**BÁO CÁO ĐỀ TÀI**

MPLS AND SEGMENT ROUTING

**Lê Bảo Tài**

Ngày … Tháng … Năm 2025

# MỤC LỤC

[MỤC LỤC i](#_Toc196061564)

[Chương 1. MPLS 1](#_Toc196061565)

[1.1. MPLS 1](#_Toc196061566)

[1.1.1. Khái quát về MPLS 1](#_Toc196061567)

[1.1.2. Các thành phần trong MPLS 3](#_Toc196061568)

[1.1.3. Nguyên lý hoạt động của MPLS 4](#_Toc196061569)

[1.1.4. Ưu và nhược điểm của MPLS 5](#_Toc196061570)

[1.2. MPLS VPN L3 8](#_Toc196061571)

[1.3. BGP 9](#_Toc196061572)

[1.3.1. BGP là gì? 9](#_Toc196061573)

[1.3.2. Autonomous System 9](#_Toc196061574)

[1.3.4. External BGP và internal BGP 10](#_Toc196061575)

[1.4. VRF 11](#_Toc196061576)

[1.4.1. Định nghĩa 11](#_Toc196061577)

[1.4.2. VRF động như thế nào? 11](#_Toc196061578)

[Chương 2. THỰC NGHIỆM 12](#_Toc196061579)

[2.1. Cấu hình BGP 12](#_Toc196061580)

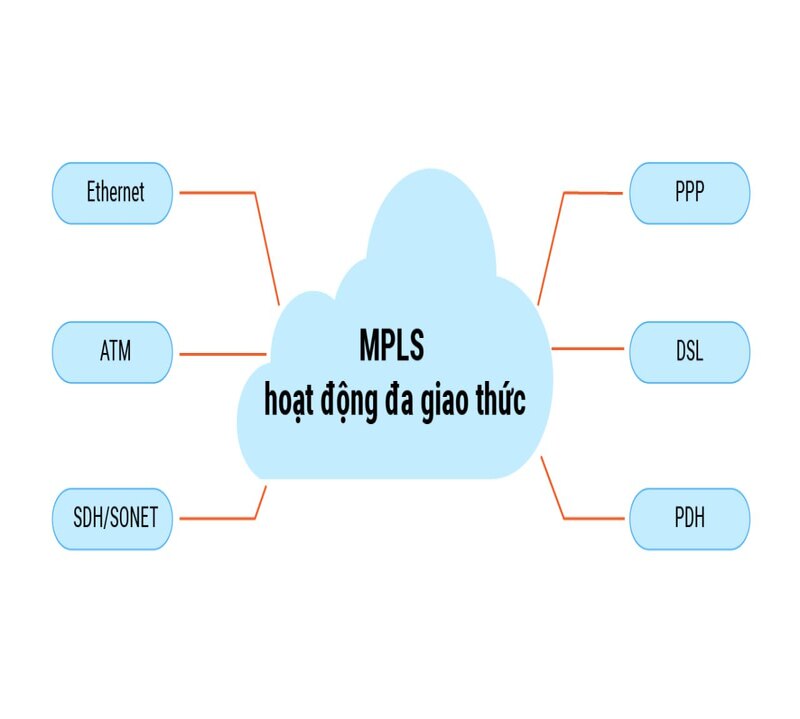
[2.2. Cấu hình MPLS VPN(BGP - VRF) 13](#_Toc196061581)

# Chương 1. MPLS

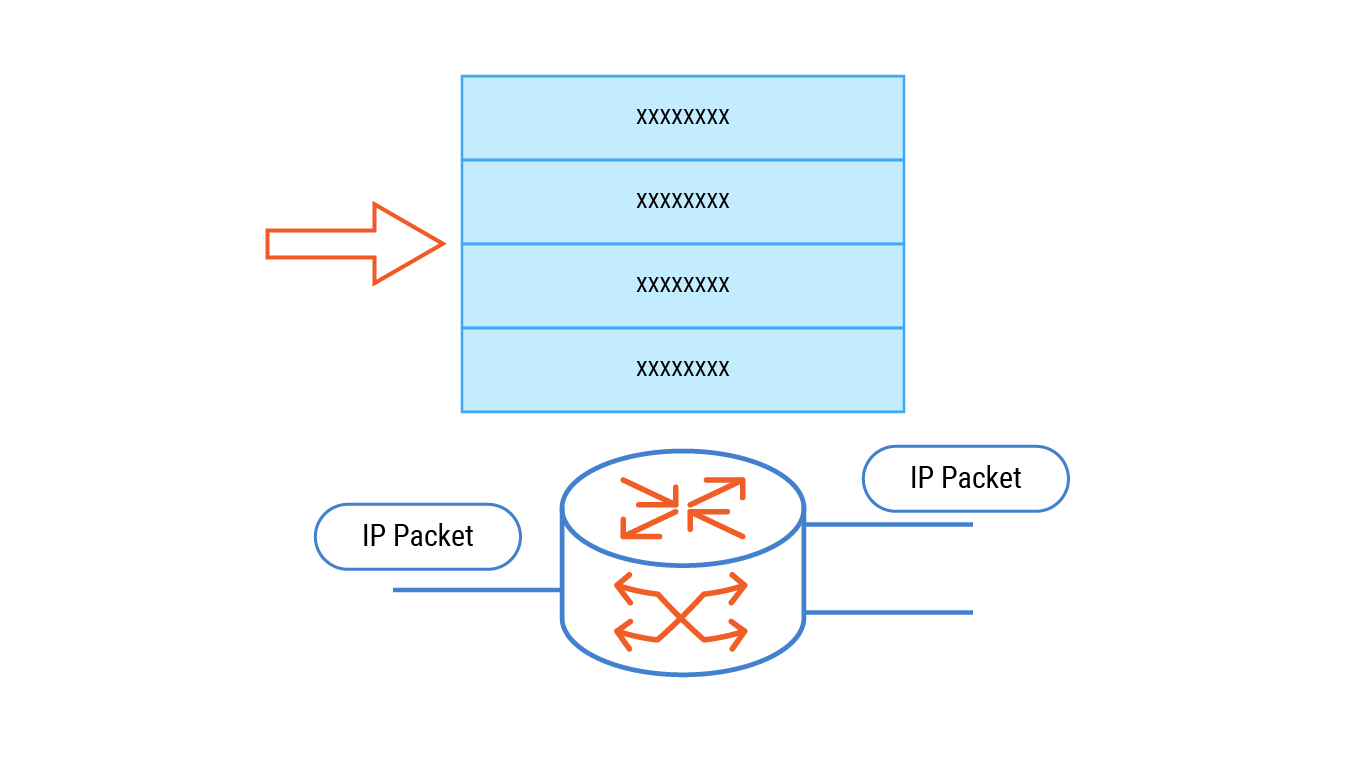
## 1.1. MPLS

### 1.1.1. Khái quát về MPLS

MPLS là gì? MPLS (Multiprotocol Label Switching) hoặc Chuyển mạch nhãn đa giao thức là công nghệ chuyển tiếp dữ liệu giúp tăng tốc và quản lý luồng lưu lượng mạng. Định tuyến lưu lượng thông qua các đường chuyển mạch nhãn để chuyển tiếp dữ liệu qua các mạng WAN riêng. MPLS mang lại độ bảo mật, tính linh hoạt cao, cung cấp QOS và các đường truyền tốt hơn so với định tuyến IP truyền thống. Chuyển mạch nhãn đa giao thức là công nghệ lý tưởng cho các doanh nghiệp cần kết nối liền mạch, đáng tin cậy cho các ứng dụng cần độ trễ tối ưu như VoIP và họp online.



MPLS có thể đóng gói nhiều giao thức mạng khác nhau, bao gồm IP, ATM, Frame Relay, SONET và Ethernet. Trong mạng Internet thông thường, các gói dữ liệu được truyền dưới dạng gói IP từ bộ định tuyến đến đích. Mỗi router phải tra cứu bảng định tuyến để xác định next-hop để chuyển tiếp packet đến đích. Trong khi đó, MPLS sử dụng label path để định tuyến packet thông qua mạng MPLS, giảm độ trễ và tăng tốc độ truyền tải dữ liệu. MPLS cung cấp chất lượng dịch vụ với tính linh hoạt cao, là công nghệ lý tưởng cho các doanh nghiệp cần kết nối liền mạch và đáng tin cậy cho các ứng dụng cần độ trễ tối ưu.



Chuyển đổi nhãn đa giao thức giúp giải quyết vấn đề tốc độ chuyển tiếp dữ liệu thông qua địa chỉ IP và bảng định tuyến. Phương pháp này sử dụng chuyển đổi nhãn để tạo một tuyến đường được hoạch định trước và kiểm soát lưu lượng mạng, giúp chuyển tiếp nhanh hơn.

Khi định tuyến, thiết bị đầu tiên sẽ xác định router đích và đường truyền để đi, gán một “nhãn” cho packet. Các router kế tiếp sẽ sử dụng label để định tuyến lưu lượng mà không cần tra cứu IP. Packet sẽ được truyền bằng định tuyến IP và gỡ bỏ label tại router cuối cùng.

MPLS là giao thức Lớp 2,5 nằm giữa Lớp 2 và Lớp 3 trong mô hình OSI.

### 1.1.2. Các thành phần trong MPLS

|  |  |
| --- | --- |
| **Thành phần** | **Chức năng** |
| LER (Label Edge Router) | Điểm vào/ra của mạng MPLS. Việc gắn nhãn (ingress) hoặc gỡ nhãn (egress) thực hiện tại node này. |
| LSR (Label Switch Router) | Router lõi trong mạng MPLS, chuyển tiếp gói tin bằng cách hoán đổi nhãn. |
| LSP (Label Switched Path) | Đường dẫn chuyển mạch nhãn được thiết lập sẵn trong mạng MPLS. |
| LFIB (Label Forwarding Information Base) | Bảng ánh xạ nhãn đầu vào với nhãn và cổng ra. |
| LDP (Label Distribution Protocol) | Giao thức phân phối ánh xạ nhãn giữa các router. |
| FEC (Forwarding Equivalence Class) | Nhóm các gói tin được xử lý và chuyển tiếp theo cùng một cách. |

### 1.1.3. Nguyên lý hoạt động của MPLS

* Phân loại gói tin

Khi gói tin vào mạng MPLS tại Ingress LER, nó được phân loại vào một FEC.

Ví dụ: Tất cả gói tin đến mạng 1.1.1.0/24 sẽ thuộc cùng một FEC.

* Gắn nhãn (Label)

Router biên (Ingress LER) gắn nhãn MPLS cho gói tin dựa trên FEC.

Nhãn này là một số 20-bit nằm giữa lớp 2 và lớp 3 (tức là giữa header Layer 2 và IP header).



* Chuyển tiếp theo nhãn

Các router trong lõi mạng MPLS (LSR/P routers) không cần kiểm tra địa chỉ IP.

Thay vào đó, chúng dùng bảng LFIB để:

Tra nhãn vào, sau đó

Thay nhãn mới (swap) và

Chuyển gói tin ra cổng phù hợp.

* Gỡ nhãn tại router thoát (Egress LER)

Khi gói tin đến router biên cuối (Egress), nhãn được gỡ bỏ.

Gói IP được chuyển tiếp như bình thường đến đích.

**Bảng nhãn sẽ được tạo như thế nào?**

Các router dùng LDP (Label Distribution Protocol) hoặc để phân phối nhãn.

Nhãn được gán cho các tuyến IP dựa trên bảng định tuyến (RIB) và lưu trong LIB (Label Information Base).

### 1.1.4. Ưu và nhược điểm của MPLS

* Ưu điểm

|  |  |
| --- | --- |
| **Ưu điểm** | **Chi tiết** |
| Chi phí | Tài nguyên mạng có thể được chia sẻ dễ dàng trong MPLS vì nó là công nghệ lớp 3. Bên cạnh đó, tất cả dữ liệu khách hàng có thể được định tuyến riêng bằng MPLS. |
| Khả năng mở rộng | Khả năng mở rộng là một tùy chọn có sẵn dễ dàng trong MPLS. Nó dễ dàng hơn nhiều so với các phương pháp khác. Theo nhu cầu, MPLS có thể được mở rộng lên và xuống. Ngay cả khi có một yêu cầu cho hàng ngàn trang web. |
| Hiệu quả | MPLS cung cấp các kết nối chất lượng cao hơn nhiều mà không bị mất gói và chập chờn. Sử dụng nó cùng với VoIP có thể dẫn đến tăng hiệu quả. Có nghĩa là có thể đạt được một hiệu suất nhất quán. |
| Độ tin cậy | Có nhiều tính năng làm cho MPLS đáng tin cậy. Vì MPLS sử dụng nhãn để chuyển tiếp các gói, nên có thể yên tâm rằng các gói sẽ được chuyển đến đúng đích. Hơn nữa, có thể ấn định lưu lượng mạng theo mức độ ưu tiên. |
| Băng thông | MPLS cho phép nhiều lưu lượng truy cập đi qua mạng. Ngoài ra, các phần khác nhau của băng thông có thể được gán cho nhiều kiểu dữ liệu khác nhau. Có nghĩa là băng thông được sử dụng tối ưu. Thông qua tất cả các phương tiện này, băng thông có thể được tăng lên. |

* Nhược điểm của MPLS

|  |  |
| --- | --- |
| Nhược điểm | Chi tiết |
| Bảo mật | Bảo mật của các giải pháp MPLS hoàn toàn nằm trong tay người dùng. Không có bất kỳ tính năng bảo mật cố hữu nào được cung cấp bởi nhà cung cấp MPLS. Tuy nhiên, bằng cách làm việc với nhà cung cấp, bạn có thể dễ dàng giảm thiểu các lỗ hổng và bảo vệ mạng ở một mức độ nào đó. |
| Bảo trì | Vì MPLS được quản lý thông qua các nhà cung cấp dịch vụ và khối lượng công việc ít hơn hiện diện trên mạng quản lý, nên việc bảo trì vẫn đòi hỏi nỗ lực đáng kể. Riêng các công việc bảo dưỡng chung không thể trực tiếp thực hiện. Việc bảo trì cần được thực hiện thông qua một ISP. Hiện đây không phải là một nhiệm vụ dễ dàng do một số hạn chế về tốc độ và sự phức tạp về kỹ thuật của ISP. |
| Kiểm soát | MPLS cũng thiếu khi nói đến toàn quyền kiểm soát mạng. Cấu hình do nhà cung cấp dịch vụ đảm nhận hoàn toàn. Quyền kiểm soát duy nhất mà người dùng có thông qua MPLS là định tuyến động. |
| Triển khai | Triển khai là một mối quan tâm lớn khi sử dụng MPLS. Nếu các văn phòng hiện diện trên các địa điểm khác nhau, nó có thể làm phức tạp quá trình. Thường mất nhiều thời gian thậm chí hàng tháng để kết nối tất cả các văn phòng. |
| Khả năng tiếp cận | MPLS không được tối ưu hóa cho các ứng dụng đám mây. Nó được sản xuất dành riêng cho kết nối điểm-điểm . Có nghĩa là không thể truy cập trực tiếp ứng dụng đám mây hoặc SaaS bằng MPLS. Mặc dù vậy, một số dịch vụ đám mây có thể truy cập được, nó đi kèm với thẻ giá. |

## 1.2. MPLS VPN L3

MPLS VPN hoạt động gần giống như MPLS nhưng được thêm tính năng VPN để tăng cường độ bảo mật giữ các site với nhau.

Nguyên lý hoạt động của MPLS: Dựa vào MPLS nguyên bản nhưng tăng cường tính bảo mật(VPN) để đảm bảo các vùng không nhận biết được địa chỉ của nhau người ta thêm vào đó VRF(Virtual Routing and Forwarding) riêng biệt cho từng khác hàng.

## 1.3. BGP

### 1.3.1. BGP là gì?

BGP, còn được gọi là Border Gateway Protocol, là giao thức định tuyến được sử dụng cho mạng Internet toàn cầu. BGP xác định các điều kiện mạng mới nhất để tìm ra đường đi tối ưu. Các điều kiện mạng này cập nhật khả năng tiếp cận và thông tin định tuyến giữa các router tại biên. BGP định tuyến lưu lượng và quản lý cách các tập tin được gửi giữa các hệ thống tự trị (AS) – các network quản lý bởi doanh nghiệp hoặc nhà mạng.

### 1.3.2. Autonomous System

Là một mạng IP lớn hoặc một nhóm mạng được điều hành bởi các nhà mạng có chính sách định tuyến thống nhất. Internet là một mạng của các mạng được tạo thành từ vô số Autonomous System nhỏ hơn. Mọi máy tính hoặc thiết bị kết nối Internet đều được kết nối với hệ thống tự trị.

Peering là cách các hệ thống tự trị giao tiếp và trao đổi lưu lượng mạng. Một phương pháp mà các hệ thống tự trị peering với nhau là thông qua các vị trí vật lý gọi là Điểm trao đổi Internet (IXP).

Các hệ thống mới liên tục xuất hiện trên Internet, trong khi các hệ thống cũ hơn thường không khả dụng. Vậy nên, mỗi Autonomous System phải duy trì thông tin về mọi tuyến đường mới lẫn cũ. Điều này được thực hiện thông qua các phiên peering. Trong các phiên peering, mỗi AS thiết lập kết nối TCP/IP với AS gần đó để trao đổi dữ liệu định tuyến. Autonomous System sử dụng thông tin này để định tuyến chính xác dữ liệu gửi đi.

Tùy thuộc vào doanh nghiệp và thỏa thuận peering, các hệ thống tự trị đôi khi tính phí lẫn nhau để chuyển lưu lượng truy cập qua mạng của họ. Chi phí truy cập có thể ảnh hưởng đến quyết định lựa chọn tuyến đường cuối cùng của BGP.

1.3.3. BGP hoạt động như thế nào?

Giao thức Border Gateway Protocol là cơ chế định tuyến lưu lượng truy cập qua Internet. Hầu hết các nhà mạng không có tuyến đường mặc định, mà chỉ có đường đi đến tất cả các tiền tố (prefix). BGP đánh giá các đường dẫn đến một tuyến đường nhất định và chọn đường tốt nhất giữa các router nhằm xác định đường dẫn tới tất cả các điểm đến.

Router không thể chọn mạng tối ưu để gửi dữ liệu khi có nhiều mạng liên kết với nó. Để truyền lưu lượng đến router gần đích nhất, BGP đánh giá tất cả các đối tác peering của router thông qua thông tin định tuyến của các đối tác peering. Thông tin định tuyến được lưu giữ trong Bảng định tuyến (RIB – Routing Information Base).

Mỗi router hoặc host lưu trữ một bảng RIB chứa thông tin về khoảng cách hoặc tuyến đường đến mạng đích để hỗ trợ kiểm soát hướng đi của các gói dữ liệu. RIB sử dụng dữ liệu từ cả các đối tác peering nội bộ lẫn đối tác bên ngoài. Các đối tác peering này đều kết nối trực tiếp với nhau. RIB liên tục cập nhật khi có các thay đổi dựa trên các chính sách về tuyến đường được sử dụng và thông tin công bố.

### 1.3.4. External BGP và internal BGP

Có hai loại BGP là external BGP (eBGP) và internal BGP (iBGP).

Các thiết bị hoặc mạng lân cận trong cùng một AS có thể sử dụng Internal BGP để định tuyến qua các mạng nội bộ. iBGP không giao tiếp với các AS khác vì quy trình chỉ xảy ra giữa hai đối tác peering nội bộ. Để liên kết các router trên mạng nội bộ, các AS có thể chọn từ các giao thức nội bộ khác.

External BGP là phần mở rộng của BGP. eBGP được sử dụng để truyền thông tin trao đổi giữa các AS riêng biệt. Điều này có nghĩa là BGP yêu cầu sử dụng các router biên (edge) để hai AS giao tiếp. Sử dụng eBGP KHÔNG yêu cầu cần sử dụng iBGP.

## 1.4. VRF

### 1.4.1. Định nghĩa

Virtual Routing and Forwarding (VRF) là một công nghệ trong bộ định tuyến mạng sử dụng giao thức Internet (IP), cho phép tạo ra nhiều bảng định tuyến riêng biệt hoạt động đồng thời trên cùng một bộ định tuyến. VRF phân tách các đường mạng thành từng phân đoạn riêng biệt mà không cần sử dụng thêm thiết bị vật lý. Vì thế, các luồng dữ liệu được tự động tách biệt, giúp tăng cường bảo mật cho mạng và giảm nhu cầu áp dụng các biện pháp mã hóa hoặc xác thực phức tạp.

Công nghệ VRF được các nhà cung cấp dịch vụ Internet (ISP) sử dụng để thiết lập các mạng riêng ảo (VPN) cho từng khách hàng, gọi là VPN Routing and Forwarding. Nhờ khả năng phân tách dữ liệu linh hoạt và bảo mật cao, VRF không chỉ đáp ứng nhu cầu quản lý mạng hiệu quả mà còn phù hợp với nhiều loại hình ứng dụng từ mạng doanh nghiệp đến dịch vụ công cộng.

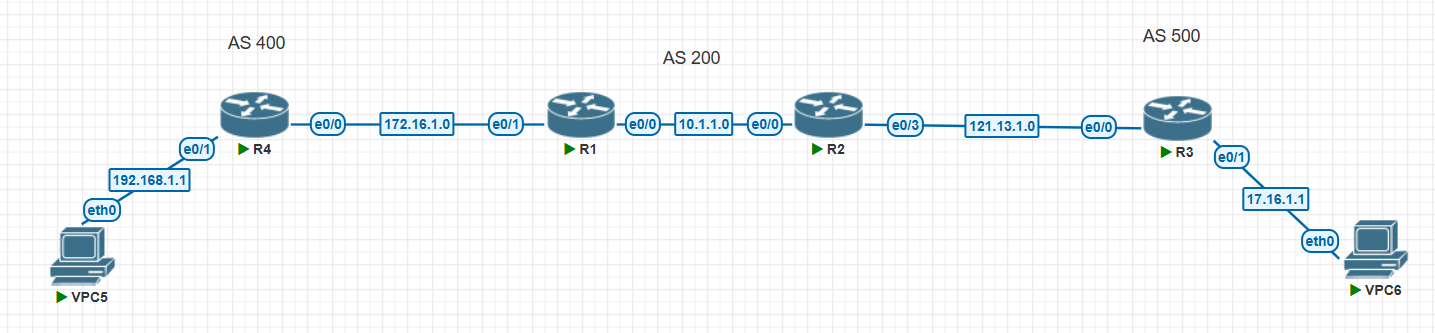
### 1.4.2. VRF động như thế nào?

VRF hoạt động như một bộ định tuyến logic nhưng khác với bộ định tuyến logic thông thường. Mỗi phiên bản VRF chỉ sử dụng một bảng định tuyến duy nhất để quản lý các đường đi cụ thể của dữ liệu, đảm bảo mỗi luồng dữ liệu được tách biệt hoàn toàn theo các phân đoạn mạng được thiết lập.

Để đảm bảo hoạt động, VRF cần có một bảng chuyển tiếp trong đó xác định điểm đến tiếp theo cho từng gói dữ liệu. Bảng này cũng liệt kê các thiết bị có thể tham gia chuyển tiếp dữ liệu và thiết lập các quy tắc cùng giao thức định tuyến để quản lý cách dữ liệu được truyền tải. Cơ chế này giúp VRF ngăn chặn lưu lượng truy cập không hợp lệ từ bên ngoài và đảm bảo rằng dữ liệu chỉ được truyền trong phạm vi đã được chỉ định.

# Chương 2. THỰC NGHIỆM

## 2.1. Cấu hình BGP



Ta có một mô hình mạng như sau: Yêu cầu thực hiện cấu hình BGP để 2 PC có thể ping tới nhau.

Đoạn từ R4 – R1 và R2 – R3 ta cấu hình eBGP

Đoạn từ R1 - R2 ta cấu hình iBGP bằng BGP,

Kết quả thực hiện ping giữ 2 PC

A screen shot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

## 2.2. Cấu hình MPLS VPN(BGP - VRF)

A diagram of a network of drones

AI-generated content may be incorrect.

Ta có mô hình mạng như sau: Yêu cầu router A và B chỉ kết nối riêng biệt.

Ta chỉ cấu hình BGP ở PE vì là kết nối trực tiếp tới CE,

Đoạn PE1 – P1 – P2 – PE2, ta cấu hình OSPF.

Còn CE ta cấu hình bằng static route.

Kết quả: hiện tại BGP giữa PE1 và PE2 vẫn chưa up dù đã ping được tới nhau.