Bảng 3.20: Cấu hình định tuyến IPv6 EIGRP trên R5 và R7

R5	**R7**
ipv6 router eigrp 1 no shutdown redistribute static interface GigabitEthernet0/0/1 ipv6 address FE80::5:2 link-local ipv6 address 2019:ABBA:BBBB:1::1/64 ipv6 eigrp 1 ipv6 enable	ipv6 router eigrp 1 no shutdown interface GigabitEthernet0/0/0 ipv6 address FE80::7:1 link-local ipv6 address 2019:ABBA:BBBB:1::3/64 ipv6 eigrp 1 ipv6 enable interface Serial0/1/0 ipv6 address FE80::7:2 link-local ipv6 address 2019:ABBA:DDDD:1::1/64 ipv6 eigrp 1 ipv6 enable interface Serial0/1/1 ipv6 address FE80::7:3 link-local ipv6 address 2019:ABBA:CCCC:1::1/64 ipv6 eigrp 1 ipv6 enable

Bảng 3.21: Cấu hình IPv6 EIGRP trên router R4

R4	
ipv6 router eigrp 1	interface GigabitEthernet0/0/0.30
no shutdown	ipv6 address FE80::4:30 link-local
interface GigabitEthernet0/0/0	ipv6 address 2019:ABBA:CDDC:2::1/64
ipv6 address FE80::4:1 link-local	ipv6 enable
ipv6 address 2019:ABBA:BBBB:1::2/64	ipv6 eigrp 1
ipv6 enable	interface GigabitEthernet0/0/0.40
ipv6 eigrp 1	ipv6 address FE80::4:40 link-local
interface GigabitEthernet0/0/0.10	ipv6 address 2019:ABBA:CDDC:3::1/64
ipv6 address FE80::4:10 link-local	ipv6 enable
ipv6 address 2019:ABBA:CDDC::1/64	ipv6 eigrp 1
ipv6 enable	interface GigabitEthernet0/0/0.50
ipv6 eigrp 1	ipv6 address FE80::4:50 link-local
interface GigabitEthernet0/0/0.20	ipv6 address 2019:ABBA:CDDC:4::1/64
ipv6 address FE80::4:20 link-local	ipv6 enable
ipv6 address 2019:ABBA:CDDC:1::1/64	ipv6 eigrp 1
ipv6 enable	
ipv6 eigrp 1	

DHCPv6 STATELESS

Bảng 3.22: Cấu hình DHCPv6 STATELESS trên R4

R4	
ipv6 dhcp pool STATE-LESS_POOL dns-server 2001:4860:4860::8888	
interface GigabitEther-net0/0/0.10	interface GigabitEther-net0/0/0.40
ipv6 nd other-config-flag	ipv6 nd other-config-flag
ipv6 dhcp server STATE-LESS_POOL	ipv6 dhcp server STATE-LESS_POOL
interface GigabitEther-net0/0/0.20	interface GigabitEther-net0/0/0.50
ipv6 nd other-config-flag	ipv6 nd other-config-flag
ipv6 dhcp server STATE-LESS_POOL	ipv6 dhcp server STATE-LESS_POOL
interface GigabitEther-net0/0/0.30	interface GigabitEther-net0/0/0.60
ipv6 nd other-config-flag	ipv6 nd other-config-flag
ipv6 dhcp server STATE-LESS_POOL	ipv6 dhcp server STATE-LESS_POOL

CHƯƠNG 4 - Q&A

4.1 Bảng địa chỉ ipv4

Địa chỉ ip của các kết nối trong khu vực chi nhánh.

Bảng 4.23: Bảng địa chỉ ip tại khu vực chi nhánh

Device	Interface	IP Address	Subnet Mask
R1	Gigabit0/0/0	172.16.7.2	255.255.255.248
	loopback0	172.16.0.1	255.255.255.254
	loopback1	172.16.2.1	255.255.255.254
R2	Gigabit0/0/0	172.16.7.3	255.255.255.248
	loopback0	172.16.4.1	255.255.255.128
R3	Gigabit0/0/0	172.16.7.4	255.255.255.248
	loopback0	172.16.5.1	255.255.255.0
	loopback1	172.16.6.1	255.255.255.128
R5	Gigabit0/0/0	172.16.7.1	255.255.255.248

Địa chỉ ip của các kết nối trong khu vực trụ sở chính.

Bảng 4.24: Bảng địa chỉ ip tại khu vực trụ sở chính

Device	Interface	IP Address	Subnet Mask
R5	Gigabit0/0/1	10.0.4.1	255.255.255.248
	Serial0/1/0	200.0.100.9	255.255.255.252
ACCESS	Serial0/1/0	200.0.100.10	255.255.255.252
	Serial0/1/1	200.0.100.13	255.255.255.252
Router0	Serial0/1/0	200.0.100.14	255.255.255.252
	Gigabit0/0/0	8.8.8.1	255.255.255.240
R6	Serial0/1/0	200.0.100.2	255.255.255.252
	g0/0/0	10.0.4.129	255.255.255.192
	tunnel0	10.0.4.9	255.255.255.252
R7	Serial0/1/0	200.0.100.5	255.255.255.252
	Serial0/1/1	200.0.100.1	255.255.255.252
	Gigabit0/0/0	10.0.4.3	255.255.255.248

Bảng 4.25: Bảng địa chỉ ip tại khu vực trụ sở chính

Device	Interface	IP Address	Subnet Mask
R8	Serial0/1/0	200.0.100.6	255.255.255.252
	g0/0/0	10.0.4.193	255.255.255.192
	tunnel0	10.0.4.10	255.255.255.252
S1	VLAN60	10.0.3.194	255.255.255.224
S2	VLAN60	10.0.3.195	255.255.255.224
S3	VLAN60	10.0.3.196	255.255.255.224
S4	VLAN60	10.0.3.197	255.255.255.224
R4	Gigabit0/0/0	10.0.4.2	255.255.255.248
	Gigabit0/0/0.10	10.0.2.1	255.255.255.254
	Gigabit0/0/0.20	10.0.0.1	255.255.255.0
	Gigabit0/0/0.30	10.0.3.1	255.255.255.128
	Gigabit0/0/0.40	10.0.3.129	255.255.255.192
	Gigabit0/0/0.50	10.0.3.225	255.255.255.240
	Gigabit0/0/0.60	10.0.3.193	255.255.255.224

4.2 Bảng địa chỉ ipv6

Địa chỉ ipv6 tại khu vực trụ sở chính

Bảng 4.26: Bảng địa chỉ ipv6 tại khu vực trụ sở chính

Device	Interface	IP Address	Subnet Mask
R5	Gigabit0/0/1	2019:ABBA:BBBB:1::1/64	FE80::5:2
	Serial0/1/0	2019:ABBA:AAAA:1::1/64	FE80::5:1
R4	Gigabit0/0/0	2019:ABBA:BBBB:1::2/64	FE80::4:1
	Gigabit0/0/0.10	2019:ABBA:CDDC::1/64	FE80::4:10
	Gigabit0/0/0.20	2019:ABBA:CDDC:1::1/64	FE80::4:20
	Gigabit0/0/0.30	2019:ABBA:CDDC:2::1/64	FE80::4:30
	Gigabit0/0/0.40	2019:ABBA:CDDC:3::1/64	FE80::4:40
	Gigabit0/0/0.50	2019:ABBA:CDDC:4::1/64	FE80::4:50

Bảng 4.27: Bảng địa chỉ ipv6 tại khu vực trụ sở chính

Device	**Interface**	**IP Address**	**Subnet Mask**
R6	Serial0/1/0	2019:ABBA:CCCC:1::2/64	FE80::6:1
	g0/0/0	2019:ABBA:EEEE:1::1/64	FE80::6:2
R7	Serial0/1/0	2019:ABBA:DDDD:1::1/64	FE80::7:2
	Serial0/1/1	2019:ABBA:CCCC:1::1/64	FE80::7:3
	Gigabit0/0/0	2019:ABBA:BBBB:1::3/64	FE80::7:1
R8	Serial0/1/0	2019:ABBA:DDDD:1::2/64	FE80::8:1
	g0/0/0	2019:ABBA:FFFF:1::1/64	FE80::8:2

CHƯƠNG 5 - KẾT LUẬN

5.1 Kết quả đạt được

Sau khi hoàn tất việc cấu hình và kiểm thử hệ thống mạng theo yêu cầu đề bài, hệ thống đã hoạt động ổn định và đáp ứng đầy đủ các mục tiêu đặt ra. Cụ thể:

- Các máy trạm tại các chi nhánh khác nhau có thể giao tiếp với nhau thông qua các giao thức định tuyến động OSPF và EIGRP.
- Các máy trạm trong mạng nội bộ có thể kết nối Internet nhờ vào cấu hình NAT Overload trên router biên.
- Việc phân chia VLAN giúp tách biệt các loại lưu lượng mạng giữa các nhóm người dùng. Các máy trạm thuộc các VLAN khác nhau vẫn có thể giao tiếp khi cần thiết thông qua Inter-VLAN Routing.
- Dịch vụ DHCP đã được triển khai thành công, giúp các máy trạm tự động nhận địa chỉ IP, gateway và DNS.
- Các cấu hình định tuyến nội bộ giữa các site đã được thiết lập hợp lý, giúp đảm bảo tính mở rộng và linh hoạt của hệ thống.

Hệ thống hoạt động ổn định, đáp ứng đầy đủ yêu cầu kết nối và phân tách mạng như mục tiêu ban đầu đã đặt ra.

5.2 Khó khăn và hạn chế

Trong quá trình triển khai, đã gặp phải một số khó khăn và hạn chế nhất định, bao gồm:

- Do công cụ mô phỏng Packet Tracer không hỗ trợ tính năng **IPv6 DHCP Relay**, chúng tôi không thể triển khai mô hình cấp phát địa chỉ IPv6 từ R7 thông qua relay tại R4 như yêu cầu. Thay vào đó, chúng tôi đã cấu hình DHCPv6 Stateless trực tiếp tại R4 để đảm bảo các máy trạm vẫn nhận được thông tin DNS.

- Việc xử lý thứ tự định tuyến giữa các giao thức và cấu hình lại địa chỉ gateway cho đúng với vai trò của router và VLAN đôi khi gây ra sự nhầm lẫn, yêu cầu phải kiểm tra kỹ lưỡng.

Mặc dù có một số hạn chế do công cụ mô phỏng, nhưng hệ thống vẫn đáp ứng đầy đủ các chức năng cần thiết và thể hiện rõ sự phân tách hợp lý giữa các phân vùng mạng.

5.3 Hướng phát triển

Trong tương lai, hệ thống có thể được mở rộng và hoàn thiện hơn với các tính năng sau:

- Cải thiện bảo mật mạng bằng cách bổ sung **Access Control List (ACL)** để kiểm soát lưu lượng giữa các VLAN hoặc giữa mạng nội bộ và Internet.
- Tích hợp hệ thống **mạng không dây (Wireless LAN)** để đáp ứng nhu cầu kết nối linh hoạt cho người dùng di động.
- Mở rộng các dịch vụ mạng như web nội bộ, file server, DNS nội bộ để mô phỏng đầy đủ hơn hạ tầng CNTT của một tổ chức.
- Cấp phát **địa chỉ IPv6 cho các chi nhánh** và triển khai mô hình DHCPv6 tập trung, cùng với việc sử dụng relay trong môi trường thực tế (ví dụ: GNS3, EVE-NG hoặc thiết bị thật).

Những cải tiến này sẽ giúp hệ thống phát triển không chỉ đúng chức năng cơ bản mà còn tiệm cận với một mạng doanh nghiệp hiện đại, với tính năng bảo mật, mở rộng và quản lý tập trung.

Tài liệu tham khảo

[1] Esmeralda Lima. (2021). DHCPv6 stateless server on a Cisco router. Truy cập tại: https://esmeraldalima.medium.com/how-to-configure-a-dhcpv6-server-on-a-cisco-router-c81238ea028

[2] VNPRO. (n.d.). Cấu hình định tuyến động OSPF. Truy cập tại: https://vnpro.vn/thu-vien/cauhinh-dinh-tuyen-dong-ospf-2351.html

[3] SecurityZone.vn. (n.d.). Cấu hình giao thức định tuyến EIGRP. Truy cập tại: https://securityzone.vn/t/lab-8-cau-hinh-giao-thuc-inh-tuyen-eigrp.125/

[4] Thegioimang.vn. (n.d.). Giao thức PPP và PPPoE, cách cấu hình xác thực PAP/CHAP. Truy cập tại: https://thegioimang.vn/.../tim-hieu-giao-thuc-ppp-va-pppoe...

[5] CNTTShop.vn. (n.d.). Cấu hình GRE Tunnel trên router Cisco. Truy cập tại: https://cnttshop.vn/blogs/cisco/gre-tunnel-la-gi-cau-hinh-gre-tunnel-router-cisco-1