TRƯỜNG ĐẠI HỌC TRÀ VINH

TRƯỜNG KỸ THUẬT VÀ CÔNG NGHỆ

ISO 9001:2015

TRANG THÀNH HIẾU

XÂY DỰNG MÔ HÌNH MẠNG WAN VỚI BẢO MẬT VÀ TỐI ƯU HIỆU SUẤT

KHOÁ LUẬN TỐT NGHIỆP

NGÀNH CÔNG NGHỆ THÔNG TIN

VĨNH LONG, NĂM 2025

TRƯỜNG ĐẠI HỌC TRÀ VINH
TRƯỜNG KỸ THUẬT VÀ CÔNG NGHỆ

XÂY DỰNG MÔ HÌNH MẠNG WAN VỚI BẢO MẬT VÀ TỐI ƯU HIỆU SUẤT

KHOÁ LUẬN TỐT NGHIỆP
NGÀNH CÔNG NGHỆ THÔNG TIN

Sinh viên thực hiện: TRANG THÀNH HIẾU
Lớp**:** DA21TTB
Mã số sinh viên: 110121023
Giảng viên hướng dẫn : ThS. HUỲNH VĂN THANH

VĨNH LONG, NĂM 2025

LỜI CAM ĐOAN

Tôi xin cam đoan đề tài "Xây dựng mô hình mạng WAN với bảo mật và tối ưu hiệu suất" là kết quả nghiên cứu và thực hiện của chính bản thân tôi dưới sự hướng dẫn của Thầy ThS. Huỳnh Văn Thanh. Tất cả các nội dung lý thuyết, mô hình, sơ đồ, bảng số liệu và kết quả mô phỏng trong báo cáo này đều được tôi trực tiếp nghiên cứu, triển khai, cấu hình và kiểm chứng. Những nội dung được trích dẫn, tham khảo từ công trình nghiên cứu, bài báo, tài liệu hoặc nguồn khác đều đã được ghi rõ nguồn gốc theo đúng quy định.

Tôi xin hoàn toàn chịu trách nhiệm về nội dung cam đoan trên.

Sinh viên thực hiện

(Ký và ghi rõ họ tên)

Trang Thành Hiếu

LỜI CẢM ƠN

Đầu tiên, tôi xin bày tỏ lòng biết ơn sâu sắc đến thầy ThS. Huỳnh Văn Thanh, giảng viên Khoa Công nghệ Thông tin, Trường Kỹ thuật và Công nghệ thuộc Trường Đại học Trà Vinh, người đã tận tình hướng dẫn, dành thời gian quý báu để định hướng và luôn đồng hành cùng tôi trong suốt quá trình thực hiện đồ án tốt nghiệp. Nhờ sự hỗ trợ và hướng dẫn tận tâm của thầy, tôi đã có cơ hội hiểu sâu hơn về kiến thức chuyên môn, để giúp tôi hoàn thành đề tài này một cách tốt nhất.

Tôi cũng xin gửi lời cảm ơn chân thành đến Ban Giám hiệu Trường Đại học Trà Vinh cùng quý thầy, cô Trường Kỹ thuật và Công nghệ đã tạo mọi điều kiện thuận lợi về cơ sở vật chất, tài liệu học tập và cung cấp một môi trường nghiên cứu tốt nhất.

Quá trình thực hiện đồ án là một chặng đường đầy thử thách nhưng cũng vô cùng ý nghĩa. Tôi đã nỗ lực không ngừng để hoàn thành các nhiệm vụ với mong muốn đạt được kết quả tốt nhất. Tuy nhiên, do kinh nghiệm và kiến thức của bản thân còn hạn chế, tôi nhận thấy đồ án của mình vẫn còn một số điểm thiếu sót. Tôi rất mong nhận được những ý kiến đóng góp chân thành từ quý thầy, cô để tôi có thể hoàn thiện hơn nữa cả về nội dung lẫn phương pháp làm việc trong tương lai.

Cuối cùng, tôi kính chúc quý thầy cô dồi dào sức khỏe, luôn thành công trong công việc và đạt được nhiều thành tựu đáng tự hào trong sự nghiệp giáo dục. Một lần nữa, tôi xin chân thành cảm ơn!

Sinh viên thực hiện

(Ký và ghi rõ họ tên)

Trang Thành Hiếu

NHẬN XÉT

(Của giảng viên hướng dẫn trong đồ án, khoá luận của sinh viên)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Giảng viên hướng dẫn

(ký và ghi rõ họ tên)

UBND TỈNH TRÀ VINH
TRƯỜNG ĐẠI HỌC TRÀ VINH

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh Phúc

BẢN NHẬN XÉT ĐỒ ÁN, KHÓA LUẬN TỐT NGHIỆP

(Của giảng viên hướng dẫn)

Họ và tên sinh viên: .....MSSV: .....

Ngành: .....Khóa: .....

Tên đề tài:.....

.....

.....

Họ và tên Giáo viên hướng dẫn: .....

Chức danh: .....Học vị: .....

NHẬN XÉT

1. Nội dung đề tài:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

2. Ưu điểm:

.....

.....

.....

.....

3. Khuyết điểm:

.....

.....

.....

.....

.....

4. Điểm mới đề tài:

.....

.....

.....

.....

.....

5. Giá trị thực trên đề tài:

.....

.....

.....

.....

.....

.....

.....

7. Đề nghị sửa chữa bổ sung:

.....

.....

.....

.....

.....

.....

.....

8. Đánh giá:

.....

.....

.....

.....

Trà Vinh, ngày tháng 8 năm 2025

Giảng viên hướng dẫn

(Ký & ghi rõ họ tên)

NHẬN XÉT

(Của giảng viên chấm trong đồ án, khoá luận của sinh viên)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Giảng viên chấm

(ký và ghi rõ họ tên)

UBND TỈNH TRÀ VINH **CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM**

TRƯỜNG ĐẠI HỌC TRÀ VINH **Độc lập - Tự do - Hạnh phúc**

BẢN NHẬN XÉT ĐỒ ÁN, KHÓA LUẬN TỐT NGHIỆP

(Của cán bộ chấm đồ án, khóa luận)

Họ và tên người nhận xét: .....

Chức danh: ..... Học vị: .....

Chuyên ngành: .....

Cơ quan công tác: .....

Tên sinh viên: .....

Tên đề tài đồ án, khóa luận tốt nghiệp: .....

.....

.....

I. Ý KIẾN NHẬN XÉT

1. Nội dung:

.....

.....

.....

.....

.....

.....

.....

.....

.....

2. Điểm mới các kết quả của đồ án, khóa luận:

.....

.....

.....

3. Ứng dụng thực tế:

.....

.....

.....

.....

.....

.....

.....

II. CÁC VẤN ĐỀ CẦN LÀM RÕ

(Các câu hỏi của giáo viên phản biện)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

III. KẾT LUẬN

(Ghi rõ đồng ý hay không đồng ý cho bảo vệ đồ án khóa luận tốt nghiệp)

.....

.....

.....

.....

.....

Trà Vinh, ngày …… tháng 8 năm 2025

Người nhận xét

(Ký & ghi rõ họ tên)

MỤC LỤC

DANH MỤC CÁC BẢNG, SƠ ĐỒ, HÌNH ẢNH

KÍ HIỆU CÁC CỤM TỪ VIẾT TẮT

STT	Kí hiệu viết tắt	Nội dung viết tắt
1	WAN	Wide Area Network
2	LAN	Local Area Network
3	VLAN	Virtual Local Area Network
4	OSPF	Open Shortest Path Firs
5	STP	Spanning Tree Protocol
6	GRE Tunnel	Generic Routing Encapsulation

CHƯƠNG 1. TỔNG QUAN

1.1. Mục tiêu của đề tài

Thiết kế và mô phỏng một hệ thống mạng WAN kết nối nhiều nhánh với nhau.

Ứng dụng các kỹ thuật như VLAN, định tuyến tĩnh và động, STP, GRE Tunnel, và Load Balancing để đảm bảo:

- Tối ưu hiệu suất mạng.

- Tăng tính dự phòng và khả năng chịu lỗi.

- Đảm bảo tính bảo mật khi truyền dữ liệu qua Internet.

1.2. Phạm vi nghiên cứu

Đề tài "Xây dựng mô hình mạng WAN với bảo mật và tối ưu hóa hiệu suất" được thực hiện trong phạm vi mô phỏng, toàn bộ mô hình của đề tài được xây dựng và kiểm thử trên phần mềm Cisco Packet Tracer một công cụ mô phỏng phổ biến trong môi trường đào tạo, nhằm thể hiện cách thức thiết kế và triển khai một hệ thống mạng WAN cơ bản cho doanh nghiệp hoặc trường học. Về mặt kỹ thuật, đề tài tập trung vào việc triển khai các công nghệ thiết yếu trong môi trường mô phỏng Cisco Packet Tracer, bao gồm định tuyến tĩnh và định tuyến động , cấu hình VLAN để phân chia mạng con, thiết lập GRE Tunnel nhằm tạo kết nối bảo mật giữa các site. Ngoài ra, đề tài cũng chú trọng đến việc tối ưu hóa hiệu suất mạng thông qua kỹ thuật cân bằng tải.

1.3. Lý do chọn đề tài

Trong bối cảnh chuyển đổi số ngày càng mạnh mẽ, các doanh nghiệp và tổ chức không còn hoạt động giới hạn trong một khu vực địa lý cố định. Việc mở rộng quy mô, kết nối nhiều chi nhánh, văn phòng làm việc ở các tỉnh, thành phố hay thậm chí ở nhiều quốc gia đang là xu hướng tất yếu. Cùng với đó, nhu cầu xây dựng một hệ thống mạng có thể đảm bảo kết nối liên tục, truyền tải dữ liệu nhanh chóng, an toàn và dễ quản lý ngày càng trở nên quan trọng hơn bao giờ hết. Mạng WAN đóng vai trò như một cầu nối quan trọng giúp các mạng LAN tại các địa điểm khác nhau

có thể kết nối và giao tiếp với nhau như một hệ thống thống nhất. Không chỉ dừng lại ở việc kết nối, mạng WAN còn đặt ra nhiều thách thức như: độ trễ khi truyền tải dữ liệu, rủi ro bảo mật từ môi trường mạng công cộng, chi phí vận hành cao và khó kiểm soát hiệu suất nếu không có giải pháp thiết kế tối ưu.

Từ những lý do thực tiễn trên, lựa chọn đề tài "Xây dựng mô hình mạng WAN với bảo mật và tối ưu hóa hiệu suất" với mục tiêu nghiên cứu và triển khai mô hình mạng WAN mô phỏng trong môi trường học thuật, đồng thời tích hợp các công nghệ hiện đại nhằm tăng cường bảo mật, độ tin cậy, hiệu năng hoạt động cũng như đảm bảo tính mở rộng linh hoạt cho hệ thống mạng. Đề tài cũng là cơ hội để áp dụng những kiến thức đã học vào việc thiết kế một hệ thống mạng WAN có tính thực tiễn cao, sát với nhu cầu triển khai trong doanh nghiệp. Bên cạnh đó, tôi cũng mong muốn nâng cao kỹ năng về phân tích hệ thống mạng, cấu hình thiết bị mạng trong môi trường mô phỏng Cisco Packet Tracer và hiểu sâu hơn về cách thức vận hành của các kiến trúc mạng phức tạp.

1.4. Đối tượng nghiên cứu

Thiết bị mạng: đóng vai trò cốt lõi trong mô hình WAN. Bao gồm router dùng để định tuyến dữ liệu giữa các mạng khác nhau, switch để kết nối các thiết bị nội bộ trong từng chi nhánh, cùng với các máy tính cá nhân và máy chủ nhằm mô phỏng hoạt động người dùng và dịch vụ thực tế.

Công nghệ và giao thức mạng: được sử dụng để xây dựng và vận hành mạng WAN. Bao gồm định tuyến tĩnh và động nhằm đảm bảo việc truyền dữ liệu được hiệu quả, VLAN để phân chia mạng nội bộ thành các phân vùng logic, GRE Tunnel để mã hoá và kết nối an toàn giữa các site qua Internet, Load Balancing nhằm tối ưu hóa hiệu suất hoạt động của mạng.

Môi trường mô phỏng: sử dụng phần mềm Cisco Packet Tracer. Đây là công cụ hỗ trợ xây dựng hệ thống mạng ảo, cho phép kiểm thử các thiết bị, công nghệ và cấu hình mạng trong môi trường giả lập. Việc sử dụng Packet Tracer giúp sinh viên có điều kiện tiếp cận và vận dụng kiến thức một cách trực quan, đồng thời đảm bảo an toàn và linh hoạt trong quá trình thử nghiệm các tình huống mạng khác nhau.

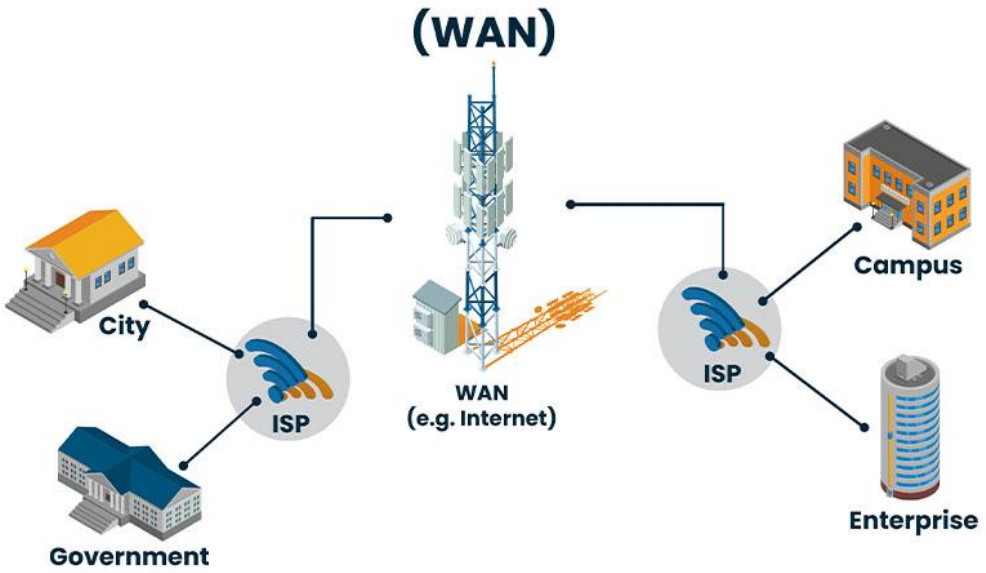
1.5. Phương pháp thực hiện

Phương pháp nghiên cứu lý thuyết: Tìm hiểu các kiến thức về mạng WAN, VLAN, STP, định tuyến, GRE Tunnel và Load balancing thông qua tài liệu học thuật, giáo trình, và tài liệu hướng dẫn của Cisco.

Phương pháp nghiên cứu thực nghiệm: Thiết kế và mô phỏng mô hình mạng trên phần mềm Cisco Packet Tracer. Thực hiện cấu hình, kiểm thử và đánh giá hiệu quả hoạt động của hệ thống mạng theo các yêu cầu đã đề ra.

CHƯƠNG 2. NGHIÊN CỨU LÝ THUYẾT

2.1. Tổng quan về mạng WAN



Hình 2.1 Mô hình mạng WAN

WAN (Wide Area Network) là loại mạng kết nối các máy tính và thiết bị từ xa, có khoảng cách kết nối lớn hơn so với mạng LAN. Nó cho phép truyền thông dữ liệu qua các kết nối định tuyến trên các khu vực địa lý khác nhau trên toàn cầu, thường là qua mạng công cộng hoặc dịch vụ viễn thông. Mục đích chính của mạng WAN là cho phép các tổ chức hoặc cá nhân truy cập vào tài nguyên trong mạng này một cách hiệu quả trên phạm vi toàn cầu, bất kể nơi họ đang kết nối trên thế giới. Các kết nối trong mạng WAN có thể sử dụng cáp đồng, cáp quang, hoặc kết nối không dây [1].

2.1.1 Công nghệ được sử dụng trong mạng WAN

2.1.1.1 MPLS (Multiprotocol Label Switching)

MPLS là một công nghệ định tuyến và chuyển tiếp dữ liệu trong mạng WAN. Cho phép các gói dữ liệu được gắn nhãn và chuyển tiếp theo các nhãn này thay vì địa chỉ IP. Điều này giúp tăng tốc độ truyền dữ liệu và cải thiện hiệu suất của mạng.

MPLS được sử dụng rộng rãi trong các doanh nghiệp và tổ chức lớn để kết nối các văn phòng và chi nhánh với nhau. Ngoài ra, còn là công nghệ được sử dụng trong mạng internet để kết nối các nhà cung cấp dịch vụ internet với nhau [1].

2.1.1.2 Frame Relay

Frame Relay là một công nghệ định tuyến và chuyển tiếp dữ liệu trong mạng WAN. Cho phép các gói dữ liệu được gửi trên các kênh ảo thay vì các đường dây vật lý, giúp giảm chi phí và tăng hiệu suất của mạng.

Frame Relay được sử dụng rộng rãi trong các doanh nghiệp và tổ chức lớn để kết nối các văn phòng và chi nhánh với nhau. Tuy nhiên, do công nghệ này đã lỗi thời, đang dần được thay thế bằng MPLS và các công nghệ mới hơn [1].

2.1.1.3 ATM (Asynchronous Transfer Mode)

ATM là một công nghệ định tuyến và chuyển tiếp dữ liệu trong mạng WAN. Cho phép các gói dữ liệu được chuyển tiếp theo các ô có kích thước cố định, giúp tăng tốc độ truyền dữ liệu và cải thiện hiệu suất của mạng.

ATM được sử dụng rộng rãi trong các doanh nghiệp và tổ chức lớn để kết nối các văn phòng và chi nhánh với nhau. Do chi phí cao và sự phát triển của các công nghệ mới hơn, ATM đang dần bị thay thế [1].

2.1.1.4 VPN (Virtual Private Network)

VPN là một công nghệ cho phép các thiết bị và mạng kết nối với nhau thông qua internet một cách an toàn và bảo mật. Cho phép các thiết bị trong mạng WAN có thể truy cập vào các tài nguyên và dữ liệu của nhau một cách dễ dàng và an toàn.

VPN được sử dụng rộng rãi trong các doanh nghiệp và tổ chức để kết nối các văn phòng và chi nhánh với nhau. Còn được sử dụng để cho phép nhân viên làm việc từ xa có thể truy cập vào mạng nội bộ của công ty một cách an toàn [1].

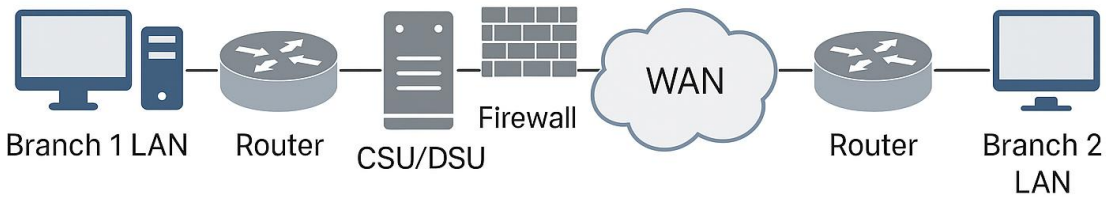
2.1.2 So sánh giữa mạng LAN và WAN

Bảng 2.1 So sánh mạng LAN và WAN

Tiêu Chí	***Mạng LAN***	***Mạng WAN***
Phạm vi	Rộng lớn, kết nối giữa các thành phố, quốc gia	Nhỏ, trong một tòa nhà hoặc khu vực

Chi phí	Cao, thuê đường truyền WAN, chi phí thiết bị & bảo trì cao	Thấp, thiết bị rẻ, không cần thuê đường truyền
Tốc độ truyền	Thấp hơn LAN (phụ thuộc vào nhà cung cấp dịch vụ và loại kết nối)	Cao (thường từ 100 Mbps đến 10 Gbps hoặc hơn)
Tính linh hoạt	Thấp hơn do phụ thuộc vào nhà cung cấp và cấu trúc liên vùng phức tạp	Cao trong nội bộ, dễ cấu hình và mở rộng
Mức độ bảo mật	Dễ bị tấn công hơn, cần các giải pháp bảo mật như VPN, mã hóa, firewall	Tốt hơn do kiểm soát nội bộ
Bảo trì & quản lý	Khó khăn, thường cần nhân sự chuyên trách và phối hợp với ISP	Dễ dàng, do quản lý nội bộ

2.1.3 Cách thức hoạt động của mạng WAN



Hình 2.2 Cách thức hoạt động mạng WAN

Mạng WAN hoạt động bằng cách kết nối nhiều mạng LAN ở nhiều vị trí địa lý khác nhau thông qua các đường truyền công cộng hoặc riêng lẻ như Internet, đường thuê hoặc mạng 4G/5G. Tại mỗi địa điểm Router sẽ đảm nhận việc định tuyến dữ liệu ra khỏi mạng LAN nội bộ. Dữ liệu này sau đó được gửi qua các thiết bị trung gian như modem, CSU/DSU hoặc thiết bị chuyển mạch WAN, rồi qua đường truyền WAN đến điểm đích.

Khi dữ liệu truyền qua WAN, nó sẽ có thể đi qua nhiều Router và thiết bị định tuyến trung gian để tìm đường tối ưu. Để đảm bảo tính bảo mật, dữ liệu có thể được mã hóa bằng VPN hoặc được bảo vệ bởi Firewall. Nếu có nhiều đường truyền, Load balancer sẽ phân phối lưu lượng đều để tối ưu hiệu suất và tránh nghẽn mạng.

Cuối cùng, khi dữ liệu đến điểm đích, router tại đó sẽ tiếp nhận và chuyển tiếp đến máy đích trong mạng LAN nội bộ tương ứng.

2.1.4 Ưu & nhược điểm của mạng WAN

2.1.4.1 Ưu điểm

Có khả năng bao phủ trong một khu vực có địa lý rộng lớn, mở rộng ra nhiều vị trí, cho phép người dùng kết nối mạng từ xa, không bị giới hạn tín hiệu.

Giúp truyền tải lượng lớn dữ liệu cùng một lúc giữa các thiết bị mạng trong hệ thống với tốc độ tương đối ổn định.

Có thể kết nối nhiều loại thiết bị đầu cuối từ máy tính bàn, laptop đến điện thoại di động, máy tính bảng,…

Sử dụng cơ sở hạ tầng kết nối của bên thứ ba, do vậy dễ dàng mở rộng phạm vi hoặc thay đổi lựa chọn kết nối nếu muốn.

Kết nối các mạng LAN nhỏ với nhau, chứa và chia sẻ phần mềm, tài nguyên lớn.

Hỗ trợ chia sẻ nhiều loại dữ liệu, tệp tin với nhau có tính bảo mật cao.

2.1.4.2 Nhược điểm

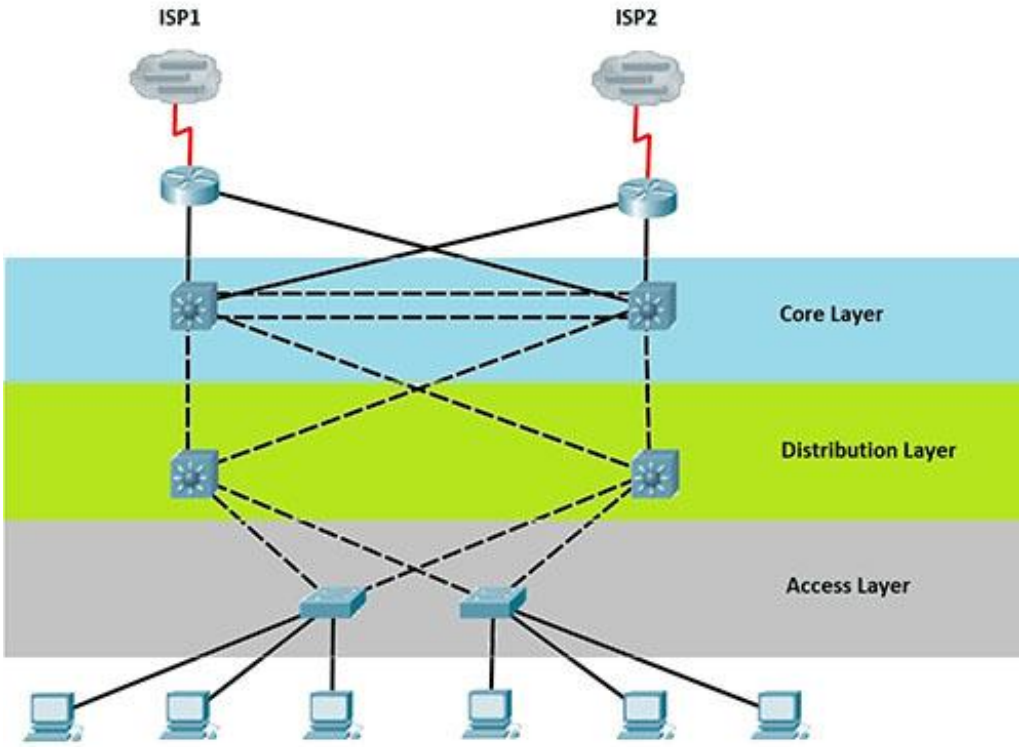
Chi phí lắp đặt và vận hành của mạng WAN khá lớn, đặc biệt là chi phí đầu tư ban đầu.

Quản lý hệ thống mạng WAN phức tạp hơn nhiều so với mạng LAN hay các mạng quy mô nhỏ khác, do vậy cần kỹ thuật viên hoặc người quản trị có chuyên môn giỏi, nhiều kinh nghiệm.

Khi xảy ra sự cố thường cần thời gian xử lý lâu hơn do hệ thống mạng và phương thức truyền tải phức tạp.

Dễ bị tấn công lấy cắp dữ liệu do sử dụng cơ sở hạ tầng mạng chung của bên thứ ba, đòi hỏi phải có cơ chế bảo mật riêng.

2.2. Mô hình mạng 3 lớp của Cisco



Hình 2.3Mô hình mạng 3 lớp của Cisco

2.2.1 Lớp truy cập (Access layer)

Lớp truy cập cho phép người dùng cuối kết nối với mạng Ethernet có dây với khả năng chia sẻ dữ liệu và tài nguyên trên mạng cục bộ. Mục đích của Access Layer là kiểm soát quyền truy cập của người dùng vào các tài nguyên trên mạng. Các thiết bị mạng được sử dụng trong lớp này là Switch và Hub. Ngày nay thiết bị Hub được sử dụng rất ít và sử dụng bộ chuyển mạch cụ thể là dùng Access Switch [2].

2.2.2 Lớp phân phối (Distribution Layer)

Lớp phân phối là lớp nằm ở giữa lớp lõi và lớp truy cập. Chức năng chính của lớp này là định tuyến dữ liệu, lọc và kiểm soát các gói tin có thể truy cập vào Core Layer. Lớp này thường bao gồm các thiết bị như bộ định tuyến router và switch nhiều lớp.

2.2.3 Lớp lõi (Core Layer)

Lớp lõi đóng vai trò như xương sống của mạng và chịu trách nhiệm vận chuyển lượng lớn lưu lượng truy cập 1 cách nhanh chóng. Lớp lõi cung cấp khả năng kết nối giữa các thiết bị trong lớp phân phối. Chúng thường là các thiết bị có tốc độ cao như bộ định tuyến router cao cấp hoặc Core Switch với các liên kết dự phòng.

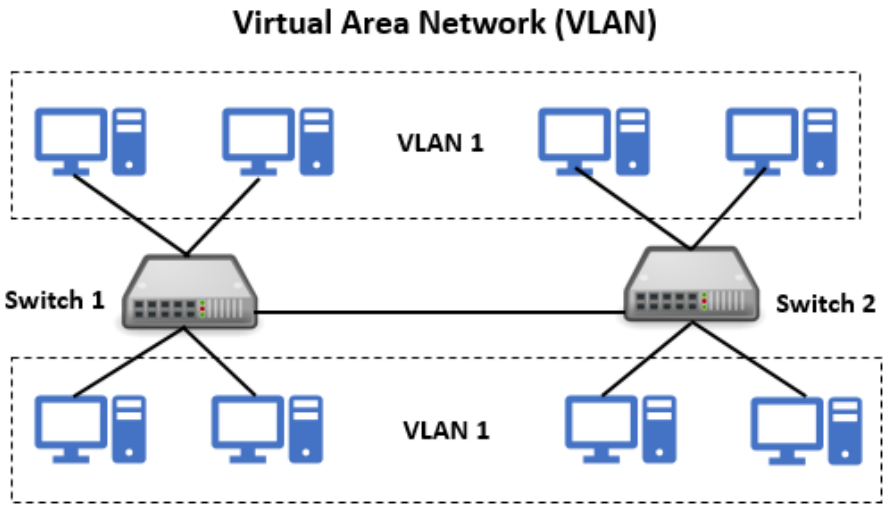
2.2.4 Chức năng của các lớp trong mô hình

Lớp Core đóng vai trò là trục chính của mạng, nơi tất cả lưu lượng từ các lớp khác được chuyển tiếp qua. Chức năng chính của lớp này là đảm bảo khả năng chuyển tiếp dữ liệu nhanh, ổn định và có tính sẵn sàng cao. Thiết bị ở lớp Core thường có hiệu năng cao, hỗ trợ đường truyền dự phòng và sử dụng các giao thức định tuyến để tối ưu hóa lưu lượng, tránh tắc nghẽn. Lớp này không xử lý các chính sách bảo mật hay quản lý truy cập mà tập trung hoàn toàn vào tốc độ và tính ổn định.

Lớp Distribution nằm giữa lớp Core và lớp Access, đóng vai trò là cầu nối giữa hai lớp này. Chức năng chính của lớp này là kiểm soát lưu lượng và phân phối dịch vụ truy cập. Điều này bao gồm việc xác định đường đi tối ưu cho dữ liệu giữa các lớp và phân phối các dịch vụ mạng từ lớp Core đến lớp Access và ngược lại. Lớp Distribution cũng đảm bảo tính linh hoạt cho việc mở rộng mạng bằng cách cung cấp các dịch vụ như VLAN, QoS và bảo mật mạng.

Lớp Access là nơi người dùng và các thiết bị kết nối trực tiếp vào mạng. Lớp này chịu trách nhiệm cung cấp quyền truy cập đến tài nguyên mạng và đảm bảo an toàn ở mức cơ bản. Chức năng bao gồm cấu hình cổng switch, quản lý VLAN, DHCP và các chính sách bảo mật mạng. Lớp Access đóng vai trò giảm tải cho các lớp phía trên bằng cách tập trung chức năng quản lý vào các lớp Distribution và Core [2].

2.3. Công nghệ VLAN (Virtual LAN)



Hình 2.4 Mô hình công nghệ VLAN

VLAN (Virtual Local Area Network) là một công nghệ ảo hóa cho phép chia một mạng vật lý thành nhiều phân đoạn mạng LAN ảo. Các thiết bị trong cùng một VLAN có thể giao tiếp với nhau như thể chúng đang ở cùng một switch, dù thực tế có thể nằm ở các vị trí khác nhau [3].

2.3.1 Lợi ích của việc sử dụng VLAN

Tăng tính bảo mật VLAN cho phép tách biệt các nhóm người dùng khác nhau, ngăn chặn sự truy cập trái phép vào các tài nguyên mạng. Điều này giúp tăng tính bảo mật cho toàn bộ hệ thống mạng.

Cải thiện hiệu suất mạng VLAN giúp giảm tải lưu lượng mạng bằng cách chỉ chuyển tiếp dữ liệu giữa các cổng thuộc cùng VLAN. Điều này giúp tăng băng thông khả dụng và cải thiện hiệu suất mạng.

Tăng khả năng quản lý VLAN cho phép chia nhỏ mạng LAN thành các nhóm logic dựa trên các tiêu chí như phòng ban, chức năng hoặc vị trí địa lý. Điều này giúp quản trị viên dễ dàng quản lý và theo dõi các nhóm thiết bị riêng biệt.

Giảm chi phí Các thiết bị có thể nằm ở các vị trí vật lý khác nhau nhưng vẫn có thể giao tiếp với nhau như thể chúng nằm trong cùng một mạng LAN. Điều này giúp giảm chi phí khi không cần tăng thêm số lượng thiết bị mạng trong hệ thống.

Tăng độ linh hoạt VLAN cho phép người quản trị dễ dàng di chuyển, thêm hoặc loại bỏ các thiết bị mà không ảnh hưởng đến cấu trúc logic của mạng. Điều này giúp tăng độ linh hoạt và tính sẵn sàng của hệ thống mạng [3].

2.3.2 Phân loại VLAN

2.3.2.1 Port - based VLAN

Port - based VLAN được biết đến là VLAN dựa trên cổng hoặc VLAN dựa trên giao diện. Đây là cách cấu hình VLAN đơn giản và phổ biến nhất. Cấu hình này cho phép quản trị viên mạng gắn VLAN theo cách thủ công, mỗi cổng Switch được gắn vào một VLAN xác định. Port - based VLAN thích hợp với hệ thống mạng có quy mô nhỏ và không phải thường xuyên thay đổi hạ tầng [3].

2.3.2.2 MAC address based VLAN

MAC address based VLAN đề cập đến việc gắn các VLAN theo địa chỉ MAC mỗi địa chỉ MAC được đánh dấu với một VLAN. Cách cấu hình này không được sử dụng nhiều do còn nhiều hạn chế trong việc quản lý. Tuy nhiên, cấu hình này cũng có ưu điểm là cải thiện đáng kể tính linh hoạt và an ninh mạng. Kể cả khi người dùng thay đổi vị trí thường xuyên, thì quản trị mạng cũng không cần phải cấu hình lại các VLAN [3].

2.3.2.3 Protocol - based VLAN

Protocol - based VLAN cách cấu hình này tương tự như MAC address based VLAN, nhưng chỉ dùng duy nhất một địa chỉ IP hoặc địa chỉ logic thay thế cho địa chỉ MAC. Hiện nay, cách cấu hình này đã không còn phổ biến nhiều do sử dụng giao thức DHCP [3].

2.4. Giao thức định tuyến (OSPF)

2.4.1 Định tuyến tĩnh (Static Routing)

Static Routing là phương pháp định tuyến trong đó người quản trị mạng phải cấu hình thủ công các đường đi trên mỗi router. Mỗi tuyến đường đến một mạng đích phải được khai báo một cách rõ ràng. Các router sẽ không tự động trao đổi thông tin định tuyến với nhau [4].

2.4.1.1 Cơ chế hoạt động

Trong mô hình định tuyến tĩnh, các tuyến đường được người quản trị cấu hình thủ công trên từng router. Khi một gói tin đến, router sẽ kiểm tra bảng định tuyến đã được thiết lập sẵn để xác định đường đi đến đích. Các tuyến đường này không thay đổi trừ khi người quản trị chủ động cập nhật lại cấu hình. Điều này đồng nghĩa với việc nếu có sự cố xảy ra như đứt kết nối hoặc thiết bị hỏng, router sẽ không có khả năng tự tìm tuyến thay thế. Static Routing không phát sinh lưu lượng mạng để trao đổi thông tin định tuyến, giúp tiết kiệm tài nguyên hệ thống nhưng lại đòi hỏi sự can thiệp liên tục từ người quản trị khi có thay đổi trong mạng [4].

2.4.1.2 Ưu & nhược điểm

Ưu điểm

Người quản trị dễ dàng kiểm soát đường đi của từng gói tin.

Tiết kiệm tài nguyên không tạo ra lưu lượng trao đổi định tuyến.

Bảo mật tốt khi không tự động cập nhật nên ít bị tấn công định tuyến.

Nhược điểm

Khi xảy ra sự cố mạng, các router không tự tìm tuyến đường thay thế.

Với mạng diện rộng, việc mở rộng sẽ gặp khó khăn khi việc cấu hình thủ công rất tốn công và dễ sai sót.

2.4.2 Định tuyến động (Dynamic Routing)

OSPF là một giao thức định tuyến động theo trạng thái liên kết, sử dụng thuật toán Dijkstra để tính toán đường đi ngắn nhất đến các đích. OSPF tự động cập nhật thông tin định tuyến giữa các router trong cùng một vùng [5].

2.4.2.1 Cơ chế hoạt động

OSPF hoạt động dựa trên nguyên tắc "link-state", tức là mỗi router sẽ thu thập thông tin về trạng thái kết nối của các router láng giềng thông qua các bản tin quảng bá trạng thái liên kết. Các thông tin này được trao đổi định kỳ và đồng bộ giữa các router trong cùng một vùng, từ đó xây dựng một cơ sở dữ liệu chung gọi là Link-

State Database. Sau đó, mỗi router sẽ sử dụng thuật toán Dijkstra để tính toán đường đi ngắn nhất đến các mạng đích và cập nhật bảng định tuyến của mình. Quá trình này được lặp lại tự động khi có bất kỳ thay đổi nào trong mạng như mất kết nối, thêm thiết bị, hoặc thay đổi cấu trúc mạng, giúp đảm bảo tính linh hoạt và khả năng tự hồi phục của hệ thống [5].

2.4.2.2 Ưu & nhược điểm

Ưu điểm

Tự động cập nhật khi có thay đổi trong mạng.

Phục hồi nhanh khi đường truyền gặp sự cố.

Tối ưu hóa đường đi và hỗ trợ chia tải (load balancing).

Hỗ trợ chia mạng lớn thành nhiều area, dễ quản lý.

Nhược điểm

Cấu hình phức tạp hơn so với định tuyến tĩnh.

Tiêu tốn một phần băng thông trên mạng để xây dựng bảng định tuyến.

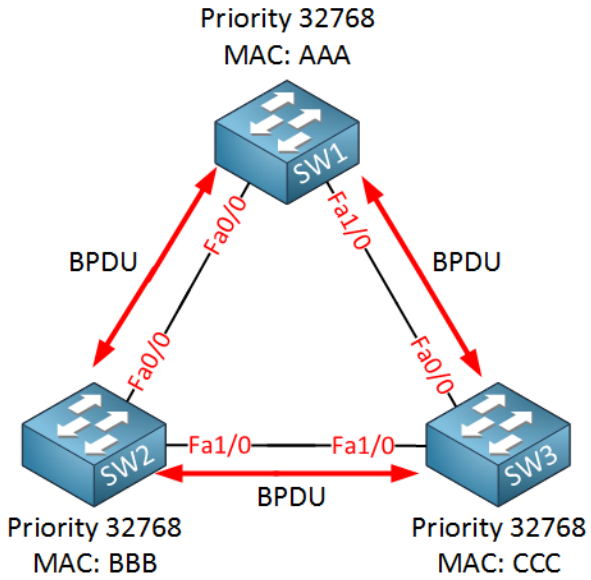
2.4.3 So sánh giữa Static Routing và Dynamic Routing

Bảng 2.2 So sánh giữa định tuyến tĩnh và định tuyến động

Tiêu chí	***Static Routing***	***OSPF Routing***
Cấu hình	Thủ công từng router	Tự động học router
Quản lý	Dễ với mạng nhỏ	Tốt cho mạng lớn, nhiều thiết bị
Tính thích ứng	Không thích ứng khi sự cố	Tự động thích ứng, tự sửa đường đi
Hiệu suất xử lý	Nhẹ, không tốn tài nguyên	Nặng hơn do xử lý LSA và tính toán
Bảo mật	Ít bị tấn công định tuyến	Cần cấu hình bảo mật (MD5, Authentication)

Khả năng mở rộng	Kém khi mạng lớn	Tốt, có thể chia vùng quản lý

2.5. Giao thức Spanning Tree Protocol (STP)



Hình 2.5 Mô hình STP

Spanning Tree Protocol là giao thức mạng Lớp 2 được sử dụng để ngăn chặn vòng lặp trong cấu trúc mạng. STP được tạo ra để tránh các vấn đề phát sinh khi máy tính trao đổi dữ liệu trên mạng cục bộ có chứa các đường dẫn dự phòng. Nếu luồng lưu lượng không được giám sát và kiểm soát cẩn thận, dữ liệu có thể bị kẹt trong một vòng lặp xoay quanh các phân đoạn mạng, ảnh hưởng đến hiệu suất và khiến lưu lượng gần như dừng lại [6].

2.5.1 Cơ chế hoạt động của STP

2.5.1.1 Lựa chọn Root Bridge

STP sẽ chọn một switch làm Root Bridge, tức là điểm trung tâm để các switch khác dựa vào đó xác định đường đi tối ưu trong mạng. Việc lựa chọn này dựa trên Bridge ID, gồm giá trị ưu tiên (priority) và địa chỉ MAC. Switch nào có Bridge ID nhỏ nhất sẽ trở thành Root Bridge. Một khi Root Bridge đã được xác định, các switch còn lại sẽ tìm cách kết nối về Root Bridge bằng đường đi ngắn nhất có thể [6].

2.5.1.2 Chọn cổng gốc

Cổng gần nhất với Root Bridge được gọi là Root Port. Mỗi Non-Root Bridge sẽ có một Root Port là đường dẫn ngắn nhất để đến Root Bridge vì mỗi Non-Root Bridge sẽ có đường dẫn tốt nhất để đến Root Bridge.

2.5.1.3 Chọn cổng được chỉ định và không được chỉ định

Cổng gốc: Luôn ở trạng thái chuyển tiếp và là đường dẫn tốt nhất và ngắn nhất để đến cổng gốc.

Cổng được chỉ định: Các cổng này cũng nằm ở phía bắc tiểu bang; chúng luôn chuyển tiếp dữ liệu.

Cổng không được chỉ định: Cổng đang trong trạng thái chặn.

2.5.2 Ưu & nhược điểm của STP

2.5.2.1 Ưu điểm

Ngăn chặn các đường dẫn có thể gây ra vòng lặp trong mạng.

Làm tăng tính ổn định của mạng bằng cách quản lý tính dự phòng của mạng.

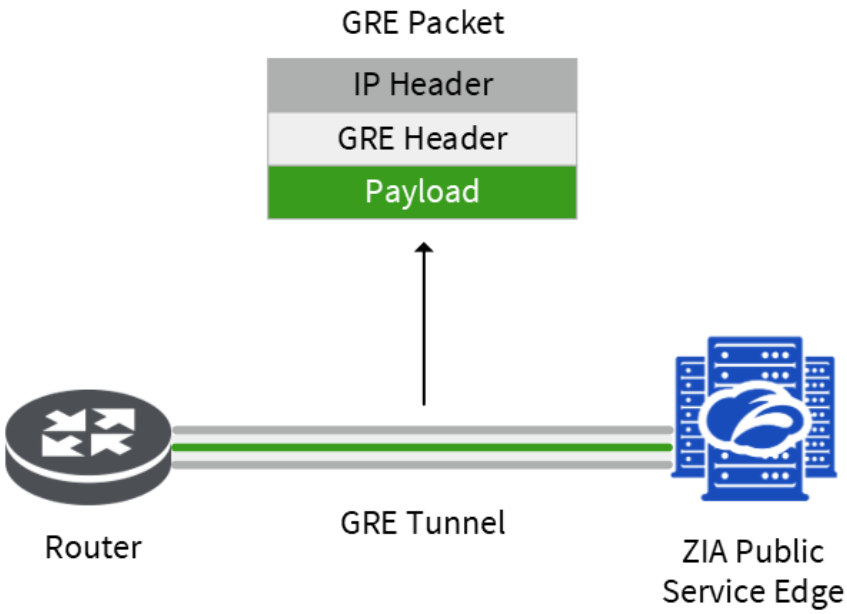
Giúp tối ưu hóa các tuyến đường dữ liệu.

2.5.2.2 Nhược điểm

Sự hội tụ của nó có thể chậm, gây ra sự chậm trễ của mạng.

Có thể chậm hơn các giao thức mới hơn trong một số thiết lập nhất định.

2.6. Giao thức GRE Tunnel (Generic Routing Encapsulation)



Hình 2.6 Mô hình GRE Tunnel

GRE là viết tắt của Generic Routing Encapsulation, là giao thức được phát triển bởi Cisco, cho phép đóng gói nhiều loại giao thức lớp Network trong các liên kết Point-to-Point. Một GRE Tunnel được sử dụng khi các gói dữ liệu cần được gửi giữa các mạng khác nhau thông qua internet. Với GRE được cấu hình, 1 đường hầm ảo được tạo giữa 2 router và các gói tin gửi giữa 2 mạng nội bộ sẽ được truyền qua GRE Tunnel [3].

2.6.1 Lợi ích của GRE Tunnel

Đường hầm GRE có thể được sử dụng để kết nối an toàn tới trung tâm dữ liệu.

GRE có thể được sử dụng để tạo đường hầm qua internet.

Đường hầm GRE cho phép giao tiếp giữa mạng IPv6 và IPv4.

Đường hầm GRE có thể được sử dụng để hỗ trợ lưu lượng đa hướng qua các mạng không hỗ trợ định tuyến đa hướng gốc [3].

2.6.2 Cơ chế hoạt động của GRE Tunnel

Đường hầm GRE hoạt động bằng cách đóng gói một giao thức mạng trong một giao thức mạng khác. Nó chỉ đơn giản là đặt một gói tin trong một gói tin khác.

Mỗi gói tin GRE mới có một tiêu đề và một tải trọng. Quá trình này cho phép truyền tải các gói tin thuộc nhiều giao thức khác nhau qua một hạ tầng mạng chỉ hỗ trợ giao thức IP.

Khi một gói tin được gửi qua GRE Tunnel, nó sẽ được bao bọc bởi một tiêu đề GRE và tiêu đề IP bên ngoài. Tiêu đề GRE chứa thông tin điều khiển, như điểm đầu và điểm cuối của tunnel, cùng các tham số cần thiết để xác định gói tin khi đến đích. Phần tải trọng là gói tin gốc cần được chuyển đến mạng đích [3].

2.6.3 Phân loại GRE Tunnel

2.6.3.1 GRE cơ bản (Point-to-Point GRE)

GRE cơ bản là dạng đơn giản nhất của đường hầm GRE, thiết lập kết nối điểm giữa hai router qua mạng không tin cậy. Nó hoạt động bằng cách đóng gói gói tin gốc vào trong một gói GRE, sau đó truyền đến thiết bị đích.

Cách thức hoạt động

Trong mô hình GRE thông thường, dữ liệu được đóng gói bằng cách đặt toàn bộ gói tin gốc thường là một gói IP vào bên trong một gói GRE mới. Sau đó, gói GRE này lại được gắn thêm một tiêu đề IP khác ở bên ngoài để định tuyến qua mạng trung gian, chẳng hạn như Internet. Khi gói tin đến đích, router nhận sẽ loại bỏ phần tiêu đề bên ngoài và phần tiêu đề GRE, rồi trích xuất lại gói tin gốc để chuyển tiếp đến đích cuối. Phương pháp này giúp truyền tải dữ liệu giữa các mạng khác nhau qua một mạng trung gian mà không bị giới hạn bởi giao thức gốc, nhưng không có cơ chế bảo mật nào đi kèm [3].

Ưu điểm

GRE cơ bản chỉ yêu cầu định nghĩa hai đầu Tunnel nguồn và đích, giúp người quản trị mạng dễ dàng triển khai và theo dõi.

GRE cho phép đóng gói các gói tin từ nhiều giao thức khác nhau như IPv4, IPv6,... vào trong giao thức IP, nhờ đó có thể kết nối các mạng khác loại.

GRE không mã hóa dữ liệu, nên thường được kết hợp với IPsec để tạo ra các VPN vừa bảo mật vừa có thể định tuyến linh hoạt.

Mỗi Tunnel chỉ kết nối giữa hai thiết bị, nên việc kiểm tra lỗi, đo lường hiệu suất hoặc giám sát mạng trở nên cụ thể và chính xác hơn.

Nhược điểm

Mỗi site muốn kết nối đến một site khác phải thiết lập riêng một Tunnel, gây phức tạp khi mở rộng mạng.

Khi mạng có nhiều chi nhánh, việc cấu hình thủ công từng Tunnel sẽ tốn thời gian và dễ sai sót.

Trong mô hình Hub-and-Spoke, GRE cơ bản đòi hỏi cấu hình Tunnel giữa Hub và từng Spoke, dẫn đến sự rườm rà và thiếu linh hoạt.

2.6.3.2 mGRE (Multipoint GRE)

mGRE là phiên bản mở rộng của GRE cho phép một router duy nhất có thể tạo nhiều kết nối GRE đến nhiều router đích khác nhau qua cùng một interface Tunnel. Điều này khắc phục nhược điểm của GRE cơ bản khi phải tạo nhiều tunnel cho nhiều site.

Cách thức hoạt động

mGRE cho phép một Tunnel duy nhất kết nối đến nhiều điểm đích khác nhau thay vì tạo từng Tunnel riêng biệt như GRE thường. Khi có dữ liệu cần gửi, router sử dụng NHRP (Next Hop Resolution Protocol) để tìm địa chỉ IP thực của điểm đích. Sau đó, dữ liệu được đóng gói vào một gói GRE duy nhất và gửi qua Tunnel đến Router đích. Tại đích, tiêu đề GRE được loại bỏ và gói gốc được chuyển tiếp. Cơ chế này giúp mở rộng mạng linh hoạt và giảm cấu hình phức tạp trong các mô hình VPN dạng Hub-and-Spoke [3].

Ưu điểm

Chỉ cần một Tunnel duy nhất trên thiết bị trung tâm để kết nối đến nhiều điểm khác. Các Spoke không cần Tunnel riêng lẻ cho mỗi điểm, tiết kiệm thời gian cấu hình và dễ mở rộng.

Với mGRE, khi thêm một site mới chỉ cần cấu hình tối thiểu trên Hub, trong khi các site còn lại không bị ảnh hưởng.

Khi mGRE được tích hợp cùng NHRP các thiết bị có thể học được địa chỉ thực của nhau, giúp định tuyến linh hoạt và tạo VPN động hiệu quả hơn.

Đây là nền tảng của các giải pháp VPN động như DMVPN (Dynamic Multipoint VPN), thường dùng trong doanh nghiệp lớn.

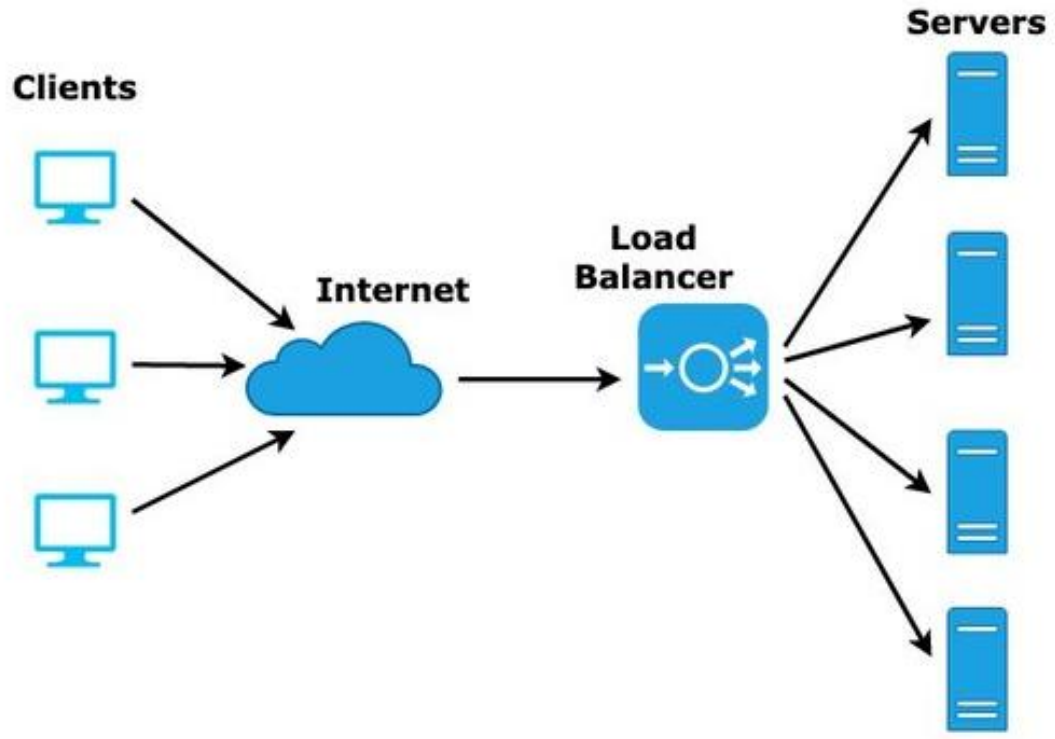
Nhược điểm

mGRE cần thêm các thành phần như NHRP để hoạt động trơn tru. Nếu không cấu hình đúng, việc định tuyến sẽ không hiệu quả.

Vì sử dụng cơ chế động và đa điểm, việc xác định nguyên nhân khi sự cố xảy ra phức tạp hơn nhiều so với GRE cơ bản.

Một số tính năng như QoS hoặc kiểm soát lưu lượng cụ thể từng điểm khó thực hiện hơn trong môi trường mGRE do tính chất chia sẻ Tunnel.

2.7. Kỹ thuật cân bằng tải (Load Balancing) trong mạng WAN



Hình 2.7 Mô hình Load Balancing

Cân bằng tải là một kỹ thuật được sử dụng để phân phối lưu lượng mạng trên một nhóm máy chủ được gọi là cụm máy chủ. Nó tối ưu hóa hiệu suất mạng, độ tin cậy và dung lượng, giảm độ trễ vì nhu cầu được phân bổ đồng đều giữa nhiều máy chủ và tài nguyên tính toán. Ngoài ra, cân bằng tải còn cung cấp khả năng chuyển đổi dự phòng. Nếu một máy chủ bị lỗi, bộ cân bằng tải ngay lập tức chuyển hướng khối lượng công việc của nó đến một máy chủ sao lưu, do đó giảm thiểu ảnh hưởng đến người dùng cuối [7].

2.7.1 Cách thức hoạt động

Cân bằng tải xử lý các yêu cầu đến từ người dùng về thông tin và các dịch vụ khác. Họ ngồi giữa các máy chủ xử lý các yêu cầu đó và internet. Khi nhận được yêu cầu, trước tiên bộ cân bằng tải sẽ xác định máy chủ nào trong nhóm khả dụng và trực tuyến, sau đó định tuyến yêu cầu đến máy chủ đó. Trong thời gian tải nặng, bộ cân bằng tải hoạt động kịp thời và có thể tự động thêm máy chủ để đáp ứng với lưu lượng truy cập tăng đột biến. Ngược lại, bộ cân bằng tải có thể làm giảm máy chủ nếu nhu cầu thấp [7].

2.7.2 Các loại cân bằng tải

Cân bằng tải phần cứng (Hardware Load Balancers) cân bằng tải phần cứng là một thiết bị phần cứng có phần mềm tích hợp chuyên dụng và độc quyền được thiết kế để xử lý một lượng lớn lưu lượng ứng dụng. Các cân bằng tải này có khả năng ảo hóa tích hợp và cho phép sử dụng nhiều phiên bản cân bằng tải ảo trên một thiết bị.

Ưu điểm: Hiệu suất vượt trội, độ trễ thấp, và đáng tin cậy. Thường đi kèm với các tính năng bảo mật tốt hơn, vì chúng chỉ được xử lý bởi tổ chức chứ không phải bởi bất kỳ bên thứ ba nào.

Nhược điểm: Chi phí đầu tư ban đầu cao, ít linh hoạt và khó mở rộng. Bên cạnh đó, cân bằng tải phần cứng đòi hỏi nhân sự có chuyên môn để cấu hình và lập trình cao.

Cân bằng tải phần mềm (Software Load Balancers) cân bằng tải phần mềm chạy trên máy ảo hoặc server hộp trắng, rất có thể là chức năng bộ điều khiển phân

phối ứng dụng (ADC). ADC thường cung cấp các tính năng bổ sung, bao gồm bộ nhớ đệm, nén và định hình lưu lượng truy cập. Phổ biến trong môi trường đám mây, cân bằng tải ảo có thể mang lại mức độ linh hoạt ca

Ưu điểm: Linh hoạt, dễ triển khai, chi phí thấp hơn và có thể dễ dàng mở rộng quy mô. Rất phù hợp với môi trường đám mây và kiến trúc microservices. Với nhiều phiên bản phần mềm hơn, cân bằng tải phần mềm có thể mở rộng quy mô lớn hơn.

Nhược điểm: Khi mở rộng quy mô vượt quá dung lượng, cân bằng tải phần mềm có thể gây ra độ trễ ban đầu. Hiệu suất có thể thấp hơn phần cứng, phụ thuộc vào tài nguyên của máy chủ mà nó chạy [7].

2.7.3 Thuật toán Load Balancing

2.7.3.1 Thuật toán cân bằng tải tĩnh

Phương pháp IP hash-based tính toán máy chủ ưa thích của một máy khách nhất định dựa trên các khóa được chỉ định, chẳng hạn như tiêu đề HTTP hoặc thông tin địa chỉ IP. Phương pháp này hỗ trợ tính bền bỉ của phiên hoặc độ bám dính, mang lại lợi ích cho các ứng dụng dựa trên thông tin trạng thái được lưu trữ dành riêng cho người dùng, chẳng hạn như giỏ hàng thanh toán trên nền tảng thương mại điện tử.

Phương pháp round-robin đi qua tất cả các máy chủ có sẵn theo thứ tự tuần tự và phân phối lưu lượng truy cập đến danh sách các máy chủ được luân phiên bằng cách sử dụng hệ thống tên miền (DNS). Máy chủ tên có thẩm quyền mang một danh sách các bản ghi "A" khác nhau và cung cấp một bản ghi để phản hồi cho mỗi truy vấn DNS.

Phương pháp weighted round-robin có trọng số cho phép quản trị viên chỉ định các trọng số khác nhau cho mỗi máy chủ. Bằng cách này, các máy chủ có thể xử lý nhiều lưu lượng truy cập hơn sẽ nhận được nhiều lưu lượng truy cập hơn một chút dựa trên trọng lượng của chúng. Trọng số được cấu hình trong bản ghi DNS [7].

2.7.3.2 Thuật toán cân bằng tải động

Phương pháp ít kết nối nhất (Least Connections) ủng hộ các máy chủ có ít giao dịch và kiểm tra đang diễn ra nhất và gửi lưu lượng truy cập đến các máy chủ có ít kết nối mở nhất. Thuật toán này giả định rằng tất cả các kết nối yêu cầu sức mạnh xử lý gần như bằng nhau.

Phương pháp kết nối ít nhất có trọng số (Weighted Least Connections) giả định rằng một số máy chủ có thể xử lý nhiều lưu lượng truy cập hơn so với các máy chủ khác. Do đó, nó cho phép quản trị viên gán các trọng số khác nhau cho mỗi máy chủ.

Cách tiếp cận thời gian phản hồi có trọng số (Weighted Response Time) sử dụng trung bình thời gian phản hồi của mỗi máy chủ và kết hợp chúng với số lượng kết nối mà mỗi máy chủ đã mở để tìm điểm đến tốt nhất cho việc gửi lưu lượng truy cập. Thuật toán này đảm bảo dịch vụ nhanh hơn, vì nó gửi lưu lượng truy cập đến các máy chủ với thời gian phản hồi nhanh nhất.

Thuật toán dựa trên tài nguyên (Resource-based) phân phối tải dựa trên tính khả dụng của tài nguyên trên mỗi máy chủ tại thời điểm đó. Trước khi phân phối lưu lượng truy cập, nó truy vấn một phần mềm chuyên dụng được gọi là tác nhân chạy trên mỗi máy chủ để đo lường tính khả dụng của bộ xử lý và bộ nhớ trung tâm [7].

2.7.4 Lợi ích của cân bằng tải

Cải thiện khả năng mở rộng cân bằng tải có thể thay đổi quy mô cơ sở hạ tầng máy chủ theo yêu cầu, tùy thuộc vào yêu cầu mạng mà không ảnh hưởng đến dịch vụ.

Cải thiện hiệu quả do giảm gánh nặng lưu lượng truy cập trên mỗi máy chủ, lưu lượng mạng lưu lượng truy cập tốt hơn và cải thiện thời gian phản hồi.

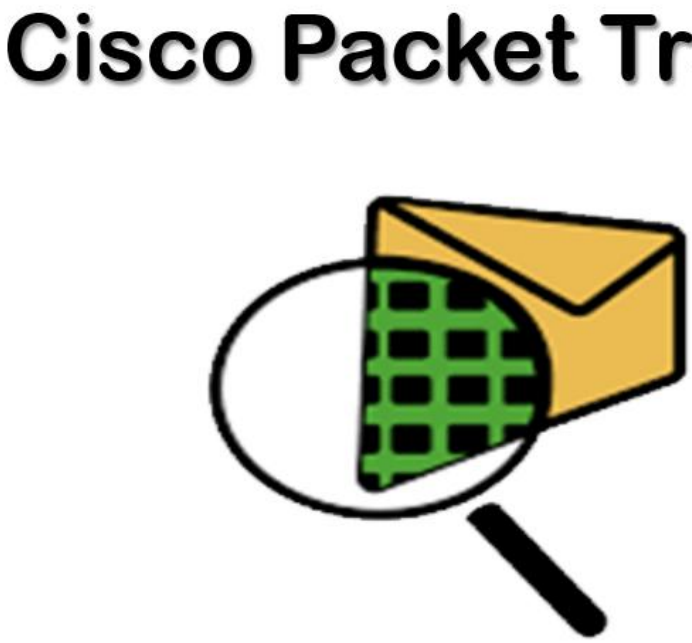
Giảm thời gian chết các công ty có sự hiện diện toàn cầu và nhiều địa điểm ở các múi giờ khác nhau có thể được hưởng lợi từ việc cân bằng tải, đặc biệt là khi nói đến bảo trì máy chủ.

Phân tích dự đoán cân bằng tải có thể cung cấp khả năng phát hiện sớm các lỗi và giúp quản lý chúng mà không ảnh hưởng đến các tài nguyên khác.

Quản lý hiệu quả thất bại trong trường hợp xảy ra lỗi, bộ cân bằng tải có thể tự động chuyển hướng lưu lượng truy cập đến các tài nguyên chức năng và các tùy chọn sao lưu.

Cải thiện bảo mật cân bằng tải thêm một lớp bảo mật bổ sung mà không yêu cầu thay đổi hoặc tài nguyên bổ sung. Khi nhiều điện toán chuyển sang đám mây, bộ cân bằng tải đang được trang bị các tính năng bảo mật, chẳng hạn như chức năng giảm tải [5].

2.8. Giới thiệu công cụ mô phỏng Cisco Packet Tracer.



Hình 2.8 Công cụ Cisco Packet Tracer

Cisco Packet Tracer là công cụ giả lập mạng do Cisco phát triển, hỗ trợ việc học tập mạng, thực hành với thiết bị router và switch. Đây là một phần mềm miễn phí, cho phép người dùng tạo cấu trúc liên kết mạng, cấu hình thiết bị, gửi các gói tin và mô phỏng mạng với nhiều hình thức trực quan.

Cisco cung cấp phần mềm này miễn phí cho các cơ sở giáo dục và sinh viên tham gia vào các chương trình đào tạo mạng của hãng cũng như chuẩn bị cho các kỳ thi chứng chỉ mạng. Đồng thời, phần mềm Cisco Packet Tracer cũng được các giảng

viên sử dụng phổ biến trong các chương trình học CCENT, CCNA giới thiệu kiến thức về kỹ thuật và hệ thống mạng [8].

2.8.1 Các tính năng nổi bật

Thiết bị không giới hạn người dùng có thể tạo và cấu hình một số lượng thiết bị mạng không giới hạn trong quá trình mô phỏng, rất tiện lợi khi thiết kế và thử nghiệm quy mô mạng phức tạp.

Học trực tuyến Packet Tracer đi kèm với nhiều tài nguyên giáo dục mạng hỗ trợ người dùng nắm vững các khái niệm và thiết bị mạng.

Môi trường tương tác Giao diện người dùng của Packet Tracer trực quan và dễ tương tác và theo dõi hiệu suất mạng mô phỏng.

Hai chế độ hoạt động chế độ thời gian thực cho phép tương tác với mạng như mạng thực tế, trong khi chế độ mô phỏng cho phép điều chỉnh tốc độ mô phỏng.

Hỗ trợ nhiều giao thức mạng phần mềm hỗ trợ các giao thức mạng phổ biến như EGRP, OSPF, RIP, ICMP, UDP, TCP và IP để người dùng thực hành.

Hỗ trợ đa ngôn ngữ Packet Tracer hỗ trợ đa ngôn ngữ, bao gồm tiếng Anh, tiếng Pháp, tiếng Đức, tiếng Trung Quốc và tiếng Nhật phù hợp với người dùng toàn cầu [8].

2.8.2 Các giao thức được hỗ trợ của Packet Tracer

Bảng 2.3 Tổng hợp các giao thức được hỗ trợ

Lớp	***Giao thức mạng***
Application	– FTP, SMTP,POP3, HTTP, TFTP, Telnet, SSH, DNS, DHCP, NTP, SNMP, AAA, ISR, VOIP, MQTT. – SCCP config và gọi hỗ trợ lệnh ISR. – Trình quản lý cuộc gọi nhanh.
Transport	TCP, UDP, thuật toán Nagle TCP và phân mảnh IP, RTP.

Network	– BGP, IPv4, ICMP, ARP, IPv6, ICMPv6, IPSec, RIPv1/v2/ng, OSPF đa vùng, OSPFv3, EIGRP, EIGRPv6. – Định tuyến tĩnh, phân phối lại tuyến, chuyển mạch đa lớp, L3 QoS, NAT, CBAC. – Dựa trên vùng tường lửa chính sách, hệ thống chống xâm nhập trên ISR, GRE VPN, IPSec VPN, HSRP, CEF, SPAN/RSPAN, L2NAT, PTP, REP, LLDP.
Network Access/Interface	– Ethernet (802.3), 802.11, HDLC, Frame Relay, PPP, PPPoE, STP, RSTP, VTP, DTP, CDP, 802.1q, PAgP, QoS L2, SLARP. – WEP đơn giản, WPA, EAP, VLANs, CSMA/CD, EtherChannel. – Hỗ trợ mạng DSL, 3G, 4G.

2.8.3 Lợi ích của Cisco Packet Tracer

Kiểm tra mạng và phát hiện lỗi Packet Tracer giúp kiểm tra và phát hiện lỗi mạng dễ dàng, từ đó cải thiện kỹ năng sửa lỗi và tối ưu hóa mạng hiệu quả.

Giảm chi phí vì là công cụ miễn phí, Packet Tracer giúp giảm đáng kể chi phí đào tạo mạng cho cả cá nhân và doanh nghiệp.

Tiết kiệm thời gian khi dùng Packet Tracer, có thể luyện tập thiết kế mạng mà không cần đến thiết bị thực tế, giúp tiết kiệm thời gian và tài nguyên.

Thực hành trong môi trường an toàn phần mềm cung cấp môi trường ảo để thực hành và thử nghiệm các kỹ thuật mạng hiệu quả mà không cần thiết bị vật lý.

Chuẩn bị cho kỳ thi chứng chỉ mạng Packet Tracer là công cụ quan trọng để luyện tập, kiểm tra kiến thức và chuẩn bị cho các chứng chỉ của Cisco như CCNA (Cisco Certified Network Associate) và CCNP (Cisco Certified Network Professional) [9].

2.8.4 Ứng dụng thực tế

Mô hình hóa mạng là công cụ hoàn hảo để thiết kế mạng và mô hình hóa chúng trước khi triển khai thực tế, giúp đảm bảo hiệu suất hoạt động đúng như mong muốn.

Tìm hiểu và thử nghiệm các giao thức phần mềm hỗ trợ nhiều giao thức mạng khác nhau, cho phép thử nghiệm và hiểu rõ cách thức hoạt động giao thức mạng cụ thể.

Nghiên cứu và phát triển dự án Packet Tracer là lựa chọn hàng đầu cho việc nghiên cứu và phát triển các dự án mạng, cho phép phát triển các ý tưởng và thử nghiệm giải pháp mạng phức tạp.

Hỗ trợ giảng dạy từ xa đây là công cụ thiết yếu giúp xây dựng bài giảng và tổ chức các hoạt động học tập mạng trực tuyến.

Tạo môi trường thử nghiệm IoT nhờ khả năng tích hợp các thiết bị IoT, Packet Tracer cho phép dễ dàng tạo và thử nghiệm các ứng dụng về kịch bản IoT.

Tích hợp phát triển ứng dụng Packet Tracer hỗ trợ tích hợp mã Python và tự động hóa mạng, giúp phát triển các ứng dụng và kịch bản thử nghiệm một cách hiệu quả [9].

CHƯƠNG 3. HIỆN THỰC HOÁ NGHIÊN CỨU

3.1. Thiết kế sơ đồ mạng tổng thể

3.1.1 Phân tích yêu cầu mạng

Kết nối đa site: Cho phép các site (campus chính và các site phụ) kết nối với nhau thông qua mạng WAN.

Khả năng mở rộng: Mạng cần có khả năng mở rộng để bổ sung thêm thiết bị, site hoặc VLAN trong tương lai.

Bảo mật: Các dữ liệu trao đổi giữa các site cần được mã hóa an toàn thông qua GRE Tunnel.

Tối ưu hóa hiệu suất: Sử dụng kỹ thuật load balancing và định tuyến OSPF nhiều Area để tăng cường hiệu suất và độ tin cậy.

Quản lý VLAN rõ ràng: Chia VLAN theo chức năng để tách biệt lưu lượng truy cập giữa các nhóm người dùng

Dễ quản trị: Hệ thống phải dễ cấu hình, giám sát và bảo trì, đồng thời hỗ trợ khôi phục nhanh khi có sự cố.

3.1.2 Thiết kế sơ đồ kết nối các site

Hệ thống mạng bao gồm:

Một trụ sở chính (Campus): Là trung tâm của hệ thống, có vai trò xử lý định tuyến liên VLAN, làm điểm trung tâm trong hệ thống OSPF.

Hai site phụ: Kết nối về campus thông qua các liên kết WAN. Các site phụ sẽ thuộc các Area OSPF khác nhau để giảm tải bảng định tuyến và tối ưu xử lý.

GRE Tunnel: Được cấu hình giữa các router chính để mã hóa thông tin truyền qua Internet.

Site trung tâm

R1 (Router trung tâm): Kết nối đến 2 router site phụ thông qua hai cổng Serial

S1 (Switch Layer 3): Định tuyến nội bộ các VLAN

S2, S3 (Switch Layer 2): Phục vụ người dùng truy cập mạng

Các switch được kết nối theo mô hình hình tam giác với EtherChannel

Thiết bị đầu cuối: PC1 đến PC4, được gán vào các VLAN tương ứng:

VLAN 10: PC1, PC2

VLAN 20: PC3

VLAN 30: PC4

Site phụ R2 (Area 1)

Router R2 kết nối đến R1 bằng Serial0/3/0

Định tuyến theo OSPF Area 1.

Cũng thiết lập Tunnel GRE đến R3.

Site phụ R3 (Area 2)

Router R3 kết nối đến R1 bằng Serial0/3/0

Định tuyến theo OSPF Area 2.

Có Tunnel GRE đến R2, hỗ trợ truyền dữ liệu riêng.

3.1.3 Phân chia VLAN và khu vực định tuyến rõ ràng

Phân chia VLAN trong site chính:

Bảng 3.1 Phân chia VLAN

VLAN ID	Tên VlAN	Địa chỉ IP
10	VLAN10	192.168.10.0/24
20	VLAN20	192.168.20.0/24
30	VLAN30	192.168.30.0/24

Khu vực định tuyến OSPF:

Bảng 3.2 Phân chia định tuyến

Router	Khu vực OSPF	Chức năng
R1	Area 0	Backbone, kết nối với tất cả
R2	Area 1	Site phụ 1
R3	Area 2	Site phụ 2

3.2. Triển khai mô hình mạng trong Cisco Packet Tracer

3.2.1 Thiết bị sử dụng

Router (R1, R2, R3): Thiết lập định tuyến liên mạng và kết nối các site (R1 – trung tâm, R2 và R3 – site phụ).

Switch Layer 3 (S1): Đóng vai trò switch phân phối, đồng thời thực hiện Inter-VLAN Routing.

Switch Layer 2 (S2, S3): Đóng vai trò switch truy cập, kết nối đến các thiết bị đầu cuối.

Thiết bị PC (từ PC-1 đến PC-4): Thiết bị đầu cuối để kiểm tra truy cập mạng và định tuyến.

3.2.2 Kết nối vật lý

Kết nối giữa các router

R1 kết nối với R2 qua cổng S0/3/0 ↔ S0/3/0, sử dụng mạng WAN 10.0.12.0/30.

R1 kết nối với R3 qua cổng S0/3/1 ↔ S0/3/0, sử dụng mạng WAN 10.0.13.0/30.

R2 kết nối với R3 qua cổng S0/3/1 ↔ S0/3/1, sử dụng mạng WAN 10.0.23.0/30.

Kết nối giữa R1 và S1 (switch Layer 3)

Cổng G0/0 của R1 được nối đến cổng G0/1 của S1 bằng kết nối cáp đồng thẳng, dùng mạng LAN 192.168.1.0/24.

Kết nối giữa các switch

S1 kết nối với S2 qua cổng Fa0/2 và Fa0/3 trên switch.

S1 kết nối với S3 qua cổng Fa0/4 và Fa0/5 trên switch.

S2 kết nối với S1 qua cổng Fa0/1 và Fa0/2 trên switch.

S2 kết nối với S3 qua cổng Fa0/3 và Fa0/4 trên switch.

S3 kết nối với S1 qua cổng Fa0/1 và Fa0/2 trên switch.

S3 kết nối với S2 qua cổng Fa0/3 và Fa0/4 trên switch.

Cả ba switch kết nối với nhau đều được cấu hình là trunk port, để truyền nhiều VLAN trên cùng một liên kết.

Kết nối giữa các switch và các PC

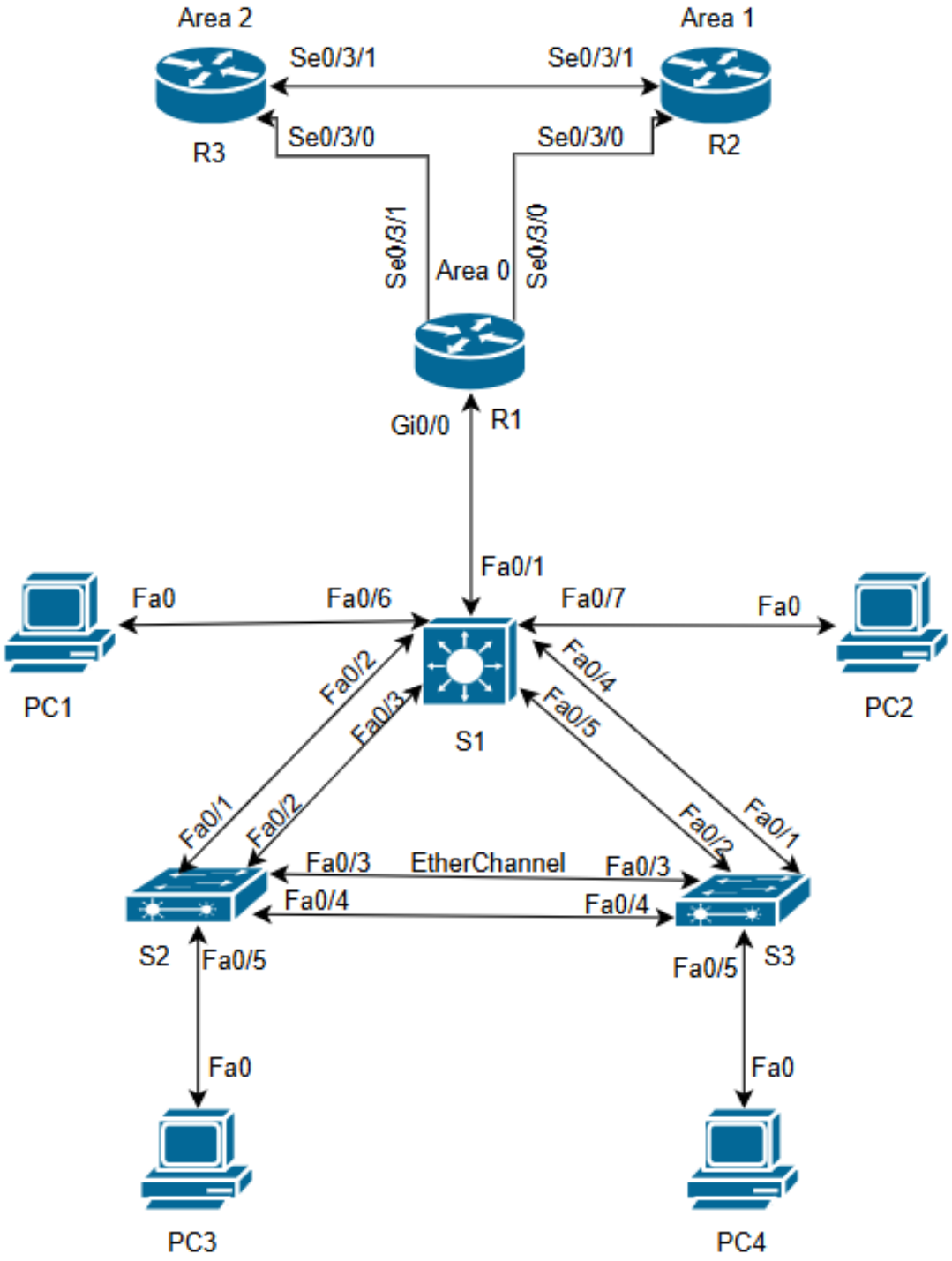
PC-1 kết nối vào S1 - cổng Fa0/6, thuộc VLAN 10.

PC-2 kết nối vào S1 - cổng Fa0/7, thuộc VLAN 10.

PC-3 kết nối vào S2 - cổng Fa0/5, thuộc VLAN 20.

PC-4 kết nối vào S3 - cổng Fa0/5, thuộc VLAN 30.

3.2.3 Triển khai mô hình



Hình 3.1 Mô hình triển khai

3.2.4 Cấu hình địa chỉ IP

Bảng 3.3 Cấu hình địa chỉ IP

Device	***Interface***	***IP Address***	***Subnet Mask***	***Default Gateway***
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/3/0	10.0.12.1	255.255.255.252	N/A
	S0/3/1	10.0.13.1	255.255.255.252	N/A
	Tunnel1	172.16.100.1	255.255.255.0	N/A
	Tunnel2	172.16.200.1	255.255.255.0	N/A
R2	S0/3/0	10.0.12.2	255.255.255.252	N/A
	Lo1	192.168.40.1	255.255.255.255	N/A
	Tunnel1	172.16.100.2	255.255.255.0	N/A
R3	S0/3/1	10.0.13.2	255.255.255.252	N/A
	Lo1	192.168.40.2	255.255.255.255	N/A
	Tunnel2	172.16.200.2	255.255.255.0	N/A
S1	VLAN 10	192.168.10.1	255.255.255.0	N/A
	VLAN 20	192.168.20.1	255.255.255.0	N/A
	VLAN 30	192.168.30.1	255.255.255.0	N/A
S2	VLAN 10	192.168.10.2	255.255.255.0	N/A
	VLAN 20	192.168.20.2	255.255.255.0	N/A
	VLAN 30	192.168.30.2	255.255.255.0	N/A
S3	VLAN 10	192.168.10.3	255.255.255.0	N/A
	VLAN 20	192.168.20.3	255.255.255.0	N/A
	VLAN 30	192.168.30.3	255.255.255.0	N/A
PC-1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC-2	NIC	192.168.10.11	255.255.255.0	192.168.10.1
PC-3	NIC	192.168.20.10	255.255.255.0	192.168.20.1
PC-4	NIC	192.168.30.10	255.255.255.0	192.168.30.1

3.3. Cấu hình VLAN và Trunking

3.3.1 Cấu hình VLAN trên các switch

Cấu hình VLAN trên S1

```
S1(config)#vlan 10
S1(config-vlan)#name VLAN10
S1(config)#vlan 20
S1(config-vlan)#name VLAN20
S1(config)#vlan 30
S1(config-vlan)#name VLAN30
```

Cấu hình VLAN trên S2

```
S2(config)#vlan 10
S2(config-vlan)#name VLAN10
S2(config)#vlan 20
S2(config-vlan)#name VLAN20
S2(config)#vlan 30
S2(config-vlan)#name VLAN30
```

Cấu hình VLAN trên S3

```
S3(config)#vlan 10
S3(config-vlan)#name VLAN10
S3(config)#vlan 20
S3(config-vlan)#name VLAN20
S3(config)#vlan 30
S3(config-vlan)#name VLAN30
```

3.3.2 Gán VLAN cho các cổng tương ứng

Sau khi đã tạo các VLAN, các cổng kết nối đến thiết bị đầu cuối (PC) được gán vào VLAN phù hợp:

Trên Switch S1

```
S1(config)#interface fa0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10


S1(config)#interface fa0/7
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
```

Trên Switch S2

```
S2(config-if)#interface fa0/5
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
```

Trên Switch S3

```
S3(config)# interface fa0/5
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 30
```

3.3.3 Cấu hình các trunk port bằng EtherChannel giữa các switch

Theo sơ đồ EtherChannel trong mô hình:

S1 – S2: sử dụng Port-Channel 1 từ các cổng fa0/2 và fa0/3

S1 – S3: sử dụng Port-Channel 2 từ các cổng fa0/4 và fa0/5

Cấu hình trên Switch S1

```
S1(config)#interface range fa0/2 - 3
S1(config-if-range)#channel-group 1 mode active
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#exit
```

```
S1(config)#interface port-channel1
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk allowed vlan 10,20,30
S1(config-if)#exit

S1(config)#interface range fa0/4 - 5
S1(config-if-range)#channel-group 2 mode active
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#exit

S1(config)#interface port-channel2
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk allowed vlan 10,20,30
```

S2 – S1: sử dụng Port-Channel 1 từ các cổng fa0/1 và fa0/2.

S2 – S3: sử dụng Port-Channel 2 từ các cổng fa0/3 và fa0/4.

Cấu hình trên Switch S2

```
S2(config)#interface range fa0/1 - 2
S2(config-if-range)#channel-group 1 mode active
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#exit

S2(config)#interface port-channel1
S2(config-if)#switchport trunk encapsulation dot1q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk allowed vlan 10,20,30
```

```
S2(config-if)#exit

S2(config)#interface range fa0/3 - 4
S2(config-if-range)#channel-group 2 mode active
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#exit

S2(config)#interface port-channel2
S2(config-if)#switchport trunk encapsulation dot1q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk allowed vlan 10,20,30
```

S3 – S1: sử dụng Port-Channel 1 từ các cổng fa0/1 và fa0/2.

S3 – S2: sử dụng Port-Channel 2 từ các cổng fa0/3 và fa0/4.

Cấu hình trên Switch S3

```
S3(config)#interface range fa0/1 - 2
S3(config-if-range)#channel-group 1 mode active
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#exit

S3(config)#interface port-channel1
S3(config-if)#switchport trunk encapsulation dot1q
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk allowed vlan 10,20,30
S3(config-if)#exit

S3(config)#interface range fa0/3 - 4
S3(config-if-range)#channel-group 2 mode active
```

```
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#exit


S3(config)#interface port-channel2
S3(config-if)#switchport trunk encapsulation dot1q
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk allowed vlan 10,20,30
```

3.4. Cấu hình Spanning Tree Protocol (STP)

3.4.1 Mục đích sử dụng STP

Trong mô hình mạng hiện tại, có ba switch (S1, S2, S3) được kết nối với nhau theo vòng lặp hình tam giác nhằm tăng tính dự phòng. Tuy nhiên, các vòng lặp Layer 2 trong mạng LAN có thể gây ra bão phát sóng (Broadcast storm), bảng địa chỉ MAC không ổn định (MAC address table instability). Do đó, cần kích hoạt giao thức Spanning Tree Protocol (STP) để phát hiện và loại bỏ các vòng lặp này, đảm bảo mạng hoạt động ổn định.

Lý do chọn S1 làm Root Bridge

Trong mô hình mạng được xây dựng, S1 là switch chính (Layer 3), chịu trách nhiệm định tuyến liên VLAN và quản lý định tuyến OSPF. Vì vậy, việc chọn S1 làm Root Bridge giúp tối ưu hóa đường đi của lưu lượng dữ liệu, giảm thiểu độ trễ và đảm bảo kiểm soát mạng tập trung.

3.4.2 Cấu hình STP trên các Switch

Cấu hình trên S1 (Root Bridge)

Giá trị priority mặc định là 32768, nên thiết lập S1 với priority = 4096 sẽ đảm bảo S1 được chọn làm Root Bridge cho VLAN 10, 20 và 30.

```
S1(config)#spanning-tree vlan 10 priority 4096
S1(config)#spanning-tree vlan 20 priority 4096
S1(config)#spanning-tree vlan 30 priority 4096
```

Cấu hình trên S2 và S3

Đối với S2 và S3 sẽ giữ nguyên priority mặc định để tránh bị chọn làm Root

```
S2(config)#spanning-tree vlan 10 priority 32768
S2(config)#spanning-tree vlan 20 priority 32768
S2(config)#spanning-tree vlan 30 priority 32768

S3(config)#spanning-tree vlan 10 priority 32768
S3(config)#spanning-tree vlan 20 priority 32768
S3(config)#spanning-tree vlan 30 priority 32768
```

3.4.3 Kiểm tả trạng thái STP

Sau khi cấu hình STP hoàn chỉnh ở S1 sẽ hiển thị dòng: This bridge is the root

```
S1#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    4106
             Address     00D0.D3E9.CB93
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay
15 sec

  Bridge ID  Priority    4106  (priority 4096 sys-id-ext 10)
             Address     00D0.D3E9.CB93
             Hello Time  2 sec  Max Age 20 sec  Forward Delay
15 sec
             Aging Time  20
```

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ----------------
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/7            Desg FWD 19        128.7    P2p
Po1              Desg FWD 12        128.27   Shr
Po2              Desg FWD 12        128.28   Shr
```

Trên S2 sẽ hiển thị địa chỉ MAC của S1 là Root ID Priority 4106

```
S2#show spanning-tree vlan 10
VLAN0010
Spanning tree enabled protocol ieee
Root ID Priority 4106
Address 00D0.D3E9.CB93
Cost 12
Port 27(Port-channel1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 8202 (priority 8192 sys-id-ext 10)
Address 00D0.BA82.A499
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20
Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- ----------------
Po1 Root FWD 12 128.27 Shr
Po2 Desg FWD 12 128.28 Shr
```

Tương tự như trên S2, S3 cũng sẽ hiển thị địa chỉ MAC của S1 là Root ID Priority 4106

```
S3#show spanning-tree vlan 10

VLAN0010

Spanning tree enabled protocol ieee

Root ID Priority 4106

Address 00D0.D3E9.CB93

Cost 12

Port 27(Port-channel1)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec


Bridge ID Priority 12298 (priority 12288 sys-id-ext 10)

Address 00D0.D340.9918

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------------- ---- --- --------- -------- ----------------

Po1 Root FWD 12 128.27 Shr

Po2 Altn BLK 12 128.28 Shr
```

3.5. Cấu hình định tuyến (tĩnh và động)

3.5.1 Mục tiêu cảu định tuyến

Việc cấu hình định tuyến trong mô hình mạng nhằm đảm bảo tất cả các mạng con thuộc các VLAN và các site khác nhau đều có thể trao đổi dữ liệu với nhau một cách ổn định và hiệu quả. Trong đó, định tuyến tĩnh được áp dụng cho các đường đặc biệt hoặc các kết nối yêu cầu tính ổn định cao, giúp kiểm soát hướng đi của gói tin. Song song đó, định tuyến động (OSPF) được triển khai để tối ưu khả năng mở rộng, giảm công tác quản trị khi mạng thay đổi, đồng thời đảm bảo các đường kết nối giữa các site có thể tự động cập nhật khi có sự cố hoặc thay đổi cấu hình.

3.5.2 Yêu cầu khi triển khai

Các router trong mô hình mạng R1, R2, R3 phải nắm được thông tin định tuyến đến tất cả các mạng, bao gồm cả mạng VLAN và các mạng loopback.

Các kết nối giữa các site được triển khai định tuyến động (OSPF) để tự động trao đổi thông tin mạng và chọn đường đi tối ưu.

Các tuyến đường đặc biệt hoặc mạng loopback cần được cấu hình định tuyến tĩnh để đảm bảo tính chính xác và ổn định.

Kết hợp với cấu hình GRE Tunnel để hỗ trợ truyền tải dữ liệu linh hoạt, đảm bảo tính bảo mật và độ tin cậy của hệ thống.

3.5.3 Cấu hình định tuyến tĩnh

Cấu hình trên R1

```
R1(config)#ip route 192.168.40.1 255.255.255.255 10.0.12.2
R1(config)#ip route 192.168.40.2 255.255.255.255 10.0.13.2
```

Địa chỉ 192.168.40.1 255.255.255.255 và 192.168.40.2 255.255.255.255 là các địa chỉ mạng Loopback của R2 và R3, dùng để giả lập các mạng nội bộ hoặc địa chỉ định danh router và việc dùng tuyến tĩnh ở đây giúp giữ đường đi cố định cho các mạng loopback, tránh phụ thuộc vào cập nhật động.

3.5.4 Cấu hình định tuyến động (OSPF)

Cấu hình trên R1

```
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 172.16.100.0 0.0.0.255 area 0
R1(config-router)#network 172.16.200.0 0.0.0.255 area 0
R1(config-router)#network 10.0.12.0 0.0.0.3 area 1
R1(config-router)#network 10.0.13.0 0.0.0.3 area 2
```

Với router-id 1.1.1.1 là định danh duy nhất cho R1 trong OSPF, Area 0 đóng vai trò là Backbone kết nối với các khu vực khác. Khi đó, Area 1 và Area 2 được tách riêng để quản lí lưu lượng tốt hơn.

Cấu hình trên R2

```
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 192.168.40.1 0.0.0.0 area 0
R2(config-router)#network 172.16.23.0 0.0.0.255 area 0
R2(config-router)#network 172.16.100.0 0.0.0.255 area 0
R2(config-router)#network 10.0.23.0 0.0.0.3 area 0
R2(config-router)#network 10.0.12.0 0.0.0.3 area 1
```

Với router-id 2.2.2.2 định danh dành cho R2. Toàn bộ các mạng vật lý và Tunnel đều thuộc Area 0 (Backbone), trừ mạng kết nối R1 (10.0.12.0) thuộc Area 1.

Cấu hình trên R3

```
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 192.168.40.0 0.0.0.255 area 0
R3(config-router)#network 172.16.23.0 0.0.0.3 area 0
R3(config-router)#network 172.16.200.0 0.0.0.3 area 0
R3(config-router)#network 10.0.23.0 0.0.0.3 area 0
R3(config-router)#network 10.0.13.0 0.0.0.3 area 2
```

Với router-id 3.3.3.3 định danh dành cho R3. Toàn bộ các mạng vật lý và Tunnel đều thuộc Area 0 (Backbone), trừ mạng kết nối R1 (10.0.13.0) thuộc Area 2.

3.6. Cấu hình GRE Tunnel

3.6.1 Tạo tunnel interface giữa các router

GRE (Generic Routing Encapsulation) cho phép tạo kết nối mạng ảo giữa các router qua hạ tầng mạng IP, giúp gói tin định tuyến như trên cùng một mạng LAN.

Trong mô hình này, triển khai 3 đường GRE Tunnel:

Tunnel1: Kết nối R1 ↔ R2.

Tunnel2: Kết nối R1 ↔ R3.

Tunnel0: Kết nối R2 ↔ R3.

3.6.2 Gán địa chỉ IP cho Tunnel

Bảng 3.4 Chia địa chỉ IP cho Tunnel

Tunnel	Router	IP Address	Router	IP Address	Subnet Mask
Tunnel1	R1	172.16.100.1	R2	172.16.100.2	255.255.255.0
Tunnel2	R1	172.16.200.1	R3	172.16.200.2	255.255.255.0
Tunnel0	R2	172.16.23.1	R3	172.16.23.2	255.255.255.252

3.6.1 Cấu hình route để đảm bảo truyền dữ liệu giữa các site qua tunnel

Cấu hình trên R1

```
R1(config)#interface tunnel1
R1(config-if)#ip address 172.16.100.1 255.255.255.0
R1(config-if)#tunnel source s0/3/0
R1(config-if)#tunnel destination 10.0.12.2


R1(config)#interface tunnel2
R1(config-if)#ip address 172.16.200.1 255.255.255.0
R1(config-if)#tunnel source s0/3/1
R1(config-if)#tunnel destination 10.0.13.2
```

Cấu hình trên R2

```
R2(config)#interface tunnel1
R2(config-if)#ip address 172.16.100.2 255.255.255.0
```

```
R2(config-if)#tunnel source s0/3/0
R2(config-if)#tunnel destination 10.0.12.1


R2(config)#interface Tunnel0
R2(config-if)#ip address 172.16.23.1 255.255.255.252
R2(config-if)#tunnel source s0/3/1
R2(config-if)#tunnel destination 10.0.23.2
```

Cấu hình trên R3

```
R3(config)#interface tunnel2
R3(config-if)#ip address 172.16.200.2 255.255.255.0
R3(config-if)#tunnel source s0/3/1
R3(config-if)#tunnel destination 10.0.13.1


R3(config)#interface Tunnel0
R3(config-if)#ip address 172.16.23.2 255.255.255.252
R3(config-if)#tunnel source s0/3/0
R3(config-if)#tunnel destination 10.0.23.1
```

3.7. Triển khai Load Balancing

3.7.1 Mục tiêu cân bằng tải

Triển khai cân bằng tải cho các gói tin đi qua hai đường hầm GRE (Tunnel1 và Tunnel2) giữa các router, nhằm tận dụng đồng thời cả hai đường truyền để tối ưu băng thông và độ tin cậy.

Tunnel1: R1 ↔ R2 ↔ R3

Tunnel2: R1 ↔ R3 ↔ R2

OSPF được cấu hình để hai đường này có cùng cost, cho phép OSPF thực hiện Equal-Cost Multi-Path (ECMP).

Đảm bảo lưu lượng được phân phối đồng đều qua Tunnel1 (R1 ↔ R2) và Tunnel2 (R1 ↔ R3).

Tăng khả năng dự phòng: Khi một kết nối gặp sự cố, toàn bộ lưu lượng sẽ tự động chuyển sang đường còn lại.

Bên cạnh đó, Tunnel0 giữa R2 ↔ R3 cũng được giữ để đảm bảo khả năng dự phòng trong định tuyến.

3.7.2 Cấu hình cân bằng tải giữa các kết nối WAN sử dụng ECMP

Cấu hình trên R1

```
R1(config)#interface tunnel1
R1(config-if)#ip ospf cost 10
R1(config-if)#exit


R1(config)#interface tunnel2
R1(config-if)#ip ospf cost 10
R1(config-if)#exit
```

Để đảm bảo cả hai đường Tunnel có cùng chi phí

```
R1(config)#router ospf 1
R1(config-router)#network 172.16.100.0 0.0.0.3 area 0
R1(config-router)#network 172.16.200.0 0.0.0.3 area 0
```

Khai báo cả Tunnel1 và Tunnel2 trong cùng Area 0 của OSPF để chúng trở thành hai đường có cùng chi phí.

OSPF sẽ tự động thực hiện ECMP vì đã đưa hai đường có cùng cost đến cùng một đích.

Cấu hình trên R2

```
R2(config)#router ospf 1
R2(config-router)#network 172.16.100.0 0.0.0.255 area 0
```

```
R2(config-router)#network 172.16.23.0 0.0.0.255 area 0
```

Ở Tunnel1 được khai báo trong Area 0 để kết nối với R1.

Còn Tunnel0 (172.16.23.x) giữa R2 ↔ R3 cũng khai báo trong Area 0 để hỗ trợ định tuyến dự phòng.

Cấu hình trên R3

```
R3(config)#router ospf 1
R3(config-router)#network 172.16.200.0 0.0.0.255 area 0
R3(config-router)#network 172.16.23.0 0.0.0.255 area 0
```

Tunnel2 khai báo để kết nối với R1.

Tunnel0 kết nối R3 ↔ R2 phục vụ cho tính dự phòng khi một trong hai đường chính mất kết nối.

3.7.3 Kiểm tra khả năng chia tải

Sử dụng lệnh *show ip route ospf* trên R1 để xác nhận rằng có 2 đường OSPF đến cùng một đích.

```
      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O     10.0.23.0 [110/2000] via 172.16.200.2, 00:10:13, Tunnel2
            [110/2000] via 172.16.100.2, 00:10:13, Tunnel1
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O     172.16.23.0 [110/2000] via 172.16.200.2, 00:10:13,
Tunnel2
                  [110/2000] via 172.16.100.2, 00:10:13,
Tunnel1
O IA  192.168.10.0 [110/2] via 192.168.1.2, 09:46:35,
GigabitEthernet0/0
O IA  192.168.20.0 [110/2] via 192.168.1.2, 09:46:35,
GigabitEthernet0/0
O IA  192.168.30.0 [110/2] via 192.168.1.2, 09:46:35,
GigabitEthernet0/0
```

```
          192.168.40.0/32 is subnetted, 2 subnets
     O        192.168.40.1 [110/1001] via 172.16.100.2, 00:10:13,
Tunnel1
     O        192.168.40.2 [110/1001] via 172.16.200.2, 00:10:13,
Tunnel2
```

Các prefix 10.0.23.0/30 và 172.16.23.0/30 có hai next-hop là Tunnel1 và Tunnel2 cùng metric điều này thể hiện ECMP đang hoạt động.

Sử dụng lệnh `traceroute` để quan sát dữ liệu được chia qua cả hai Tunnel.

```
     R1#traceroute 172.16.23.2
     Type escape sequence to abort.
     Tracing the route to 172.16.23.2
     1    172.16.100.2 11 msec 1 msec 10 msec


     R1#traceroute 192.168.40.2
     Type escape sequence to abort.
     Tracing the route to 192.168.40.2
     1    172.16.200.2 1 msec 1 msec 7 msec
```

3.7.4 Tính dự phòng khi mất kết nối

Mục tiêu: nếu một Tunnel down, thò toàn bộ lưu lượng sẽ chuyển sang Tunnel còn lại.

Kiểm tra trên R1

```
     R1(config)#interface Tunnel1
     R1(config-if)#shutdown
```

Sử dụng lệnh *`show ip route ospf`* kiểm tra các tuyến qua Tunnel1 biến mất, chỉ còn qua Tunnel2

```
     R1#show ip route ospf
          10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
```

```
     O     10.0.23.0 [110/2000] via 172.16.200.2, 00:00:26, Tunnel2
          172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
     O        172.16.23.0 [110/2000] via 172.16.200.2, 00:00:26,
Tunnel2
     O       172.16.100.0 [110/3000] via 172.16.200.2, 00:00:26,
Tunnel2
     O     IA     192.168.10.0     [110/2]     via     192.168.1.2,
4294967283:4294967237:
4294967250, GigabitEthernet0/0
     O     IA     192.168.20.0     [110/2]     via     192.168.1.2,
4294967283:4294967237:
4294967250, GigabitEthernet0/0
     O     IA     192.168.30.0     [110/2]     via     192.168.1.2,
4294967283:4294967237:
4294967250, GigabitEthernet0/0
          192.168.40.0/32 is subnetted, 2 subnets
     O         192.168.40.1 [110/2001] via 172.16.200.2, 00:00:26,
Tunnel2
     O      192.168.40.2      [110/1001]      via      172.16.200.2,
4294967273:4294967260, Tunnel2
```

CHƯƠNG 4. KẾT QUẢ THỰC NGHIỆM

4.1. Mô phỏng hệ thống trên phần mềm

4.1.1 Môi trường mô phỏng

Để kiểm chứng hiệu quả của mô hình mạng đã thiết kế, toàn bộ hệ thống được triển khai và mô phỏng trên phần mềm Cisco Packet Tracer phiên bản mới nhất. Đây là công cụ cho phép cấu hình và vận hành các thiết bị mạng một cách sát với thực tế, đồng thời hỗ trợ quan sát lưu lượng, kiểm thử kết nối và đánh giá hiệu suất.

Môi trường mô phỏng được chuẩn bị dựa trên các thông số đã cấu hình ở Chương 3, tất cả các thiết bị đều đã được cấu hình hoàn chỉnh, bao gồm:

Định tuyến OSPF nhiều Area (Area 0, Area 1, Area 2)

Triển khai EtherChannel giữa các switch để tăng băng thông

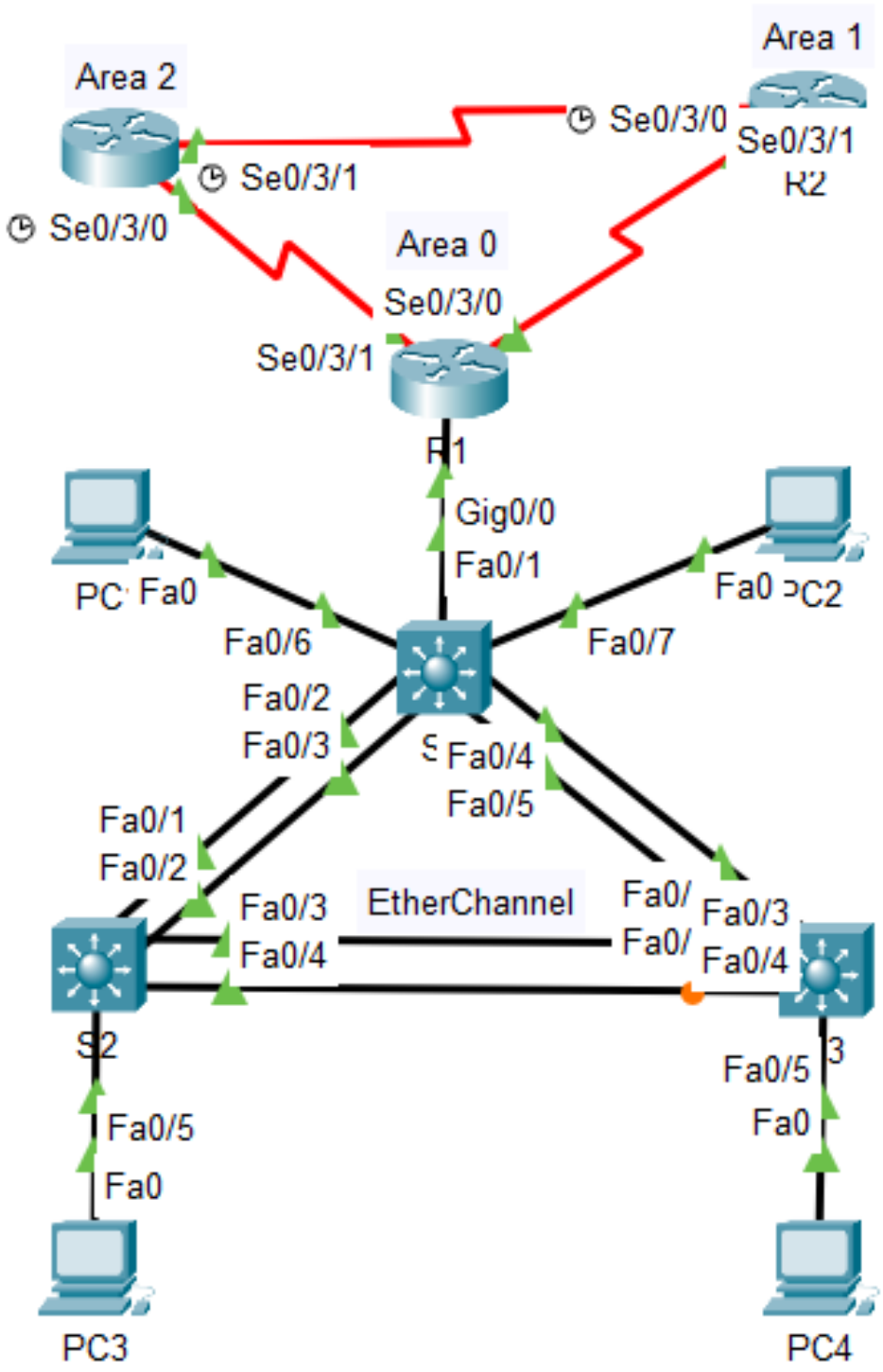
Phân chia VLAN và cấu hình định tuyến liên VLAN

Kích hoạt STP nhằm loại bỏ vòng lặp

Thiết lập GRE Tunnel giữa các Router

Cấu hình Load Balancing để phân phối lưu lượng

4.1.2 Sơ đồ mô hình sau khi cấu hình hoàn chỉnh



Hình 4.1 Mô hình triển khai hoàn chỉnh

Trong mô hình:

Router R1: Đóng vai trò trung tâm, thuộc Area 0 trong OSPF, kết nối tới R2 (Area 1) và R3 (Area 2) qua các cổng Serial.

Router R2 và R3: Ngoài việc kết nối tới R1 qua OSPF, hai router này còn thiết lập GRE Tunnel nhằm đảm bảo một kênh truyền riêng giữa Area 1 và Area 2, hỗ trợ truyền dữ liệu các giao thức không được hỗ trợ trực tiếp trên mạng WAN vật lý.

Switch S1 (Layer 3): Thực hiện định tuyến liên VLAN, tham gia vào OSPF và kết nối tới R1. Đây là thành phần trung tâm của mạng LAN.

Switch S2 và S3 (Layer 2): Quản lý VLAN, kết nối tới S1 bằng EtherChannel nhằm tăng băng thông và cung cấp khả năng dự phòng khi một đường truyền xảy ra sự cố.

PC1 – PC4: Được phân bổ vào các VLAN khác nhau, phục vụ kiểm thử các kịch bản kết nối nội bộ, liên VLAN và truyền dữ liệu qua GRE Tunnel.

4.1.3 Quy trình triển khai mô phỏng

Quá trình mô phỏng trên Cisco Packet Tracer được thực hiện theo các bước:

Xây dựng mô hình vật lý:

Kéo thả các thiết bị Router, Switch, PC vào giao diện mô phỏng.

Kết nối bằng cáp Serial cho đường WAN, cáp Ethernet cho kết nối LAN, và ghép các cổng thành EtherChannel giữa các switch.

Cấu hình từng thiết bị:

Router: Gán địa chỉ IP cho các interface, cấu hình OSPF nhiều Area, thiết lập GRE Tunnel, kiểm tra bảng định tuyến.

Switch Layer 3 (S1): Cấu hình VLAN, gán IP cho SVI, bật routing, định tuyến OSPF và EtherChannel.

Switch Layer 2 (S2, S3): Cấu hình VLAN, cấu hình trunk – port, tham gia EtherChannel, bật STP.

Kiểm tra ban đầu:

Ping giữa các thiết bị để đảm bảo kết nối cơ bản.

Kiểm tra trạng thái EtherChannel (show etherchannel summary), GRE Tunnel (show interface tunnel), và OSPF (show ip ospf neighbor).

4.1.4 Hoạt động tổng thể của mô hình sau khi cấu hình

OSPF nhiều Area hoạt động ổn định, các router nhận và trao đổi đầy đủ bảng định tuyến.

GRE Tunnel giữa R1 – R2, R1 – R3 và R2 – R3 cho phép các gói tin từ PC1 tới PC4 đi theo đường bảo mật riêng, ngay cả khi tuyến OSPF trực tiếp bị gián đoạn.

EtherChannel tăng gấp đôi băng thông giữa S1 – S2 và S1 – S3, đồng thời vẫn duy trì kết nối khi một trong các đường truyền gặp sự cố.

STP đảm bảo không có vòng lặp Layer 2, giúp mạng hoạt động ổn định.

Load Balancing phân phối lưu lượng giữa các đường OSPF song song, tối ưu hiệu suất sử dụng đường truyền.

4.2. Kiểm tra kết nối và định tuyến

4.2.1 Kiểm tra kết nối giữ các thiết bị

Kiểm tra ping nội bộ trong cùng VLAN

Thực hiện lệnh *ping* từ PC1 (VLAN10) đến PC2 (VLAN10)

```
C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

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

Kết quả trên cho thấy nội bộ VLAN10 hoạt động bình thường.

Kiểm tra ping giữa các VLAN khác nhau

Thực hiện lệnh *ping* từ PC1 (VLAN10) đến PC3 (VLAN20)

```
C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Định tuyến liên VLAN hoạt động tốt, S1 đã xử lý gói tin từ VLAN10 sang VLAN20 thành công.

Thực hiện lệnh *ping* từ PC1 (VLAN10) đến PC4 (VLAN30)

```
C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.30.1:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Định tuyến từ VLAN10 sang VLAN30 thành công, chứng tỏ định tuyến liên VLAN ổn định.

4.2.2 Kiểm tra bảng định tuyến OSPF

Sau khi cấu hình hoàn chỉnh, tiến hành kiểm tra bảng định tuyến bằng lệnh *show ip route ospf* cụ thể trên từng router để xác nhận việc học các tuyến từ các Area khác qua giao thức OSPF.

Kiểm tra trên R1

```
R1#show ip route ospf
     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O       10.0.23.0 [110/2000] via 172.16.200.2, Tunnel2
                  [110/2000] via 172.16.100.2, Tunnel1
     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O       172.16.23.0 [110/2000] via 172.16.200.2, Tunnel2
                    [110/2000] via 172.16.100.2, Tunnel1
O IA 192.168.10.0 [110/2] via 192.168.1.2, GigabitEthernet0/0
O IA 192.168.20.0 [110/2] via 192.168.1.2, GigabitEthernet0/0
O IA 192.168.30.0 [110/2] via 192.168.1.2, GigabitEthernet0/0
     192.168.40.0/32 is subnetted, 2 subnets
O       192.168.40.1 [110/1001] via 172.16.100.2, Tunnel1
O       192.168.40.2 [110/1001] via 172.16.200.2, Tunnel2
```

Theo kết quả ta thấy được:

R1 học được mạng 10.0.23.0 và 172.16.23.0 từ cả hai hướng qua Tunnel1 và Tunnel2 có thể đảm bảo dự phòng.

Các mạng VLAN nội bộ 192.168.10.0, 192.168.20.0, 192.168.30.0 được quảng bá qua OSPF đến các router khác.

Định tuyến đến các địa chỉ loopback trên R2, R3 là 192.168.40.1 và 192.168.40.2 thành công.

Kiểm tra trên R2

```
R2#show ip route ospf
     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O IA    10.0.13.0 [110/1064] via 172.16.23.2, Tunnel0
     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O       172.16.200.0 [110/2000] via 172.16.23.2, Tunnel0
                     [110/2000] via 172.16.100.1, Tunnel1
O    192.168.1.0 [110/1001] via 172.16.100.1, Tunnel1
O IA 192.168.10.0 [110/1002] via 172.16.100.1, Tunnel1
O IA 192.168.20.0 [110/1002] via 172.16.100.1, Tunnel1
O IA 192.168.30.0 [110/1002] via 172.16.100.1, Tunnel1
     192.168.40.0/24 is variably subnetted, 3 subnets, 2 masks
O       192.168.40.2 [110/1001] via 172.16.23.2, Tunnel0
```

Theo kết quả:

R2 học được mạng 10.0.13.0 và 172.16.200.0 từ cả hai hướng (Tunnel0 và Tunnel1).

Mạng VLAN từ 192.168.10.0, 192.168.20.0, 192.168.30.0 đã được định tuyến đầy đủ qua Tunnel1.

Định tuyến đến Loopback 192.168.40.2 cũng thành công.

Kiểm tra trên R3

```
R3#show ip route ospf
     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O IA    10.0.12.0 [110/1064] via 172.16.23.1, Tunnel0
     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O       172.16.100.0 [110/2000] via 172.16.200.1, Tunnel2
```

```
                        [110/2000] via 172.16.23.1, Tunnel0
     O    192.168.1.0 [110/1001] via 172.16.200.1, Tunnel2
     O IA 192.168.10.0 [110/1002] via 172.16.200.1, Tunnel2
     O IA 192.168.20.0 [110/1002] via 172.16.200.1, Tunnel2
     O IA 192.168.30.0 [110/1002] via 172.16.200.1, Tunnel2
          192.168.40.0/24 is variably subnetted, 3 subnets, 2 masks
     O       192.168.40.1 [110/1001] via 172.16.23.1, Tunnel0
```

Từ kết quả:

R3 nhận được mạng 10.0.12.0 và 172.16.100.0 qua cả hai hướng Tunnel0 và Tunnel2 đảm bảo hỗ trợ cân bằng tải và dự phòng.

Toàn bộ VLAN đã được định tuyến qua Tunnel2.

Có định tuyến đến Loopback 192.168.40.1 từ R1 qua Tunnel0.

4.2.3 Kiểm tra trạng thái OSPF

Sử dụng lệnh *show ip ospf neghbor* để xác nhận các router đã hình thành quan hệ láng giềng (adjacency) qua các liên kết vật lý và GRE Tunnel.

Trạng thái OSPF trên R1

```
     R1#show ip ospf neighbor
     Neighbor ID      Pri    State              Dead Time    Address
Interface
     4.4.4.4           1    FULL/DR          00:00:39    192.168.1.2
Gig0/0
     2.2.2.2           0    FULL/  -         00:00:39    172.16.100.2
Tunnel1
     3.3.3.3           0    FULL/  -         00:00:30    172.16.200.2
Tunnel2
     2.2.2.2            0    FULL/   -        00:00:39     10.0.12.2
Serial0/3/0
```

```
     3.3.3.3           0    FULL/   -        00:00:39     10.0.13.2
Serial0/3/1
```

Theo kết quả trên thì R1 có 5 láng giềng OSPF:

4.4.4.4 Router tại LAN nội bộ, ở trạng thái FULL/DR trên Gi0/0.

2.2.2.2 và 3.3.3.3 hình thành láng giềng qua cả đường hầm (Tunnel1, Tunnel2) và đường Serial vật lý (Serial0/3/0, Serial0/3/1).

>> Điều này chứng tỏ R1 đã kết nối đa đường với R2 và R3, đảm bảo khả năng dự phòng.

Trạng thái OSPF trên R2

```
     R2#show ip ospf neighbor

     Neighbor ID      Pri    State            Dead Time    Address
Interface
     3.3.3.3           0    FULL/   -         00:00:36     10.0.23.2
Serial0/3/1
     3.3.3.3          0    FULL/   -         00:00:36     172.16.23.2
Tunnel0
     1.1.1.1          0    FULL/   -         00:00:36     172.16.100.1
Tunnel1
     1.1.1.1           0    FULL/   -         00:00:37     10.0.12.1
Serial0/3/0
```

Với kết quả trên thì R2 có 4 phiên OSPF neighbor:

3.3.3.3 qua cả Tunnel0 và Serial0/3/1.

1.1.1.1 qua cả Tunnel1 và Serial0/3/0.

>> Mô hình này cho phép R2 có hai đường dự phòng tới cả R1 và R3.

Trạng thái OSPF trên R3

```
     R3#show ip ospf neighbor

     Neighbor ID      Pri    State            Dead Time    Address
Interface
```

```
     1.1.1.1           0   FULL/  -        00:00:39    172.16.200.1
Tunnel2
     2.2.2.2           0    FULL/  -         00:00:39     10.0.23.1
Serial0/3/1
     2.2.2.2           0   FULL/  -        00:00:30    172.16.23.1
Tunnel0
     1.1.1.1           0    FULL/  -         00:00:39     10.0.13.1
Serial0/3/0
```

Tương tự như R2, R3 cũng có 4 láng giềng OSPF:

1.1.1.1 (R1) qua Tunnel2 và Serial0/3/0.

2.2.2.2 (R2) qua Tunnel0 và Serial0/3/1.

>> Tất cả đều ở trạng thái Full, chứng tỏ các liên kết hoạt động ổn định.

4.2.4 Kiểm tra trạng thái EtherChannel

Sau khi đã cấu hình gộp cổng thành công, sử dụng lệnh *show etherchannel summary* để kiểm tra trạng thái các cổng sau khi gộp.

Kết quả trên S1

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


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

```
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+---------------------------

1      Po1(SU)           LACP   Fa0/2(P) Fa0/3(P)
2      Po2(SU)           LACP   Fa0/4(P) Fa0/5(P)
```

EtherChannel trên S1 hoạt động bình thường, kết nối song song đã được gộp thành 1 đường logic duy nhất.

Kết quả trên S2

```
S2#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

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

Group  Port-channel  Protocol    Ports
------+-------------+-----------+---------------------------

1      Po1(SU)           LACP   Fa0/1(P) Fa0/2(P)
```

```
2       Po2(SU)           LACP    Fa0/3(P) Fa0/4(P)
```

EtherChannel đã được tạo thành công, hoạt động ở Layer 2, trạng thái Up.

Kết quả trên S3

```
S3#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

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

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------

1      Po1(SU)           LACP    Fa0/1(P) Fa0/2(P)
2      Po2(SU)           LACP    Fa0/3(P) Fa0/4(P)
```

EtherChannel đã được tạo thành công, hoạt động ở Layer 2, trạng thái Up.

>> Tất cả đã ở trạng thái (P) trên tất cả Switch, chứng tỏ EtherChannel đang hoạt động ổn định.

4.2.5 Xác minh Spanning Tree Protocol (STP)

Sau khi đã cấu hình STP, sử dụng lệnh *show spanning-tree vlan 10* trên từng switch để xác định Root Bridge, xác nhận không có vòng lặp và vai trò của từng cổng trên switch.

Kết quả trên S1

```
S1#show spanning-tree vlan 10
VLAN0010
Root ID Priority 4106
Address 00D0.D3E9.CB93
This bridge is the root
Interface        Role Sts Cost      Prio.Nbr Type
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/7            Desg FWD 19        128.7    P2p
Po1              Desg FWD 12        128.27   Shr
Po2              Desg FWD 12        128.28   Shr
```

S1 thực sự là Root Bridge cho VLAN 10

Các Port-channel (Po1, Po2) trên S1 đều ở trạng thái Designated / Forwarding điều đó có nghĩa là S1 đang gửi BPDU và giữ vai trò Designated cho các liên kết này.

Kết quả trên S2

```
Root ID ... 00D0.D3E9.CB93 (S1)
Interface        Role Sts Cost      Prio.Nbr Type
Po1              Root FWD 12        128.27   Shr
Po2              Desg FWD 12        128.28   Shr
```

S2 hiển thị Po1 là Root / Forwarding → Po1 trên S2 là đường dẫn tới Root

Kết quả trên S3

```
Root ID ... 00D0.D3E9.CB93 (S1)
```

```
Interface        Role Sts Cost      Prio.Nbr Type
Po1              Root FWD 12        128.27   Shr
Po2              Altn BLK 12        128.28   Shr
```

S3 có Po1 là Root / Forwarding cũng là đường dẫn tới Root và Po2 là Alternate / Blocked → STP đã chặn Po2 trên S3 để phá vòng lặp, đây là hành vi bình thường và mong muốn để duy trì loop-free topology.

Bên cạnh đó, Cost, Port và Role hiển thị nhất quán giữa các switch điều này chứng tỏ STP converged ổn định.

4.3. Kiểm tra hiệu quả của GRE Tunnel

4.3.1 Kiểm tra trạng thái Tunnel

Trên R1

```
R1#show ip interface brief | include Tunnel
Tunnel1 172.16.100.1 YES manual up up
Tunnel2 172.16.200.1 YES manual up up
```

Trên R2

```
R2#show ip interface brief | include Tunnel
Tunnel0 172.16.23.1 YES manual up up
Tunnel1 172.16.100.2 YES manual up up
```

Trên R3

```
R3#show ip interface brief | include Tunnel
Tunnel0 172.16.23.2 YES manual up up
Tunnel2 172.16.200.2 YES manual up up
```

Mục đích là đảm bảo Tunnel ở trạng thái up/up và line protocol up. GRE Tunnel đã được thiết lập thành công, sẵn sàng truyền dữ liệu.

4.3.2 Ping kiểm tra end – to – end qua GRE

Sử dụng Loopback để kiểm tra ping trên R1

Ping từ R1 – R2

```
R1#ping 192.168.40.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/10/18 ms
```

Ping từ R1 – R3

```
R1#ping 192.168.40.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
2/9/16 ms
```

Cả 2 kết quả trên đều ping thành công 100% chứng tỏ GRE Tunnel hoạt động tốt. Dữ liệu có thể đi qua các router và xác nhận đường đi end - to - end ổn định.

4.4. Đánh giá khả năng Load Balancing

4.4.1 Kiểm tra phân phối tải

Sử dụng lệnh *show ip route ospf* trên R1 để quan sát định tuyến OSPF

```
R1#show ip route ospf
```

```
   10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O     10.0.23.0 [110/2000] via 172.16.100.2, 00:46:23, Tunnel1
                  [110/2000] via 172.16.200.2, 00:46:23, Tunnel2
   172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O     172.16.23.0 [110/2000] via 172.16.100.2, 00:46:23, Tunnel1
                    [110/2000] via 172.16.200.2, 00:46:23, Tunnel2
O          IA  192.168.10.0  [110/2]  via  192.168.1.2,  00:47:21,
GigabitEthernet0/0
O          IA  192.168.20.0  [110/2]  via  192.168.1.2,  00:47:21,
GigabitEthernet0/0
O          IA  192.168.30.0  [110/2]  via  192.168.1.2,  00:47:21,
GigabitEthernet0/0
   192.168.40.0/32 is subnetted, 2 subnets
O     192.168.40.1 [110/1001] via 172.16.100.2, 00:46:23, Tunnel1
O     192.168.40.2 [110/1001] via 172.16.200.2, 00:46:23, Tunnel2
```

Các mạng như 192.168.40.1 (loopback R2) và 192.168.40.2 (loopback R3) có nhiều tuyến đường cùng chi phí (multi-path) qua Tunnel1 và Tunnel2. Điều này chứng tỏ OSPF đã học được nhiều đường tới cùng một đích, cho phép phân phối tải.

4.4.2 Kiểm tra luồng dữ liệu

Sử dụng *traceroute* từ R1 tới Loopback R2

```
R1#traceroute 192.168.40.1
Type escape sequence to abort.
Tracing the route to 192.168.40.1
1   172.16.100.2 11 msec 12 msec 1 msec
```

Theo kết quả cho thấy lưu lượng có thể đi qua Tunnel1 hoặc Tunnel2, tùy OSPF lựa chọn. Khi một tunnel bị shutdown, OSPF tự động chuyển lưu lượng sang tunnel còn lại, chứng tỏ tính dự phòng và phân phối tải hoạt động tốt.

4.4.3 Hiệu quả cân bằng tải

Hiệu quả cân bằng tải trong mô hình này được thể hiện thông qua việc GRE Tunnel kết hợp OSPF cho phép chia đều lưu lượng qua nhiều đường đến cùng một đích (ECMP). Khi R1 muốn gửi dữ liệu đến R2 hoặc R3, OSPF sẽ tham chiếu metric của các tuyến Tunnel1 và Tunnel2. Nếu các tuyến có chi phí bằng nhau, OSPF sẽ chia tải giữa hai đường này, thay vì gửi toàn bộ dữ liệu qua một tunnel duy nhất.

Điều này đem lại một số lợi ích rõ rệt:

Tối ưu sử dụng băng thông khi có nhiều tunnel, mỗi tunnel sẽ chịu một phần lưu lượng, tránh tình trạng quá tải trên một đường duy nhất.

Tăng tính dự phòng nếu một tunnel bị sự cố (shutdown hoặc lỗi vật lý), OSPF sẽ tự động chuyển lưu lượng sang tunnel còn lại mà không làm gián đoạn kết nối, đảm bảo mạng vẫn hoạt động ổn định.

Cân bằng tải thực tế trong quá trình ping hoặc gửi dữ liệu lớn giữa các router, các gói dữ liệu được phân phối đều qua cả hai tunnel, thể hiện tính cân bằng tải thực sự trong môi trường WAN mô phỏng.

Dễ quản lý và mở rộng khi thêm nhiều đường tunnel hoặc mạng LAN mới, OSPF vẫn tự động cân bằng lưu lượng, giúp quản lý mạng đơn giản hơn và tăng khả năng mở rộng trong tương lai.

4.5. Phân tích hiệu suất và độ tin cậy của mô hình

4.5.1 Hiệu suất truyền dữ liệu

Tốc độ truyền tải nhờ việc triển khai EtherChannel để gộp băng thông giữa các switch, hệ thống đạt tốc độ truyền dữ liệu cao hơn so với sử dụng một đường truyền đơn lẻ. Điều này giúp giảm đáng kể thời gian truyền tải gói tin và cải thiện hiệu suất tổng thể của mạng.

Định tuyến tối ưu với OSPF giúp chọn đường đi ngắn nhất dựa trên chi phí (cost), đảm bảo dữ liệu được truyền qua tuyến đường có hiệu suất tốt nhất. Trong trường hợp một liên kết gặp sự cố, OSPF tự động cập nhật bảng định tuyến để chuyển hướng gói tin sang tuyến khả dụng khác mà không cần can thiệp thủ công.

4.5.2 Khả năng mở rộng

Mô hình hỗ trợ dễ dàng mở rộng bằng cách thêm router, switch hoặc các liên kết mạng mới. Các cơ chế như VLAN, OSPF nhiều Area và GRE tunnel giúp việc tích hợp các site hoặc phân vùng mạng mới diễn ra nhanh chóng, không ảnh hưởng nhiều đến cấu trúc hiện tại.

4.5.3 Độ tin cậy của hệ thống

Cơ chế dự phòng nhờ sự kết hợp giữa EtherChannel và STP, mạng vẫn duy trì kết nối khi một cổng hoặc một liên kết vật lý bị hỏng. EtherChannel giúp giữ nguyên hoạt động khi một đường trong nhóm bị ngắt, trong khi STP ngăn chặn vòng lặp và bảo vệ tính toàn vẹn của mạng.

Khả năng khôi phục nhanh trong các thử nghiệm mô phỏng sự cố, thời gian hội tụ của OSPF và quá trình khôi phục lưu lượng thông qua liên kết dự phòng diễn ra nhanh chóng, đảm bảo dịch vụ không bị gián đoạn đáng kể.

4.5.4 Độ ổn định khi tải cao

Trong các bài kiểm tra mô phỏng lượng truy cập đồng thời lớn, mô hình vẫn duy trì hiệu suất ổn định. Nhờ cơ chế cân bằng tải của OSPF và băng thông mở rộng của EtherChannel, các liên kết không bị quá tải cục bộ, hạn chế tình trạng tắc nghẽn mạng.

CHƯƠNG 5. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

5.1. Kết luận

Sau quá trình nghiên cứu, thiết kế và triển khai, đề tài "Xây dựng mô hình mạng WAN với bảo mật và tối ưu hóa hiệu suất" Ứng dụng các kỹ thuật như VLAN, OSPF, EtherChannel, STP, GRE Tunnel, và Load Balancing đã hoàn thành đầy đủ các mục tiêu đã đề ra ban đầu. Mô hình được xây dựng đáp ứng các yêu cầu về:

Một hệ thống mạng WAN kết nối nhiều nhánh với nhau.

Phân chia mạng hợp lý và tối ưu hiệu suất mạng.

Đảm bảo tính bảo mật khi truyền dữ liệu qua Internet.

Tối ưu băng thông và đảm bảo khả năng dự phòng.

Kết nối liên mạng giữa các site thông qua đường truyền WAN ảo (GRE Tunnel).

Việc áp dụng đồng thời nhiều công nghệ mạng cho phép khai thác tối đa ưu điểm của từng thành phần: VLAN hỗ trợ phân tách và quản lý lưu lượng, STP ngăn chặn vòng lặp lớp 2, EtherChannel tăng băng thông và dự phòng liên kết, OSPF định tuyến tối ưu, GRE Tunnel giúp kết nối mạng LAN từ xa thông qua hạ tầng trung gian.

Qua các bước kiểm tra và đánh giá đã chứng minh được hệ thống hoạt động ổn định, có khả năng tự động phục hồi khi mất một tuyến kết nối và phân phối tải hợp lý trên các đường truyền. Điều này khẳng định tính khả thi của mô hình trong các ứng dụng thực tế đối với doanh nghiệp nhiều chi nhánh.

5.2. Kết quả đạt được

Trong quá trình thực hiện, đề tài đã đạt được những kết quả sau:

Thiết kế và triển khai thành công mô hình mạng WAN với các thiết bị được cấu hình đồng bộ và hoạt động đúng chức năng.

Phân chia VLAN hợp lý, giúp tách biệt các miền quảng bá, nâng cao hiệu quả quản lý và bảo mật cơ bản.

Cấu hình STP và EtherChannel để đảm bảo dự phòng đường truyền, loại bỏ vòng lặp, đồng thời tận dụng tối đa băng thông hiện có.

Triển khai OSPF đa vùng kết hợp GRE Tunnel để kết nối các mạng LAN từ xa, đảm bảo định tuyến tối ưu.

Kiểm tra và đánh giá khả năng cân bằng tải và dự phòng: khi một đường truyền gặp sự cố, lưu lượng được tự động chuyển hướng sang tuyến còn lại, giảm thiểu thời gian gián đoạn dịch vụ.

Tích luỹ kinh nghiệm triển khai các công nghệ mạng nâng cao, tạo nền tảng cho các ứng dụng và nghiên cứu sâu hơn trong tương lai.

5.3. Hướng phát triển

Mặc dù đã đáp ứng được mục tiêu đề ra ban đầu. Tuy nhiên, mô hình vẫn có thể tiếp tục mở rộng và nâng cao hiệu quả thông qua các hướng sau:

Tăng cường bảo mật triển khai ACL, tường lửa, VPN IPsec và xác thực người dùng nhằm bảo vệ dữ liệu trên đường truyền.

Nâng cấp lên SD-WAN tối ưu hoá việc sử dụng nhiều kết nối WAN, quản lý tập trung và tăng tính linh hoạt.

Triển khai hệ thống giám sát mạng sử dụng SNMP, NetFlow hoặc các giải pháp mã nguồn mở để theo dõi, phân tích và cảnh báo sự cố kịp thời.

Mở rộng quy mô mô hình thử nghiệm kết nối nhiều site hơn, kết hợp nhiều nhà cung cấp dịch vụ khác nhau để đánh giá tính ổn định và khả năng mở rộng.

DANH MỤC TÀI LIỆU HAM KHẢO

[1] A. W. Services, “WAN - Giải thích về mạng diện rộng,” [Trực tuyến]. Available: https://aws.amazon.com/vi/what-is/wan/. [Đã truy cập 6 2025].

[2] M. Karimyar, “Cách cấu hình đường hầm đóng gói định tuyến chung (GRE) trong mạng,” [Trực tuyến]. Available: https://www.servermania.com/kb/articles/how-to-configure-a-generic-routing-encapsulation-gre-tunnel-in-networking. [Đã truy cập 7 2025].

[3] L. V. Tuấn, “GRE Tunnel là gì? Hướng dẫn cấu hình GRE Tunnel Trên Router Cisco,” [Trực tuyến]. Available: https://cnttshop.vn/blogs/cisco/gre-tunnel-la-gi-cau-hinh-gre-tunnel-router-cisco-1. [Đã truy cập 7 2025].

[4] L. Đ. Kiên, “Giao thức Spanning Tree,” [Trực tuyến]. Available: https://viblo.asia/p/giao-thuc-spanning-tree-stp-spanning-tree-protocol-W13VM8OGLY7. [Đã truy cập 6 2025].

[5] V. IDC, “Các loại Load Balancer và lợi ích của Load Balancing,” [Trực tuyến]. Available: https://viettelidc.com.vn/tin-tuc/load-balancing-la-gi-cac-loai-load-balancer-va-loi-ich-cua-load-balancer. [Đã truy cập 6 2025].

[6] N. T. Hùng, “Tác dụng và Cách cấu hình Giao thức STP,” [Trực tuyến]. Available: https://vienthongxanh.vn/giao-thuc-spanning-tree-protocol-tac-dung-vcach-cau-hinh/. [Đã truy cập 7 2025].

[7] “Load balancing là gì? So sánh cân bằng tải phần cứng và phần mềm,” GMO-Z.com RUNSYSTEM, [Trực tuyến]. Available: https://cloud.z.com/vn/news/load-balancing/. [Đã truy cập 7 2025].

[8] “Cisco Networking Academy,” Cisco Packet Academy, [Trực tuyến]. Available: https://www.netacad.com/about-networking-academy/packet-tracer/. [Đã truy cập 6 2025].

[9] H. Nguyễn, “Cisco Packet Tracer là gì? Tổng quan về phần mềm Cisco Packet Tracer,” VIETNIX, [Trực tuyến]. Available: https://vietnix.vn/cisco-packet-tracer-la-gi/. [Đã truy cập 7 2025].