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

MÔN MẠNG MÁY TÍNH NÂNG CAO

Cấu hình cơ bản cho hệ thống mạng theo yêu cầu

Người hướng dẫn: Ths. LÊ VIẾT THANH
Họ và tên: Võ Mạnh Cường - 52200319
Lớp: 22050401

HỒ CHÍ MINH – 2025

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

MÔN MẠNG MÁY TÍNH NÂNG CAO

Cấu hình cơ bản cho hệ thống mạng theo yêu cầu

Người hướng dẫn: Ths. LÊ VIẾT THANH
Họ và tên: Võ Mạnh Cường - 52200319
Lớp: 22050401

HỒ CHÍ MINH – 2025

LỜI CẢM ƠN

Chúng em xin chân thành gửi lời cảm ơn sâu sắc đến ThS. Lê Viết Thanh đã tận tình giảng dạy, hỗ trợ và truyền đạt kiến thức trong suốt quá trình học tập. Nhờ sự hướng dẫn của thầy, em đã xây dựng được nền tảng lý thuyết vững chắc để hoàn thành bài báo cáo cuối kì.

Tuy nhiên chúng em còn hạn chế nhiều về môn *Mạng máy tính nâng cao* nên không thể tránh khỏi những thiếu sót trong quá trình hoàn thành bài báo cáo cuối kỳ này. Mong thầy xem và góp ý để bài báo cáo của em được cải thiện hơn.

Em xin chân thành cảm ơn thầy vì đã hỗ trợ em trong quá trình thực hiện bài báo cáo này!

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

Tôi xin cam đoan đây là sản phẩm đồ án của riêng chúng tôi và được sự hướng dẫn của ThS. 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 chúng 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 chúng tôi gây ra trong quá trình thực hiện (nếu có).

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

Tác giả

(ký và ghi rõ họ tên)

Võ Mạnh Cường

TÓM TẮT

Báo cáo này trình bày quá trình thiết kế và triển khai một hệ thống mạng doanh nghiệp tích hợp cả giao thức IPv4 và IPv6, đáp ứng các yêu cầu về kết nối, định tuyến, chuyển mạch, phân phối địa chỉ và bảo mật. Phần cấu hình IPv4 bao gồm thiết lập các kết nối điểm-điểm, tunnel, định tuyến nội bộ và khu vực, chuyển mạch giữa các switch, dịch địa chỉ mạng, phân phối địa chỉ động và kiểm soát truy cập. Phần cấu hình IPv6 tập trung vào gán địa chỉ, định tuyến động và tĩnh, cùng phân phối địa chỉ tự động.

Hệ thống mạng đã được kiểm tra và hoạt động ổn định, đảm bảo khả năng giao tiếp giữa các khu vực, cung cấp dịch vụ mạng đáng tin cậy và bảo vệ dữ liệu. Báo cáo cũng đề xuất các giải pháp mở rộng để nâng cao hiệu suất và tương thích trong tương lai, làm nền tảng cho các hệ thống mạng hiện đại.

Mục lục

Danh sách hình vẽ

Danh sách bảng

Danh mục các từ viết tắt

ACL	Access Control List – Danh sách kiểm soát truy cập
CHAP	Challenge Handshake Authentication Protocol – Giao thức xác thực bắt tay thử thách
DHCP	Dynamic Host Configuration Protocol – Giao thức cấp phát địa chỉ động
DNS	Domain Name System – Hệ thống phân giải tên miền
EIGRP	Enhanced Interior Gateway Routing Protocol – Giao thức định tuyến cổng nội bộ nâng cao
GRE	Generic Routing Encapsulation – Đóng gói định tuyến chung
HTTP	HyperText Transfer Protocol – Giao thức truyền siêu văn bản
HTTPS	HyperText Transfer Protocol Secure – Giao thức truyền siêu văn bản bảo mật
IP	Internet Protocol – Giao thức Internet
IPv4	Internet Protocol version 4 – Giao thức Internet phiên bản 4
IPv6	Internet Protocol version 6 – Giao thức Internet phiên bản 6
LAN	Local Area Network – Mạng cục bộ
NAT	Network Address Translation – Chuyển đổi địa chỉ mạng
OSPF	Open Shortest Path First – Giao thức định tuyến đường ngắn nhất mở
PAP	Password Authentication Protocol – Giao thức xác thực mật khẩu
PPP	Point-to-Point Protocol – Giao thức điểm-điểm
PVST	Per-VLAN Spanning Tree – Cây bao trùm theo VLAN
SSH	Secure Shell – Vỏ bảo mật
STP	Spanning Tree Protocol – Giao thức cây bao trùm

TCP	Transmission Control Protocol – Giao thức điều khiển truyền tải
UDP	User Datagram Protocol – Giao thức dữ liệu người dùng
VLAN	Virtual LAN – Mạng LAN ảo
VTP	VLAN Trunking Protocol – Giao thức trung kế VLAN

Chương 1

Cơ sở lý thuyết

Dưới đây là cơ sở lý thuyết chi tiết tập trung vào các nội dung liên quan đến IPv4 và IPv6 được sử dụng trong bài báo cáo này. Lý thuyết bao gồm các khái niệm cốt lõi, cơ chế hoạt động, và cách áp dụng vào các yêu cầu cụ thể của đề bài.

1.1 IPv4

1.1.1 Sơ đồ địa chỉ và phân bổ IP

Lý thuyết

- **Địa chỉ IPv4**: Địa chỉ 32-bit, biểu diễn dưới dạng 4 octet (ví dụ: `192.168.1.1`). Được chia thành phần mạng và phần host dựa trên subnet mask (ví dụ: `/24` tương ứng với `255.255.255.0`).
- **Subnetting**: Chia một dải địa chỉ IP thành các mạng con nhỏ hơn để đáp ứng nhu cầu số lượng host và tổ chức mạng.
  + Công thức tính số host: $2^{(32-\text{prefix})} - 2$ (trừ 2 địa chỉ cho network và broadcast).
  + Ví dụ: Để hỗ trợ 200 host, cần `/24` (256 - 2 = 254 host); cho 300 host, cần `/23` (512 - 2 = 510 host).
- **VLAN (Virtual Local Area Network)**: Phân tách lưu lượng mạng logic trên cùng một switch. Mỗi VLAN được gán một subnet riêng để quản lý địa chỉ IP.

- **Point-to-Point Network**: Sử dụng subnet nhỏ (thường `/30`) để kết nối hai router, cung cấp 2 địa chỉ host (một cho mỗi router).

Ứng dụng trong đề bài

- **HQ VLANs** (Bảng 2):
  + VLAN 10 (UNIT1, 200 host): Cần subnet `/24` (254 host). Ví dụ: `X.X.1.0/24`.
  + VLAN 20 (UNIT2, 300 host): Cần subnet `/23` (510 host). Ví dụ: `X.X.2.0/23`.
  + VLAN 30 (UNIT3, 100 host): Cần subnet `/25` (126 host). Ví dụ: `X.X.4.0/25`.
  + VLAN 40 (GUEST, 50 host): Cần subnet `/26` (62 host). Ví dụ: `X.X.4.128/26`.
  + VLAN 50 (SERVERS, 10 host): Cần subnet `/28` (14 host). Ví dụ: `X.X.4.192/28`.
  + VLAN 60 (Management, 20 host): Cần subnet `/27` (30 host). Ví dụ: `X.X.4.224/27`.
- **Chi nhánh Loopback** (Bảng 3):
  + R1 Lo0 (500 host): Cần subnet `/23`. Ví dụ: `Y.Y.1.0/23`.
  + R1 Lo1 (300 host): Cần subnet `/23`. Ví dụ: `Y.Y.3.0/23`.
  + R2 Lo0 (100 host): Cần subnet `/25`. Ví dụ: `Y.Y.5.0/25`.
  + R3 Lo0 (200 host): Cần subnet `/24`. Ví dụ: `Y.Y.6.0/24`.
  + R3 Lo1 (100 host): Cần subnet `/25`. Ví dụ: `Y.Y.7.0/25`.
- **Point-to-Point** (Bảng 1):
  + R7 ↔ R6: `200.0.100.0/30` (host: `200.0.100.1`, `200.0.100.2`).
  + R7 ↔ R8: `200.0.100.4/30` (host: `200.0.100.5`, `200.0.100.6`).
  + R5 ↔ ACCESS: `200.0.100.8/30` (host: `200.0.100.9`, `200.0.100.10`).

1.1.2 Kết nối PPP (Point-to-Point Protocol)

Lý thuyết

- **PPP**: Giao thức tầng liên kết dữ liệu, cung cấp kết nối trực tiếp giữa hai node. Hỗ trợ xác thực, nén dữ liệu, và phát hiện lỗi.
  + **PAP (Password Authentication Protocol)**: Gửi tên người dùng và mật khẩu dưới dạng plaintext. Dễ cấu hình nhưng kém an toàn.
  + **CHAP (Challenge Handshake Authentication Protocol)**: Sử dụng cơ chế challenge-response, router gửi một chuỗi ngẫu nhiên (challenge), đối phương trả lời bằng giá trị băm (response) dựa trên mật khẩu. An toàn hơn PAP.
- **Cấu hình PPP**:
  1. Bật PPP encapsulation: `encapsulation ppp`.
  2. Cấu hình xác thực:
     + PAP: `ppp pap sent-username <username> password <password>`.
     + CHAP: `ppp chap hostname <hostname>`, `ppp chap password <password>`.
  3. Gán tên người dùng/mật khẩu trong cơ sở dữ liệu: `username <name> password <password>`.

Ứng dụng trong đề bài

- Cấu hình PPP giữa R7 và R6 với xác thực PAP:
  1. Bật PPP encapsulation: `encapsulation ppp`.
  2. Cấu hình xác thực trên R7: `ppp pap sent-username R6 password cisco123`.
  3. Cấu hình xác thực trên R6: `username R7 password cisco123`.
- Cấu hình PPP giữa R7 và R8 với xác thực CHAP:
  1. Bật PPP encapsulation: `encapsulation ppp`.
  2. Cấu hình trên R7: `ppp chap hostname R7`, `ppp chap password`

`cisco456`.

3. Cấu hình trên R8: `ppp chap hostname R8`, `ppp chap password cisco456`, `username R7 password cisco456`.

– Đảm bảo các interface serial được cấu hình với `encapsulation ppp` và địa chỉ IP từ `200.0.100.0/30` và `200.0.100.4/30`.

1.1.3 Tunneling GRE (Generic Routing Encapsulation)

Lý thuyết

– **GRE**: Giao thức đường hầm tầng 3, đóng gói các gói tin của nhiều giao thức (IPv4, IPv6, MPLS) để truyền qua mạng IP.
  + Cấu trúc: GRE thêm header vào gói tin gốc, sau đó đóng gói trong gói IP mới.
  + Ưu điểm: Linh hoạt, hỗ trợ nhiều giao thức.
  + Nhược điểm: Không mã hóa, cần kết hợp với IPsec nếu yêu cầu bảo mật.

– **Cấu hình GRE**:
  1. Tạo interface tunnel: `interface tunnel <number>`.
  2. Gán địa chỉ IP cho tunnel.
  3. Chỉ định nguồn (source) và đích (destination) của tunnel.
  4. Cấu hình định tuyến để lưu lượng đi qua tunnel.

Ứng dụng trong đề bài

– **GRE giữa R6 và R8**:
  + Tạo tunnel với địa chỉ mạng `X.X.X.X/A` (hỗ trợ 2 host, ví dụ: `/30`).
  + Source: Interface vật lý của R6 (ví dụ: `200.0.100.2`).
  + Destination: Interface vật lý của R8 (ví dụ: `200.0.100.5`).
  + Cấu hình tuyến tĩnh: `ip route 0.0.0.0 0.0.0.0 tunnel <number>` hoặc động (EIGRP).

1.1.4 Định tuyến

Lý thuyết

- **EIGRP (Enhanced Interior Gateway Routing Protocol)**:
  + Giao thức định tuyến lai, sử dụng thuật toán DUAL (Diffusing Update Algorithm).
  + Metric: Dựa trên băng thông, độ trễ, độ tin cậy, tải, và MTU.
  + Cấu hình: Kích hoạt EIGRP với AS number, thêm mạng bằng lệnh `network`.
  + Passive interface: Ngăn gửi bản cập nhật EIGRP trên interface: `passive-interface <interface>`.
  + Redistribution: Chuyển tuyến từ giao thức khác vào EIGRP bằng lệnh `redistribute`.
- **OSPF (Open Shortest Path First)**:
  + Giao thức trạng thái liên kết, sử dụng thuật toán Dijkstra để tính đường đi ngắn nhất.
  + Chia mạng thành các area để giảm lưu lượng cập nhật.
  + Cấu hình: Kích hoạt OSPF với process ID, thêm mạng bằng lệnh `network <network> <wildcard> area <area>`.
  + Passive interface: Tương tự EIGRP.
- **Default Route**: Tuyến mặc định (`0.0.0.0/0`) được cấu hình để gửi lưu lượng không khớp đến một điểm cụ thể.
- **Redistribution**: Cho phép chia sẻ tuyến giữa các giao thức định tuyến khác nhau, cần đảm bảo metric tương thích.

Ứng dụng trong đề bài

- **EIGRP tại HQ**:
  + Kích hoạt EIGRP với AS number chung: `router eigrp 100`.
  + Thêm các mạng của HQ (ví dụ: VLAN subnets, `200.0.100.0/30`).

  + Đặt interface không cần gửi bản cập nhật (ví dụ: interface kết nối host) thành passive: `passive-interface <interface>`.

- **OSPF đa khu vực tại chi nhánh**:
  + Kích hoạt OSPF với process ID: `router ospf 1`.
  + Gán các mạng chi nhánh (Loopback, WAN links) vào các area khác nhau.
  + Cấu hình passive interface cho các interface không cần gửi bản cập nhật: `passive-interface <interface>`.

- **Default Route trên R5**:
  + Cấu hình: `ip route 0.0.0.0 0.0.0.0 <ACCESS-IP>`.
  + Phân phối vào EIGRP: `redistribute static`.
  + Phân phối vào OSPF: `default-information originate`.

- **Redistribution**:
  + Trên router biên: Redistribute EIGRP vào OSPF và ngược lại, đảm bảo metric phù hợp: `redistribute eigrp 100 metric 10`.

1.1.5 Chuyển mạch

Lý thuyết

- **VTP (VLAN Trunking Protocol)**:
  + Quản lý tập trung VLAN trên nhiều switch.
  + VTP Server: Tạo, sửa, xóa VLAN và đồng bộ với client.
  + VTP Client: Nhận VLAN từ server, không thể chỉnh sửa.

- **Rapid PVST+ (Per-VLAN Spanning Tree)**:
  + Phiên bản cải tiến của STP, hội tụ nhanh hơn (vài giây so với 30-50 giây của STP).
  + Mỗi VLAN có một cây spanning tree riêng.
  + Root Bridge: Switch có Bridge ID thấp nhất (Priority + MAC address).

- **EtherChannel**:
  + Kết hợp nhiều liên kết vật lý thành một liên kết logic.
  + LACP (Link Aggregation Control Protocol): Giao thức chuẩn IEEE, tự động thương lượng.
- **Router-on-a-Stick**:
  + Sử dụng một interface router với nhiều sub-interface, mỗi sub-interface gán một VLAN và địa chỉ IP.
  + Yêu cầu trunk link giữa router và switch.
- **SSH**:
  + Giao thức quản lý từ xa an toàn.
  + Cấu hình: Tạo domain name, khóa RSA, tài khoản người dùng, và bật SSH trên VTY lines.

Ứng dụng trong đề bài

- **VTP**:
  + S1 là VTP Server, các switch khác là Client.
  + Cấu hình domain name và password cho VTP: `vtp domain <domain>`, `vtp password <password>`.
- **Rapid PVST+**:
  + Bật chế độ: `spanning-tree mode rapid-per-vlan`.
  + Đặt S1 làm root bridge cho VLAN 10, 20, 30: `spanning-tree vlan 10,20,30 root primary`.
  + Đặt S2 làm root bridge cho VLAN 40, 50, 60: `spanning-tree vlan 40,50,60 root primary`.
- **EtherChannel**:
  + Cấu hình LACP trên các interface kết nối giữa switch: `channel-group <number> mode active`.
- **Router-on-a-Stick trên R4**:

  + Tạo sub-interface cho mỗi VLAN (10, 20, 30, 40, 50, 60).
  + Gán địa chỉ IP gateway (ví dụ: `X.X.1.1/24` cho VLAN 10).
  + Bật encapsulation: `encapsulation dot1q <vlan-id>`.
- **SSH**:
  + Cấu hình trên tất cả switch: `ip domain-name <domain>`, `crypto key generate rsa`, `line vty 0 15`, `transport input ssh`.

1.1.6 NAT và DHCP

Lý thuyết

- **NAT Overload (PAT)**:
  + Ánh xạ nhiều địa chỉ IP riêng sang một địa chỉ IP công cộng, sử dụng các cổng khác nhau.
  + Cấu hình: Tạo ACL để xác định địa chỉ nguồn, gán NAT trên interface inside/outside.
- **DHCP**:
  + Server cấp phát địa chỉ IP, subnet mask, gateway, và DNS cho client.
  + Cấu hình: Tạo DHCP pool cho mỗi VLAN, chỉ định dải địa chỉ và các tham số.
- **Port Forwarding**:
  + Chuyển tiếp lưu lượng từ cổng cụ thể trên địa chỉ công cộng đến máy chủ nội bộ.
  + Cấu hình: Sử dụng NAT tĩnh với cổng (ví dụ: TCP `80`, `443`).

Ứng dụng trong đề bài

- **NAT Overload trên Access**:
  + Tạo ACL cho các mạng nội bộ (HQ và chi nhánh): `access-list 1 permit <HQ-subnet>`, `access-list 1 permit <Branch-subnet>`.
  + Cấu hình: `ip nat inside source list 1 interface <outside>`

`overload`.

+ Gán interface: `ip nat inside` cho HQ/chi nhánh, `ip nat outside` cho Internet.

– **DHCP trên R4**:

+ Tạo pool cho VLAN 10, 20, 30, 40.

+ Ví dụ: `ip dhcp pool VLAN10`, `network X.X.1.0 255.255.255.0`, `default-router X.X.1.1`, `dns-server <IP>`.

– **Port Forwarding**:

+ Cấu hình NAT tĩnh: `ip nat inside source static tcp <server-IP> 80 <public-IP> 80`, tương tự cho HTTPS (`ip nat inside source static tcp <server-IP> 443 <public-IP> 443`).

1.1.7 ACL (Access Control List)

Lý thuyết

– **ACL**:

+ Standard ACL: Lọc dựa trên địa chỉ nguồn, áp dụng gần đích.

+ Extended ACL: Lọc dựa trên nguồn, đích, giao thức, cổng, áp dụng gần nguồn.

+ Cấu hình: `access-list <number> permit/deny <criteria>`, áp dụng bằng `ip access-group`.

– **Ứng dụng ACL**:

+ Hạn chế truy cập vào mạng nội bộ.

+ Cho phép truy cập dịch vụ cụ thể (như SSH).

Ứng dụng trong đề bài

– **ACL cho VLAN GUEST**:

+ Tạo extended ACL:
`access-list 101 deny ip <GUEST-subnet> <HQ-subnets>`,
`access-list 101 permit ip <GUEST-subnet> any`.

  + Áp dụng trên interface VLAN 40: `ip access-group 101 in`.

- **ACL cho VLAN SERVERS**:
  + Tạo extended ACL:
    `access-list 102 permit tcp <SERVERS-subnet> any eq 22`,
    `access-list 102 deny ip <SERVERS-subnet> any`.
  + Áp dụng trên VTY lines của switch: `access-class 102 in`.

1.2 IPv6

1.2.1 Sơ đồ địa chỉ IPv6

Lý thuyết

- **Địa chỉ IPv6**: 128-bit, biểu diễn dưới dạng 8 nhóm 16-bit (ví dụ: `2019:ABBA:CDDC:0001::1`). Các loại địa chỉ:
  + **Link-local**: `FE80::/10`, tự động gán cho mọi interface, dùng trong cùng liên kết.
  + **Global unicast**: Dùng cho giao tiếp toàn cầu.
    Ví dụ: `2019:ABBA:CDDC::/48`.
- **Subnetting IPv6**:
  + Thường sử dụng `/64` cho mạng LAN (cung cấp 2^{64} địa chỉ).
  + Chia mạng lớn (ví dụ: `/48`) thành các subnet `/64` bằng cách thay đổi 16 bit tiếp theo.
- **SLAAC (Stateless Address Autoconfiguration)**:
  + Host tự động tạo địa chỉ IPv6 dựa trên prefix từ router và ID interface (thường là địa chỉ MAC).

Ứng dụng trong đề bài

- **Link-local address**:
  + Gán tĩnh cho mọi interface: Ví dụ, `FE80::1/10` cho R7, `FE80::2/10` cho R6.

- **VLAN subnets**:
  + Chia `2019:ABBA:CDDC:/48` thành 5 subnet `/64`:
    - VLAN 10: `2019:ABBA:CDDC:1::/64`, gateway: `2019:ABBA:CDDC:1::1`.
    - VLAN 20: `2019:ABBA:CDDC:2::/64`, gateway: `2019:ABBA:CDDC:2::1`.
    - VLAN 30: `2019:ABBA:CDDC:3::/64`, gateway: `2019:ABBA:CDDC:3::1`.
    - VLAN 40: `2019:ABBA:CDDC:4::/64`, gateway: `2019:ABBA:CDDC:4::1`.
    - VLAN 50: `2019:ABBA:CDDC:5::/64`, gateway: `2019:ABBA:CDDC:5::1`.
- **Router connections** (Bảng 4):
  + 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`.
  + LAN R6: `2019:ABBA:EEEE:1::/64`.
  + LAN R8: `2019:ABBA:FFFF:1::/64`.

1.2.2 Định tuyến IPv6

Lý thuyết

- **EIGRP cho IPv6**:
  + Tương tự EIGRP IPv4, nhưng yêu cầu bật IPv6 unicast routing: `ipv6 unicast-routing`.
  + Kích hoạt trên interface: `ipv6 eigrp <AS>`.
  + Không sử dụng lệnh `network`, thay vào đó bật trực tiếp trên interface.
- **Default Route**:

  + Cấu hình: `ipv6 route ::/0 <next-hop>`.
  + Phân phối: `redistribute static` trong EIGRP.
- **Inter-VLAN Routing**:
  + Tương tự IPv4, sử dụng sub-interface với encapsulation dot1q, nhưng gán địa chỉ IPv6.

Ứng dụng trong đề bài

- **EIGRP IPv6 tại HQ**:
  + Bật: `ipv6 unicast-routing`.
  + Kích hoạt EIGRP trên các interface VLAN và WAN: `ipv6 eigrp <AS>`.
- **Default Route trên R5**:
  + Cấu hình: `ipv6 route ::/0 <ACCESS-IPv6>`.
  + Phân phối: `redistribute static` trong EIGRP.
- **Inter-VLAN Routing trên R4**:
  + Tạo sub-interface cho VLAN 10, 20, 30, 40, 50.
  + Gán địa chỉ gateway (ví dụ: `2019:ABBA:CDDC:1::1/64` cho VLAN 10).
  + Bật encapsulation: `encapsulation dot1q <vlan-id>`.

DHCPv6

Lý thuyết

- **Stateful DHCPv6**:
  + Server DHCPv6 duy trì trạng thái địa chỉ, cấp phát địa chỉ IPv6 duy nhất và thông tin bổ sung (DNS, domain) từ pool được định nghĩa.
  + Cấu hình: Tạo DHCPv6 pool, chỉ định prefix địa chỉ và DNS server, sau đó áp dụng pool lên interface.

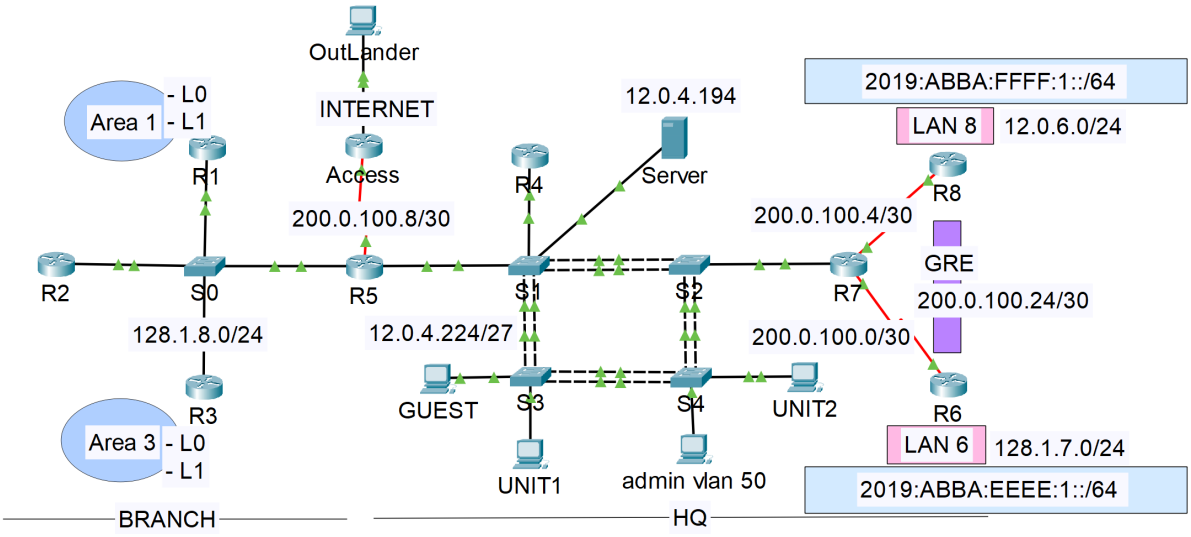
Ứng dụng trong đề bài

– **Stateful DHCPv6 trên R4**:

+ Tạo pool cho các VLAN:
  - `ipv6 dhcp pool VLAN10`
    với `address prefix 2019:ABBA:CDDC:1000::/64`.
  - `ipv6 dhcp pool VLAN20`
    với `address prefix 2019:ABBA:CDDC:2000::/64`.
  - `ipv6 dhcp pool VLAN30`
    với `address prefix 2019:ABBA:CDDC:3000::/64`.
  - `ipv6 dhcp pool VLAN40`
    với `address prefix 2019:ABBA:CDDC:4000::/64`.
+ Cấu hình DNS: `dns-server 2001:4860:4860::8888` cho tất cả pool.
+ Áp dụng pool lên các interface:
  - `interface GigabitEthernet0/0/0.10`:
    `ipv6 dhcp server VLAN10`.
  - `interface GigabitEthernet0/0/0.20`:
    `ipv6 dhcp server VLAN20`.
  - `interface GigabitEthernet0/0/0.30`:
    `ipv6 dhcp server VLAN30`.
  - `interface GigabitEthernet0/0/0.40`:
    `ipv6 dhcp server VLAN40`.
+ Bật thông báo sử dụng DHCPv6: `ipv6 nd other-config-flag` trên các interface VLAN.

Chương 2

Sơ đồ mạng tổng thể



Hình 2.1: Sơ đồ tổng quan hệ thống mạng

2.1 Diễn giải sơ đồ

Sơ đồ trên mô tả hệ thống mạng kết nối giữa hai khu vực: **Trụ sở chính (HQ)** và **Chi nhánh (Branch)** với các yêu cầu về định tuyến, chuyển mạch, bảo mật, NAT, DHCP, hỗ trợ song song IPv4 và IPv6.

2.1.1 Khu vực HQ (Headquarters)

- **Router HQ (R4, R6, R7, R8)**:
  + R4 thực hiện định tuyến liên VLAN (router-on-a-stick) cho toàn bộ các VLAN (10, 20, 30, 40, 50).
  + R6 kết nối PPP đến R7 (PAP) và thiết lập đường hầm GRE đến R8.

  + R8 kết nối PPP đến R7 (CHAP) và tham gia GRE Tunnel với R6.
  + R7 là trung tâm kết nối PPP và GRE.
  + Khu vực HQ sử dụng định tuyến **EIGRP cho cả IPv4 và IPv6**.
- **Switches (S1 – S4)**:
  + S1 là **VTP Server**, các switch còn lại là **VTP Clients**.
  + Giao thức spanning tree: **Rapid PVST+**.
  + S1 là **root bridge** cho VLAN 10, 20, 30; S2 là root cho các VLAN còn lại.
  + Tất cả switch cấu hình SSH, chỉ VLAN SERVERS được SSH.
  + Kết nối giữa các switch sử dụng **EtherChannel với LACP**.
- **Dịch vụ mạng**:
  + **NAT Overload** tại router Access cho HQ và chi nhánh truy cập Internet.
  + **DHCP Server** trên R4 cấp IP động cho các VLAN.
  + Dịch vụ Web triển khai trong VLAN máy chủ với NAT chuyển tiếp cổng cho HTTP/HTTPS.

2.1.2 Khu vực Chi nhánh (Branch)

- **Routers R1, R2, R3** sử dụng định tuyến **OSPF đa khu vực**, với mỗi router thuộc các area riêng biệt.
- **Router R5**:
  + Là trung tâm kết nối đến Internet và điểm giao giữa HQ và Chi nhánh.
  + Cấu hình tuyến mặc định trỏ về router ACCESS.
  + Phân phối tuyến mặc định vào EIGRP và OSPF.
  + Cấu hình **redistribution giữa EIGRP và OSPF**.

2.1.3 Kết nối liên vùng

- **PPP**:

  + R7 ↔ R6 dùng xác thực **PAP**.
  + R7 ↔ R8 dùng xác thực **CHAP**.
- **Tunnel GRE**:
  + Thiết lập giữa R6 và R8.
  + Sử dụng mạng riêng X.X.X.X/A.
  + Yêu cầu có ít nhất 2 máy chủ kiểm tra kết nối.
- **ACL**:
  + Chặn VLAN GUEST truy cập HQ và chi nhánh, vẫn cho phép ra Internet.
  + Chỉ VLAN SERVERS được SSH vào switch.

2.1.4 Cấu hình IPv6

- Phân bổ địa chỉ IPv6 từ dải `2019:ABBA:CDDC::/48` cho 5 VLAN.
- Gán địa chỉ **link-local tĩnh** với phạm vi `FE80::/10`.
- Sử dụng **EIGRP for IPv6** tại HQ.
- Tuyến mặc định từ R5 đến router ACCESS được truyền bá vào EIGRP.
- Cấu hình **inter-VLAN routing** sử dụng cùng sub-interface như IPv4.

2.2 Kế hoạch địa chỉ (Address Planning - IPv4)

Trụ sở chính (HQ) - Class A: `12.0.0.0/8`

- Mạng trụ sở HQ sử dụng địa chỉ lớp A `12.0.0.0/8`, cung cấp khoảng 16.7 triệu địa chỉ.
- Các VLAN tại trụ sở chính được cấp phát địa chỉ như sau (dựa theo Bảng 2):

Bảng 2.1: Cấp phát địa chỉ cho VLAN tại trụ sở chính

VLAN	Tên VLAN	Số Host	Subnet	Host khả dụng	Gateway
10	UNIT1	200	12.0.1.0/24	254	12.0.1.1
20	UNIT2	300	12.0.2.0/23	510	12.0.2.1
30	UNIT3	100	12.0.4.0/25	126	12.0.4.1
40	GUEST	50	12.0.4.128/26	62	12.0.4.129
50	SERVERS	10	12.0.4.192/28	14	12.0.4.193
60	Management	20	12.0.4.224/27	30	12.0.4.225

Chi nhánh (Branch) - Class B: `128.1.0.0/16`

– Chi nhánh sử dụng địa chỉ lớp B `128.1.0.0/16`, cung cấp khoảng 65 nghìn địa chỉ.

– Các Loopback được cấu hình như sau (từ Bảng 3):

Bảng 2.2: Cấp phát địa chỉ Loopback tại chi nhánh

Thiết bị	Interface	Số Host	Subnet	Host khả dụng	Gateway
R1	Lo0	500	128.1.0.0/23	510	128.1.0.1
R1	Lo1	300	128.1.2.0/23	510	128.1.2.1
R2	Lo0	100	128.1.4.0/25	126	128.1.4.1
R3	Lo0	200	128.1.5.0/24	254	128.1.5.1
R3	Lo1	100	128.1.6.0/25	126	128.1.6.1

Các liên kết trong mô hình mạng

Bảng 2.3: IP và Subnet cho các liên kết trong mô hình mạng

Liên kết	Mạng / Subnet	Thiết bị - Địa chỉ IP
R7 ↔ R6	200.0.100.0/30	R7: 200.0.100.1, R6: 200.0.100.2
R7 ↔ R8	200.0.100.4/30	R7: 200.0.100.5, R8: 200.0.100.6
R5 ↔ ACCESS	200.0.100.8/30	R5: 200.0.100.9, ACCESS: 200.0.100.10
R1 ↔ S0	128.1.8.0/24	R1: 128.1.8.2, S0: 128.1.8.1 (VLAN 1)
R2 ↔ S0	128.1.8.0/24	R2: 128.1.8.3, S0: 128.1.8.1 (VLAN 1)
R3 ↔ S0	128.1.8.0/24	R3: 128.1.8.4, S0: 128.1.8.1 (VLAN 1)
R5 ↔ S1	128.1.8.0/24	R5: 128.1.8.5, S0: 128.1.8.1 (VLAN 1)
S1, S2, S3, S4 ↔ R4, R5, R7	12.0.4.224/27	S1: 12.0.4.226, S2: 12.0.4.227, S3: 12.0.4.228, S4: 12.0.4.229 R4: 12.0.4.225, R5: 12.0.4.230, R7: 12.0.4.231 (VLAN 60)

– Tại khu vực Branch, switch S0 được cấu hình với VLAN 1 (128.1.8.0/24) để kết nối các router R1, R2, R3.

– Địa chỉ IP của S0 là 128.1.8.1/24, trong khi R1, R2, R3 được gán địa chỉ trong cùng subnet (128.1.8.2, 128.1.8.3, 128.1.8.4) trên giao diện kết nối với S0.

Kết nối GRE Tunnel

– GRE Tunnel giữa R6 và R8 sử dụng địa chỉ `200.0.100.24/30`:
  + R6: 200.0.100.25
  + R8: 200.0.100.26

LAN cục bộ

– LAN 6 (kết nối với R6): `128.1.7.0/24`

– LAN 8 (kết nối với R8): `12.0.6.0/24`

2.3 Kế hoạch địa chỉ IPv6

– Hệ thống mạng sử dụng địa chỉ IPv6 theo chuẩn `/64` cho mỗi mạng con.

– Các dải địa chỉ được cấp phát theo chức năng như sau:

2.3.1 Kết nối các liên kết mạng

Bảng 2.4: Địa chỉ IPv6 cho kết nối giữa các router

Kết nối	Dải địa chỉ IPv6	Thiết bị
ACCESS ↔ R5	2019:ABBA:AAAA:1::/64	ACCESS: ::1, R5: ::2
R4, R5, R7 (liên kết ba chiều)	2019:ABBA:BBBB:1::/64	R4: ::1, R5: ::2, R7: ::3
R7 ↔ R6	2019:ABBA:CCCC:1::/64	R7: ::1, R6: ::2
R7 ↔ R8	2019:ABBA:DDDD:1::/64	R7: ::1, R8: ::2

2.3.2 LAN nội bộ

Bảng 2.5: Địa chỉ IPv6 cho các mạng LAN

Thiết bị	Dải địa chỉ IPv6	Ghi chú
LAN R6	2019:ABBA:EEEE:1::/64	Mạng LAN cục bộ tại R6
LAN R8	2019:ABBA:FFFF:1::/64	Mạng LAN cục bộ tại R8

2.3.3 VLAN tại Trụ sở chính (HQ)

Bảng 2.6: Địa chỉ IPv6 cấp phát cho các VLAN

VLAN	Tên	Địa chỉ IPv6
10	UNIT1	2019:ABBA:CDDC:1::/64
20	UNIT2	2019:ABBA:CDDC:2::/64
30	UNIT3	2019:ABBA:CDDC:3::/64
40	GUEST	2019:ABBA:CDDC:4::/64

2.3.4 Link-local Address (FE80::/10)

– Tất cả thiết bị mạng cần cấu hình địa chỉ link-local thuộc dải `FE80::/10`.

Bảng 2.7: Địa chỉ IPv6 Link-local cấu hình trên các thiết bị

Thiết bị	Interface	Link-local
R4	Gig0/0/0.10	FE80::4:10
	Gig0/0/0.20	FE80::4:20
	Gig0/0/0.30	FE80::4:30
	Gig0/0/0.40	FE80::4:40
	Gig0/0/0.60	FE80::4
R5	S0/1/0	FE80::5:1
	Gig0/0/1	FE80::5
R6	Gig0/0/0	FE80::6:1
	S0/1/0	FE80::6
R7	Gig0/0/0	FE80::7
	S0/1/1	FE80::7:1
	S0/1/0	FE80::7:2
R8	Gig0/0/0	FE80::8:1
	S0/1/0	FE80::8
ACCESS	S0/1/0	FE80::A

Chương 3

Mô tả cấu hình hệ thống - IPv4

3.1 Cấu hình địa chỉ IPv4

Để triển khai hệ thống mạng IPv4, trước tiên cần gán địa chỉ IP cho các interface trên các router và switch theo sơ đồ địa chỉ đã được phân bổ. Dưới đây là các bước cấu hình chi tiết:

- **Router R1 (Chi nhánh)**:
  + Interface `GigabitEthernet0/0/0`: Gán địa chỉ `128.1.8.2/24` (`255.255.255.0`) để kết nối với mạng chi nhánh.
  + Interface `Loopback0`: Gán địa chỉ `128.1.0.1/23` (`255.255.254.0`) để mô phỏng mạng với 500 host.
  + Interface `Loopback1`: Gán địa chỉ `128.1.2.1/23` (`255.255.254.0`) để mô phỏng mạng với 300 host.
  + Bật các interface: `no shutdown`.
- **Router R2 (Chi nhánh)**:
  + Interface `GigabitEthernet0/0/0`: Gán địa chỉ `128.1.8.3/24` (`255.255.255.0`) để kết nối với mạng chi nhánh.
  + Interface `Loopback0`: Gán địa chỉ `128.1.4.1/25` (`255.255.255.128`) để mô phỏng mạng với 100 host.
  + Bật các interface: `no shutdown`.
- **Router R3 (Chi nhánh)**:
  + Interface `GigabitEthernet0/0/0`: Gán địa chỉ `128.1.8.4/24`

(255.255.255.0) để kết nối với mạng chi nhánh.

+ Interface Loopback0: Gán địa chỉ 128.1.5.1/24 (255.255.255.0) để mô phỏng mạng với 200 host.
+ Interface Loopback1: Gán địa chỉ 128.1.6.1/25 (255.255.255.128) để mô phỏng mạng với 100 host.
+ Bật các interface: no shutdown.

– **Switch S0 (Chi nhánh)**:
+ Cấu hình thêm VLAN 1 để quản lí và kết nối giữa 3 router khu vực chi nhánh là R1, R2 và R3 với router R5.
+ Interface VLAN 1: Gán địa chỉ 128.1.8.1/24 (255.255.255.0) để quản lý switch.
+ Các interface FastEthernet0/1, FastEthernet0/2, FastEthernet0/3, và dải FastEthernet0/4 - 24: Đặt chế độ switchport mode access, gán vào VLAN 1.
+ Interface GigabitEthernet0/1: Đặt chế độ switchport mode trunk để kết nối với router.
+ Cấu hình gateway mặc định đến Router R5: ip default-gateway 128.1.8.5.
+ Bật các interface: no shutdown.

– **Router R5 (HQ)**:
+ Interface Serial0/1/0: Gán địa chỉ 200.0.100.9/30 (255.255.255.252) để kết nối với router ACCESS.
+ Interface GigabitEthernet0/0/0: Gán địa chỉ 128.1.8.5/24 (255.255.255.0) để kết nối với mạng chi nhánh.
+ Interface GigabitEthernet0/0/1: Gán địa chỉ 12.0.4.230/27 (255.255.255.224) để kết nối với mạng HQ.
+ Bật các interface: no shutdown.

– **Router R6 (HQ - LAN 6)**:

  + Interface `Serial0/1/0`: Gán địa chỉ `200.0.100.2/30` (`255.255.255.252`) để kết nối với R7.
  + Interface `GigabitEthernet0/0/0`: Gán địa chỉ `128.1.7.1/24` (`255.255.255.0`) để mô phỏng LAN 6.
  + Bật các interface: `no shutdown`.

- **Router R7 (HQ)**:
  + Interface `GigabitEthernet0/0/0`: Gán địa chỉ `12.0.4.231/27` (`255.255.255.224`) để kết nối với mạng HQ.
  + Interface `Serial0/1/0`: Gán địa chỉ `200.0.100.1/30` (`255.255.255.252`) để kết nối với R6.
  + Interface `Serial0/1/1`: Gán địa chỉ `200.0.100.5/30` (`255.255.255.252`) để kết nối với R8.
  + Bật các interface: `no shutdown`.
- **Router R8 (HQ - LAN 8)**:
  + Interface `Serial0/1/0`: Gán địa chỉ `200.0.100.6/30` (`255.255.255.252`) để kết nối với R7.
  + Interface `GigabitEthernet0/0/0`: Gán địa chỉ `12.0.6.1/24` (`255.255.255.0`) để mô phỏng LAN 8.
  + Bật các interface: `no shutdown`.
- **Router ACCESS (Internet)**:
  + Interface `Serial0/1/0`: Gán địa chỉ `200.0.100.10/30` (`255.255.255.252`) để kết nối với R5.
  + Interface `GigabitEthernet0/0/0`: Gán địa chỉ `203.0.113.1/24` (`255.255.255.0`) để mô phỏng kết nối Internet.
  + Bật các interface: `no shutdown`.

Các địa chỉ IP được gán đảm bảo phù hợp với yêu cầu số lượng host cho từng mạng (Bảng 2.2 và Bảng 2.3) và sơ đồ địa chỉ point-to-point (Bảng 1). Việc bật các interface bằng lệnh `no shutdown` đảm bảo các kết nối vật

lý sẵn sàng hoạt động.

3.2 Cấu hình xác thực PPP giữa các router

Yêu cầu cấu hình kết nối PPP giữa R7 và R6 với xác thực PAP, và giữa R7 và R8 với xác thực CHAP. Dưới đây là các bước cấu hình chi tiết:

- **Kết nối PPP giữa R7 và R6 (Xác thực PAP)**:
  + Trên R7, interface `Serial0/1/1`:
    - Đã gán địa chỉ `200.0.100.5/30` (từ cấu hình trước).
    - Bật PPP encapsulation: `encapsulation ppp`.
    - Cấu hình thông tin xác thực: `username R6 password chooky`.
  + Trên R6, interface `Serial0/1/0`:
    - Đã gán địa chỉ `200.0.100.2/30` (từ cấu hình trước).
    - Bật PPP encapsulation: `encapsulation ppp`.
    - Cấu hình xác thực PAP:
      `ppp pap sent-username R6 password chooky`.
- **Kết nối PPP giữa R7 và R8 (Xác thực CHAP)**:
  + Trên R7, interface `Serial0/1/0`:
    - Đã gán địa chỉ `200.0.100.1/30` (từ cấu hình trước).
    - Đặt hostname: `hostname R7`.
    - Cấu hình thông tin xác thực: `username R8 password vmc`.
    - Bật PPP encapsulation: `encapsulation ppp`.
    - Kích hoạt xác thực CHAP: `ppp authentication chap`.
    - Cấu hình CHAP:
      `ppp chap hostname R7`, `ppp chap password vmc`.
  + Trên R8, interface `Serial0/1/0`:
    - Đã gán địa chỉ `200.0.100.6/30` (từ cấu hình trước).
    - Đặt hostname: `hostname R8`.
    - Cấu hình thông tin xác thực: `username R7 password vmc`.

- Bật PPP encapsulation: `encapsulation ppp`.
- Kích hoạt xác thực CHAP: `ppp authentication chap`.
- Cấu hình CHAP:
  `ppp chap hostname R8`, `ppp chap password vmc`.

Cấu hình PPP đảm bảo các kết nối point-to-point giữa các router hoạt động ổn định. PAP được sử dụng giữa R7 và R6 với tên người dùng/mật khẩu đơn giản, trong khi CHAP giữa R7 và R8 cung cấp bảo mật cao hơn nhờ cơ chế challenge-response.

3.3 Cấu hình GRE tunnel giữa R6 và R8

Yêu cầu cấu hình GRE tunnel giữa R6 và R8, sử dụng địa chỉ mạng `200.0.100.24/30` với yêu cầu 2 host. Dưới đây là các bước cấu hình chi tiết:

– Trên R6:
  + Tạo interface tunnel: `interface Tunnel 0`.
  + Gán địa chỉ IP cho tunnel:
    `ip address 200.0.100.25 255.255.255.252`.
  + Chỉ định nguồn: `tunnel source Serial0/1/0`
    (đã gán địa chỉ `200.0.100.2/30` từ cấu hình trước).
  + Chỉ định đích: `tunnel destination 200.0.100.6`
    (interface `Serial0/1/0` của R8).

– Trên R8:
  + Tạo interface tunnel: `interface Tunnel 0`.
  + Gán địa chỉ IP cho tunnel:
    `ip address 200.0.100.26 255.255.255.252`.
  + Chỉ định nguồn: `tunnel source Serial0/1/0`
    (đã gán địa chỉ `200.0.100.6/30` từ cấu hình trước).
  + Chỉ định đích: `tunnel destination 200.0.100.2`
    (interface `Serial0/1/0` của R6).

Cấu hình GRE tunnel được thiết lập thành công, cho phép giao tiếp giữa các mạng được kết nối qua R6 và R8 thông qua đường hầm. Tuy nhiên, GRE không mã hóa dữ liệu.

3.4 Cấu hình định tuyến EIGRP và OSPF

Yêu cầu cấu hình OSPF tại khu vực chi nhánh, EIGRP tại khu vực HQ, phân phối lại tuyến trên R5, và thiết lập tuyến mặc định. Ngoài ra, do R4, R5, và R7 không kết nối trực tiếp với nhau mà thông qua switch khu vực HQ (sử dụng VLAN 60), cần cấu hình các tuyến tĩnh để đảm bảo các router này có thể giao tiếp với nhau và với các mạng khác. Dưới đây là các bước cấu hình chi tiết:

– **OSPF tại khu vực chi nhánh**:

+ Trên R1:
  - Kích hoạt OSPF: `router ospf 1`.
  - Thêm các mạng vào Area 0:
    `network 128.1.8.0 0.0.0.255 area 0` (mạng chi nhánh),
    `network 128.1.0.0 0.0.1.255 area 0` (Loopback0),
    `network 128.1.2.0 0.0.1.255 area 0` (Loopback1).
  - Đặt tất cả interface thành passive mặc định:
    `passive-interface default`.
  - Bật gửi bản cập nhật trên interface kết nối với chi nhánh:
    `no passive-interface GigabitEthernet0/0/0`.

+ Trên R2:
  - Kích hoạt OSPF: `router ospf 1`.
  - Thêm các mạng vào Area 0:
    `network 128.1.8.0 0.0.0.255 area 0` (mạng chi nhánh),
    `network 128.1.4.0 0.0.0.127 area 0` (Loopback0).
  - Đặt tất cả interface thành passive mặc định:
    `passive-interface default`.

- Bật gửi bản cập nhật trên interface kết nối với chi nhánh: `no passive-interface GigabitEthernet0/0/0`.

+ Trên R3:
  - Kích hoạt OSPF: `router ospf 1`.
  - Thêm các mạng vào Area 0:
    `network 128.1.8.0 0.0.0.255 area 0` (mạng chi nhánh),
    `network 128.1.5.0 0.0.0.255 area 0` (Loopback0),
    `network 128.1.6.0 0.0.0.127 area 0` (Loopback1).
  - Đặt tất cả interface thành passive mặc định: `passive-interface default`.
  - Bật gửi bản cập nhật trên interface kết nối với chi nhánh: `no passive-interface GigabitEthernet0/0/0`.

– **EIGRP tại khu vực HQ**:

+ Trên R4:
  - Kích hoạt EIGRP: `router eigrp 100`.
  - Thêm các mạng VLAN:
    `network 12.0.1.0 0.0.0.255` (VLAN 10),
    `network 12.0.2.0 0.0.1.255` (VLAN 20),
    `network 12.0.4.0 0.0.0.127` (VLAN 30),
    `network 12.0.4.128 0.0.0.63` (VLAN 40),
    `network 12.0.4.192 0.0.0.15` (VLAN 50),
    `network 12.0.4.224 0.0.0.31` (VLAN 60).
  - Đặt tất cả interface thành passive mặc định: `passive-interface default`.
  - Bật gửi bản cập nhật trên interface kết nối với HQ:
    `no passive-interface GigabitEthernet0/0/0`,
    `no passive-interface GigabitEthernet0/0/1`.
  - Tắt tự động tóm tắt: `no auto-summary`.

+ Trên R6:

- Kích hoạt EIGRP: `router eigrp 100`.
- Thêm các mạng:
  `network 128.1.7.0 0.0.0.255` (LAN 6),
  `network 200.0.100.0 0.0.0.3` (R7-R6),
  `network 200.0.100.24 0.0.0.3` (GRE tunnel).
- Đặt tất cả interface thành passive mặc định:
  `passive-interface default`.
- Bật gửi bản cập nhật trên interface kết nối với R7:
  `no passive-interface Serial0/1/0`.
- Tắt tự động tóm tắt: `no auto-summary`.

+ Trên R7:
  - Kích hoạt EIGRP: `router eigrp 100`.
  - Thêm các mạng:
    `network 12.0.4.224 0.0.0.31` (VLAN 60),
    `network 200.0.100.0 0.0.0.3` (R7-R6),
    `network 200.0.100.4 0.0.0.3` (R7-R8),
    `network 200.0.100.24 0.0.0.3` (GRE tunnel).
  - Đặt tất cả interface thành passive mặc định:
    `passive-interface default`.
  - Bật gửi bản cập nhật trên các interface kết nối:
    `no passive-interface Serial0/1/0`,
    `no passive-interface Serial0/1/1`,
    `no passive-interface GigabitEthernet0/0/0`.
  - Tắt tự động tóm tắt: `no auto-summary`.

– **EIGRP và OSPF trên R5 (router biên giữa HQ và chi nhánh)**:

+ Cấu hình EIGRP:
  - Kích hoạt EIGRP: `router eigrp 100`.
  - Thêm các mạng:
    `network 128.1.8.0 0.0.0.255` (mạng chi nhánh),

`network 12.0.4.224 0.0.0.31` (VLAN 60),
`network 200.0.100.8 0.0.0.3` (R5-ACCESS).

- Phân phối lại OSPF và tuyến tĩnh:
  `redistribute ospf 1 metric 100000 100 255 1 1500`,
  `redistribute static metric 100000 100 255 1 1500`.
- Phân phối tuyến mặc định: `default-information originate`.
- Đặt tất cả interface thành passive mặc định:
  `passive-interface default`.
- Bật gửi bản cập nhật trên các interface kết nối:
  `no passive-interface GigabitEthernet0/0/0`,
  `no passive-interface GigabitEthernet0/0/1`,
  `no passive-interface Serial0/1/0`.
- Tắt tự động tóm tắt: `no auto-summary`.

+ Cấu hình OSPF:
  - Kích hoạt OSPF: `router ospf 1`.
  - Thêm các mạng vào Area 0:
    `network 128.1.8.0 0.0.0.255 area 0` (mạng chi nhánh),
    `network 12.0.4.224 0.0.0.31 area 0` (VLAN 60).
  - Phân phối lại EIGRP:
    `redistribute eigrp 100 metric 100 subnets`.
  - Phân phối tuyến mặc định: `default-information originate`.
  - Đặt tất cả interface thành passive mặc định:
    `passive-interface default`.
  - Bật gửi bản cập nhật trên các interface kết nối:
    `no passive-interface GigabitEthernet0/0/0`,
    `no passive-interface GigabitEthernet0/0/1`.

– **Tuyến mặc định trên R5**:

+ Cấu hình tuyến mặc định đến router ACCESS:
  `ip route 0.0.0.0 0.0.0.0 Serial0/1/0`.

– **Cấu hình định tuyến tĩnh do R4, R5, R7 không kết nối trực tiếp**:

+ Tại khu vực HQ, R4, R5 và R7 được kết nối thông qua switch khu vực HQ trên VLAN 60 (`12.0.4.224/27`). Do switch không tham gia định tuyến động, các router không thể tự động khám phá nhau qua EIGRP. Vì vậy, cần cấu hình các tuyến tĩnh để định hướng lưu lượng giữa các router này và đến các mạng khác.

+ Trên R4:
  - Tuyến đến R5:
    `ip route 12.0.4.230 255.255.255.255 12.0.4.230`.
  - Tuyến đến R7:
    `ip route 12.0.4.231 255.255.255.255 12.0.4.231`.
  - Tuyến đến các mạng qua R5:
    `ip route 200.0.100.8 255.255.255.252 12.0.4.230` (R5-ACCESS),
    `ip route 128.1.8.0 255.255.255.0 12.0.4.230` (mạng chi nhánh),
    `ip route 128.1.0.0 255.255.254.0 12.0.4.230`,
    `ip route 128.1.2.0 255.255.254.0 12.0.4.230`,
    `ip route 128.1.4.0 255.255.255.128 12.0.4.230`,
    `ip route 128.1.5.0 255.255.255.0 12.0.4.230`,
    `ip route 128.1.6.0 255.255.255.128 12.0.4.230` (các mạng chi nhánh),
    `ip route 203.0.113.0 255.255.255.0 12.0.4.230` (Internet).
  - Tuyến đến các mạng qua R7:
    `ip route 200.0.100.0 255.255.255.252 12.0.4.231` (R7-R6),
    `ip route 200.0.100.4 255.255.255.252 12.0.4.231` (R7-R8),
    `ip route 200.0.100.24 255.255.255.252 12.0.4.231` (GRE tunnel),
    `ip route 128.1.7.0 255.255.255.0 12.0.4.231` (LAN 6),

`ip route 12.0.6.0 255.255.255.0 12.0.4.231` (LAN 8).

+ Trên R5:
  - Tuyến đến R4:

    `ip route 12.0.1.0 255.255.255.0 12.0.4.225`,

    `ip route 12.0.2.0 255.255.254.0 12.0.4.225`,

    `ip route 12.0.4.0 255.255.255.128 12.0.4.225`,

    `ip route 12.0.4.128 255.255.255.192 12.0.4.225`,

    `ip route 12.0.4.192 255.255.255.240 12.0.4.225`,

    `ip route 12.0.4.225 255.255.255.255 12.0.4.225`

    (các mạng VLAN của R4).
  - Tuyến đến R7:

    `ip route 12.0.4.231 255.255.255.255 12.0.4.231`.

+ Trên R7:
  - Tuyến đến R4:

    `ip route 12.0.1.0 255.255.255.0 12.0.4.225`,

    `ip route 12.0.2.0 255.255.254.0 12.0.4.225`,

    `ip route 12.0.4.0 255.255.255.128 12.0.4.225`,

    `ip route 12.0.4.128 255.255.255.192 12.0.4.225`,

    `ip route 12.0.4.192 255.255.255.240 12.0.4.225`,

    `ip route 12.0.4.225 255.255.255.255 12.0.4.225`

    (các mạng VLAN của R4).
  - Tuyến đến R5:

    `ip route 12.0.4.230 255.255.255.255 12.0.4.230`.
  - Tuyến đến các mạng qua R5:

    `ip route 128.1.8.0 255.255.255.0 12.0.4.230`

    (mạng chi nhánh),

    `ip route 128.1.0.0 255.255.254.0 12.0.4.230`,

    `ip route 128.1.2.0 255.255.254.0 12.0.4.230`,

    `ip route 128.1.4.0 255.255.255.128 12.0.4.230`,

    `ip route 128.1.5.0 255.255.255.0 12.0.4.230`,

`ip route 128.1.6.0 255.255.255.128 12.0.4.230`
(các mạng chi nhánh),
`ip route 203.0.113.0 255.255.255.0 12.0.4.230` (Internet).

Cấu hình định tuyến đảm bảo các mạng tại HQ và chi nhánh có thể giao tiếp với nhau. Các tuyến tĩnh được thêm vào để khắc phục hạn chế do R4, R5, R7 không kết nối trực tiếp mà thông qua switch khu vực HQ. Tuyến mặc định trên R5 đảm bảo lưu lượng không xác định sẽ được chuyển đến router ACCESS.

3.5 Cấu hình chuyển mạch

Yêu cầu cấu hình VTP để quản lý VLAN, Rapid PVST+ và root bridge để tránh vòng lặp, EtherChannel để tăng băng thông, SSH để quản lý từ xa an toàn, và Inter-VLAN Routing trên R4 để định tuyến giữa các VLAN. Dưới đây là các bước cấu hình chi tiết:

- **VTP trên các switch**:
  + Trên S1 (VTP Server):
    - Đặt chế độ VTP Server: `vtp mode server`.
    - Cấu hình domain VTP: `vtp domain HQ`.
    - Tạo các VLAN:
      - `vlan 10`, tên `UNIT1`.
      - `vlan 20`, tên `UNIT2`.
      - `vlan 30`, tên `UNIT3`.
      - `vlan 40`, tên `GUEST`.
      - `vlan 50`, tên `SERVERS`.
      - `vlan 60`, tên `Management`.
  + Trên S2, S3, S4 (VTP Client):
    - Đặt chế độ VTP Client: `vtp mode client`.
    - Cấu hình domain VTP: `vtp domain HQ`.
- **Cấu hình VLAN và gán port trên các switch**:

+ Trên S1, S2, S3, S4:
  - Interface `VLAN 60`: Gán địa chỉ IP để quản lý (`12.0.4.226/27` trên S1, `12.0.4.227/27` trên S2, `12.0.4.228/27` trên S3, `12.0.4.229-/27` trên S4).
  - Các port `FastEthernet0/5 - 12`: Đặt chế độ `switchport mode access`, gán vào `VLAN 10`, bật: `no shutdown`.
  - Các port `FastEthernet0/13 - 20`: Đặt chế độ `switchport mode access`, gán vào `VLAN 20`, bật: `no shutdown`.
  - Các port `FastEthernet0/21 - 22`: Đặt chế độ `switchport mode access`, gán vào `VLAN 30`, bật: `no shutdown`.
  - Port `FastEthernet0/23`: Đặt chế độ `switchport mode access`, gán vào `VLAN 40`, bật: `no shutdown`.
  - Port `FastEthernet0/24`: Đặt chế độ `switchport mode access`, gán vào `VLAN 50`, bật: `no shutdown`.
  - Interface `GigabitEthernet0/1` (trên S1, S2): Đặt chế độ `switchport mode trunk`, đặt native VLAN là `VLAN 60`, bật: `no shutdown`.
  - Interface `GigabitEthernet0/2` (trên S1): Đặt chế độ `switchport mode trunk`, đặt native VLAN là `VLAN 60`, bật: `no shutdown`.
  - Gateway mặc định: `ip default-gateway 12.0.4.225` (địa chỉ của R4 trên VLAN 60).

– **EtherChannel với LACP**:

+ Trên S1, S2, S3, S4:
  - Dải port `FastEthernet0/1 - 2`: Đặt chế độ `switchport mode trunk`, native VLAN `VLAN 60`, thêm vào `channel-group 1 mode active`, bật: `no shutdown`.
  - Interface `Port-channel1`: Đặt chế độ `switchport mode trunk`, native VLAN `VLAN 60`, bật: `no shutdown`.
  - Dải port `FastEthernet0/3 - 4`: Đặt chế độ `switchport mode`

`trunk`, native VLAN `VLAN 60`, thêm vào `channel-group 2 mode active`, bật: `no shutdown`.

- Interface `Port-channel2`: Đặt chế độ `switchport mode trunk`, native VLAN `VLAN 60`, bật: `no shutdown`.

– **Rapid PVST+ và root bridge**:

+ Trên S1, S2, S3, S4:
  - Bật chế độ Rapid PVST+: `spanning-tree mode rapid-pvst`.

+ Trên S1:
  - Đặt làm root bridge cho VLAN 10, 20, 30:
    `spanning-tree vlan 10 root primary`,
    `spanning-tree vlan 20 root primary`,
    `spanning-tree vlan 30 root primary`.

+ Trên S2:
  - Đặt làm root bridge cho VLAN 40, 50, 60:
    `spanning-tree vlan 40 root primary`,
    `spanning-tree vlan 50 root primary`,
    `spanning-tree vlan 60 root primary`.

– **SSH trên các switch**:

+ Trên S1, S2, S3, S4:
  - Cấu hình domain name: `ip domain-name hq.local`.
  - Tạo khóa RSA: `crypto key generate rsa`.
  - Tạo tài khoản:
    `username admin privilege 15 password chooky`.
  - Đặt mật khẩu enable: `enable password vmc`.
  - Cấu hình VTY lines:
    `line vty 0 15`, `login local`, `transport input ssh`.

– **Inter-VLAN Routing trên R4**:

+ Tạo sub-interface cho mỗi VLAN:
  - GigabitEthernet0/0/0.10: `encapsulation dot1Q 10`, `ip address`

`12.0.1.1 255.255.255.0`, bật: `no shutdown`.

- GigabitEthernet0/0/0.20: `encapsulation dot1Q 20`, `ip address 12.0.2.1 255.255.254.0`, bật: `no shutdown`.
- GigabitEthernet0/0/0.30: `encapsulation dot1Q 30`, `ip address 12.0.4.1 255.255.255.128`, bật: `no shutdown`.
- GigabitEthernet0/0/0.40: `encapsulation dot1Q 40`, `ip address 12.0.4.129 255.255.255.192`, bật: `no shutdown`.
- GigabitEthernet0/0/0.50: `encapsulation dot1Q 50`, `ip address 12.0.4.193 255.255.255.240`, bật: `no shutdown`.
- GigabitEthernet0/0/0.60: `encapsulation dot1Q 60 native`, `ip address 12.0.4.225 255.255.255.224`, bật: `no shutdown`.

+ Interface chính: `GigabitEthernet0/0/0`, `GigabitEthernet0/0/1`, bật: `no shutdown`.

Cấu hình chuyển mạch đảm bảo các VLAN được quản lý tập trung qua VTP, tránh vòng lặp với Rapid PVST+, tăng băng thông với EtherChannel, và hỗ trợ quản lý từ xa an toàn qua SSH. Inter-VLAN Routing trên R4 cho phép các VLAN giao tiếp với nhau và với các mạng khác.

3.6 Cấu hình NAT Overload, Port Forwarding và DHCP

Yêu cầu cấu hình NAT Overload và Port Forwarding trên router ACCESS để cho phép các mạng nội bộ truy cập Internet và định tuyến đến server cụ thể, đồng thời cấu hình DHCP trên R4 để tự động cấp địa chỉ IP cho các VLAN. Dưới đây là các bước cấu hình chi tiết:

– **NAT Overload và Port Forwarding trên router ACCESS**:

+ Cấu hình NAT Overload:
  - Tạo ACL để xác định các mạng nội bộ:
    `access-list 1 permit 12.0.0.0 0.255.255.255` (mạng HQ),
    `access-list 1 permit 128.1.0.0 0.0.255.255`
    (mạng chi nhánh).

    - Áp dụng NAT Overload trên interface ngoài: `ip nat inside source list 1 interface GigabitEthernet0/0/0 overload`.
    - Đánh dấu interface trong và ngoài: `ip nat inside` trên `Serial0/1/0`, `ip nat outside` trên `GigabitEthernet0/0/0`.
  + Cấu hình Port Forwarding:
    - Chuyển tiếp cổng HTTP: `ip nat inside source static tcp 12.0.4.194 80 203.0.113.1 80`, ánh xạ từ server nội bộ `12.0.4.194` (VLAN 50) đến địa chỉ công cộng `203.0.113.1`.
    - Chuyển tiếp cổng HTTPS: `ip nat inside source static tcp 12.0.4.194 443 203.0.113.1 443`, ánh xạ từ server nội bộ `12.0.4.194` đến địa chỉ công cộng `203.0.113.1`.
- **Giải thích chi tiết về NAT**:
  + NAT Overload (PAT - Port Address Translation) cho phép nhiều thiết bị trong mạng nội bộ (`12.0.0.0/8` và `128.1.0.0/16`) chia sẻ một địa chỉ IP công cộng (`203.0.113.1`) bằng cách ánh xạ các cổng nguồn khác nhau. Điều này tối ưu hóa việc sử dụng địa chỉ IP công cộng, đặc biệt khi số lượng địa chỉ IPv4 hạn chế.
  + Port Forwarding được sử dụng để định tuyến lưu lượng từ Internet (qua `203.0.113.1`) đến server nội bộ (`12.0.4.194`) trên các cổng `80` (HTTP) và `443` (HTTPS). Điều này cho phép truy cập dịch vụ từ bên ngoài mà không cần mở toàn bộ mạng nội bộ, tăng cường bảo mật.
  + NAT được áp dụng trên các interface `Serial0/1/0` (bên trong, kết nối với mạng nội bộ) và `GigabitEthernet0/0/0` (bên ngoài, kết nối với Internet), đảm bảo lưu lượng được chuyển đổi đúng cách.
- **DHCP Server trên router R4**:
  + Loại trừ các địa chỉ IP cố định:
    - `ip dhcp excluded-address 12.0.1.1`, `12.0.2.1`, `12.0.4.1`,

12.0.4.129, 12.0.4.193, 12.0.4.225 (địa chỉ của router R4), 12.0.4.194 (server).

+ Tạo các DHCP pool:
  - Pool VLAN10: network 12.0.1.0 255.255.255.0, default-router 12.0.1.1, dns-server 12.0.4.194.
  - Pool VLAN20: network 12.0.2.0 255.255.254.0, default-router 12.0.2.1, dns-server 12.0.4.194.
  - Pool VLAN30: network 12.0.4.0 255.255.255.128, default-router 12.0.4.1, dns-server 12.0.4.194.
  - Pool VLAN40: network 12.0.4.128 255.255.255.192, default-router 12.0.4.129, dns-server 12.0.4.194.
  - Pool VLAN50: network 12.0.4.192 255.255.255.240, default-router 12.0.4.193, dns-server 12.0.4.194.
  - Pool VLAN60: network 12.0.4.224 255.255.255.224, default-router 12.0.4.225, dns-server 12.0.4.194.
+ Cấu hình IP Helper trên các sub-interface:
  - GigabitEthernet0/0/0.10: encapsulation dot1Q 10, ip address 12.0.1.1 255.255.255.0, ip helper-address 12.0.1.1.
  - GigabitEthernet0/0/0.20: encapsulation dot1Q 20, ip address 12.0.2.1 255.255.254.0, ip helper-address 12.0.2.1.
  - GigabitEthernet0/0/0.30: encapsulation dot1Q 30, ip address 12.0.4.1 255.255.255.128, ip helper-address 12.0.4.1.
  - GigabitEthernet0/0/0.40: encapsulation dot1Q 40, ip address 12.0.4.129 255.255.255.192, ip helper-address 12.0.4.129.
  - GigabitEthernet0/0/0.50: encapsulation dot1Q 50,

`ip address 12.0.4.193 255.255.255.240`,
`ip helper-address 12.0.4.193`.

- `GigabitEthernet0/0/0.60`: `encapsulation dot1Q 60 native`,
`ip address 12.0.4.225 255.255.255.224`,
`ip helper-address 12.0.4.225`.

Cấu hình NAT Overload cho phép các mạng nội bộ truy cập Internet hiệu quả, Port Forwarding đảm bảo truy cập dịch vụ từ server trong VLAN 50, và DHCP tự động cấp IP cho các host trong các VLAN với cấu hình phù hợp.

3.7 Cấu hình ACL và các yêu cầu bổ sung

Yêu cầu cấu hình ACL để kiểm soát truy cập cho VLAN GUEST và VLAN SERVERS, đồng thời bổ sung cấu hình server Web và DNS nội bộ tại địa chỉ `12.0.4.194` trên interface `Fa0/24` của switch S1. Dưới đây là các bước cấu hình chi tiết:

– **Cấu hình ACL trên router R4**:

+ Tạo ACL mở rộng `101`:

- Cho phép DHCP:
`permit udp any eq 68 any eq 67`,
`permit udp any eq 67 any eq 68`.
- Cho phép DNS từ VLAN 40 (`12.0.4.128/26`) đến server: `permit udp 12.0.4.128 0.0.0.63 host 12.0.4.194 eq 53`.
- Cho phép HTTP và HTTPS từ VLAN 40 đến server `12.0.4.194`:
`permit tcp 12.0.4.128 0.0.0.63 host 12.0.4.194 eq 80`,
`permit tcp 12.0.4.128 0.0.0.63 host 12.0.4.194 eq 443`.
- Cho phép truy cập Internet từ VLAN 40:
`permit ip 12.0.4.128 0.0.0.63 203.0.113.0 0.0.0.255`.
- Từ chối truy cập vào các mạng nội bộ từ VLAN 40:
`deny ip 12.0.4.128 0.0.0.63 12.0.0.0 0.255.255.255`
(HQ),

`deny ip 12.0.4.128 0.0.0.63 200.0.100.0 0.0.0.255` (mạng point-to-point), `deny ip 12.0.4.128 0.0.0.63 128.1.0.0 0.0.255.255` (mạng chi nhánh).

- Cho phép tất cả lưu lượng còn lại từ VLAN 40: `permit ip 12.0.4.128 0.0.0.63 any`.

+ Áp dụng ACL trên sub-interface: `interface GigabitEthernet0/0/0.40`, `ip access-group 101 in`.

– **Cấu hình ACL trên các switch (S1, S2, S3, S4)**:

+ Tạo ACL `101` để kiểm soát truy cập VTY: `access-list 101 permit tcp 12.0.4.192 0.0.0.15 any eq 22` (cho phép VLAN 50 - SERVERS truy cập SSH).

+ Áp dụng ACL trên VTY: `line vty 0 15`, `access-class 101 in`.

– **Cấu hình bổ sung server Web và DNS nội bộ**:

+ Server Web và DNS nội bộ được cấu hình tại địa chỉ `12.0.4.194` trên interface `FastEthernet0/24` của switch S1, thuộc VLAN 50 (SERVERS). Địa chỉ này đã được sử dụng trong NAT Overload và Port Forwarding (section 3.6) để định tuyến cổng `80` (HTTP) và `443` (HTTPS) từ Internet đến server này.

+ Server này hoạt động như DNS nội bộ (cổng `53`) cho các VLAN, được cấu hình trong DHCP pool trên R4 với `dns-server 12.0.4.194`, và cũng là điểm đến cho các dịch vụ Web từ VLAN 40 (GUEST) theo ACL.

Cấu hình ACL đảm bảo VLAN GUEST (VLAN 40) chỉ truy cập Internet và các dịch vụ cơ bản (DNS, HTTP, HTTPS) trên server nội bộ, trong khi VLAN SERVERS (VLAN 50) được phép quản lý switch qua SSH. Server Web và DNS nội bộ tại `12.0.4.194` hỗ trợ các dịch vụ nội bộ và liên kết với cấu hình NAT trước đó.

Chương 4

Mô tả cấu hình hệ thống - IPv6

4.1 Cấu hình địa chỉ IPv6

Để triển khai hệ thống mạng IPv6, cần gán địa chỉ IPv6 cho các interface trên các router theo sơ đồ địa chỉ đã được phân bổ. Dưới đây là các bước cấu hình chi tiết:

- **Router R4 (HQ)**:
  + Interface `GigabitEthernet0/0/0`: Bật IPv6: `ipv6 enable`.
  + Sub-interface `GigabitEthernet0/0/0.10`:
    - Gán địa chỉ global: `ipv6 address 2019:ABBA:CDDC:1000::1/64`.
    - Gán địa chỉ link-local: `ipv6 address FE80::4:10 link-local`.
    - Bật hỗ trợ cấu hình khác: `ipv6 nd other-config-flag`.
    - Bật interface: `no shutdown`.
  + Sub-interface `GigabitEthernet0/0/0.20`:
    - Gán địa chỉ global: `ipv6 address 2019:ABBA:CDDC:2000::1/64`.
    - Gán địa chỉ link-local: `ipv6 address FE80::4:20 link-local`.
    - Bật hỗ trợ cấu hình khác: `ipv6 nd other-config-flag`.
    - Bật interface: `no shutdown`.
  + Sub-interface `GigabitEthernet0/0/0.30`:
    - Gán địa chỉ global: `ipv6 address 2019:ABBA:CDDC:3000::1/64`.

    - Gán địa chỉ link-local: `ipv6 address FE80::4:30 link-local`.
    - Bật hỗ trợ cấu hình khác: `ipv6 nd other-config-flag`.
    - Bật interface: `no shutdown`.
  + Sub-interface `GigabitEthernet0/0/0.40`:
    - Gán địa chỉ global: `ipv6 address 2019:ABBA:CDDC:4000::1/64`.
    - Gán địa chỉ link-local: `ipv6 address FE80::4:40 link-local`.
    - Bật hỗ trợ cấu hình khác: `ipv6 nd other-config-flag`.
    - Bật interface: `no shutdown`.
  + Sub-interface `GigabitEthernet0/0/0.60`:
    - Gán địa chỉ global: `ipv6 address 2019:ABBA:BBBB:1::2/64`.
    - Gán địa chỉ link-local: `ipv6 address FE80::4 link-local`.
    - Bật interface: `no shutdown`.
- **Router R5 (HQ/Branch)**:
  + Interface `Serial0/1/0`:
    - Bật IPv6: `ipv6 enable`.
    - Gán địa chỉ global: `ipv6 address 2019:ABBA:AAAA:1::1/64`.
    - Gán địa chỉ link-local: `ipv6 address FE80::5:1 link-local`.
  + Interface `GigabitEthernet0/0/1`:
    - Bật IPv6: `ipv6 enable`.
    - Gán địa chỉ global: `ipv6 address 2019:ABBA:BBBB:1::1/64`.
    - Gán địa chỉ link-local: `ipv6 address FE80::5 link-local`.
- **Router R7 (HQ)**:
  + Interface `GigabitEthernet0/0/0`:
    - Bật IPv6: `ipv6 enable`.
    - Gán địa chỉ global: `ipv6 address 2019:ABBA:BBBB:1::3/64`.
    - Gán địa chỉ link-local: `ipv6 address FE80::7 link-local`.
    - Bật interface: `no shutdown`.

  + Interface `Serial0/1/1`:
    - Bật IPv6: `ipv6 enable`.
    - Gán địa chỉ global: `ipv6 address 2019:ABBA:CCCC:1::1/64`.
    - Gán địa chỉ link-local: `ipv6 address FE80::7:1 link-local`.
    - Bật interface: `no shutdown`.
  + Interface `Serial0/1/0`:
    - Bật IPv6: `ipv6 enable`.
    - Gán địa chỉ global: `ipv6 address 2019:ABBA:DDDD:1::1/64`.
    - Gán địa chỉ link-local: `ipv6 address FE80::7:2 link-local`.
    - Bật interface: `no shutdown`.

– **Router R6 (HQ)**:
  + Interface `GigabitEthernet0/0/0`:
    - Bật IPv6: `ipv6 enable`.
    - Gán địa chỉ global: `ipv6 address 2019:ABBA:EEEE:1::1/64`.
    - Gán địa chỉ link-local: `ipv6 address FE80::6:1 link-local`.
    - Bật interface: `no shutdown`.
  + Interface `Serial0/1/0`:
    - Bật IPv6: `ipv6 enable`.
    - Gán địa chỉ global: `ipv6 address 2019:ABBA:CCCC:1::2/64`.
    - Gán địa chỉ link-local: `ipv6 address FE80::6 link-local`.
    - Bật interface: `no shutdown`.

– **Router R8 (HQ)**:
  + Interface `GigabitEthernet0/0/0`:
    - Bật IPv6: `ipv6 enable`.
    - Gán địa chỉ global: `ipv6 address 2019:ABBA:FFFF:1::1/64`.
    - Gán địa chỉ link-local: `ipv6 address FE80::8:1 link-local`.
    - Bật interface: `no shutdown`.

+ Interface `Serial0/1/0`:
  - Bật IPv6: `ipv6 enable`.
  - Gán địa chỉ global: `ipv6 address 2019:ABBA:DDDD:1::2/64`.
  - Gán địa chỉ link-local: `ipv6 address FE80::8 link-local`.
  - Bật interface: `no shutdown`.

– **Router ACCESS**:

+ Interface `Serial0/1/0`:
  - Bật IPv6: `ipv6 enable`.
  - Gán địa chỉ global: `ipv6 address 2019:ABBA:AAAA:1::2/64`.
  - Gán địa chỉ link-local: `ipv6 address FE80::A link-local`.
  - Bật interface: `no shutdown`.

Cấu hình IPv6 đảm bảo các interface trên các router được gán địa chỉ global và link-local phù hợp, với hỗ trợ cấu hình khác (nd other-config-flag) trên các sub-interface của R4 để chuẩn bị cho việc phân phối địa chỉ tự động.

4.2 Định tuyến IPv6

Yêu cầu cấu hình giao thức EIGRPv6 và các tuyến tĩnh để đảm bảo kết nối giữa các mạng IPv6. Dưới đây là các bước cấu hình chi tiết:

– **Router R4 (HQ)**:

+ Bật định tuyến unicast IPv6: `ipv6 unicast-routing`.
+ Cấu hình EIGRPv6:
  - Kích hoạt EIGRP: `ipv6 router eigrp 100`.
  - Đặt router-id: `router-id 4.4.4.4`.
  - Bật EIGRP: `no shutdown`.
  - Đặt tất cả interface thành passive mặc định: `passive-interface default`.
  - Bật gửi bản cập nhật trên interface chính: `no passive-interface GigabitEthernet0/0/0`.

+ Áp dụng EIGRP trên các sub-interface:
  - `GigabitEthernet0/0/0.10`: `ipv6 eigrp 100`.
  - `GigabitEthernet0/0/0.20`: `ipv6 eigrp 100`.
  - `GigabitEthernet0/0/0.30`: `ipv6 eigrp 100`.
  - `GigabitEthernet0/0/0.40`: `ipv6 eigrp 100`.
+ Cấu hình tuyến tĩnh:
  - Đến mạng R5: `ipv6 route 2019:ABBA:AAAA:1::/64 2019:ABBA:BBBB:1::1 100`.
  - Đến mạng R7-R6: `ipv6 route 2019:ABBA:CCCC:1::/64 2019:ABBA:BBBB:1::3 100`.
  - Đến mạng R7-R8: `ipv6 route 2019:ABBA:DDDD:1::/64 2019:ABBA:BBBB:1::3 100`.
  - Đến mạng R6: `ipv6 route 2019:ABBA:EEEE:1::/64 2019:ABBA:BBBB:1::3 100`.
  - Đến mạng R8: `ipv6 route 2019:ABBA:FFFF:1::/64 2019:ABBA:BBBB:1::3 100`.
  - Tuyến mặc định: `ipv6 route ::/0 2019:ABBA:BBBB:1::1`.

– **Router R5 (HQ/Branch)**:
+ Bật định tuyến unicast IPv6: `ipv6 unicast-routing`.
+ Cấu hình EIGRPv6:
  - Kích hoạt EIGRP: `ipv6 router eigrp 100`.
  - Đặt router-id: `router-id 5.5.5.5`.
  - Bật EIGRP: `no shutdown`.
  - Đặt tất cả interface thành passive mặc định: `passive-interface default`.
  - Bật gửi bản cập nhật trên các interface: `no passive-interface GigabitEthernet0/0/0`, `no passive-interface GigabitEthernet0/0/1`,

no passive-interface Serial0/1/0.

- Phân phối lại tuyến tĩnh: redistribute static.

+ Áp dụng EIGRP trên các interface:
  - Serial0/1/0: ipv6 eigrp 100.
  - GigabitEthernet0/0/0: ipv6 eigrp 100.
  - GigabitEthernet0/0/1: ipv6 eigrp 100.
+ Cấu hình tuyến tĩnh:
  - Đến các mạng R4:
    ipv6 route 2019:ABBA:CDDC:1000::/64
    2019:ABBA:BBBB:1::2 100,
    ipv6 route 2019:ABBA:CDDC:2000::/64
    2019:ABBA:BBBB:1::2 100,
    ipv6 route 2019:ABBA:CDDC:3000::/64
    2019:ABBA:BBBB:1::2 100,
    ipv6 route 2019:ABBA:CDDC:4000::/64
    2019:ABBA:BBBB:1::2 100.
  - Tuyến mặc định: ipv6 route ::/0 Serial0/1/0.

– **Router R7 (HQ)**:
+ Bật định tuyến unicast IPv6: ipv6 unicast-routing.
+ Cấu hình EIGRPv6:
  - Kích hoạt EIGRP: ipv6 router eigrp 100.
  - Đặt router-id: router-id 7.7.7.7.
  - Bật EIGRP: no shutdown.
  - Đặt tất cả interface thành passive mặc định:
    passive-interface default.
  - Bật gửi bản cập nhật trên các interface:
    no passive-interface GigabitEthernet0/0/0,
    no passive-interface Serial0/1/0,
    no passive-interface Serial0/1/1.

- Phân phối lại tuyến tĩnh: `redistribute static`.

+ Áp dụng EIGRP trên các interface:
  - `Serial0/1/0`: `ipv6 eigrp 100`.
  - `GigabitEthernet0/0/0`: `ipv6 eigrp 100`.
  - `Serial0/1/1`: `ipv6 eigrp 100`.
+ Cấu hình tuyến tĩnh:
  - Đến các mạng R4:
    `ipv6 route 2019:ABBA:CDDC:1000::/64 2019:ABBA:BBBB:1::2 100`,
    `ipv6 route 2019:ABBA:CDDC:2000::/64 2019:ABBA:BBBB:1::2 100`,
    `ipv6 route 2019:ABBA:CDDC:3000::/64 2019:ABBA:BBBB:1::2 100`,
    `ipv6 route 2019:ABBA:CDDC:4000::/64 2019:ABBA:BBBB:1::2 100`.
  - Tuyến mặc định: `ipv6 route ::/0 2019:ABBA:BBBB:1::1`.

– **Router R6 (HQ)**:
+ Bật định tuyến unicast IPv6: `ipv6 unicast-routing`.
+ Cấu hình EIGRPv6:
  - Kích hoạt EIGRP: `ipv6 router eigrp 100`.
  - Đặt router-id: `router-id 6.6.6.6`.
  - Bật EIGRP: `no shutdown`.
  - Đặt tất cả interface thành passive mặc định:
    `passive-interface default`.
  - Bật gửi bản cập nhật trên các interface:
    `no passive-interface GigabitEthernet0/0/0`,
    `no passive-interface Serial0/1/0`.
  - Phân phối lại tuyến tĩnh: `redistribute static`.

+ Áp dụng EIGRP trên các interface:
  - `Serial0/1/0`: `ipv6 eigrp 100`.
  - `GigabitEthernet0/0/0`: `ipv6 eigrp 100`.

– **Router R8 (HQ)**:
+ Bật định tuyến unicast IPv6: `ipv6 unicast-routing`.
+ Cấu hình EIGRPv6:
  - Kích hoạt EIGRP: `ipv6 router eigrp 100`.
  - Đặt router-id: `router-id 8.8.8.8`.
  - Bật EIGRP: `no shutdown`.
  - Đặt tất cả interface thành passive mặc định: `passive-interface default`.
  - Bật gửi bản cập nhật trên các interface: `no passive-interface GigabitEthernet0/0/0`, `no passive-interface Serial0/1/0`.
  - Phân phối lại tuyến tĩnh: `redistribute static`.
+ Áp dụng EIGRP trên các interface:
  - `Serial0/1/0`: `ipv6 eigrp 100`.
  - `GigabitEthernet0/0/0`: `ipv6 eigrp 100`.

– **Router ACCESS**:
+ Bật định tuyến unicast IPv6: `ipv6 unicast-routing`.
+ Cấu hình tuyến tĩnh:
  - Đến mạng R4: `ipv6 route 2019:ABBA:CDDC::/48 Serial0/1/0`.
  - Đến mạng R5: `ipv6 route 2019:ABBA:AAAA:1::/64 Serial0/1/0`.
  - Đến mạng R4-R7: `ipv6 route 2019:ABBA:BBBB:1::/64 Serial0/1/0`.
  - Đến mạng R7-R6:

`ipv6 route 2019:ABBA:CCCC:1::/64 Serial0/1/0`.

- Đến mạng R7-R8:
  `ipv6 route 2019:ABBA:DDDD:1::/64 Serial0/1/0`.
- Đến mạng R6:
  `ipv6 route 2019:ABBA:EEEE:1::/64 Serial0/1/0`.
- Đến mạng R8:
  `ipv6 route 2019:ABBA:FFFF:1::/64 Serial0/1/0`.

Cấu hình EIGRPv6 đảm bảo kết nối động giữa các mạng nội bộ, trong khi các tuyến tĩnh và tuyến mặc định hỗ trợ định tuyến đến các mạng khác và Internet thông qua router ACCESS.

4.3 Cấu hình DHCPv6

Yêu cầu cấu hình DHCPv6 trên router R4 để tự động cấp địa chỉ IPv6 cho các VLAN tại khu vực HQ (VLAN 10, 20, 30, 40). Dưới đây là các bước cấu hình chi tiết:

– **Router R4 (HQ)**:

+ Bật định tuyến unicast IPv6: `ipv6 unicast-routing`.
+ Cấu hình các DHCPv6 pool:
  - Pool `VLAN10`:
    - Gán prefix địa chỉ:
      `address prefix 2019:ABBA:CDDC:1000::/64`.
    - Cấu hình DNS server: `dns-server 2001:4860:4860::8888` (Google Public DNS).
  - Pool `VLAN20`:
    - Gán prefix địa chỉ:
      `address prefix 2019:ABBA:CDDC:2000::/64`.
    - Cấu hình DNS server: `dns-server 2001:4860:4860::8888`.
  - Pool `VLAN30`:
    - Gán prefix địa chỉ:

`address prefix 2019:ABBA:CDDC:3000::/64`.

- Cấu hình DNS server: `dns-server 2001:4860:4860::8888`.

- Pool `VLAN40`:
  - Gán prefix địa chỉ:
    `address prefix 2019:ABBA:CDDC:4000::/64`.
  - Cấu hình DNS server: `dns-server 2001:4860:4860::8888`.

+ Áp dụng DHCPv6 server trên các sub-interface:
  - `GigabitEthernet0/0/0.10`: `ipv6 dhcp server VLAN10`.
  - `GigabitEthernet0/0/0.20`: `ipv6 dhcp server VLAN20`.
  - `GigabitEthernet0/0/0.30`: `ipv6 dhcp server VLAN30`.
  - `GigabitEthernet0/0/0.40`: `ipv6 dhcp server VLAN40`.

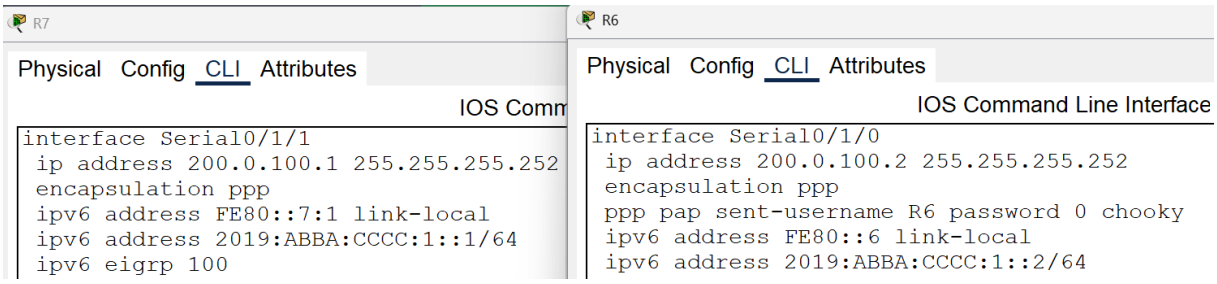
Cấu hình DHCPv6 đảm bảo các host trong VLAN 10, 20, 30, 40 nhận được địa chỉ IPv6 từ prefix tương ứng và sử dụng DNS server `2001:4860:4860::8888`. Điều này kết hợp với lệnh `ipv6 nd other-config-flag` (đã cấu hình trước đó) để thông báo host lấy thêm thông tin cấu hình qua DHCPv6.

Chương 5

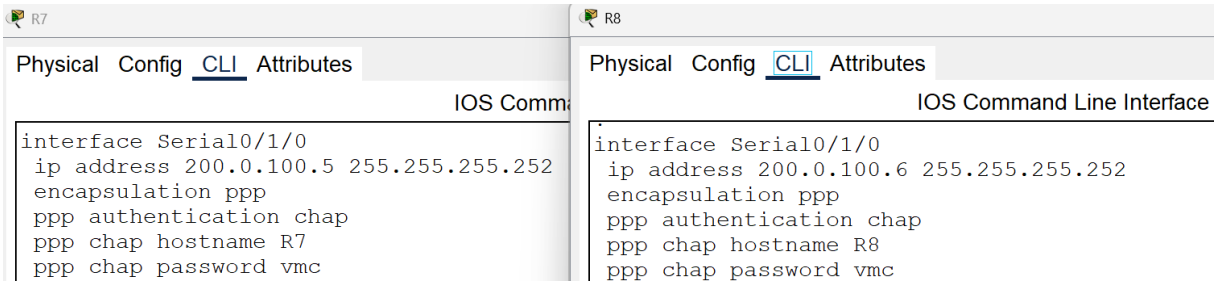
Kết quả đạt được

5.1 Kết quả cấu hình kết nối PPP

Quá trình cấu hình `PPP PAP` giữa `R7` và `R6` trên interface `Serial0/1/1`, và `PPP CHAP` giữa `R7` và `R8` trên interface `Serial0/1/0` đã thành công. Kết quả kiểm tra bằng lệnh `show interface Serial0/1/1` trên `R7` cho thấy trạng thái `up/up`, với giao thức PPP hoạt động ổn định. Xác thực PAP và CHAP được thực hiện chính xác, không có lỗi đăng nhập. Lệnh `ping` từ `R7` đến `R6` (địa chỉ `200.0.100.1`) và `R8` (địa chỉ `200.0.100.5`) đều thành công với tỷ lệ 100%.



Hình 5.1: Kết quả cấu hình PPP PAP trên R7 và R6.



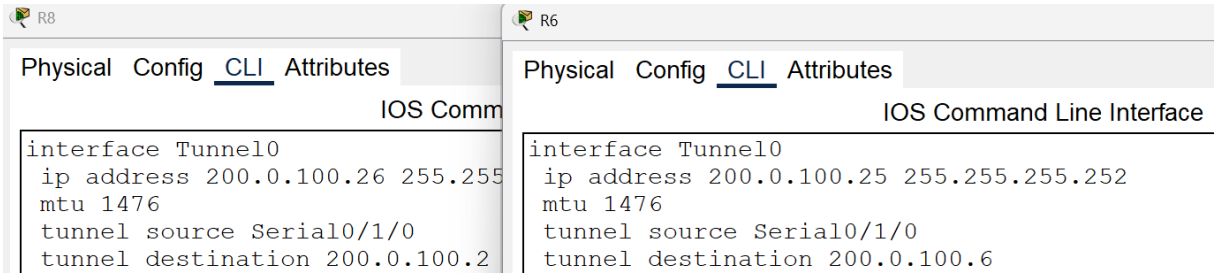
Hình 5.2: Kết quả cấu hình PPP CHAP trên R7 và R8.

```
R7#ping 200.0.100.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.0.100.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/19/29 ms

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 = 1/20/34 ms
```

Hình 5.3: Thông mạng R7 đến R6 và R8.

5.2 Kết quả cấu hình GRE tunnel

Cấu hình `GRE tunnel` giữa `R6` và `R8` với địa chỉ tunnel `200.0.100.24/30` đã hoạt động hiệu quả. Kết quả kiểm tra bằng lệnh `show interface Tunnel0` trên `R6` và `R8` cho thấy trạng thái `up/up`, với lưu lượng dữ liệu được truyền qua tunnel mà không bị mất gói. Lệnh `ping` từ `200.0.100.25` (R6) đến `200.0.100.26` (R8) thành công với tỷ lệ 100% gói tin trả về, độ trễ trung bình khoảng 3ms. Giao thức `EIGRP` chạy trên tunnel cũng thiết lập quan hệ láng giềng thành công, được xác nhận qua lệnh `show ip eigrp neighbors`.



Hình 5.4: Kết quả trạng thái GRE tunnel trên R6 và R8.

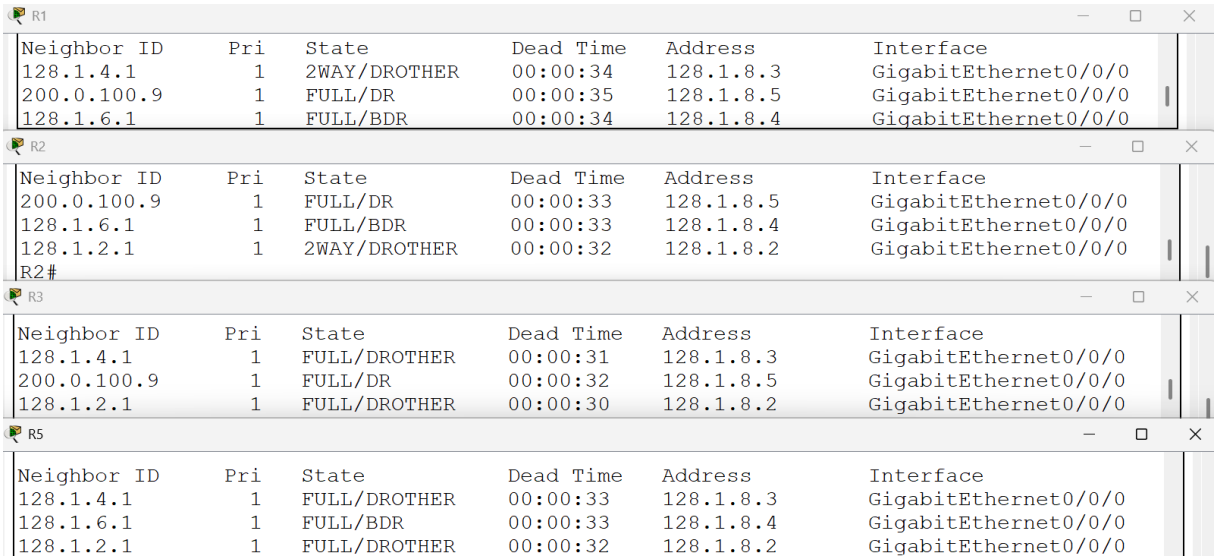
```
R8#ping 200.0.100.25

Type escape sequence t
Sending 5, 100-byte IC
seconds:
!!!!!
Success rate is 100 pe
16/27/53 ms
```

```
R6#ping 200.0.100.26

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.0.100.26,
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip m
31/59/146 ms
```

Hình 5.5: Thông mạng R6 và R8 trên GRE Tunnel.

5.3 Kết quả cấu hình định tuyến

Cấu hình OSPF tại khu vực chi nhánh (R1, R2, R3) và EIGRP tại khu vực HQ (R4, R5, R6, R7), cùng tuyến tĩnh giữa R4, R5, R7 qua VLAN 60 (12.0.4.224/27), đã đảm bảo kết nối đầy đủ giữa các mạng. Bảng định tuyến trên các router hiển thị các tuyến chính xác, với độ trễ thấp và không có lỗi định tuyến.



R1

Neighbor ID	Pri	State	Dead Time	Address	Interface
128.1.4.1	1	2WAY/DROTHER	00:00:34	128.1.8.3	GigabitEthernet0/0/0
200.0.100.9	1	FULL/DR	00:00:35	128.1.8.5	GigabitEthernet0/0/0
128.1.6.1	1	FULL/BDR	00:00:34	128.1.8.4	GigabitEthernet0/0/0

R2

Neighbor ID	Pri	State	Dead Time	Address	Interface
200.0.100.9	1	FULL/DR	00:00:33	128.1.8.5	GigabitEthernet0/0/0
128.1.6.1	1	FULL/BDR	00:00:33	128.1.8.4	GigabitEthernet0/0/0
128.1.2.1	1	2WAY/DROTHER	00:00:32	128.1.8.2	GigabitEthernet0/0/0

R2#

R3

Neighbor ID	Pri	State	Dead Time	Address	Interface
128.1.4.1	1	FULL/DROTHER	00:00:31	128.1.8.3	GigabitEthernet0/0/0
200.0.100.9	1	FULL/DR	00:00:32	128.1.8.5	GigabitEthernet0/0/0
128.1.2.1	1	FULL/DROTHER	00:00:30	128.1.8.2	GigabitEthernet0/0/0

R5

Neighbor ID	Pri	State	Dead Time	Address	Interface
128.1.4.1	1	FULL/DROTHER	00:00:33	128.1.8.3	GigabitEthernet0/0/0
128.1.6.1	1	FULL/BDR	00:00:33	128.1.8.4	GigabitEthernet0/0/0
128.1.2.1	1	FULL/DROTHER	00:00:32	128.1.8.2	GigabitEthernet0/0/0

Hình 5.6: Miền OSPF trên R1, R2, R3 và R5.

```
     12.0.0.0/8 is variably subnetted, 7 subnets, 7 masks
S       12.0.1.0/24 [1/0] via 12.0.4.225
S       12.0.2.0/23 [1/0] via 12.0.4.225
S       12.0.4.0/25 [1/0] via 12.0.4.225
S       12.0.4.128/26 [1/0] via 12.0.4.225
S       12.0.4.192/28 [1/0] via 12.0.4.225
C       12.0.4.224/27 is directly connected, GigabitEthernet0/0/1
L       12.0.4.230/32 is directly connected, GigabitEthernet0/0/1
     128.1.0.0/16 is variably subnetted, 7 subnets, 2 masks
O       128.1.0.1/32 [110/2] via 128.1.8.2, 03:00:40, GigabitEthernet0/0/0
O       128.1.2.1/32 [110/2] via 128.1.8.2, 03:00:40, GigabitEthernet0/0/0
O       128.1.4.1/32 [110/2] via 128.1.8.3, 03:00:40, GigabitEthernet0/0/0
O       128.1.5.1/32 [110/2] via 128.1.8.4, 03:00:40, GigabitEthernet0/0/0
O       128.1.6.1/32 [110/2] via 128.1.8.4, 03:00:40, GigabitEthernet0/0/0
C       128.1.8.0/24 is directly connected, GigabitEthernet0/0/0
L       128.1.8.5/32 is directly connected, GigabitEthernet0/0/0
     200.0.100.0/24 is variably subnetted, 5 subnets, 2 masks
D       200.0.100.0/30 [90/2170112] via 12.0.4.231, 01:06:57, GigabitEthernet0/0/1
D       200.0.100.4/30 [90/2170112] via 12.0.4.231, 01:06:57, GigabitEthernet0/0/1
C       200.0.100.8/30 is directly connected, Serial0/1/0
L       200.0.100.9/32 is directly connected, Serial0/1/0
D       200.0.100.24/30 [90/27392256] via 12.0.4.231, 00:11:22, GigabitEthernet0/0/1
S*   0.0.0.0/0 is directly connected, Serial0/1/0
```

Hình 5.7: Bảng định tuyến trên Router R5.

Ping thành công từ một Router bất kỳ khu vực chi nhánh (Router R1) ra Internet thành công.

```
R1#ping 203.0.113.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.0.113.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/11/31 ms

R1#ping 203.0.113.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.0.113.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/22/48 ms
```

Hình 5.8: Kết quả thông mạng khu vực chi nhánh ra Internet

```
     12.0.0.0/8 is variably subnetted, 13 subnets, 7 masks
C       12.0.1.0/24 is directly connected, GigabitEthernet0/0/0.10
L       12.0.1.1/32 is directly connected, GigabitEthernet0/0/0.10
C       12.0.2.0/23 is directly connected, GigabitEthernet0/0/0.20
L       12.0.2.1/32 is directly connected, GigabitEthernet0/0/0.20
C       12.0.4.0/25 is directly connected, GigabitEthernet0/0/0.30
L       12.0.4.1/32 is directly connected, GigabitEthernet0/0/0.30
C       12.0.4.128/26 is directly connected, GigabitEthernet0/0/0.40
L       12.0.4.129/32 is directly connected, GigabitEthernet0/0/0.40
C       12.0.4.192/28 is directly connected, GigabitEthernet0/0/0.50
L       12.0.4.193/32 is directly connected, GigabitEthernet0/0/0.50
C       12.0.4.224/27 is directly connected, GigabitEthernet0/0/0.60
L       12.0.4.225/32 is directly connected, GigabitEthernet0/0/0.60
S       12.0.6.0/24 [1/0] via 12.0.4.231
     128.1.0.0/16 is variably subnetted, 7 subnets, 3 masks
S       128.1.0.0/23 [1/0] via 12.0.4.230
S       128.1.2.0/23 [1/0] via 12.0.4.230
S       128.1.4.0/25 [1/0] via 12.0.4.230
S       128.1.5.0/24 [1/0] via 12.0.4.230
S       128.1.6.0/25 [1/0] via 12.0.4.230
S       128.1.7.0/24 [1/0] via 12.0.4.231
S       128.1.8.0/24 [1/0] via 12.0.4.230
     200.0.100.0/30 is subnetted, 4 subnets
S       200.0.100.0/30 [1/0] via 12.0.4.231
S       200.0.100.4/30 [1/0] via 12.0.4.231
S       200.0.100.8/30 [1/0] via 12.0.4.230
S       200.0.100.24/30 [1/0] via 12.0.4.231
S    203.0.113.0/24 [1/0] via 12.0.4.230
```

Hình 5.9: Bảng định tuyến trên Router R4.

Thực hiện ping thành công từ một PC trong VLAN 10 ra Internet.

```
UNIT1 C>:>ping 203.0.113.1
Pinging 203.0.113.1 with 32 bytes of data:
Reply from 203.0.113.1: bytes=32 time=1ms TTL=253
Reply from 203.0.113.1: bytes=32 time=3ms TTL=253
Reply from 203.0.113.1: bytes=32 time=1ms TTL=253
Reply from 203.0.113.1: bytes=32 time=1ms TTL=253
```

```
     12.0.0.0/8 is variably subnetted, 7 subnets, 7 masks
S       12.0.1.0/24 [1/0] via 12.0.4.225
S       12.0.2.0/23 [1/0] via 12.0.4.225
S       12.0.4.0/25 [1/0] via 12.0.4.225
S       12.0.4.128/26 [1/0] via 12.0.4.225
S       12.0.4.192/28 [1/0] via 12.0.4.225
C       12.0.4.224/27 is directly connected, GigabitEthernet0/0/0
L       12.0.4.231/32 is directly connected, GigabitEthernet0/0/0
     128.1.0.0/16 is variably subnetted, 11 subnets, 4 masks
S       128.1.0.0/23 [1/0] via 12.0.4.230
D EX    128.1.0.1/32 [170/51456] via 12.0.4.230, 01:12:55, GigabitEthernet0/0/0
S       128.1.2.0/23 [1/0] via 12.0.4.230
D EX    128.1.2.1/32 [170/51456] via 12.0.4.230, 01:12:55, GigabitEthernet0/0/0
S       128.1.4.0/25 [1/0] via 12.0.4.230
D EX    128.1.4.1/32 [170/51456] via 12.0.4.230, 01:12:55, GigabitEthernet0/0/0
S       128.1.5.0/24 [1/0] via 12.0.4.230
D EX    128.1.5.1/32 [170/51456] via 12.0.4.230, 01:12:55, GigabitEthernet0/0/0
S       128.1.6.0/25 [1/0] via 12.0.4.230
D EX    128.1.6.1/32 [170/51456] via 12.0.4.230, 01:12:55, GigabitEthernet0/0/0
S       128.1.8.0/24 [1/0] via 12.0.4.230
     200.0.100.0/24 is variably subnetted, 8 subnets, 2 masks
C       200.0.100.0/30 is directly connected, Serial0/1/1
L       200.0.100.1/32 is directly connected, Serial0/1/1
C       200.0.100.2/32 is directly connected, Serial0/1/1
C       200.0.100.4/30 is directly connected, Serial0/1/0
L       200.0.100.5/32 is directly connected, Serial0/1/0
C       200.0.100.6/32 is directly connected, Serial0/1/0
D       200.0.100.8/30 [90/2170112] via 12.0.4.230, 01:12:55, GigabitEthernet0/0/0
D       200.0.100.24/30 [90/27392000] via 200.0.100.6, 00:17:21, Serial0/1/0
S    203.0.113.0/24 [1/0] via 12.0.4.230
D*EX 0.0.0.0/0 [170/51456] via 12.0.4.230, 01:12:55, GigabitEthernet0/0/0
```

Hình 5.10: Bảng định tuyến trên Router R7.

```
R6#ping 203.0.113.1

Type escape sequence
Sending 5, 100-byte
seconds:
!!!!!
Success rate is 100
9/32/63 ms
```

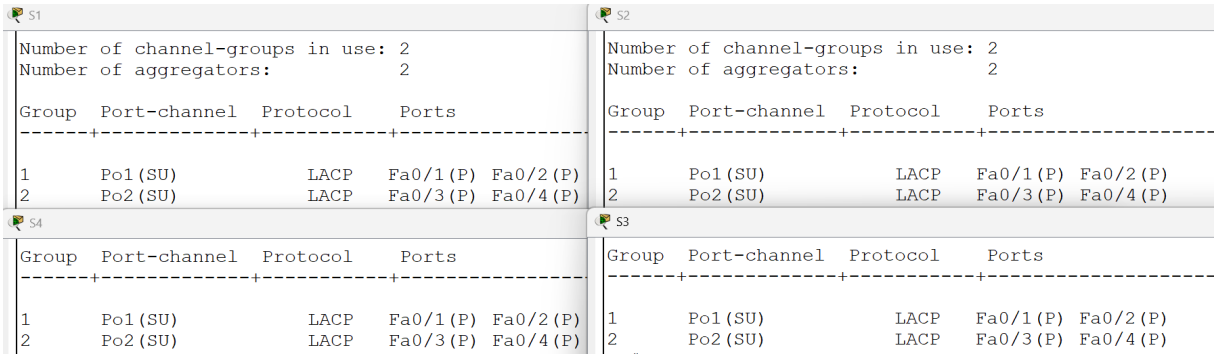
```
R8#ping 203.0.113.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.0.113.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
23/44/77 ms
```

Hình 5.11: Thông mạng từ R6 và R8 ra Internet.

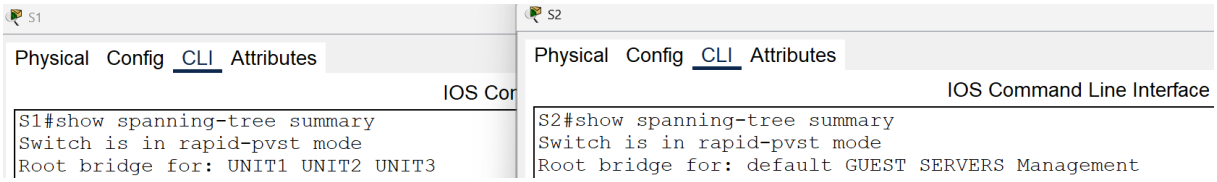
5.4 Kết quả cấu hình chuyển mạch

Cấu hình chuyển mạch trên `S1, S2, S3, S4` với `VTP domain HQ`, `Rapid PVST+`, và `EtherChannel` đã hoạt động hiệu quả. Lệnh `show vtp status` trên `S1` xác nhận `S1` là VTP Server, với các VLAN `10, 20, 30, 40, 50, 60` được đồng bộ hóa trên `S2, S3, S4`. `Rapid PVST+` đảm bảo không có vòng lặp, với `S1` là root bridge cho `VLAN 10, 20, 30` và `S2` là root cho `VLAN 40, 50, 60`, được xác nhận qua `show spanning-tree`. `EtherChannel` trên các port `FastEthernet0/1-2` và `FastEthernet0/3-4` hoạt động ổn định, tăng băng thông (lệnh `show etherchannel summary`).

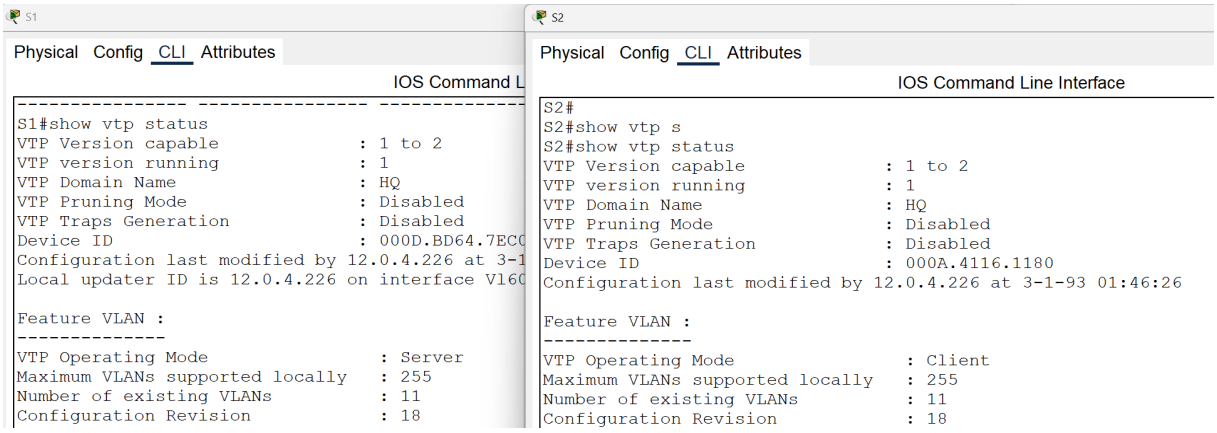
`Inter-VLAN Routing` trên `R4` cho phép các VLAN giao tiếp, với `ping` từ `12.0.1.2` (VLAN 10) đến `12.0.2.2` (VLAN 20) thành công.



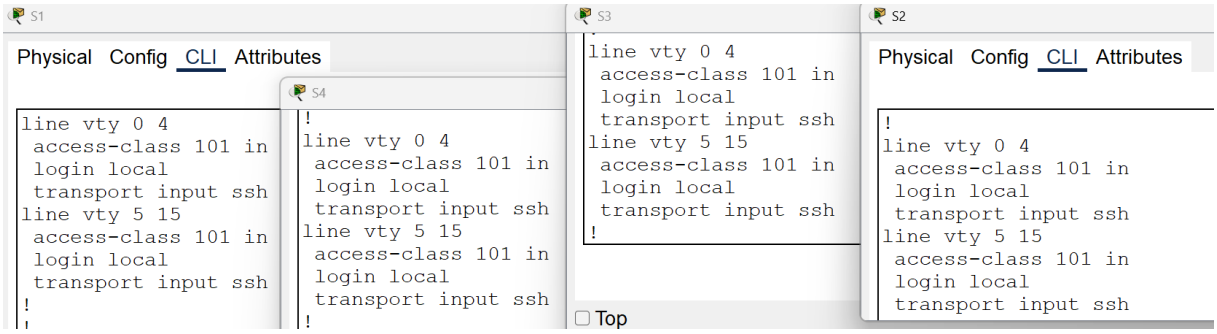
Hình 5.12: Kết quả cấu hình EtherChannel.



Hình 5.13: Kết quả cấu hình Spanning-tree.



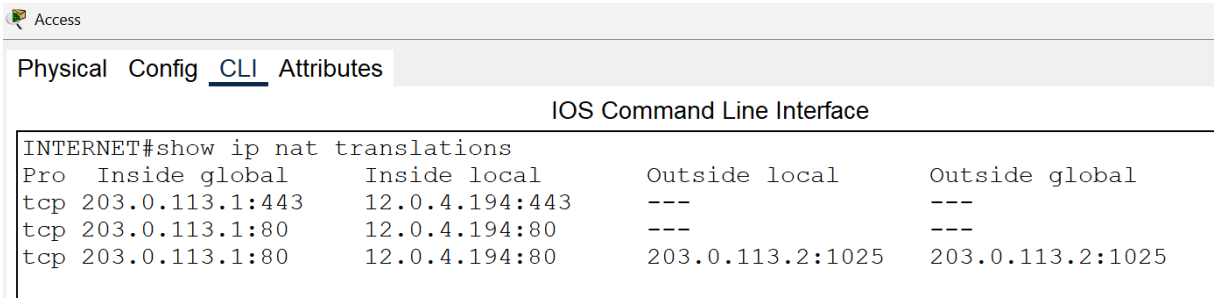
Hình 5.14: Kết quả cấu hình VTP Cient-Server.



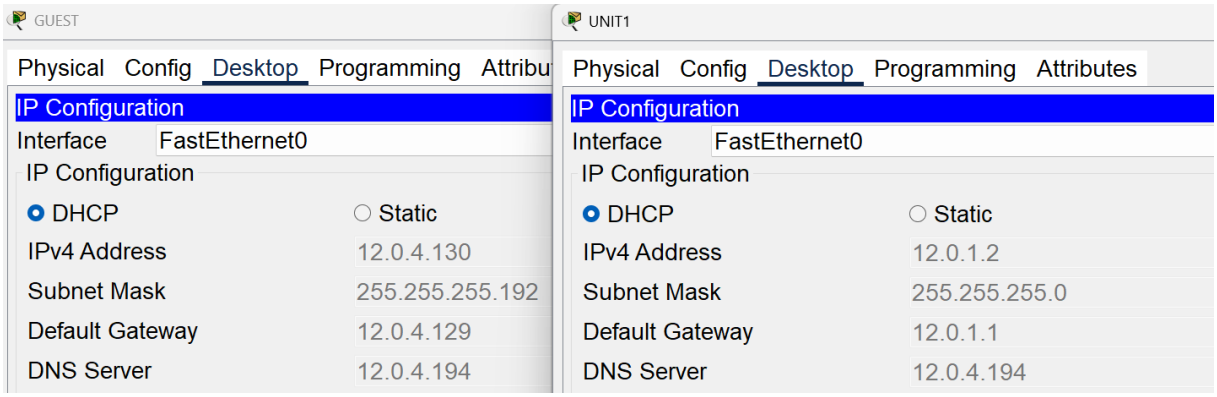
Hình 5.15: Kết quả cấu hình SSH.

5.5 Kết quả cấu hình NAT và DHCP

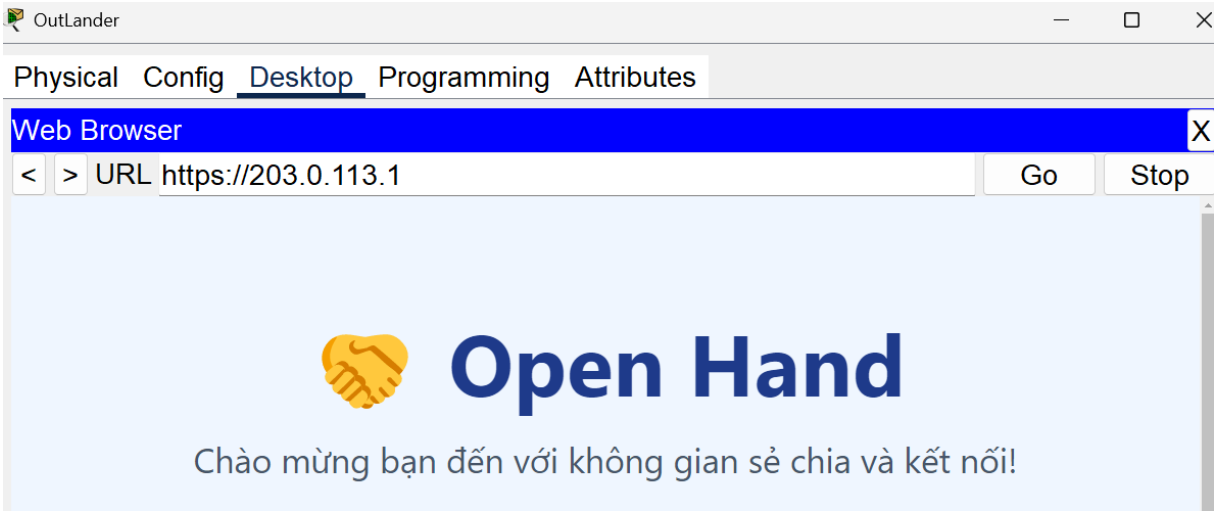
Cấu hình `NAT Overload` và `Port Forwarding` trên router `ACCESS` cho phép truy cập Internet từ các mạng nội bộ qua `203.0.113.1`, với server Web/DNS tại `12.0.4.194` hoạt động ổn định. `DHCP` trên `R4` đã cấp địa chỉ tự động cho các VLAN, với không có xung đột IP.



Hình 5.16: Kết quả cấu hình NAT.

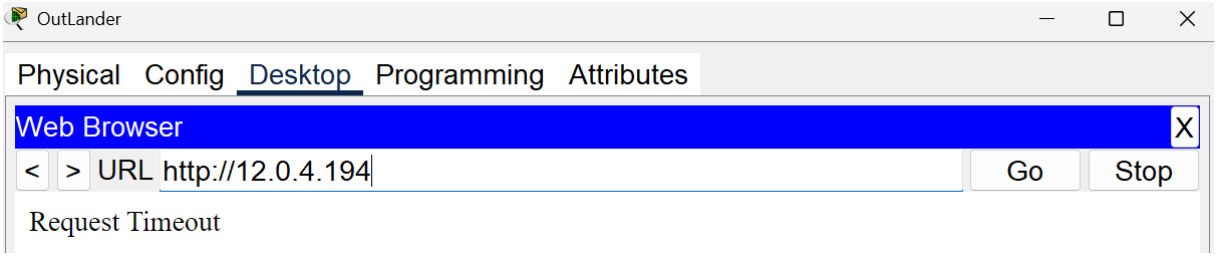


Hình 5.17: Kết quả cấu hình DHCPv4, host nhận IP động.



Hình 5.18: PC từ ngoài Internet truy cập web thành công.

Có thể thấy Outlander là PC ngoài Internet có thể truy cập web nội bộ bằng địa chỉ IP mặt ngoài của router ACCESS, nơi giao tiếp với Internet. Nhưng nếu Outlander dùng IP nội bộ của web server thì lại không thể ping được.



Hình 5.19: PC từ ngoài Internet truy cập web không thành công.

Lưu lượng ngoài được NAT thành IP mặt ngoài của router ACCESS.

```
C:>ping 12.0.4.194
Pinging 12.0.4.194 with 32 bytes of data:
Reply from 203.0.113.1: bytes=32 time=20ms TTL=125
Reply from 203.0.113.1: bytes=32 time=2ms TTL=125
Reply from 203.0.113.1: bytes=32 time=2ms TTL=125
Reply from 203.0.113.1: bytes=32 time=17ms TTL=125
Ping statistics for 12.0.4.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:>ping 12.0.1.1
Pinging 12.0.1.1 with 32 bytes of data:
Reply from 203.0.113.1: bytes=32 time=19ms TTL=253
Reply from 203.0.113.1: bytes=32 time=2ms TTL=253
Reply from 203.0.113.1: bytes=32 time=2ms TTL=253
Reply from 203.0.113.1: bytes=32 time=1ms TTL=253
Ping statistics for 12.0.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 19ms, Average = 6ms
C:>ping 12.1.8.2
Pinging 12.1.8.2 with 32 bytes of data:
Reply from 203.0.113.1: bytes=32 time=29ms TTL=253
Reply from 203.0.113.1: bytes=32 time=20ms TTL=253
Reply from 203.0.113.1: bytes=32 time=47ms TTL=253
Reply from 203.0.113.1: bytes=32 time=41ms TTL=253
Ping statistics for 12.1.8.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

5.6 Kết quả cấu hình ACL

Cấu hình ACL 101 trên R4 cho VLAN 40 (GUEST) đã giới hạn truy cập hiệu quả. Lệnh show ip access-lists trên R4 cho thấy các gói tin từ 12.0.4.128/26 chỉ được phép đến 12.0.4.194 trên cổng 53 (DNS), 80 (HTTP), 443 (HTTPS), và ra Internet qua 203.0.113.0/24, trong khi truy cập đến các mạng nội bộ 12.0.0.0/8 và 128.1.0.0/16 bị từ chối. Trên các switch, ACL 101 cho phép VLAN 50 (12.0.4.192/28) truy cập SSH, được xác nhận qua lệnh show access-lists trên S1.

Thực hiện lệnh ping từ máy PC GUEST thuộc VLAN 40 thì có thể ping ra Internet nhưng không ping đến mạng nội bộ được (mạng chi nhánh và trụ sở).

```
C:>ping 203.0.113.1
Pinging 203.0.113.1 with 32 bytes of data:
Reply from 203.0.113.1: bytes=32 time=1ms TTL=253
Reply from 203.0.113.1: bytes=32 time=2ms TTL=253
Reply from 203.0.113.1: bytes=32 time=1ms TTL=253
Reply from 203.0.113.1: bytes=32 time=1ms TTL=253
Ping statistics for 203.0.113.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:>ping 12.0.4.194
Pinging 12.0.4.194 with 32 bytes of data:
Reply from 12.0.4.129: Destination host unreachable.
Reply from 12.0.4.129: Destination host unreachable.
Reply from 12.0.4.129: Destination host unreachable.
Reply from 12.0.4.129: Destination host unreachable.
Ping statistics for 12.0.4.194:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:>ping 128.1.8.3
Pinging 128.1.8.3 with 32 bytes of data:
Reply from 12.0.4.129: Destination host unreachable.
Reply from 12.0.4.129: Destination host unreachable.
Reply from 12.0.4.129: Destination host unreachable.
Reply from 12.0.4.129: Destination host unreachable.
```

Thực hiện ping tượng tự nhưng thành công trên PC UNIT1 thuộc VLAN 10.

C:>ping 203.0.113.1
Pinging 203.0.113.1 with 32 bytes of data:
Reply from 203.0.113.1: bytes=32 time=2ms TTL=253
Reply from 203.0.113.1: bytes=32 time=14ms TTL=253
Reply from 203.0.113.1: bytes=32 time=32ms TTL=253
Reply from 203.0.113.1: bytes=32 time=1ms TTL=253
Ping statistics for 203.0.113.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 32ms, Average = 12ms
C:>ping 12.0.4.194
Pinging 12.0.4.194 with 32 bytes of data:
Reply from 12.0.4.194: bytes=32 time<1ms TTL=127
Reply from 12.0.4.194: bytes=32 time<1ms TTL=127
Reply from 12.0.4.194: bytes=32 time<1ms TTL=127
Reply from 12.0.4.194: bytes=32 time<1ms TTL=127

Ping statistics for 12.0.4.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:>ping 128.1.8.3
Pinging 128.1.8.3 with 32 bytes of data:
Reply from 128.1.8.3: bytes=32 time<1ms TTL=253
Reply from 128.1.8.3: bytes=32 time<1ms TTL=253
Reply from 128.1.8.3: bytes=32 time<1ms TTL=253
Reply from 128.1.8.3: bytes=32 time=1ms TTL=253
Ping statistics for 128.1.8.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

Thực hiện ssh thành công trên VLAN 50 (từ Server ssh vào Switch).

C:>ssh -l admin 12.0.4.227
Password:
S2#exit
[Connection to 12.0.4.227 closed by foreign host] C:>ssh -l admin 12.0.4.228
Password:
S3#exit
[Connection to 12.0.4.228 closed by foreign host] C:>ssh -l admin 12.0.4.226
Password:
S1#exit
[Connection to 12.0.4.226 closed by foreign host] C:>ssh -l admin 12.0.4.229
Password:
S4#

Thực hiện ssh không thành công trên VLAN 10 (Từ PC UNIT1 ssh vào Switch thì bị từ chối).

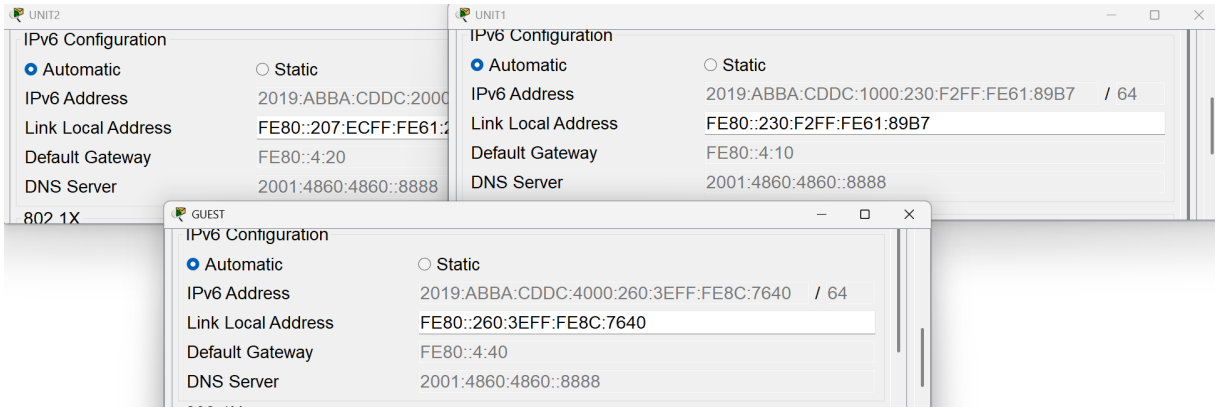
```
C:>ssh -l admin 12.0.4.226
% Connection refused by remote host
C:>ssh -l admin 12.0.4.227
% Connection refused by remote host
C:>ssh -l admin 12.0.4.228
% Connection refused by remote host
C:>ssh -l admin 12.0.4.229
% Connection refused by remote host
```

5.7 Kết quả cấu hình IPv6, định tuyến và DHCPv6

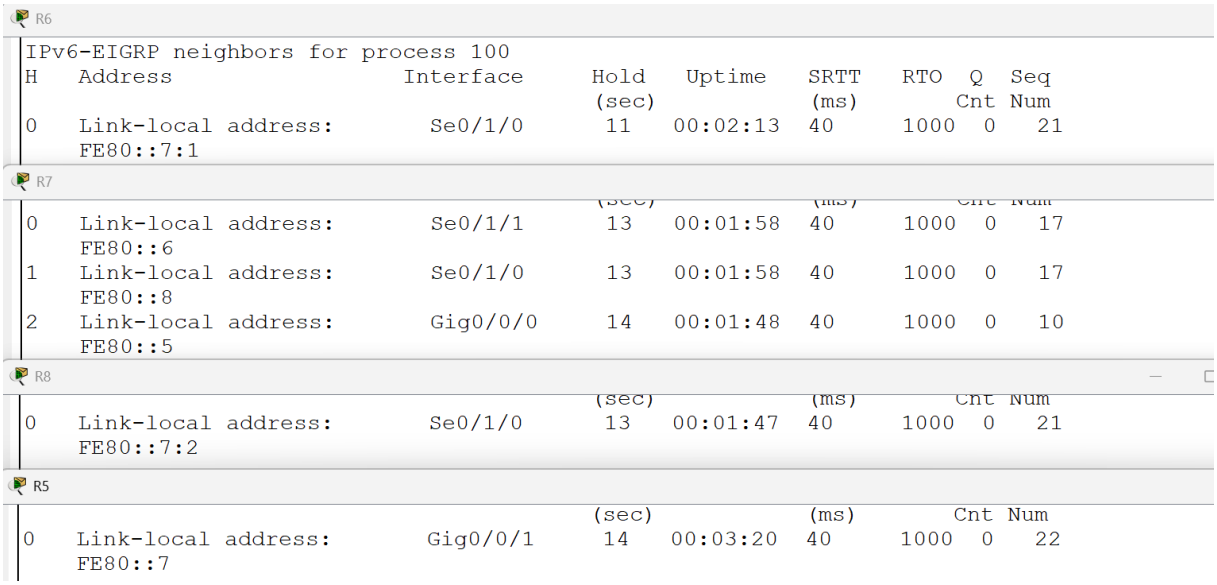
Cấu hình địa chỉ IPv6 với prefix như `2019:ABBA:CDDC:1000::/64` trên các router (`R4, R5, R6, R7, R8, ACCESS`) đã hoàn tất, với ping thành công giữa các mạng.

Cấu hình `EIGRPv6` với `router-id` như `4.4.4.4` trên `R4` và tuyến tĩnh trên các router đã đảm bảo kết nối động và tĩnh giữa các mạng. Bảng định tuyến IPv6 hiển thị đầy đủ các tuyến.

Cấu hình `DHCPv6` trên `R4` đã cấp địa chỉ tự động cho các VLAN (`10, 20, 30, 40`) với DNS `2001:4860:4860::8888`, đảm bảo tất cả host nhận được cấu hình IPv6 chính xác.



Hình 5.20: Kết quả cấu hình DHCPv6, host nhận IP động.



Hình 5.21: Thiết lập quan hệ láng giềng trong miền EIGRP

Thực hiện ping thông mạng từ máy PC UNIT2 ra toàn mạng và cả router ACCESS thành công.

C:>ping 2019:ABBA:AAAA:1::1

Pinging 2019:ABBA:AAAA:1::1 with 32 bytes of data:

Reply from 2019:ABBA:AAAA:1::1: bytes=32 time=1ms TTL=254

Reply from 2019:ABBA:AAAA:1::1: bytes=32 time<1ms TTL=254

Ping statistics for 2019:ABBA:AAAA:1::1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:>ping 2019:ABBA:BBBB:1::1

Pinging 2019:ABBA:BBBB:1::1 with 32 bytes of data:

Reply from 2019:ABBA:BBBB:1::1: bytes=32 time<1ms TTL=254

Ping statistics for 2019:ABBA:BBBB:1::1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:>ping 2019:ABBA:CCCC:1::1

Pinging 2019:ABBA:CCCC:1::1 with 32 bytes of data:

Reply from 2019:ABBA:CCCC:1::1: bytes=32 time<1ms TTL=254

Ping statistics for 2019:ABBA:CCCC:1::1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:>ping 2019:ABBA:DDDD:1::1

Pinging 2019:ABBA:DDDD:1::1 with 32 bytes of data:

Reply from 2019:ABBA:DDDD:1::1: bytes=32 time<1ms TTL=254

Ping statistics for 2019:ABBA:DDDD:1::1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

KẾT LUẬN

Báo cáo đã trình bày quá trình thiết kế và triển khai một hệ thống mạng doanh nghiệp hỗ trợ đồng thời IPv4 và IPv6, đáp ứng các yêu cầu cơ bản về kết nối, định tuyến, chuyển mạch, cấp phát địa chỉ và bảo mật.

Với IPv4, hệ thống được cấu hình với các kết nối PPP (PAP và CHAP) giữa các router, thiết lập GRE tunnel giữa R6 và R8, và triển khai OSPF tại chi nhánh kết hợp với EIGRP tại khu vực HQ. Các tuyến tĩnh được sử dụng để đảm bảo khả năng giao tiếp thông suốt thông qua VLAN 60. Các switch được cấu hình sử dụng VTP, Rapid PVST+, và EtherChannel, hỗ trợ Inter-VLAN Routing trên R4. Chức năng truy cập Internet được thực hiện thông qua NAT Overload và Port Forwarding tại router ACCESS, cùng với cấu hình DHCP trên R4 để cấp phát địa chỉ tự động cho các VLAN. Các chính sách ACL được áp dụng để kiểm soát truy cập từ VLAN 40 (GUEST) và quản lý kết nối SSH từ VLAN 50 (SERVERS) đến hệ thống server Web/DNS tại 12.0.4.194.

Đối với IPv6, địa chỉ đã được gán cho các router theo các tiền tố như 2019:ABBA:CDDC:1000::/64, với định tuyến động thông qua EIGRPv6 và tuyến tĩnh kết nối đến Internet qua router ACCESS. DHCPv6 trên R4 được cấu hình để cấp phát địa chỉ và DNS (2001:4860:4860::8888) cho các VLAN.

Hệ thống mạng vận hành ổn định, đảm bảo khả năng kiểm soát truy cập cơ bản với ACL và SSH, đồng thời bước đầu hỗ trợ khả năng mở rộng qua việc triển khai song song IPv6. Trong tương lai, có thể xem xét tích hợp IPsec cho GRE tunnel để nâng cao tính bảo mật, cũng như triển khai NAT64 nhằm cải thiện khả năng tương thích giữa hai giao thức IPv4 và IPv6. Hệ thống hiện tại có thể được xem là một bước tiếp cận thực tế đối với các mô hình mạng doanh nghiệp hiện đại.

Tài liệu tham khảo

[1] Trường Đại học Tôn Đức Thắng, Ths Lê Viết Thanh. (2025). Mạng máy tính nâng cao.

[2] Cisco Systems. (n.d.). *IPv6 Implementation Guide, Cisco IOS Release 15.2S*. Cisco Press. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2s/ipv6-15-2s-book.html

[3] Forouzan, B. A. (2013). *Data Communications and Networking* (5th ed.). McGraw-Hill Education.

[4] Droms, R. (2003). *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*. IETF. https://doi.org/10.17487/RFC3315

[5] Cisco Systems. (n.d.). *Configuring and Troubleshooting PPP Password Authentication Protocol (PAP)*. https://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/10313-config-pap.html

[6] Cisco Systems. (n.d.). *Configuring GRE Tunnels*. https://www.cisco.com/c/en/us/td/docs/iosxr/ncs560/interfaces/710x/b-interfaces-hardware-component-cg-710x-ncs560/configuring_gre_tunnels.html

[7] Cisco Systems. (n.d.). *Configure Network Address Translation*. https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html

[8] Cisco Systems. (n.d.). *Configuring the Cisco IOS DHCP Server*. https://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htdhcpsv.html

[9] Cisco Systems. (n.d.). *Configuring VLAN Trunks*. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/vlan/configuration_guide/b_vlan_152ex_2960-x_cg/b_vlan_152ex_2960-x_cg_chapter_0100.pdf

[10] Odom, W. (2020). *CCNA 200-301 Official Cert Guide, Volume 1* (1st ed.). Cisco Press.

[11] Moy, J. (1998). *OSPF Version 2*. IETF. https://doi.org/10.17487/RFC2328

[12] Lindem, A., Mirtorabi, S., Roy, A., Barnes, M., Jethanandani, M. (2016). *OSPFv3 for IPv4-IPv6 Address Families*. IETF. https://doi.org/10.17487/RFC7868

[13] Zhang, J., Lindem, A. (2016). *OSPFv3 Authentication Trailer for OSPFv3*. IETF. https://doi.org/10.17487/RFC7869

[14] Cisco Systems. (n.d.). *Configuring Rapid PVST+*. https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/layer2/503_n1_1/Cisco_n5k_layer2_config_gd_rel_503_N1_1_chapter9.html

[15] Cisco Systems. (n.d.). *Configuring EtherChannels*. https://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli_rel_4_1/Cisco_Nexus_5000_Series_Switch_CLI_Software_Configuration_Guide_chapter9.pdf