

**ĐẠI HỌC QUỐC GIA HÀ NỘI  
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ**

**NGUYỄN VĂN TÂN**

**KỸ THUẬT ĐIỀU KHIỂN LƯU LƯỢNG MẠNG TRÊN  
HỆ THỐNG IP SỬ DỤNG CÔNG NGHỆ MPLS**

**LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN**

Hà Nội, 6/2018

**ĐẠI HỌC QUỐC GIA HÀ NỘI  
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ**

**NGUYỄN VĂN TÂN**

**KỸ THUẬT ĐIỀU KHIỂN LƯU LƯỢNG MẠNG TRÊN  
HỆ THỐNG IP SỬ DỤNG CÔNG NGHỆ MPLS**

Ngành: Công nghệ thông tin

Chuyên ngành: Truyền dữ liệu và mạng máy tính

Mã số:

**LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN**

**NGƯỜI HƯỚNG DẪN KHOA HỌC:**

**PGS.TS NGUYỄN ĐÌNH VIỆT**

Hà Nội – 6/2018

# LỜI CAM ĐOAN

Tôi xin cam đoan nội dung trình bày trong luận văn này là do tôi tự nghiên cứu tìm hiểu dựa trên các tài liệu và tôi trình bày theo ý hiểu của bản thân dưới sự hướng dẫn trực tiếp của Thầy Nguyễn Đình Việt. Các nội dung nghiên cứu, tìm hiểu và kết quả thực nghiệm là hoàn toàn trung thực.

Luận văn này của tôi chưa từng được ai công bố trong bất cứ công trình nào.

Trong quá trình thực hiện luận văn này tôi đã tham khảo đến các tài liệu của một số tác giả, tôi đã ghi rõ tên tài liệu, nguồn gốc tài liệu, tên tác giả và tôi đã liệt kê trong mục “TÀI LIỆU THAM KHẢO” ở cuối luận văn.

Học viên

Nguyễn Văn Tân

# LỜI CẢM ƠN

Để hoàn thành luận văn, trước hết tôi xin chân thành cảm ơn các thầy, cô giáo đã tận tình hướng dẫn, giảng dạy tôi trong suốt quá trình học tập, nghiên cứu tại Khoa Công Nghệ Thông Tin - Trường Đại học Công Nghệ - Đại học quốc gia Hà Nội.

Đặc biệt, xin chân thành cảm ơn thầy giáo PGS.TS Nguyễn Đình Việt đã hướng dẫn tận tình, chu đáo giúp tôi hoàn thành luận văn này.

Mặc dù có nhiều cố gắng để thực hiện song với kiến thức, kinh nghiệm bản thân, chắc chắn không thể tránh khỏi thiếu sót chưa thấy được. Tôi rất mong nhận được đóng góp của các thầy, cô, bạn bè, đồng nghiệp để luận văn được hoàn thiện hơn.

Hà Nội, tháng 6 năm 2018

Học viên

Nguyễn Văn Tân

# MỤC LỤC

LỜI CAM ĐOAN .....	1
LỜI CẢM ƠN .....	1
MỤC LỤC .....	1
DANH MỤC CÁC KÝ HIỆU VÀ CHỮ VIẾT TẮT.....	1
DANH MỤC HÌNH VẼ.....	2
LỜI MỞ ĐẦU .....	1
<b>Chương 1: Công nghệ chuyển mạch nhãn đa giao thức.....</b>	<b>2</b>
<b>1.1 Tổng quan .....</b>	<b>2</b>
<b>1.2 Kiến trúc mạng MPLS.....</b>	<b>2</b>
1.2.1 Miền MPLS (MPLS Domain) .....	2
1.2.2 Bộ định tuyến chuyển mạch nhãn (LSR-Label Switching Router) [3] .....	3
1.2.3 FEC (Forwarding equivalence class) [3].....	3
1.2.4 Giao thức phân bố nhãn (LDP-Label Distribution Protocol) .....	4
1.2.5 Đường chuyển mạch nhãn (LSP-Label Switch Path) [3] .....	5
1.2.6 Nhãn .....	6
1.2.7 Ngăn xếp nhãn.....	7
1.2.8 Cơ sở dữ liệu nhãn (Label Information Base – LIB).....	7
1.2.9 Bảng chuyển tiếp mạch nhãn (LFIB – Label Forwarding Information Base).....	7
1.2.10 Hoán đổi nhãn (Label Swapping).....	7
1.2.11 Mặt phẳng chuyển tiếp và mặt phẳng điều khiển.....	7
1.2.12 Thuật toán chuyển tiếp nhãn (Label Forwarding Algorithm) .....	8
<b>1.3 Phương thức hoạt động .....</b>	<b>8</b>
1.3.1 Các thao tác nhãn .....	9
1.3.2 Hoạt động cơ bản của mạng MPLS.....	11
1.3.3 Chế độ hoạt động.....	13
<b>1.4 Các ứng dụng của MPLS .....</b>	<b>17</b>
<b>1.5 Tổng kết .....</b>	<b>17</b>
<b>Chương 2: Kỹ thuật điều khiển lưu lượng MPLS TE .....</b>	<b>18</b>
<b>2.1 Giới thiệu về Traffic Engineering và MPLS Traffic Engineering .....</b>	<b>18</b>
2.1.1 Traffic Engineer là gì?.....	18
2.1.2 Cơ bản về Kỹ thuật lưu lượng trong MPLS .....	18
<b>2.2 Hoạt động của Kỹ thuật lưu lượng trong MPLS .....</b>	<b>18</b>
2.2.1 Sự phân phối thông tin Traffic Engineering.....	18

2.2.2	Điều kiện với IGP.....	19
2.2.3	Mở rộng OSPF với Traffic Engineering.....	20
2.2.4	Flood bởi IGP.....	20
2.2.5	Cơ chế định tuyến và cost của TE LSP .....	21
2.2.6	Thuộc tính của link Traffic Engineering .....	21
2.2.7	Các thuộc tính của MPLS TE tunnel.....	22
<b>2.3</b>	<b>Cách tính toán đường đi của Traffic Engineering.....</b>	<b>22</b>
2.3.1	Path setup option .....	22
2.3.2	Setup và holding priority.....	23
2.3.3	PCALC – Path Calculation .....	23
2.3.4	Resource Reservation Protocol (RSVP – Giao thức dành trước tài nguyên).....	24
<b>2.4</b>	<b>Chuyển tiếp lưu lượng vào MPLS – TE tunnel.....</b>	<b>27</b>
2.4.1	Static Routing.....	27
2.4.2	Policy – Base Routing.....	27
2.4.3	Autoroute announce. ....	27
2.4.4	Forwarding adjacency .....	28
2.4.5	Class-based tunnel selection.....	28
<b>2.5</b>	<b>Bảo vệ và phục hồi .....</b>	<b>28</b>
2.5.1	Path Protection .....	28
2.5.2	Fast Reroute (FRR) .....	28
<b>2.6</b>	<b>Tổng kết .....</b>	<b>32</b>
<b>Chương 3: Thiết lập thử nghiệm mạng MPLS-TE trên thiết bị mạng thật.....</b>		<b>33</b>
<b>3.1</b>	<b>Mục đích.....</b>	<b>33</b>
<b>3.2</b>	<b>Phương pháp thực hiện .....</b>	<b>33</b>
<b>3.3</b>	<b>Mô hình thực thể.....</b>	<b>33</b>
3.3.1	So sánh hội tụ giữa hệ thống mạng sử dụng MPLS-TE và IP thuần.....	33
3.3.2	Kết hợp QoS đảm bảo chất lượng dịch vụ và cấp phát băng thông động.....	35
<b>3.4</b>	<b>Môi trường thực nghiệm .....</b>	<b>39</b>
<b>Chương 4: Kết luận .....</b>		<b>41</b>
<b>4.1</b>	<b>Vấn đề đặt ra .....</b>	<b>41</b>
<b>4.2</b>	<b>Ứng dụng của MPLS-TE.....</b>	<b>41</b>
<b>4.3</b>	<b>Kết quả đạt được.....</b>	<b>41</b>
<b>4.4</b>	<b>Đề xuất cải tiến .....</b>	<b>41</b>



# DANH MỤC CÁC KÝ HIỆU VÀ CHỮ VIẾT TẮT

ATM	Asynchronous Transfer Mode	Chế độ truyền dẫn không đồng bộ
CEF	Cisco Express Forwarding	Chuyên tiếp với mục đích riêng biệt của Cisco
CR-LDP	Constrained Routing-LDP	Định tuyến cưỡng bức-LDP
DLCI	Data Link Connection Identifier	Nhận dạng kết nối liên kết dữ liệu
EGP	Edge Gateway Protocol	Giao thức định tuyến công biên
FEC	Forwarding Equivalent Class	Lớp chuyển tiếp tương đương
FR	Frame Relay	Chuyên tiếp khung
IETF	Internet Engineering Task Force	Nhóm tác vụ kỹ thuật Internet
IGP	<i>Interior Gateway Protocol</i>	Giao thức công nội bộ
IP	Internet Protocol	Giao thức Internet
LDP	Label Distribution Protocol	Giao thức phân bổ nhãn
LER	Label Edge Router	Router biên nhãn
LIB	Label Information Base	Cơ sở thông tin nhãn
LSP	Label Switched Path	Đường dẫn chuyển mạch nhãn
LSR	Label Switch Router	Router chuyển mạch nhãn
MPLS	Multiprotocol Label Switching	Chuyển mạch nhãn đa giao thức
OSPF	Open Shortest Path First	Giao thức đường đi ngắn nhất đầu tiên
QoS	Quality of Service	Chất lượng dịch vụ
RFC	Request For Comment	Bản yêu cầu ý kiến của IETF
TCP	Transmission Control Protocol	Giao thức điều khiển truyền dẫn
TE	Traffic Engineering	Kỹ thuật lưu lượng
TTL	Time To Live	Thời gian sống
UDP	User Datagram Protocol	Giao thức lược đồ dữ liệu
VPN	Virtual Private Network	Mạng riêng ảo
WAN	Wide Area Network	Mạng diện rộng



# DANH MỤC HÌNH VẼ

Hình 1.1: Miền MPLS. ....	2
Hình 1.2: Upstream và downstream LSR.....	3
Hình 1.3: Vùng hoạt động của LDP. ....	4
Hình 1.4: Giao thức LDP với các giao thức khác. ....	5
Hình 1.5: Cấu trúc của nhãn MPLS .....	6
Hình 1.6: Ngăn xếp nhãn.....	7
Hình 1.7: Kiến trúc một nút MPLS .....	8
Hình 1.8: Điều khiển độc lập.....	9
Hình 1.9: Điều khiển theo yêu cầu. ....	10
Hình 1.10: Các ánh xạ hỗ trợ vận chuyển. ....	11
Hình 1.11: Hoạt động của MPLS. ....	12
Hình 1.12: Phân phối nhãn trong chế độ khung MPLS.....	14
Hình 1.13: Chuyển tiếp gói tin trong chế độ khung MPLS.....	14
Hình 1.14: Tiến trình truyền TTL IP sang nhãn.....	16
Hình 2.1: RSVP cho TE và nhãn.....	25
Hình 2.2: Thuộc tính Session .....	26
Hình 2.3: Sự quảng bá của RSVP PATH và RESV .....	26
Hình 2.4: RSVP SE Style .....	27
Hình 2.5: Link Protection .....	29
Hình 2.6: Vận chuyển lưu lượng khi link protection chưa active .....	30
Hình 2.7: Vận chuyển lưu lượng khi link protection đã active .....	30
Hình 2.8: Node Protection .....	31
Hình 2.9: Node Protection Active .....	32
Hình 3.1: Mô hình chi tiết cho cấu hình mô phỏng MPLS TE .....	33
Hình 3.2: Mô hình đo thời gian hội tụ giữa MPLS-TE và IP.....	34
Hình 3.3: Máy đo truyền lưu lượng vào hệ thống mạng .....	34
Hình 3.4: Bảng định tuyến để thấy Site 1 qua Site 2 bằng định tuyến IP .....	34
Hình 3.5: Kết quả hội tụ mạng IP thuần trên máy đo.....	35
Hình 3.6: Bảng định tuyến để thấy Site 1 qua Site 2 bằng định tuyến MPLS-TE .....	35
Hình 3.7: Kết quả hội tụ mạng MPLS-TE trên máy đo .....	35
Hình 3.8: Mô hình đo QoS cấp băng thông động và đảm bảo chất lượng dịch vụ .....	36

Hình 3.9: Bảng định tuyến thể hiện đường đi VoIP và Data qua MPLS-TE.....	36
Hình 3.10: Cấu hình QoS cấp băng thông động và độ ưu tiên.....	37
Hình 3.11: Bảng thông luồng VoIP và Data truyền vào mạng.....	37
Hình 3.12: Băng thông VoIP tăng lên khi VoIP cần lấy lại băng thông.....	38
Hình 3.13: Băng thông Data giảm xuống khi VoIP cần lấy lại băng thông.....	38
Hình 3.14: Độ rớt gói của VoIP và Data khi đường truyền nghẽn.....	39
Hình 3.15: Công ty SVTech.....	39
Hình 3.16: Phòng LAB thiết bị mạng.....	40
Hình 3.17: Không gian làm việc của kỹ sư SVTech.....	40

# LỜI MỞ ĐẦU

Ngày nay hầu hết các dịch vụ Viễn thông, Công nghệ Thông tin đều sử dụng hạ tầng mạng IP để truyền tải, đòi hỏi chất lượng dịch vụ truyền tải phải đảm bảo tốc độ nhanh, không bị gián đoạn dịch vụ. Công nghệ IP là một công nghệ đã được sử dụng rộng rãi và hiệu quả ngay từ khi mạng Internet mới ra đời, nhưng cũng có những hạn chế nhất định, thí dụ: chưa thể đáp ứng được đòi hỏi cao về tốc độ chuyển mạch, khả năng hội tụ mạng thấp, vì vậy một công nghệ mới ra đời là MPLS (Multiprotocol Label Switching), công nghệ chuyển mạch nhãn đa giao thức cùng với các kỹ thuật điều khiển lưu lượng để đảm bảo tốc độ chuyển mạch nhanh, tối ưu đường đi lưu lượng mạng.

Với các nhà cung cấp dịch vụ Viễn thông, công nghệ thông tin lớn, việc đảm bảo chất lượng dịch vụ, tối ưu lưu lượng mạng luôn là một vấn đề lớn, được đề cập và xử lý xuyên suốt quá trình cung cấp dịch vụ cho người dùng. Công nghệ MPLS với kỹ thuật điều khiển lưu lượng (MPLS – TE Traffic Engineering) sẽ đáp ứng được các nhu cầu về tốc độ truyền tải cao, điều chỉnh lưu lượng mạng theo nhu cầu để tối ưu hệ thống mạng, đảm bảo độ hội tụ về dịch vụ để giảm thiểu gián đoạn thông tin nhỏ nhất có thể.

Đề tài này sẽ phân tích những giải pháp của kỹ thuật MPLS – TE để giải quyết các vấn đề về tối ưu tài nguyên mạng (bằng kỹ thuật điều khiển hướng đi lưu lượng), giảm thời gian gián đoạn thông tin nhỏ nhất (bằng các cơ chế bảo vệ, chuyển mạch lưu lượng khi có sự cố mạng), đảm bảo chất lượng dịch vụ cho các ứng dụng quan trọng (bằng việc kết hợp QoS trong MPLS – TE).

Báo cáo được tổ chức thành 4 chương với nội dung chính như sau:

- ❖ Chương 1: Công nghệ chuyển mạch nhãn đa giao thức: Giới thiệu các khái niệm cơ bản, các thành phần kiến trúc, cơ chế hoạt động cơ bản của công nghệ chuyển mạch nhãn MPLS.
- ❖ Chương 2: Kỹ thuật điều khiển lưu lượng MPLS-TE.
- ❖ Chương 3: Thiết lập thử nghiệm mạng MPLS-TE trên thiết bị mạng thật: Thực hiện cấu hình thử nghiệm các tình huống về MPLS-TE trên thiết bị mạng thật.
- ❖ Chương 4: Kết luận.

# Chương 1: Công nghệ chuyển mạch nhãn đa giao thức

## 1.1 Tổng quan

Công nghệ chuyển mạch nhãn đa giao thức ra đời để cải thiện tốc độ chuyển mạch gói tin trong mạng, nhằm đảm bảo chất lượng dịch vụ.

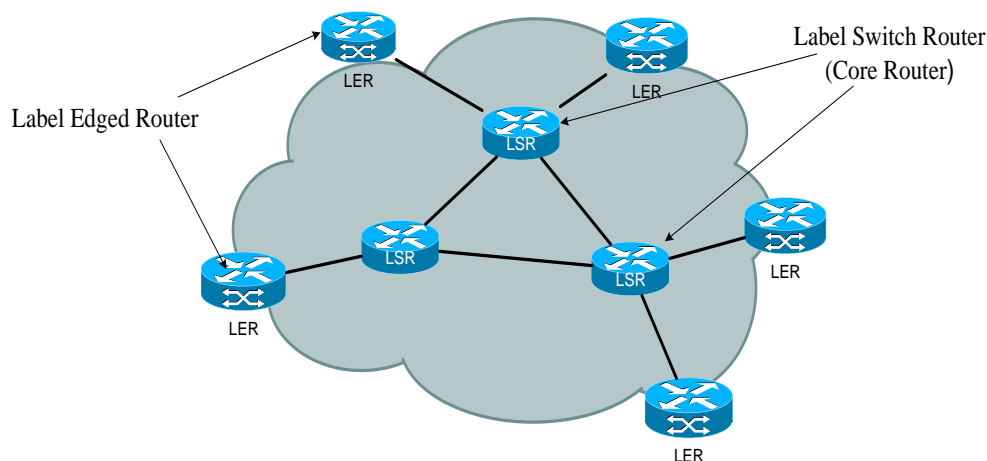
Chuyển mạch nhãn đa giao thức sử dụng nhãn gán vào mỗi gói tin để chuyển tiếp trong mạng, nhãn MPLS hoạt động ở giữa chuyển mạch lớp 2 và định tuyến lớp 3. Nhãn được gán cho mỗi gói tin IP và quảng bá giữa các thiết bị router trong mạng, mỗi router xây dựng một bảng nhãn để xác định hướng chuyển tiếp gói tin. MPLS sử dụng bảng nhãn và cơ chế hoán đổi nhãn để chuyển tiếp gói tin, không sử dụng địa chỉ IP đích. Công nghệ MPLS áp dụng cho cả các hệ thống mạng sử dụng ATM, Frame Relay.

- ❖ **MPLS là công nghệ chuyển mạch nhanh được Cisco phát triển và IETF chuẩn hóa.**
- ❖ **Kết hợp giữa chuyển mạch Layer 2 và định tuyến Layer 3.**
- ❖ **Hỗ trợ tất cả các giao thức IP và non-IP.**
- ❖ **Sử dụng nhãn để chuyển tiếp gói tin.**
- ❖ **MPLS được ứng dụng chủ yếu ở mạng của ISP.**

## 1.2 Kiến trúc mạng MPLS

### 1.2.1 Miền MPLS (MPLS Domain)

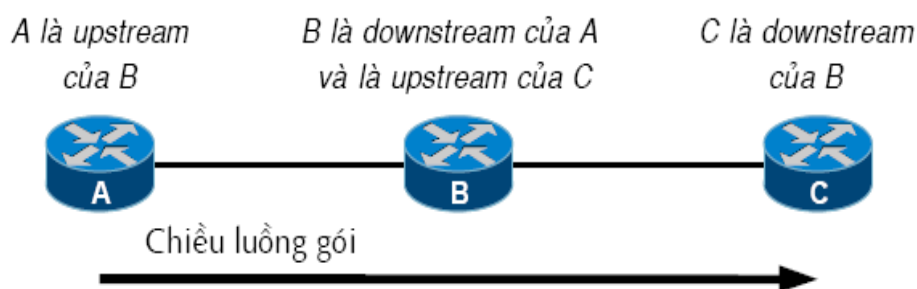
Là tập hợp toàn bộ các nút mạng chạy MPLS trong cùng một hệ thống mạng.



Hình 1.1: Miền MPLS.

[5] Miền MPLS gồm có 2 phần: Phần lõi (core) và phần biên (edge). Các nút mạng trong miền MPLS là các router chuyển mạch nhãn LSR (Label Switch Router). Các nút mạng phần lõi là core-LSR, các nút mạng biên là LER (Label Edge Router).

Nếu một LER là đầu vào của luồng dữ liệu thì được gọi là ingress-LER, còn nếu là đầu ra của luồng dữ liệu thì được gọi là egress-LER, như vậy một LER vừa có thể là ingress-LER vừa là egress-LER tùy theo luồng lưu lượng.



Hình 1.2: Upstream và downstream LSR.

Upstream-LSR (ingress-LSR) là luồng gói tin vào và downstream-LSR (egress-LSR) là luồng gói tin ra.

### 1.2.2 Bộ định tuyến chuyển mạch nhãn (LSR-Label Switching Router) [3]

LSR (Label Switching Router) là thiết bị thực hiện quá trình chuyển gói dữ liệu trong mạng bằng kỹ thuật chuyển mạch nhãn: gỡ nhãn cũ và gắn nhãn mới cho gói.

Cấu trúc cơ bản của một thiết bị LSR có hai thành phần chính : thành phần điều khiển (control component) còn được gọi là mặt phẳng điều khiển (control component) và thành phần định tuyến (forwarding component), còn được gọi là thành phần dữ liệu (data component).

Mặt phẳng điều khiển sử dụng các giao thức định tuyến IP để xây dựng nên bảng định tuyến. Từ những thông tin này, thành phần điều khiển sẽ tiến hành quá trình ấn định nhãn với các nút mạng lân cận.

Thành phần chuyển tiếp (forwarding component) sử dụng thông tin của quá trình này để tạo bảng cơ sở thông tin nhãn LIB (Label Information Based). Khi nhận được gói dữ liệu, LSR sẽ sử dụng giá trị nhãn của gói và bảng định tuyến nhãn để tìm ra và gắn một giá trị nhãn mới thích hợp cho gói dữ liệu.

#### LSR rìa

Có hai loại : Ingress LSR và Egress LSR. Cấu trúc của Edge LSR có đôi chút khác biệt so với LSR.

Gói dữ liệu khi đến Ingress LSR là gói dữ liệu IP truyền thống. Căn cứ vào thông tin trong tiêu đề IP và bảng định tuyến nhãn LIB, LSR sẽ ấn định một giá trị nhãn thích hợp cho gói dữ liệu và chuyển nó đến LSR tiếp theo.

Nhiệm vụ của Egress LSR thì ngược lại. Egress LSR gỡ bỏ nhãn cuối cùng của gói dữ liệu và từ đây gói dữ liệu sẽ được định tuyến như một gói IP thông thường.

Trong cấu trúc Egress LSR, thành phần chuyển tiếp (forwarding component) có thêm bảng định tuyến IP. Với thành phần này, Edge LSR có thể định tuyến các gói dữ liệu IP truyền thống.

### 1.2.3 FEC (Forwarding equivalence class) [3]

FEC là một nhóm hay một luồng gói tin được chuyển tiếp trên cùng một tuyến đường, tất cả các gói tin cùng FEC sẽ được gắn cùng một nhãn giống nhau.

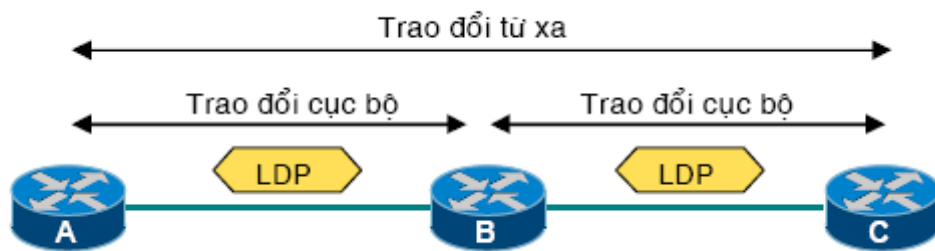
Thiết bị ingress-LER sử dụng một số đặc điểm sau để xác định các gói tin cùng FEC:

- Địa chỉ IP đích thuộc cùng lớp mạng (cùng NetID).
- Các gói tin Multicast thuộc cùng một địa chỉ Multicast.
- Địa chỉ IP đích thuộc bảng định tuyến của giao thức BGP, có chung BGP next-hop.

#### 1.2.4 Giao thức phân bố nhãn (LDP-Label Distribution Protocol)

##### Khái niệm về LDP

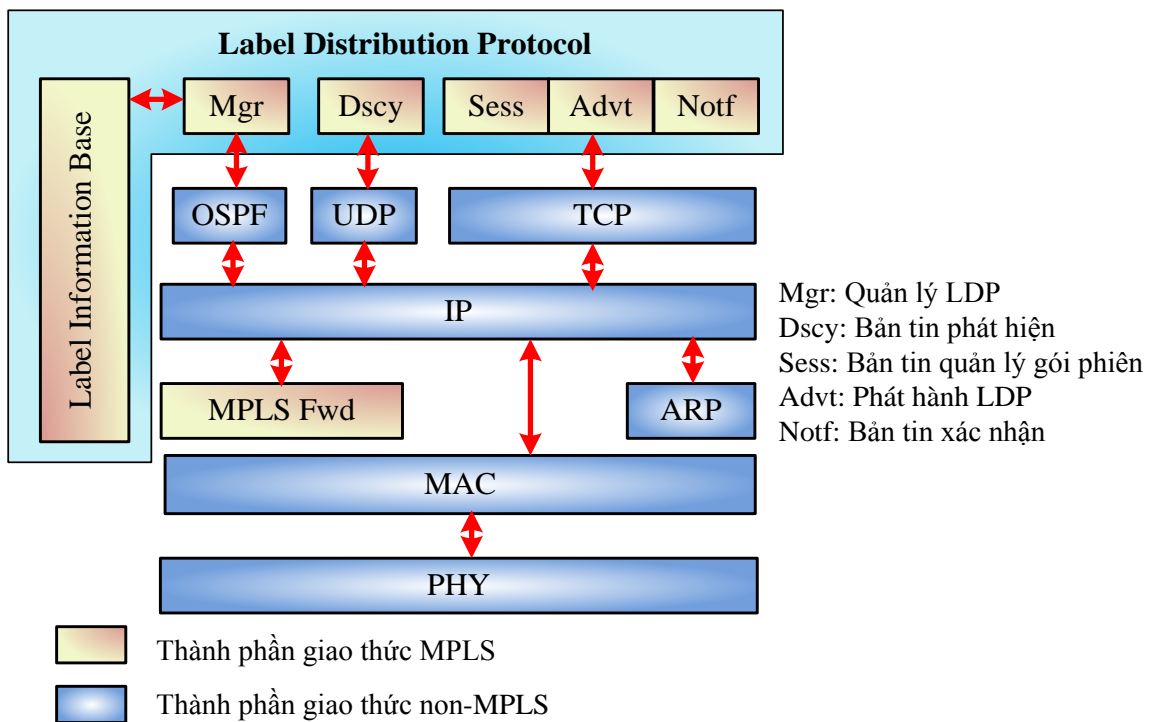
Giao thức phân phối nhãn được sử dụng để gán nhãn cho các gói tin và phân phối nhãn giữa các thiết bị thuộc cùng miền MPLS, bao gồm nhiều bản tin tra đổi để các thiết bị mạng sử dụng nhãn chuyển tiếp gói tin.



Hình 1.3: Vùng hoạt động của LDP.

Giao thức phân phối nhãn LDP có các đặc trưng cơ bản sau đây:

- LDP sử dụng bản tin Hello để tìm kiếm và thiết lập neighbor giữa các thiết bị kết nối trực tiếp nhau trong miền MPLS.
- Ngoài bản tin Hello để thiết lập neighbor sử dụng giao thức UDP thì LDP sử dụng giao thức TCP để đảm bảo độ tin cậy của các bản tin.
- Sơ đồ thiết lập LDP:



Hình 1.4: Giao thức LDP với các giao thức khác.

### [3] Các bản tin LDP

Có tổng cộng 11 bản tin LDP: Notification, Hello, Initialization, KeepAlive, Address, Address Withdraw, Label Mapping, Label Request, Label Abort Request, Label Withdraw, Label Release:

**Dạng bản tin Initialization:** Bản tin được gửi ban đầu để trao đổi và thiết lập kết nối giữa 2 LSR. Các LSR nhận được sẽ trả lời KeepAlive nếu đáp ứng được các tham số trao đổi, nếu không đáp ứng được thì LSR sẽ trả lời thông báo có lỗi và kết thúc phiên.

**Dạng bản tin KeepAlive:** Bản tin KeepAlive gửi định kỳ theo thời gian người quản trị cấu hình để các LSR thông báo với neighbor là vẫn đang hoạt động, nếu sau thời gian trên mà các LSR không nhận được bản tin KeepAlive của một LSR nào đó thì các LSR sẽ xác định LSR đó không còn tồn tại và loại bỏ khỏi neighbor.

**Dạng bản tin Label Mapping:** Bản tin Label Mapping được sử dụng để quảng bá nhãn trong miền MPLS, bản tin được sử dụng khi có cập nhật mới trong mạng, hoặc khi có sự thay đổi định tuyến.

**Dạng bản tin Label Withdraw:** Bản tin này được sử dụng để xóa bỏ nhãn không còn tồn tại do thay đổi định tuyến hoặc lỗi kết nối, thông báo cho các LSR biết liên kết không còn sử dụng được cho tuyến đường của các FEC.

**Dạng bản tin Label Request:** Yêu cầu nút mạng nhận dữ liệu của FEC nào đó với nhãn được xác định.

**Dạng bản tin Label Release:** Được sử dụng khi LSR nhận thấy nút mạng tiếp theo không còn chuyển tiếp được gói tin trong tuyến đường của FEC nữa.

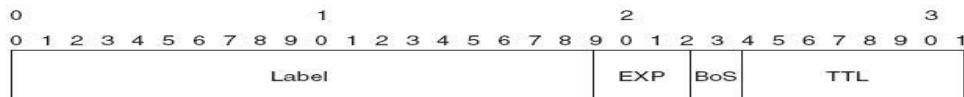
### 1.2.5 Đường chuyển mạch nhãn (LSP-Label Switch Path) [3]

Đường chuyển mạch nhãn này được thiết lập từ ingress LSR đến Egress LSR để chuyển gói trong mạng bằng kỹ thuật chuyển mạch nhãn. Các LSP được thiết lập từ thông tin định tuyến IGP hay từ sự lựa chọn con đường đến đích tốt nhất của định tuyến IGP.

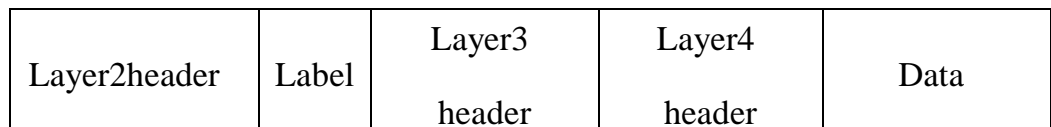
### 1.2.6 Nhãn

[3] Một nhãn MPLS có độ dài 32 bit cố định với cấu trúc xác định.

Nhãn được chèn thêm vào giữa chuyển mạch lớp 2 và định tuyến lớp 3.



#### Shimheader



Hình 1.5: Cấu trúc của nhãn MPLS

#### Các trường thông tin trong nhãn MPLS:

- *Trường nhãn (label field)*: Bao gồm 20 bit đầu, bit 0 đến 15 sử dụng cho các ứng dụng đặc biệt, bit từ 16 sử dụng cho không gian nhãn.
- *Trường EXP - experimental*: Gồm 3 bit từ 20 đến 22. Trường này được sử dụng trong QoS trên nền MPLS, đánh dấu các giá trị QoS cho các luồng dữ liệu để phân biệt và áp dụng các chính sách đảm bảo chất lượng dịch vụ trong miền MPLS.
- *Trường ngăn xếp (stack field)*: chỉ có 1 bit thứ 23. Bit này có giá trị là 1 khi đây là nhãn cuối cùng trong ngăn xếp, giá trị là 0 khi đây là các nhãn khác trong ngăn xếp. sử dụng ngăn xếp nhãn để ứng dụng cho các trường hợp cần nhiều hơn một nhãn (như ứng dụng VPN trong MPLS).
- *Trường TTL (Time to live TTL)*: Gồm 8 bit từ 24 đến 31, có chức năng như ở trong IP header, giảm đi 1 khi đi qua một nút mạng. Được sử dụng để tránh vòng lặp gói tin trong mạng, khi TTL giảm về 0 mà gói tin chưa tới đích thì gói tin này sẽ bị hủy bỏ để tránh vòng lặp trong mạng.

#### Các loại nhãn đặc biệt [2]

- *Untagged*: Gói tin đến nút Edge LSR và thực hiện bóc nhãn để chuyển thành gói tin IP và chuyển đến đích.
- *Nhãn Implicit-null hay POP*: Nhãn này được nút Edge LSR gán và quảng bá cho nút LSR kế cận, khi gói tin đến nút LSR kế cận này sẽ bóc nhãn và chuyển



gói tin IP đến nút Edge LSR.

- *Nhãn Explicit-null*: Nhãn này được nút Edge LSR gán và quảng bá cho nút LSR kế cận, có giá trị bằng 0, nhằm giữ giá trị EXP trong miền MPLS đến tận nút Edge LSR để xử lý QoS cho gói tin.
- *Nhãn Aggregate*: Khi gặp nhãn này LSR sẽ bóc hết nhãn trong ngăn xếp của gói tin để còn mỗi IP và tìm kiếm trong bảng định tuyến IP để chuyển tiếp gói tin.

### 1.2.7 Ngăn xếp nhãn

[3]

Có những ứng dụng cần nhiều hơn một nhãn để chuyển tiếp gói tin trong mạng MPLS (ví dụ ứng dụng VPN). Trường ngăn xếp trong nhãn hỗ trợ việc này. Nhãn đầu tiên trong ngăn xếp là nhãn đỉnh có giá trị bit là 0, nhãn cuối cùng là nhãn đáy có giá trị bit là 1, các nhãn còn lại trong ngăn xếp có giá trị bit là 0.

Label	EXP	0	TTL
Label	EXP	0	TTL
...			
Label	EXP	1	TTL

Hình 1.6: Ngăn xếp nhãn

### 1.2.8 Cơ sở dữ liệu nhãn (Label Information Base – LIB)

Là bảng chứa thông tin dữ liệu phân phối nhãn trong miền MPLS của các nút mạng. Bảng LIB là cơ sở để xây dựng nên bảng chuyển tiếp gói tin dựa vào thông tin nhãn. [2]

### 1.2.9 Bảng chuyển tiếp mạch nhãn (LFIB – Label Forwarding Information Base)

Bảng chứa dữ liệu thông tin nhãn đầu vào, nhãn đầu ra, công ra của gói tin trên các LSR, phục vụ cho việc hoán đổi nhãn chuyển tiếp gói tin trong miền MPLS. [2]

### 1.2.10 Hoán đổi nhãn (Label Swapping)

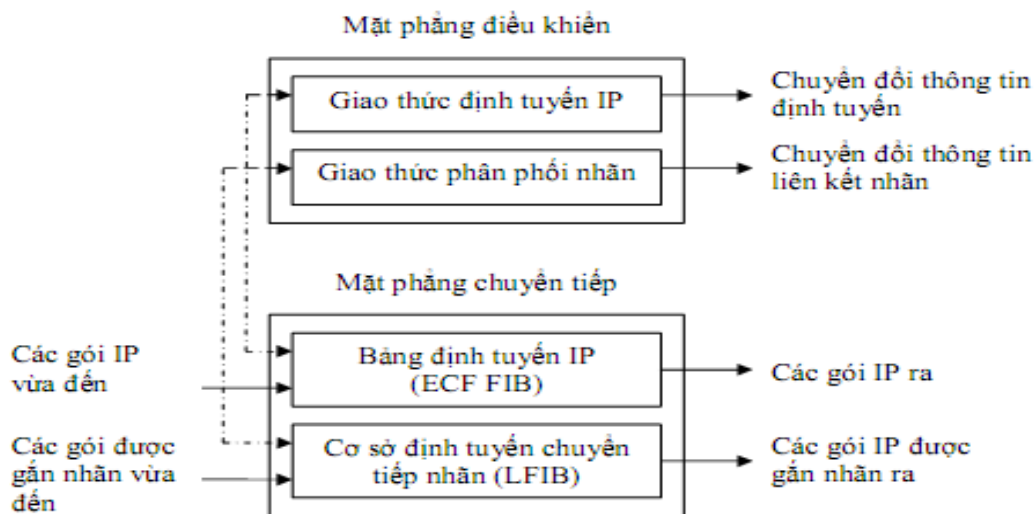
[2]

Khi gói tin đến LSR thì LSR dựa vào nhãn đầu vào để ánh xạ vào bảng LFIB tìm thông tin nhãn đầu ra, công ra, sau đó thực hiện hoán đổi nhãn để chuyển gói tin đi.

Chuyển tiếp gói chưa có nhãn được thực hiện ở ingress-LER, LER dựa vào bảng FIB xác định hướng chuyển tiếp gói tin sau đó dựa vào bảng LFIB để gán nhãn cho gói tin và chuyển đến nút LSR kế cận.

### 1.2.11 Mặt phẳng chuyển tiếp và mặt phẳng điều khiển

Một nút LSR trong miền MPLS có hai mặt phẳng: mặt phẳng chuyển tiếp và mặt phẳng điều khiển:



Hình 1.7: Kiến trúc một nút MPLS

### **Mặt phẳng chuyển tiếp (Forwarding plane) [5]**

Mặt phẳng chuyển tiếp sử dụng bảng LFIB để hoán đổi nhãn và chuyển tiếp gói tin tới đầu ra. Mặt phẳng chuyển tiếp được xây dựng từ mặt phẳng điều khiển, cụ thể để xây dựng bảng LFIB cần phải có thông tin phân phối nhãn trong bảng LIB.

### **Mặt phẳng điều khiển (Control Plane) [5]**

Mặt phẳng điều khiển chịu trách nhiệm xây dựng thông tin phân phối nhãn. Để thực hiện thì trong miền MPLS cần chạy một giao thức định tuyến kiểu link-state để quảng bá các dải IP trong mạng, xây dựng nên bảng RIB (Routing Information Base), từ thông tin bảng RIB hệ thống mạng chạy giao thức phân phối nhãn (LDP) để học thông tin nhãn của các IP trong bảng RIB. Dựa vào thông tin trong bảng RIB LSR xây dựng nên bảng chuyển tiếp gói tin IP (FIB – Forwarding Information Base) và sự kết hợp giữa bảng LIB và bảng FIB sẽ xây dựng nên được bảng LFIB để thực hiện hoán đổi nhãn chuyển tiếp gói tin trong miền MPLS.

### **1.2.12 Thuật toán chuyển tiếp nhãn (Label Forwarding Algorithm)**

[3]

Các LSR sử dụng thuật toán hoán đổi nhãn để chuyển tiếp gói tin. LSR dựa vào giá trị nhãn đầu vào (input lable), ánh xạ vào bảng LFIB để tìm kiếm và thay thế input lable bằng nhãn ra (outgoing lable), gửi qua giao tiếp cổng ra tương ứng đến nút LSR kế tiếp đã được xác định.

Các thuật toán chuyển tiếp thông thường (IP) sử dụng nhiều thông tin trong IP header để xác định thông tin chuyển tiếp gói tin, MPLS chỉ dùng một thuật toán chuyển tiếp dựa trên sự hoán đổi nhãn (Label swapping). LSR chỉ truy xuất bộ nhớ đơn để lấy ra các thông tin cần thiết để chuyển tiếp gói, như vậy MPLS có khả năng chuyển tiếp gói tin nhanh hơn.

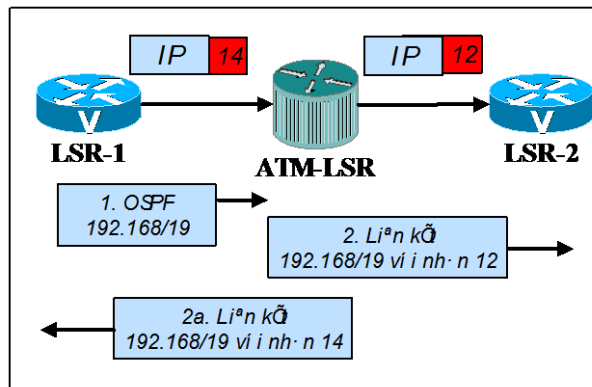
### **1.3 Phương thức hoạt động**

### 1.3.1 Các thao tác nhãn

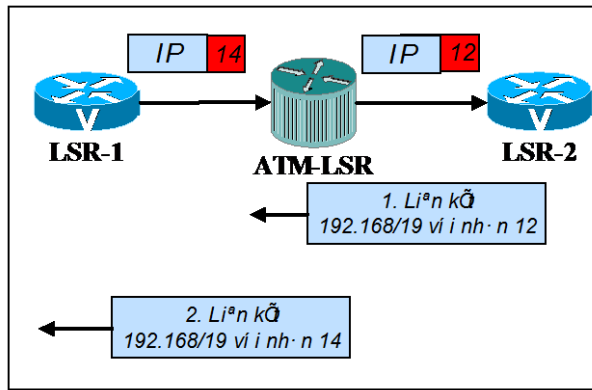
**Liên kết nhãn (Label binding):** là thủ tục liên kết một nhãn với một FEC. Quá trình liên kết nhãn được thực hiện bởi downstream LSR. Giá trị của nhãn có thể là duy nhất trong một giao diện (per - interface) hoặc duy nhất trong tất cả các giao diện của LSR (per - platform). Sau đó, downstream LSR thông báo cho upstream LSR về liên kết mới được tạo ra.

**Điều khiển gán nhãn (Label Control):** để thực hiện chuyển tiếp gói tin qua mạng chuyển mạch nhãn đa giao thức, nhãn được gán và phân phối trong các node mạng MPLS, MPLS hỗ trợ hai kiểu điều khiển gán nhãn vào lớp chuyển tiếp tương đương FEC: điều khiển gán nhãn độc lập và theo yêu cầu. Hai ví dụ dưới đây mô tả kiểu điều khiển này. Hình 1.8 và hình 1.9.

Trên hình 1.8, LSR-1 sử dụng OSPF để phát hành tiền tố địa chỉ 192.168/19 tới ATM-LSR, sau khi nhận được phát hành này LSR-ATM độc lập gán nhãn vào trong luồng FEC và phát hành địa chỉ nhãn này tới các LSR lân cận, các nhãn là các nhãn rỗng lấy được lấy ra từ ngăn xếp nhãn. Ưu điểm cơ bản của phương pháp này là các nhãn được gán chỉ khi có phát hành địa chỉ, giả thiết là mạng có độ hội tụ định tuyến nhanh (các bảng định tuyến trong miền định tuyến ổn định và đồng bộ với các bộ định tuyến khác) thì bước liên kết gán nhãn được thực hiện rất nhanh. Tuy nhiên, các bộ định tuyến chuyển mạch nhãn phải thiết lập thỏa thuận với các LSR lân cận về lớp chuyển tiếp tương đương sẽ sử dụng. Nếu quyết định khác với lớp chuyển tiếp tương đương, hoặc một số lớp chuyển tiếp tương đương không có các đường dẫn chuyển mạch nhãn liên kết với chúng, thậm chí có nhưng chúng không khả dụng thì quá trình gán nhãn không được đảm bảo.



Hình 1.8: Điều khiển độc lập.



Hình 1.9: Điều khiển theo yêu cầu.

Phương pháp điều khiển gán nhãn theo yêu cầu đảm bảo chắc chắn rằng tất cả các LSR trên đường dẫn chuyên mạch nhãn sử dụng cùng FEC được khởi tạo gán nhãn. Mặt hạn chế của phương pháp này là thời gian thiết lập LSP, một số quan điểm cho rằng phương pháp này có vẻ kém hiệu quả, một số khác lại cho rằng phương pháp điều khiển gán nhãn theo yêu cầu sẽ hỗ trợ rất tốt cho vấn đề định tuyến ràng buộc. Trên thực tế, công nghệ chuyển mạch nhãn đa giao thức MPLS thực hiện cả hai phương pháp trên.

**Ngăn xếp nhãn (Label Stack):** để hỗ trợ khả năng phân cấp nhằm đáp ứng sự mở rộng của mạng, MPLS cho phép một gói tin có thể mang nhiều nhãn. Các nhãn này được xếp liền nhau theo cấu trúc dữ liệu ngăn xếp tức là vào trước ra sau. Bit S sẽ chỉ ra nhãn đó có phải là nhãn cuối cùng (đáy ngăn xếp) của gói tin hay không. Do vậy, có ba thao tác liên quan đến nhãn là: push, pop, và đổi nhãn (swap). Các thao tác xử lý nhãn chỉ quan tâm đến nhãn nằm trên cùng của ngăn xếp. Ngăn xếp nhãn cho phép nhiều thành phần điều khiển tác động lên một gói tin, và các thành phần này ít hoặc không phụ thuộc vào nhau.

**Việc tạo ngăn xếp nhãn phải tuân theo các quy tắc sau:** khi một LSR đẩy một nhãn vào một gói tin đã được gán nhãn sẵn thì nhãn mới phải tương ứng với FEC mà LSR đầu ra đã gán nhãn ban đầu. Như vậy, tại LSR đầu ra của LSP, phải thực hiện hai lần tra bảng: một lần cho nhãn cần pop và một lần cho nhãn còn lại. Để tăng hiệu quả hoạt động, MPLS đưa ra khái niệm nút ngay sát LSR đầu ra (Penultimate Hop) thực hiện thao tác pop nhãn ra khỏi ngăn xếp và gửi gói tin đến LSR đầu ra. Tại LSR đầu ra, chỉ cần thực hiện một thao tác tra bảng. Mục đích của việc pop tại nút áp chót là để mỗi LSR chỉ thực hiện một lần tra bảng.

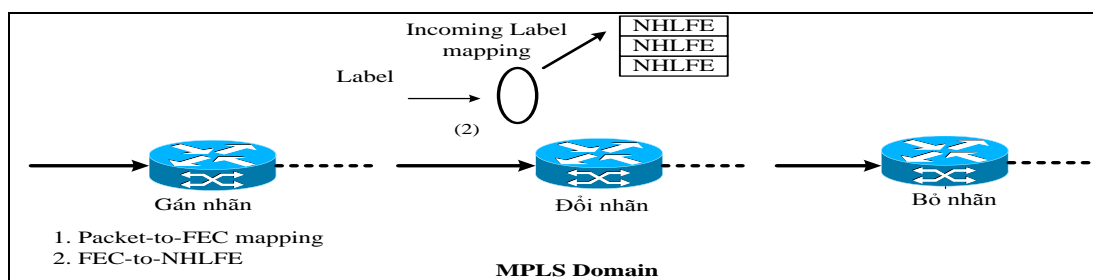
**Các ánh xạ và bảng hỗ trợ:** Các bảng và ánh xạ được sử dụng để hỗ trợ sự phối hợp hoạt động của nhãn đến và nhãn đi, cũng như việc quản lý ngăn xếp nhãn. Chuyển nhãn đến nút tiếp theo (NHLFE - Next Hop Label Forwarding Entry) được sử dụng để quản lý một gói tin đã được gán nhãn. Nó bao gồm các thông tin sau: Nút tiếp theo (next hop) của gói tin và nhãn mới (outing label) hoặc push/pop đối với ngăn xếp nhãn.

Ngoài ra, còn có thể có các thông tin về đóng gói dữ liệu ở tầng datalink, thông tin về chính sách quản lý gói tin. Có thể có nhiều NHLFE cùng tồn tại cho một FEC trong bảng chuyển tiếp.

**Ánh xạ ILM (Incoming Label Map):** ánh xạ mỗi nhãn đầu vào thành một tập hợp các NHLFE. Nhãn ở trên cùng của ngăn xếp được sử dụng làm chỉ mục của ánh xạ để tìm ra một tập hợp các NHLFE, dựa vào các thông tin này, LSR sẽ xử lý các nhãn của gói tin đó rồi mới chuyển tiếp gói tin đi.

**Ánh xạ FTN (FEC-To-NHLFE Map):** ánh xạ mỗi FEC ứng với một tập hợp NHLFE. Quá trình này được thực hiện đối với các gói tin chưa được gán nhãn, những gói tin này sẽ được gán nhãn trước khi chuyển đến nút tiếp theo trong mạng.

Các ánh xạ này được minh họa trong hình 1.10. Tại biên mạng, gói tin được phân tích phần tiêu đề và ánh xạ vào một FEC. Tiếp đó, FEC được ánh xạ để tìm ra NHLFE rồi vận chuyển gói tin vào trong mạng. Tại mỗi node trong mạng, các nhãn được ánh xạ thành NHLFE để xác định cách quản lý gói tin rồi được chuyển đến node tiếp theo.



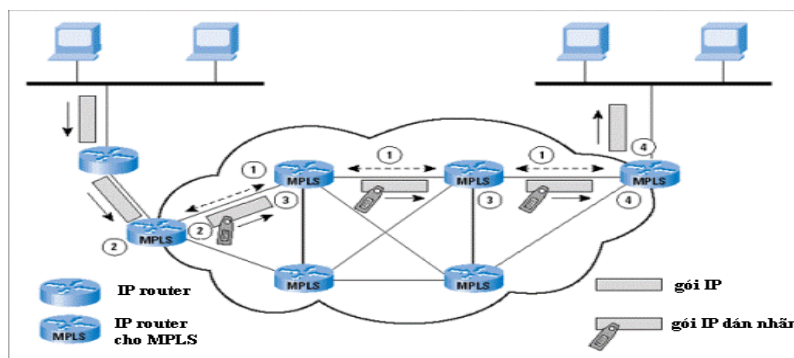
Hình 1.10: Các ánh xạ hỗ trợ vận chuyển.

**Trộn nhãn (Label merging):** Nhiều gói đến với các nhãn khác nhau và cùng đi ra một giao diện để đến node tiếp theo có thể được LSP gán chung một nhãn. Sau khi các gói được gán chung một nhãn, thông tin về các gói đến từ các giao diện khác nhau với các nhãn khác nhau bị mất đi. Do vậy, vấn đề cần phải phối hợp hoạt động giữa các LSR có khả năng trộn và LSR không có khả năng này.

Quy tắc của hoạt động trộn nhãn là khá đơn giản: nếu LSR hỗ trợ khả năng trộn nhãn thì chỉ cần gửi một nhãn cho FEC, nếu LSR không hỗ trợ khả năng trộn nhãn thì phải gửi một nhãn cho mỗi FEC, nếu một upstream LSR không hỗ trợ khả năng trộn nhãn thì nó phải yêu cầu một nhãn cho một FEC.

### 1.3.2 Hoạt động cơ bản của mạng MPLS

MPLS thực hiện bốn bước như minh họa trong hình 1.11 để chuyển gói qua một miền MPLS.



Hình 1.11: Hoạt động của MPLS.

**Bước 1- Báo hiệu:** Với bất kỳ loại lưu lượng nào vào mạng MPLS, các bộ định tuyến sẽ xác định một liên kết giữa một nhãn ứng với mức ưu tiên FEC của loại lưu lượng đó. Sau khi thực hiện thủ tục liên kết nhãn như trên, mỗi bộ định tuyến sẽ tạo các mục trong bảng cơ sở dữ liệu thông tin nhãn (LIB- Label Information Base). Tiếp đó, MPLS thiết lập một đường chuyển mạch nhãn LSP và các tham số về QoS của đường đó. Để thực hiện bước 1, cần phải có hai giao thức để trao đổi thông tin giữa các bộ định tuyến là:

- Giao thức định tuyến bên trong một miền để trao đổi các thông tin về đường đi.
- Giao thức phân phối nhãn: Các nhãn phải được gán cho các gói ứng với FEC của nó. Vì giá trị của nhãn chỉ mạng tính cục bộ giữa hai bộ định tuyến liền kề nhau nên cần phải có cơ chế đảm bảo, xuyên suốt các bộ định tuyến trên cùng LSP, thống nhất về việc liên kết giá trị nhãn với FEC. Như vậy, cần có một giao thức dùng để xác định đường và phân phối nhãn giữa các LSR.

**Bước 2 - Dán nhãn (push):** Khi một gói đến LER đầu vào, LER sau khi xác định các tham số QoS sẽ phân gói này vào một loại FEC, tương ứng với một LSP nào đó. Sau đó, LER gán cho gói này một nhãn phù hợp vào chuyển tiếp gói dữ liệu vào trong mạng. Nếu LSP chưa có sẵn thì MPLS phải thiết lập một LSP mới như ở bước 1.

**Bước 3 - Vận chuyển gói dữ liệu:** Sau khi đã vào trong mạng MPLS, tại mỗi LSR, gói dữ liệu sẽ được xử lý như sau:

- Bỏ nhãn các gói đến và gán cho gói đó một nhãn mới ở đầu ra (đổi nhãn).
- Chuyển tiếp gói dữ liệu đến LSR kế tiếp dọc theo LSP.

**Bước 4 - Tách nhãn (pop):** LER ở đầu ra sẽ cắt bỏ nhãn, phân tích tiêu đề IP (hoặc xử lý nhãn tiếp theo trong stack) và vận chuyển gói dữ liệu đó đến đích.

Vài đặc điểm chính trong hoạt động của MPLS

- Một miền MPLS (MPLS domain) bao gồm các bộ định tuyến hỗ trợ MPLS đặt liền tiếp nhau và liên tục.
- FEC cho một gói được xác định bằng một hoặc nhiều tham số do người quản trị mạng chỉ định.

- Cơ chế chuyển tiếp của MPLS được thực hiện bằng cách tra cứu trong một bảng đã định nghĩa trước (ánh xạ giữa các giá trị nhãn và các địa chỉ của hop tiếp theo). Trong một mạng IP, mỗi bộ định tuyến đều phải phân tích tiêu đề của gói IP, dài và phức tạp, sau đó đưa ra quyết định định tuyến với địa chỉ IP đích. Đơn giản hơn, MPLS chỉ cần đọc giá trị nhãn ngắn và độ dài cố định, sau đó chuyển tiếp gói đó theo giá trị có sẵn trong bảng LIB.
- Một PHB (per-hop-behavior) có thể được xác định ở mỗi LSR cho một FEC nào đó. PHB xác định mức ưu tiên khi xếp hàng của gói tương ứng với FEC và chính sách hủy gói (khi nghẽn mạch)
- Các gói tin được gửi có thể có cùng LER vào và ra nhưng có thể khác nhau FEC. Vì vậy, chúng được đánh nhãn khác nhau, được xử lý theo PHB khác nhau ở các LSR, và có thể được vận chuyển qua mạng theo các LSP khác nhau.

Ba khái niệm cơ bản của MPLS là FEC, LSP và nhãn. Phần quan trọng nhất trong MPLS chính là quan hệ hoạt động của ba thành phần này. Về cơ bản, MPLS phân các lưu lượng thành các loại FEC. Lưu lượng thuộc một FEC sẽ được chuyển qua miền MPLS theo một đường LSP. Từng gói dữ liệu sẽ được xem như thuộc một FEC bằng việc sử dụng các nhãn cục bộ. Như vậy, MPLS sẽ có một số yêu cầu sau:

- Lưu lượng vào mạng phải thuộc một FEC tương ứng.
- Cần phải có một giao thức định tuyến để xác định cấu trúc cũng như tình trạng hoạt động hiện thời của mạng, dựa vào thông tin đó, một LSP có thể được gán cho một FEC. Như vậy, giao thức định tuyến phải có khả năng thu thập và sử dụng thông tin để hỗ trợ các yêu cầu QoS của FEC.
- Một LSR phải biết rõ LSP cho một FEC, phải dành một nhãn đến cho LSP đó và phải thông báo nhãn đó cho các LSR khác gửi gói thuộc FEC này.

### 1.3.3 Chế độ hoạt động

Có hai chế độ hoạt động đối với MPLS: chế độ hoạt động khung ( Frame-mode) và chế độ tế bào ( Cell-mode ).

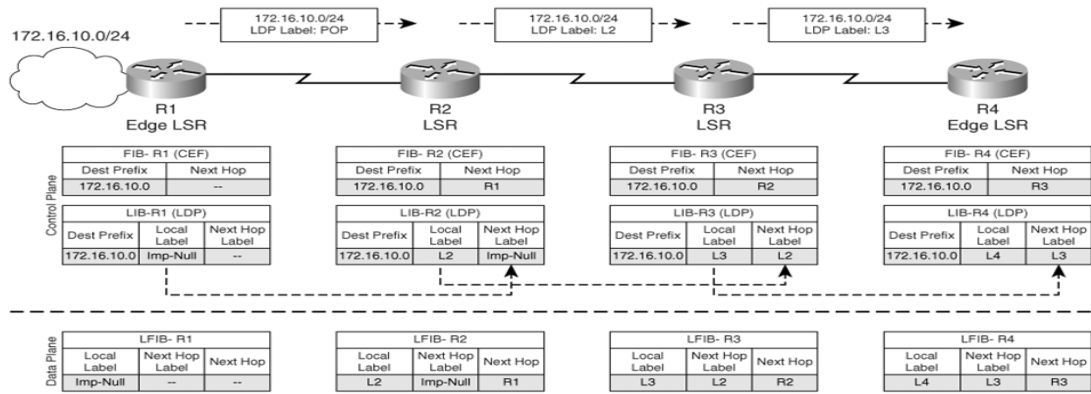
#### **Chế độ khung [2]**

Cơ chế này được ứng dụng cho mạng IP thông thường. Mặt phẳng điều khiển sẽ đảm nhiệm vai trò gán và phân phối nhãn, xây dựng các cơ sở dữ liệu nhãn, mặt phẳng chuyển tiếp sẽ thực hiện hoán đổi nhãn để chuyển tiếp gói tin.

#### **Hoạt động của chế độ khung MPLS**

Hình 1.12 cho thấy sự cấp và phân phối nhãn trong chế độ khung MPLS như thế nào. Trong hình gồm có 2 router LSR rìa, R1 và R4, kết nối với 2 router LSR, R2 và R3. Sau khi IGP hội tụ và thiết lập phiên LDP, các LSR gán một nhãn cho mạng 172.16.10.0/24 và quảng bá nhãn này ngược dòng, như miêu tả trong hình 1.12. Vì

vậy, các thành phần trong kiến trúc điều khiển và kiến trúc dữ liệu như FIB, LFIB, và LIB, thì được quảng bá với các giá trị tương ứng, như trong hình 1.12.

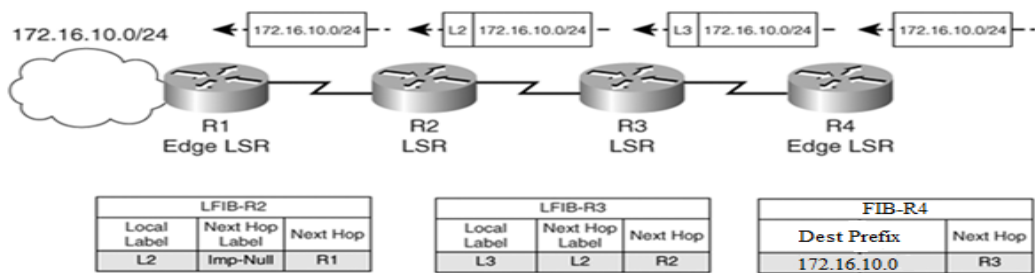


Hình 1.12: Phân phối nhãn trong chế độ khung MPLS

Như mô tả trong hình 1.12, LSR rìa R1 gán một nhãn cục bộ implicit-null (hoặc pop) và quảng bá đến LSR ngược dòng R2. Các LSR R2 và R3 gán các nhãn cục bộ L2 và L3, một cách lần lượt cho mạng 172.16.10.0 và quảng bá chúng theo ngược dòng. Phân phối nhãn có thể là phân phối dòng xuống theo yêu cầu hoặc phân phối dòng xuống không theo yêu cầu, chỉ khác biệt ở điểm phân phối nhãn theo yêu cầu, LSR ngược dòng yêu cầu một nhãn cho một mạng đích.

Sau khi cấp phát và phân phối nhãn, các thành phần FIB, LIB, LFIB thì như mô tả trong hình 1.12 được tham chiếu đến tiến tố mạng 172.16.10.0.

Chuyển tiếp một gói dữ liệu đến đích 172.16.10.0 trong miền MPLS thì được đưa ra trong hình 1.12. LSR R4 gán nhãn L3 (nhãn cho chặng kế tiếp khi nó được học từ LSR xuôi dòng) và chuyển tiếp gói tin mang nhãn đến LSR xuôi dòng LSR R3. R3 thực hiện một hoán đổi nhãn với nhãn đầu vào L3 thành nhãn đầu ra L2. Trên R2, nhãn đầu vào L2 được ánh xạ đến một nhãn implicit-null. Vì vậy LSR R2 loại bỏ nhãn trên cùng (L2) và chuyển gói tin IP sau khi gỡ nhãn đến LSR rìa R1, như biểu diễn trong hình 1.13.



Hình 1.13: Chuyển tiếp gói tin trong chế độ khung MPLS

### Ngăn vòng lặp trong chế độ khung MPLS

Các giao thức phân phối nhãn, như LDP và TDP, phần lớn dựa vào kỹ thuật chống vòng lặp được cung cấp bởi IGP được thực thi trong miền MPLS. Tuy nhiên, để tránh vòng lặp vô tận của các gói trong miền MPLS, trường TTL trong tiêu đề nhãn được sử dụng. Chức năng của trường TTL trong tiêu đề nhãn cũng giống với trường TTL trong



tiêu đề IP. Giá trị TTL là một số nguyên từ 0 đến 255, và được giảm dần sau mỗi lần gói tin đi qua một router hoặc một LSR.

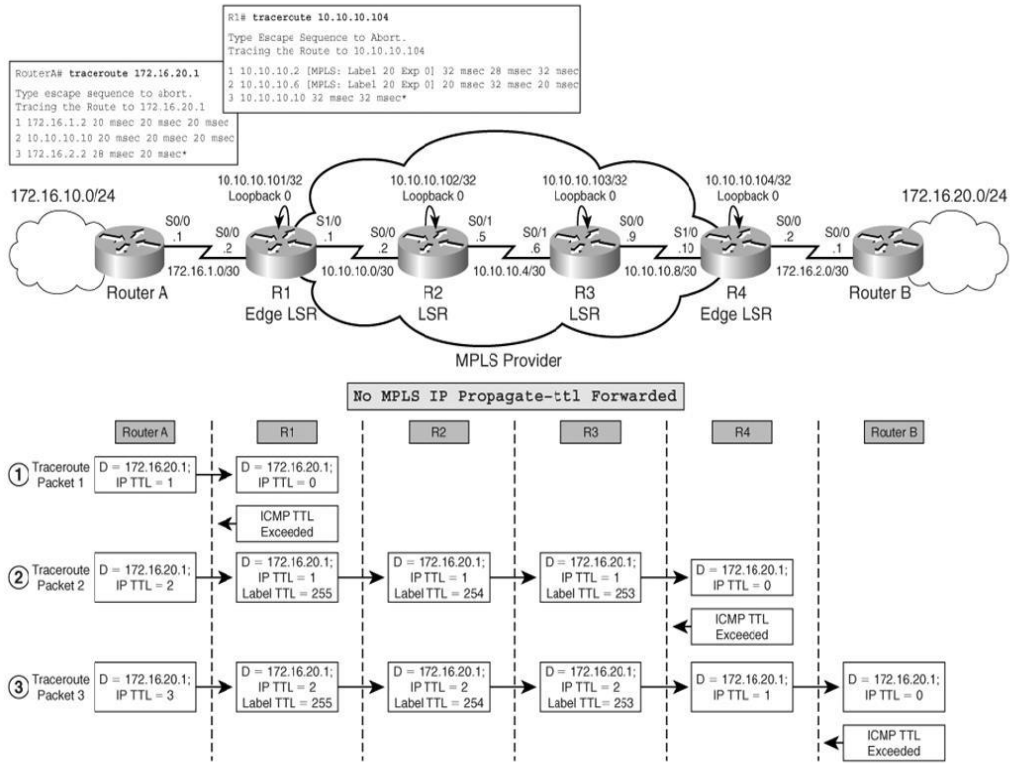
Khi giá trị TTL của một gói tin IP trở về 0, router sẽ huỷ bỏ gói tin IP, và một thông điệp ICMP được khởi tạo thông báo “TTL đã hết hạn” để gửi đến địa chỉ nguồn của gói tin IP. Kỹ thuật này ngăn chặn gói tin IP không bị định tuyến tiếp khi rơi vào vòng lặp. Tiến trình thực hiện tương tự với giá trị TTL của nhãn.

Khi một gói tin IP đi vào vùng chuyển mạch nhãn, router có chức năng như LSR rìa sẽ sao chép giá trị TTL từ tiêu đề gói tin IP gắn vào giá trị TTL của nhãn. Khi gói tin mang nhãn gặp một LSR, giá trị TTL trong nhãn bị giảm một đơn vị. Tiến trình này tiếp diễn cho đến khi gói tin mang nhãn được chuyển đổi trở về gói tin IP thuần túy tại LSR rìa trong vùng MPLS, và giá trị TTL trong nhãn sẽ được sao chép trở lại trường TTL trong tiêu đề gói tin IP. Tiến trình này gọi là truyền TTL IP sang nhãn.

Tiến trình này có thể bị vô hiệu trong vùng MPLS. Khi tiến trình này tắt, giá trị TTL IP sẽ không sao chép sang giá trị TTL trong nhãn, và thay vào đó giá trị 255 được ghi vào trường TTL trong nhãn.

Hình 1.14 cho một ví dụ về trường hợp tiến trình truyền TTL IP sang nhãn bị vô hiệu. Những trình tự sau lần lượt xảy ra khi một lệnh **traceroute** được thực thi trên router A đến router B trong vùng MPLS:

1. Router A gửi một gói traceroute đến mạng địa chỉ 172.16.20.1 với một giá trị TTL IP là 1. Khi gói tin này được nhận bởi router R1 (LSR rìa), giá trị TTL bị giảm trở về 0 và một thông điệp ICMP TTL quá độ được gửi về nguồn.
2. Router A gửi một gói tin traceroute đến địa chỉ 172.16.20.1 với giá trị TTL IP là 2. Router R1 nhận gói tin này và giảm giá trị TTL IP đi 1. Bởi vì tiến trình truyền TTL từ IP sang nhãn đã bị vô hiệu nên giá trị TTL IP không chép sang giá trị TTL nhãn. Gói tin được chuyển mạch nhãn từ R1 với giá trị TTL trong nhãn là 255. Router R2 và router R3 chuyển tiếp gói tin đi đến đích nhưng chỉ giảm giá trị TTL trong nhãn mà không giảm giá trị TTL IP. Tại router R4, giá trị TTL IP của gói tin bị giảm về 0 và một thông điệp ICMP TTL quá độ được gửi về nguồn.
3. Router A gửi một gói tin traceroute đến địa chỉ 172.16.20.1 với giá trị TTL IP là 3. Router R1 nhận gói tin này và giảm giá trị TTL IP về 2 và chuyển mạch nhãn gói tin với giá trị TTL trong nhãn là 255 đến R2. Router R2 và R3 giảm giá trị TTL trong nhãn. Tại router R4 giá trị TTL IP của gói tin bây giờ bị giảm đi 1. Router R4 chuyển tiếp gói tin đến router R3, nơi mà giá trị TTL IP bị giảm về 0 và một thông điệp ICMP TTL quá độ được gửi về nguồn.



Hình 1.14: Tiến trình truyền TTL IP sang nhãn

## **Chế độ tế bào [2]**

Khi sử dụng liên kết ATM giữa các thiết bị, MPLS áp dụng các tế bào, không phải các khung. Các tế bào được sử dụng để chuyển tiếp thông tin mặt phẳng dữ liệu. Khi các nhãn ATM được sử dụng trong một mạng MPLS lõi, chế độ hoạt động của MPLS được gọi là chế độ tế bào MPLS.

Trong chế độ tế bào MPLS, các LSR trong mạng lõi MPLS là các chuyển mạch ATM, chuyển tiếp dữ liệu dựa trên tiêu đề ATM. Nếu ATM LSR chỉ có chức năng chuyển mạch ATM thuần túy (mặt phẳng dữ liệu), một thành phần điều khiển bên ngoài được gọi là bộ điều khiển chuyển mạch nhãn (LSC) cần có để phổ biến thông tin thành phần điều khiển. Trong vài trường hợp, LSR ATM có khả năng quảng bá thông tin thành phần điều khiển cùng với thông tin thành phần dữ liệu, vì thế sẽ không đòi hỏi một thành phần điều khiển bên ngoài.

Khi ATM LSR có một LSC bên ngoài dành cho việc trao đổi thông tin thành phần điều khiển, chuyển mạch ATM trong ATM LSR lúc đó chỉ thực hiện nhiệm vụ chuyển tiếp dữ liệu. Để kích hoạt MPLS trong vùng ATM, trường VPI/VCI trong tiêu đề ATM được sử dụng để gắn nhãn. Kỹ thuật này cho phép chuyển tiếp các gói tin dữ liệu mang nhãn trong vùng ATM.

### **1.4 Các ứng dụng của MPLS**

Mạng MPLS có nhiều ứng dụng trong đó có 2 ứng dụng chủ yếu: [1]

- Dịch vụ mạng riêng ảo (VPN – Virtual Private Network): VPN là ứng dụng thiết lập đường truyền riêng cho các tổ chức, doanh nghiệp cần kết nối các chi nhánh với nhau. Các VPN được dành riêng đường truyền trên hệ thống mạng (độc lập về định tuyến) nên có độ bảo mật cao. VPN là đường hầm trong suốt trong hệ thống mạng của nhà cung cấp dịch vụ để thực hiện kết nối các điểm khách hàng với nhau. Có 2 loại VPN là layer 2 VPN và layer 3 VPN. Layer 2 là việc định tuyến IP giữa các điểm của khách hàng do khách hàng tự làm chủ, nhà cung cấp chỉ tạo đường hầm kết nối cho khách hàng. Layer 3 là việc định tuyến thông kết nối giữa các điểm của khách hàng sẽ do nhà cung cấp thực hiện.
- Điều khiển lưu lượng (TE – Traffic Engineering): Kỹ thuật điều khiển, lái các luồng lưu lượng theo mong muốn của người quản trị để tối ưu hiệu suất sử dụng tài nguyên mạng, tránh việc tồn tại những kết nối bị tắc nghẽn trong khi các kết nối khác còn thừa nhiều tài nguyên. Đảm bảo độ hội tụ thời gian đưa mạng về trạng thái ổn định nhanh chóng và hiệu quả, đảm bảo chất lượng dịch vụ truyền.

### **1.5 Tổng kết**

Chương 1 đã đưa ra được các lý thuyết về MPLS:

- Khái niệm và ưu điểm của MPLS.
- Cấu trúc của một miền MPLS.
- Các khái niệm cụ thể trong MPLS.
- Cơ chế hoạt động của các nút mạng MPLS.

## Chương 2: Kỹ thuật điều khiển lưu lượng MPLS TE

### 2.1 Giới thiệu về Traffic Engineering và MPLS Traffic Engineering

#### 2.1.1 Traffic Engineer là gì?

Kỹ thuật điều khiển lưu lượng (TE - Traffic Engineering) là kỹ thuật điều khiển đường truyền của lưu lượng qua mạng, để cải thiện hiệu suất sử dụng tài nguyên mạng, tránh trường hợp có kết nối mạng bị nghẽn trong khi các kết nối khác chưa được dùng hết. Ngoài ra, còn để đảm bảo chọn được đường truyền tốt nhất và thời gian hội tụ mạng cao, bảo vệ được dịch vụ truyền.

#### 2.1.2 Cơ bản về Kỹ thuật lưu lượng trong MPLS

MPLS-TE sử dụng đường hầm TE (TE tunnel) để kiểm soát lưu lượng trên đường truyền đến một đích cụ thể.

Các vấn đề cần làm rõ khi tìm hiểu về kỹ thuật điều khiển lưu lượng: [3]

- Sự phân phối thông tin (Information distribution): Trao đổi, phân phối thông tin về các thuộc tính của đường truyền (metric, bandwidth, delay, jitter,...).
- Tính toán và thiết lập đường truyền (Path calculation and setup): Cơ chế, thuật toán xác định để tạo các đường hầm LSP (TE tunnel) có đường đi tốt nhất.
- Giao thức báo hiệu (RSVP) để thiết lập, duy trì TE tunnel và có thể đặt trước tài nguyên theo mong muốn.
- Chuyển tiếp lưu lượng vào một đường hầm (Forwarding traffic down a tunnel): Các kỹ thuật để đẩy lưu lượng vào đường hầm.

MPLS TE có các ưu điểm sau: [3]

- MPLS TE cung cấp sự phân phối traffic hiệu quả đi qua mạng, tránh cho các link bị quá tải và không được sử dụng.
- MPLS TE tính toán được bandwidth của link.
- MPLS tính toán các thuộc tính của link (instance, delay, jitter).
- MPLS tự động điều chỉnh để thay đổi bandwidth và các thuộc tính của link.
- Định tuyến theo địa chỉ nguồn được áp dụng trong TE.

### 2.2 Hoạt động của Kỹ thuật lưu lượng trong MPLS

#### 2.2.1 Sự phân phối thông tin Traffic Engineering

[3, 4]

Trong Cisco IOS, một cơ sở dữ liệu TE được xây dựng từ thông tin TE mà giao thức link-state cung cấp. Cơ sở dữ liệu này chứa tất cả các link được enable MPLS TE và các tính chất, thuộc tính của chúng. Từ cơ sở dữ liệu này, path calculation (PCALC) hoặc constrained SPF (CSPF) tính toán đường đi ngắn nhất thỏa mãn ràng buộc (quan trọng nhất là băng thông) từ head end đến tail end LSR. PCALC và CSPF là thuật toán shortest path first (SPF) được ứng dụng cho MPLS TE. Ta cấu hình băng thông cần thiết và các thuộc tính của TE tunnel trên head end LSR. PCALC sẽ so sánh lưu

bảng thông cần thiết và thuộc tính của TE tunnel với các thuộc tính như vậy của link, từ tất cả các path có thể, nó sẽ lấy đường ngắn nhất. Sự tính toán này được thực hiện tại Head end LSR.

LSR trung tâm của LSP cần biết nhãn đi vào và đi ra cho TE tunnel, nó chỉ có thể học từ head end hoặc LSR trung tâm khác qua giao thức truyền tín hiệu RSVP.

Về bản chất, RSVP truyền tín hiệu TE tunnel khắp đường đi từ head end đến tail end LSR, những thứ đó là kết quả của sự tính toán từ cơ sở dữ liệu TE của Head end LSR. RSVP truyền tín hiệu để lấy được những thông tin nhãn được thiết lập tại mỗi LSR. Gói RSVP PATH được gửi từ head end đến tail end LSR để mang một yêu cầu cho một nhãn MPLS cần có thông tin. RSVP RESV được gửi lại từ tail end đến head end LSR mang thông tin nhãn MPLS mà mỗi LSR trong LSP có thể dùng để vận chuyển lưu lượng TE. RSVP còn kiểm tra TE tunnel có thể thiết lập các ràng buộc được hay không. Head end tính toán một đường có thể làm TE LSP nên nó có thể đã có TE tunnel khác chiếm băng thông trên LSR trung tâm, và OSPF hay IS-IS không quảng bá nó. Vì vậy có thể băng thông còn lại không đủ để TE tunnel đó có thể thiết lập nên ta cần phải có một giao thức truyền tín hiệu để chắc chắn băng thông đã được đặt trước ở mỗi router.

RSVP PATH được định tuyến qua mạng như thế nào? Explicit Route Object (ERO) cung cấp *hop* mà RSVP PATH phải đi qua để truyền tín hiệu TE tunnel. Một dãy *hop* hay path là kết quả tính toán của head end router. Tại mỗi hop RSVP PATH sẽ đặt trước băng thông và đề nghị một nhãn. Cuối cùng nó đến tail end router, router này sẽ gửi lại RESV trở về head end. RSVP RESV này trả về một nhãn mà MPLS data plane có thể dùng để vận chuyển gói tin của MPLS TE tunnel qua LSP. RESV cũng đề nghị LSR trung tâm cung cấp một lượng băng thông cho link của TE LSP.

### 2.2.2 Điều kiện với IGP

[3]

IGP phải có khả năng gửi tất cả thông tin của link đến tất cả router trong khu vực mà TE được enable. Chỉ có giao thức loại link-state là có thể làm việc này vì nó flood các trạng thái của link của một router đến tất cả các router khác trong cùng khu vực.

Head end cần tất cả thông tin của cấu trúc mạng để tìm ra các đường có thể, nhưng nó cũng cần có các tính chất của link đó. Các tính chất này là tập hợp của thông tin tài nguyên của link. Giao thức loại link state phải được mở rộng để mang những thông tin này.

Các tài nguyên TE của link là:

- TE metric
- Maximum bandwidth
- Maximum reservable bandwidth
- Unreserved bandwidth
- Administrative group

TE metric là trường ta có thể dùng để xây dựng một TE topology và nó khác với IP topology. TE metric có thể khác với OSPF cost hoặc IS-IS metric của link.

Maximum bandwidth là tổng bandwidth của link. Giá trị này chính là giá trị của đường vật lý hay giá trị bandwidth được cấu hình trên interface.

Maximum reservable bandwidth là tổng bandwidth dành riêng cho TE tunnel. Ta có thể thiết lập nó bằng lệnh **ip rsvp bandwidth**.

Unreserved bandwidth là phần còn lại của bandwidth có thể cung cấp cho TE. Nó là hiệu của maximum reservable bandwidth trừ đi bandwidth đã được đặt trước.

Administrative group là một trường 32 bit dùng để xác định tính chất của link. Ví dụ một bit có thể mang ý nghĩa link này là pos link với tốc độ lớn hơn OC 48, hoặc link có delay nhỏ hơn 100ms. Những tài nguyên này được flood khi nó có thay đổi hoặc theo thời gian đã hạn định. Nếu router không hiểu những thông tin của gói link-state mở rộng nó chỉ cần lờ đi.

### 2.2.3 Mở rộng OSPF với Traffic Engineering

[3]

RFC 2370 đưa ra một phần mở rộng cho giao thức OSPF, 3 LSA mới được định nghĩa và gọi là opaque LSA. Chúng giúp OSPF mang thông tin mà OSPF cần hoặc thông tin dành cho các ứng dụng khác. Những LSA này chính là thứ mà MPLS TE cần để truyền thông tin của nó.

Ba loại opaque LSA chỉ khác nhau cách flooding. Opaque LSA type 9 chỉ flood đến link-local; opaque LSA type 10 flood đến một area và opaque LSA type 11 flood đến toàn AS. Như vậy type 9 được gửi đến link nhưng không bao giờ chuyển tiếp qua bên kia, type 10 bị chặn bởi area border router, type 11 được flood toàn OSPF domain giống như type 5. MPLS TE sử dụng type 10 cho MPLS TE trong area.

### 2.2.4 Flood bởi IGP

[3]

IGP flood những thông tin TE trong các trường hợp sau:

- Trạng thái link thay đổi.
- Cấu hình thay đổi.
- Chu kì flood.
- Thay đổi ở reserved bandwidth.
- Sau khi thiết lập tunnel thất bại.

Cơ chế hoạt động này giống với hoạt động trong mạng IP, OSPF sẽ flood theo chu kì 30 phút. Ta có thể cấu hình thời gian này với câu lệnh **time pacing lsa-group giây**. Ta cũng có thể cấu hình khoảng thời gian trong chu kì cho TE. Flood định kì được sử dụng bởi vì thay đổi nhỏ trong reserved bandwidth không gây nên flood. Thông tin TE được flood định kì sau 3 phút. Để thay đổi ta sử dụng câu lệnh sau trong mode global **mpls traffic-eng link-management timers periodic-flooding {giây}**.

Thay đổi nhỏ nào trong reserved bandwidth mà không gây flood? Đó là khi một link có rất nhiều bandwidth chưa được đặt trước, tunnel sẽ dễ dàng tìm đủ bandwidth link đó hơn là còn ít unreserved bandwidth. Đó là lí do tại sao trigger được đặt để

flood thông tin khi mức bandwidth được đặt trước trên link gần với mức cao hơn là mức thấp của băng thông được đặt trước. Trigger có 2 tập hợp: một cho bandwidth giảm xuống, và một cho bandwidth đi lên. Trigger mặc định cho giảm xuống là 100, 99, 98, 97, 96, 95, 90, 85, 80, 75, 60, 45, 30, và 15. Trigger mặc định cho đi lên là 15, 30, 45, 60, 75, 80, 85, 90, 95, 96, 97, 98, 99, 100.

Trường hợp cuối cùng khi router flood thông tin trạng thái link là khi một tunnel không thể thiết lập. Nó có thể do một tunnel gắng thiết lập LSP qua RSVP nhưng RSVP không thể báo hiệu LSP đó. Lí do có thể làm một tunnel khác vừa đặt trước bandwidth của link trên đường đó. Tất nhiên nó chỉ xảy ra khi IGP không flood thông tin của link này bởi vì mức của reserved bandwidth chưa chạm mức flood. Bởi vì thiết lập thất bại trên router ở vùng trung tâm, router đó sẽ flood thông tin đó lại đến head end và head end sẽ loại link đó ra khỏi tính toán CSPF.

### 2.2.5 Cơ chế định tuyến và cost của TE LSP

[3]

Khi tính toán path cho TE tunnel, một vài thuộc tính được sử dụng và kết quả của việc tính toán này là path ngắn nhất và khả thi nhất từ tất cả các path với thuộc tính của các link phù hợp với yêu cầu đề ra của TE tunnel.

### 2.2.6 Thuộc tính của link Traffic Engineering

[3]

Mọi link enable MPLS TE đều có các thuộc tính cần được flood để head end router có thể tìm ra link nào phù hợp với TE tunnel. Một link đã enable TE có các thuộc tính sau:

- Maximum reservable bandwidth.
- Attribute flags.
- TE metric.
- Shared risk link group.
- Maximum reservable sub-pool bandwidth.

**Maximum Reservable Bandwidth:** là bandwidth có thể đặt trước tối đa trong global pool, pool này được tất cả các TE thông thường sử dụng. Câu lệnh thiết lập lượng bandwidth này là **ip rsvp bandwidth interface-kbps**.

**Attribute Flags:** một link có các cờ thuộc tính đi cùng với nó bằng cách sử dụng câu lệnh sau : **mpls traffic-eng attribute-flags thuộc tính**. Cờ thuộc tính chỉ ra tài nguyên của link, khả năng của link, hay các chính sách quản trị. Chúng còn chỉ ra một tunnel có tài nguyên đặc biệt đi qua link đó hay không. Trường này gồm 32 bit và không có cấu trúc gì cả. Mỗi bit có thể set hoặc để trống(0). Khi cấu hình tunnel trên head end router, ta có thể cấu hình affinity bit và một mask để điều khiển khi nào thì tunnel được cho phép đi qua link với những cờ thuộc tính đó. Affinity bit cũng dài 32 bit và so khớp 1-1 với cờ thuộc tính của link. Mask của affinity bit chỉ ra thuộc tính nào cần kiểm tra với cờ thuộc tính của link. Nếu bit thứ *n* trong Mask được set thì bit thứ *n* trong cờ thuộc tính phải trùng với bit thứ *n* trong affinity bit. Nếu bit không được

set thì chúng sẽ không so sánh bit đó. Affinity bit được cấu hình bằng lệnh **tunnel mpls traffic-eng affinity** thuộc tính *[mask mask-value]* trên interface tunnel trong head-end router.

**TE Metric:** ta có thể thay đổi TE metric của một link với câu lệnh: **mpls traffic-eng administrative-weight** *weight*. Mặc định của TE metric chính là cost của link. Một tunnel lấy IGP cost của link để tính toán khi cần chọn path qua mạng. Ta có thể cho head-end router sử dụng TE metric thay vì IGP cost của link để định tuyến tunnel qua mạng. Phần này nằm trong “Dual TE Metrics”.

**Shared Risk Link Group:** là tính chất của một link mà người quản trị gán cho nó để cho biết các link đó dùng một cáp chung. Nếu cáp đó bị down thì sẽ có một vài link bị ảnh hưởng và cùng chịu tổn thất. SRLG sẽ được flood bởi IGP và được sử dụng khi backup tunnel được dùng.

**Maximum Reservable Sub-pool Bandwidth:** sub-pool là một pool nơi mà các sub-pool hoặc DiffServ-aware TE tunnel nhận băng thông của chúng

## 2.2.7 Các thuộc tính của MPLS TE tunnel

[3]

Các tính chất của TE tunnel bao gồm:

- Địa chỉ đích của tunnel.
- Bảng thông chỉ định.
- Affinity.
- Setup và holding priority.
- Tái tối ưu hóa.
- Path option

Địa chỉ đích tunnel là một MPLS TE router ID của tail end LSR mà tunnel được route đến. Bảng thông chỉ định của TE tunnel là lượng băng thông cần thiết của TE tunnel. Ta có thể cấu hình:

**Tunnel mpls traffic-eng bandwidth [sub-pool|global] *bandwidth*.**

Từ **global** chỉ ra một TE tunnel bình thường, còn **sub-pool** chỉ ra một DiffServ-aware TE tunnel. Affinity bit và mask được cấu hình trên interface của head end router. Setup và holding priority, tái tối ưu hóa và path option sẽ được giải thích ở phần tiếp theo.

## 2.3 Cách tính toán đường đi của Traffic Engineering

Cách đặt đường hầm TE phụ thuộc vào các yếu tố sau: [3]

- Path setup option.
- Setup và holding priority.
- Attribute flags và affinity bit.
- Tái tối ưu.

### 2.3.1 Path setup option



Ta có thể cấu hình path option trên mode tunnel của head end router, có 2 cách để thiết lập một tunnel: tĩnh và động. Thiết lập tĩnh là ta phải kiểm tra các router định chạy TE tunnel, kể cả tail end. Ta cũng có thể lựa chọn TE router ID hoặc địa chỉ link của router ở giữa. Thiết lập động là ta để head end tìm ra đường nào thì đặt TE tunnel tốt nhất, cách này ta chỉ phải chọn địa chỉ đích cho TE tunnel.

Ta có thể cấu hình nhiều hơn một hay nhiều path option tĩnh hay động miễn là chúng khác độ ưu tiên. Độ ưu tiên là số từ 1 đến 1000. Giá trị càng thấp thì nó càng được ưu tiên cao. Path có độ ưu tiên sẽ được kiểm tra trước nếu nó không phù hợp router sẽ chuyển qua path có độ ưu tiên thấp hơn. Nếu tất cả các path đều không phù hợp thì tunnel interface trên head end sẽ ở chế độ down.

### 2.3.2 Setup và holding priority

Các tunnel có một tầm quan trọng khác nhau trong mạng. Điển hình là tunnel dài hơn sẽ quan trọng hơn tunnel ngắn. Tất nhiên tunnel cần băng thông nhiều hơn cũng quan trọng hơn tunnel cần ít băng thông. Những tunnel quan trọng hơn thường được báo hiệu chậm hơn. Chúng ta sẽ thấy tunnel quan trọng hơn sẽ có nguy cơ không tìm được path hoặc không được định tuyến. TE tunnel có sự ưu tiên để đảm bảo tunnel quan trọng hơn sẽ chiếm tunnel ít quan trọng.

Ta có 2 thuộc tính ưu tiên: setup và holding. Hai giá trị này càng nhỏ thì tunnel càng quan trọng. Giá trị setup chỉ ra tunnel có thể chiếm tunnel khác, còn holding chỉ ra trọng số mà tunnel có thể giữ đường link nó đã đặt trước. Một tunnel có setup nhỏ hơn holding của tunnel thứ 2 thì nó có thể chiếm tunnel thứ 2 đó. Nó có nghĩa là những tunnel mới được báo hiệu thì sẽ chiếm đường hầm đã có sẵn. Hai độ ưu tiên này có thể cấu hình bằng câu lệnh sau:

**Tunnel mpls traffic-eng priority setup-priority [holding-priority]**

Các TE tunnel quan trọng thường có setup và holding nhỏ để có thể chiếm các tunnel khác và không bị chiếm. Các giá trị có thể chọn cho 2 giá trị ưu tiên này chạy từ 0->7. 0 qui định độ ưu tiên lớn nhất. Như vậy ta có thể cho hai giá trị ưu tiên của các tunnel yêu cầu băng thông lớn giá trị nhỏ để chúng có thể chiếm và đặt trước băng thông, các tunnel có lượng băng thông yêu cầu nhỏ hơn sẽ dễ dàng lấp vào lượng băng thông còn lại. Setup không được nhỏ hơn giá trị của holding, nếu không tunnel như vậy có thể chiếm tunnel khác và bị chính tunnel đó chiếm lại.

Các TE tunnel quan trọng thường có setup và holding nhỏ để có thể chiếm các tunnel khác và không bị chiếm. Các giá trị có thể chọn cho 2 giá trị ưu tiên này chạy từ 0->7. 0 qui định độ ưu tiên lớn nhất. Như vậy ta có thể cho hai giá trị ưu tiên của các tunnel yêu cầu băng thông lớn giá trị nhỏ để chúng có thể chiếm và đặt trước băng thông, các tunnel có lượng băng thông yêu cầu nhỏ hơn sẽ dễ dàng lấp vào lượng băng thông còn lại. Setup không được nhỏ hơn giá trị của holding, nếu không tunnel như vậy có thể chiếm tunnel khác và bị chính tunnel đó chiếm lại.

### 2.3.3 PCALC – Path Calculation

[3, 4]

PCALC là thuật toán SPF đặc biệt được sử dụng bởi MPLS TE. SPF là thuật toán được OSPF và IS-IS sử dụng để tính toán đường đi ngắn nhất. Chuẩn mực của SPF là mức cost nhỏ nhất của mỗi prefix IP. Đối với TE nó cần tính toán đến các tài nguyên

và ràng buộc của link do OSPF hoặc IS-IS mở rộng đưa về. PCALC có thể tính toán path không chỉ dựa trên đường ngắn nhất mà còn dựa trên tài nguyên của chúng. Những link không đủ tài nguyên sẽ bị xóa khỏi SPF tree khi CSPF chạy. Ngoài ra điểm khác biệt khác nữa giữa SPF và CSPF, PCALC là nó chạy trên một đơn vị (TE tunnel). Kết quả của CSPF không phải là một bảng routing mà là một path. Path này là một chuỗi các địa chỉ IP, nó chính là địa chỉ của các link. Dãy địa chỉ này sẽ dùng để thiết lập hoặc truyền tín hiệu TE LSP. PCALC chỉ xây dựng duy nhất một path tốt nhất. Nếu có các path có cùng cost và ràng buộc thì nó sẽ chọn path có băng thông tối thiểu lớn nhất. Nếu vẫn còn các path giống nhau, path nào có ít hop hơn sẽ được chọn. Nếu vẫn còn nhiều path, Cisco IOS sẽ chọn 1 path để chạy TE tunnel.

#### **2.3.4 Resource Reservation Protocol (RSVP – Giao thức dành trước tài nguyên)**

[3]

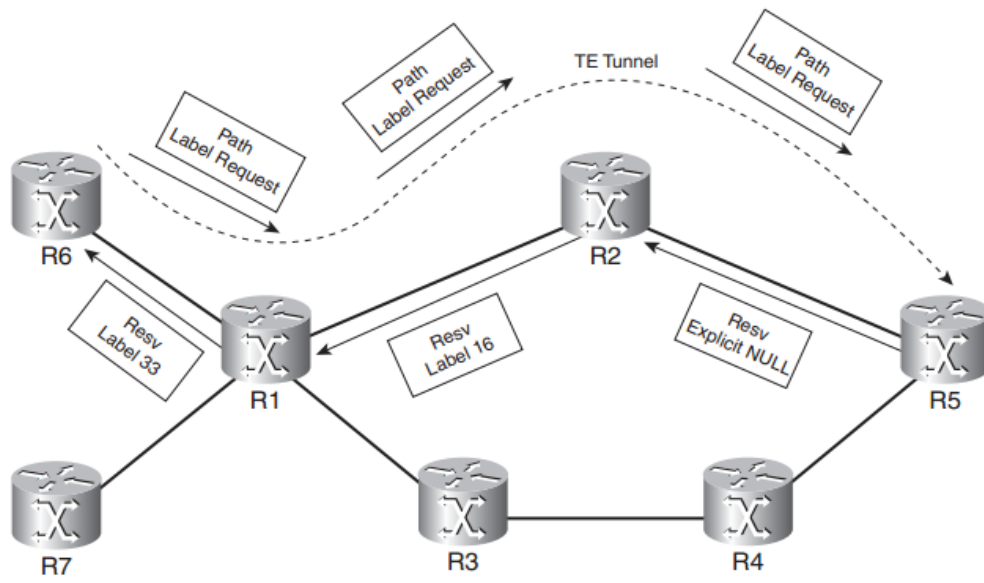
RSVP đã được mở rộng để phát tín hiệu TE tunnel, bởi vì RSVP lúc đầu được phát triển để phát tín hiệu cho Intergrated Services. Nói cách khác, RSVP được dùng để phát tín hiệu cho QoS trong mạng.

RSVP sử dụng hai gói tin PATH và RESV để báo hiệu một path. Head end sẽ gửi gói PATH đến tail end, còn RESV gửi path ngược lại đến head end. Head end tính toán để lựa chọn một path tốt nhất từ TE database. Path này được cấu hình bởi một explicit path option bởi người sử dụng trên tunnel interface. Mỗi hop mà TE tunnel đi qua sẽ đặt một ERO (đối tượng tuyến đường minh), nó là một dãy đã được sắp xếp của địa chỉ Ip của interface, với mỗi địa chỉ IP trên một LSR. Gói PATH được gửi từ head end đến router kế tiếp. Router kế tiếp này loại địa chỉ Ip của nó khỏi ERO, và thấy địa chỉ IP kế tiếp để chuyển gói PATH đến địa chỉ đó. Nó cứ tiếp tục như vậy cho đến khi đến tail end. Sau đó tail end gửi lại một gói RESV cùng với path mà gói PATH đi qua nhưng với hướng ngược lại.

##### **2.3.4.1 RSVP và Nhãn**

RSVP truyền tín hiệu path cho TE tunnel, nhưng nó cũng có nhiệm vụ mang nhãn MPLS để gói tin có thể được chuyển mạch trên path chạy TE tunnel.

Gói PATH mang Label Request Object. Khi tail end router nhận được Label Request Object, nó gán nhãn cho TE tunnel và quảng bá nó cho upstream router trong Label Object của gói RESV. Khi upstream router nhận label này, nó sẽ gán label này là outgoing label cho TE tunnel. Nó lại tiếp tục gán nhãn và gửi đến upstream router của nó. Việc này được diễn ra cho đến khi gói RESV chạm head end. Việc quảng bá nhãn này là hop-by-hop.



Hình 2.1: RSVP cho TE và nhãn

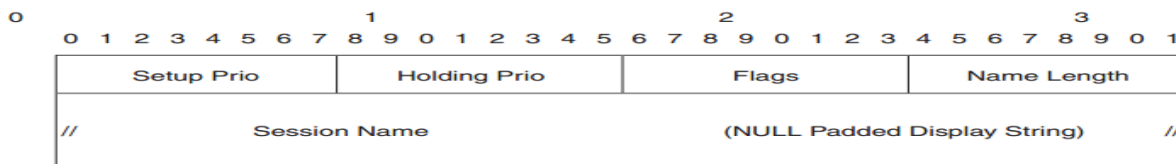
### 2.3.4.2 Ghi lại đối tượng đường đi (Record Route Object)

Một RSVP mới chính là Record Route Object (RRO). PATH và RESV mang đối tượng này, nó lưu địa chỉ IP của router mà TE tunnel đã đi qua. Path ở trong RSVP Path Info giống với path ở trong RRO, mặc dù nó có thể khác nếu như TE LSP được tái định tuyến tạm thời vào một đường backup tunnel.

### 2.3.4.3 Những thông tin mang bởi RSVP

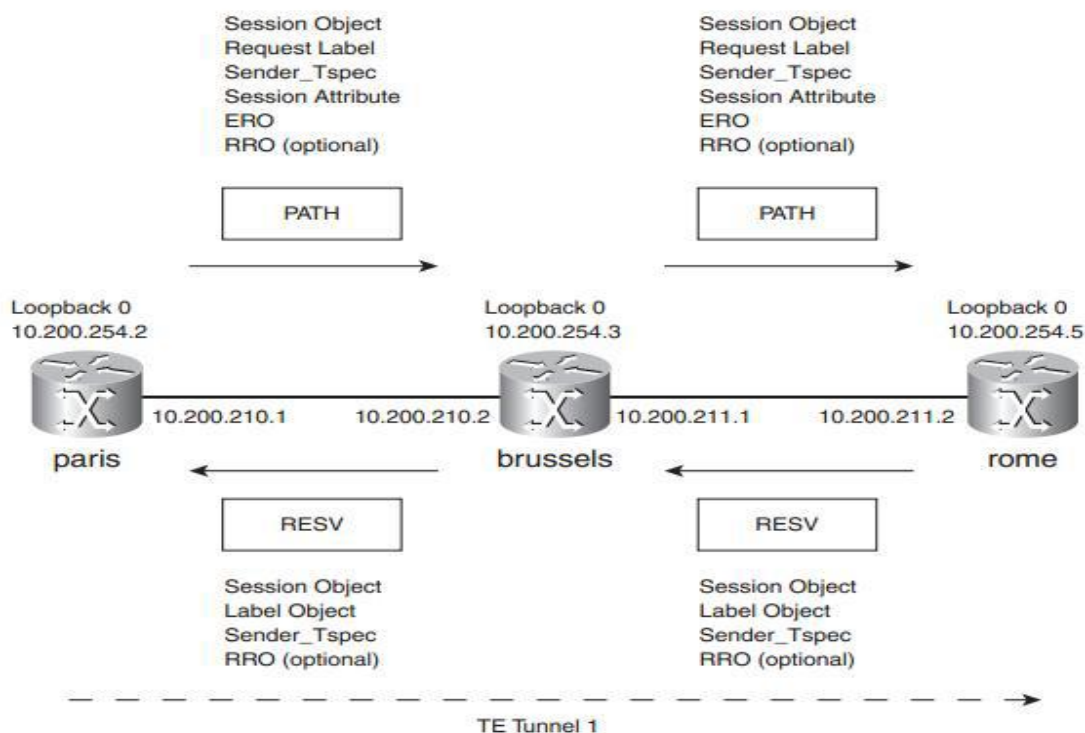
Lượng băng thông yêu cầu cho TE tunnel là thuộc tính quan trọng nhất của TE. Nó được chứa trong SENDER\_TSPEC với kiểu byte/s.

Thuộc tính Session có chứa các giá trị setup và holding priority và một số flag. Những flag này có thể chỉ định local protection có được bật hay không



Hình 2.2: Thuộc tính Session

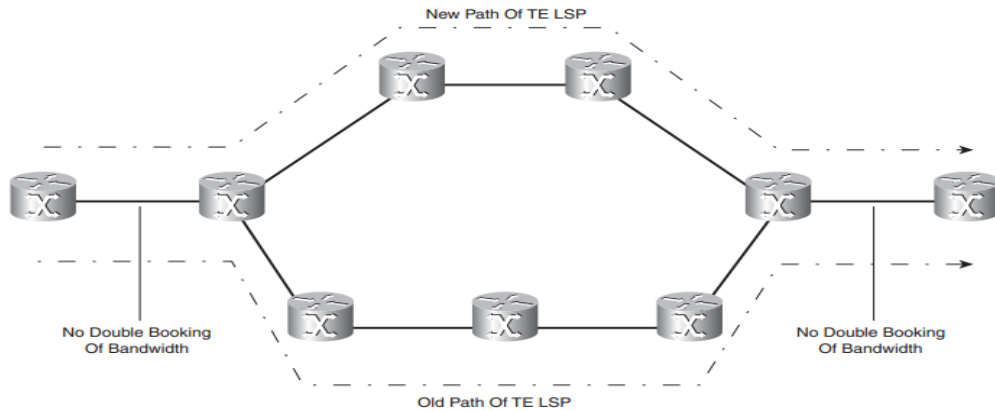
Tổng hợp lại ta có cách thức hoạt động của RSVP như hình sau:



Hình 2.3: Sự quảng bá của RSVP PATH và RESV

### 2.3.4.4 Shared Explicit Style

Shared Explicit Style là kiểu RSVP được sử dụng cho TE nhằm đảm bảo khi TE LSP được tái định tuyến, tunnel mới phải được tạo trước khi tunnel cũ bị down. Băng thông đã được đăng ký sẽ được sử dụng cho cả tunnel cũ và mới. Tunnel cũ và mới không được đặt trước tại link dùng chung đó cùng một thời điểm.



Hình 2.4: RSVP SE Style

### 2.3.4.5 Các gói tin của RSVP

Một số gói RSVP mà TE sử dụng ngoài PATH và RESV.

- **PathTear:** là gói giống PATH nhưng được gửi khi head end router muốn báo hiệu là TE tunnel sẽ down( người quản trị dùng lệnh shutdown trên tunnel interface).
- **ResvTear:** tương tự như RESV nhưng được gửi bởi tail end để xác nhận việc nhận gói PathTear.
- **PathErr:** là gói được gửi đến head end từ các LSR khác thông báo là link được sử dụng bởi TE LSP đã bị down hoặc LSR nhận PATH với thông tin sai lệch.

## 2.4 Chuyển tiếp lưu lượng vào MPLS – TE tunnel

[3]

Các cách chuyển tiếp lưu lượng vào tunnel:

- Static Routing.
- Policy - Based Routing.
- Autoroute announce.
- Forwarding adjacency.
- Class-based tunnel selection.

### 2.4.1 Static Routing

Là cách đơn giản và dễ dàng nhất để chuyển tiếp lưu lượng vào TE tunnel. Ta chỉ cần cấu hình một static route ở trên head end router với câu lệnh

**ip route IP-address mask tunnel number.**

### 2.4.2 Policy – Base Routing

Sử dụng một chính sách được cấu hình trên incoming interface để gửi traffic đến một next hop nào đó. Khi sử dụng PBR ta có thể chuyển tiếp dựa vào IP source hoặc loại giao thức. Ta dùng câu lệnh của route map như trong ví dụ sau:

```
ip policy route-map pbr
route-map pbr permit 10
match ip address 100
set interface Tunnel1
```

### 2.4.3 Autoroute announce.

**Tunnel mpls traffic-eng autoroute announce** là câu lệnh được cấu hình trên tunnel interface của headend để LSR có thể thêm địa chỉ IP đích và bảng định tuyến

với TE tunnel như là next hop hay outgoing interface. Cơ bản, autoroute announce chỉnh sửa thuật toán SPF để LSR có thể thêm dãy IP downstream của tailend route vào bảng định tuyến với TE tunnel là next hop.

#### 2.4.4 Forwarding adjacency

Đưa TE tunnel tham gia vào định tuyến trong IGP, lúc này router sẽ học route IGP qua TE tunnel như một link kết nối trực tiếp giữa các router trong cùng area và chuyển tiếp lưu lượng vào TE tunnel. Trên head end sử dụng câu lệnh sau để thực hiện:

```
tunnel mpls traffic-eng forwarding-adjacency {holdtime value}
```

#### 2.4.5 Class-based tunnel selection

Hỗ trợ việc điều khiển lưu lượng theo từng loại dịch vụ (class of service – CoS) dựa vào giá trị EXP (giá trị QoS cho từng loại lưu lượng trong MPLS). Với mỗi loại lưu lượng sẽ thực hiện chuyển vào một TE tunnel riêng, giá trị EXP có 3 bit nên hỗ trợ 8 loại lưu lượng chuyển tiếp vào 8 TE tunnel khác nhau.

Trong TE tunnel trên dead end router thực hiện câu lệnh sau:

```
tunnel mpls traffic-eng exp [list-of-exp-values] [default]
```

### 2.5 Bảo vệ và phục hồi

Mạng hỏng, hay chính xác hơn, có các thành phần trong mạng không hoạt động được nữa, có rất nhiều nguyên nhân gây ra điều này, được chia thành 2 loại chính: là do nút mạng và do liên kết mạng. Và để làm hạn chế những tác động tiêu cực khi mạng hỏng, MPLS TE có khả năng hướng các con đường lưu lượng ngắn nhất của các giao thức IGP để hạn chế mất gói tin ở những nút và kết nối bị hỏng trên mạng, khả năng này gọi là FRR (Fast Reroute -Tái định tuyến nhanh) hoặc MPLS TE Protection (Sự bảo vệ của MPLS TE).

Bảo vệ có thể được chia làm các loại:

- Bảo vệ đường đi (Path Protection) –Hay còn gọi là bảo vệ đầu cuối.
- Bảo vệ cục bộ (Local Protection):
  - Bảo vệ nút (FRR - node protection)
  - Bảo vệ kết nối(FRR - link protection)

#### 2.5.1 Path Protection

Bảo vệ end to end tuyến đường LSP từ head end node đến tail end node. Một LSP thứ 2 được thiết lập để sẵn sàng dự phòng cho LSP chính. Khi LSP bị mất kết nối thì head end sẽ thực hiện chuyển lưu lượng qua LSP dự phòng.

Các dấu hiệu để xác định LSP chính bị lỗi và cần chuyển qua LSP dự phòng:

- Head end nhận các bản tin Path erro hoặc resv tear từ giao thức báo hiệu RSVP.
- Thông báo từ RSVP hello đến một neighbor bị mất.
- BFD (Bidirectional Forwarding Detection) mất kết nối đến một neighbor.
- IGP mất kết nối đến một neighbor.

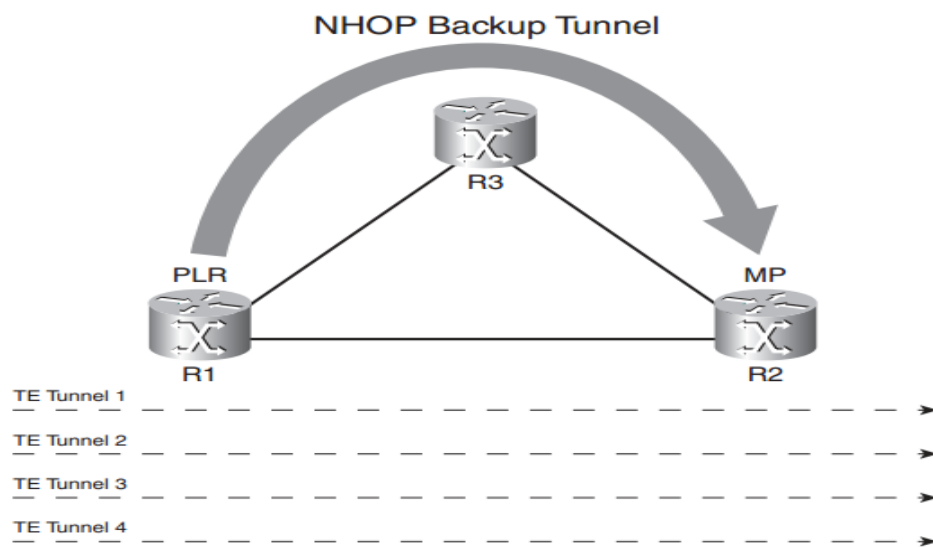
#### 2.5.2 Fast Reroute (FRR)

[3, 4]

TE thường được sử dụng trong mạng core nơi có lưu lượng trên link rất cao. Nếu một link hoặc router down, traffic sẽ bị dồn ứ và drop. Tuy việc tái định tuyến chỉ tốn vài giây nhưng đối với các link có VoidIp đi qua thì đó là một vấn đề lớn. Vì thế ta sử dụng Link và Node Protection với TE để đảm bảo lưu lượng không bị mất mát. Ngoài ra cách triển khai nó là khá dễ dàng. Phần tiếp theo nói về hai cách bảo vệ cục bộ với TE: Link protection và node protection. Hai cách này có điểm chung là việc backup càng gần router bị lỗi càng tốt, cả hai đều cung cấp cách sửa chữa cục bộ. Nó nhanh chóng chuyển qua tunnel backup nếu protected link bị down hay lỗi.

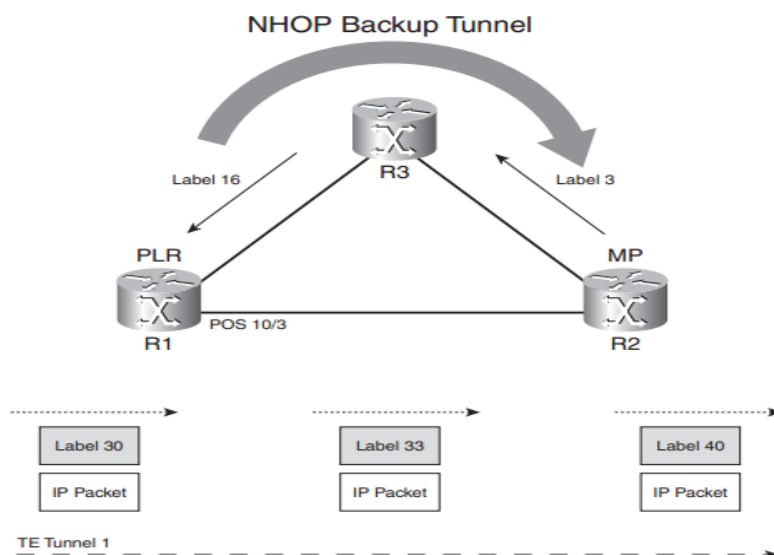
### 2.5.2.1 FRR – link Protection

Với link protection, một link sử dụng bởi TE sẽ được bảo vệ. Như vậy có nghĩa là tất cả các tunnel đi qua link đó đều được bảo vệ bởi một backup tunnel. Hình dưới chỉ ra một mạng nhỏ có link R1-R2 được bảo vệ bởi backup tunnel R1-R3-R2. Và nó chỉ bảo vệ theo hướng R1->R2.

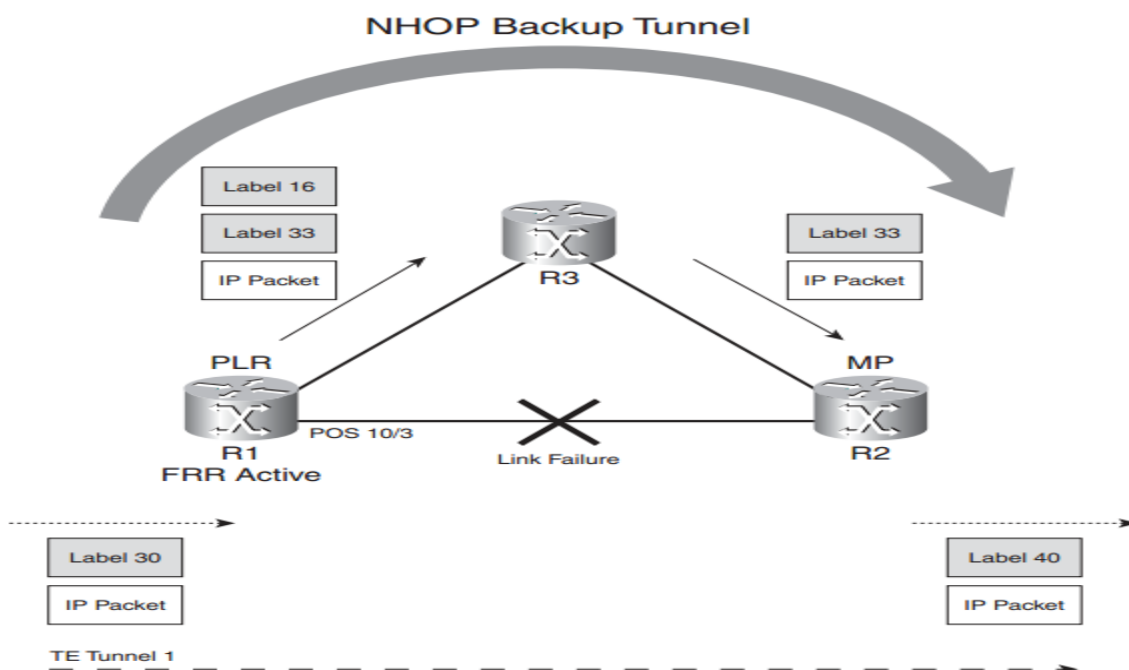


Hình 2.5: Link Protection

Trong link protection, backup tunnel được gọi là *next-hop (NHOP) bypass tunnel* và điểm bắt đầu tại Point of Repair (PLR). PLR ở hình trên chính là R1. Backup tunnel luôn kết nối đến next hop router ở đây chính là R2 hay còn gọi là Merge Point (MP). Backup tunnel là một explicit path được RSVP truyền tín hiệu.



Hình 2.6: Vận chuyển lưu lượng khi link protection chưa active



Hình 2.7: Vận chuyển lưu lượng khi link protection đã active

PLR sử dụng backup tunnel để mang TE LSP tạm thời mà thôi do link bị lỗi hay down nên PLR sẽ gửi một PathErr đến head end. Khi head end của protected tunnel nhận được nó sẽ tính toán một path mới cho tunnel đó. Khi hoàn tất báo hiệu và LSP tunnel được tái định tuyến thì backup tunnel sẽ không được sử dụng nữa. Khi link bị lỗi thì PLR vẫn gửi các gói PATH của tunnel bị lỗi qua backup tunnel để đảm bảo không có sự sai lệch.



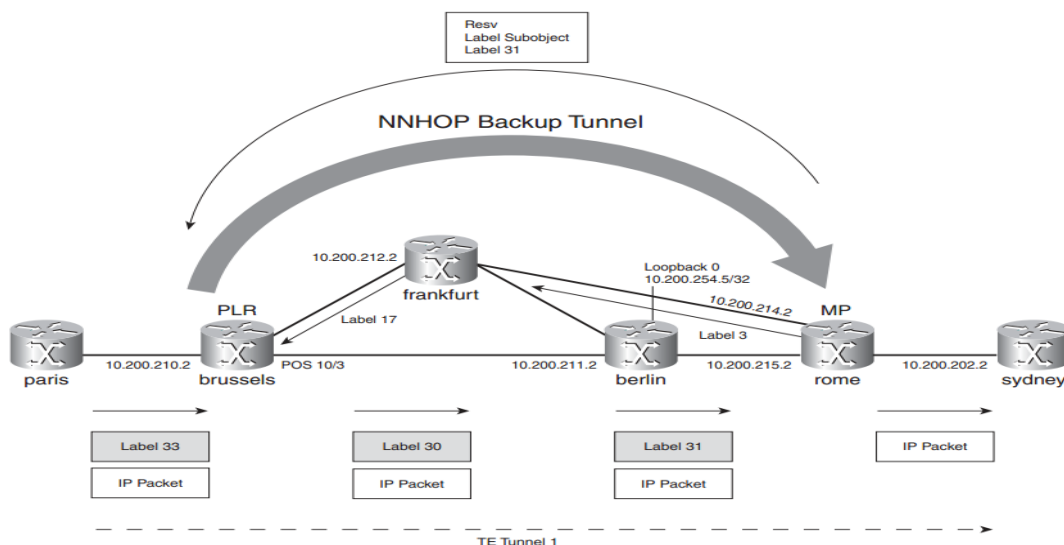
Nhược điểm của link protection là NHOP tunnel bảo vệ một link nên khi lượng traffic đi qua backup tunnel có thể không đáp ứng được và gây nghẽn. Vì thế nó chỉ được dùng backup tạm thời mà thôi.

Nếu việc tái định tuyến của protected TE LSP không có kết quả do head end không tìm được một path phù hợp. Ví dụ điển hình là TE tunnel chỉ có một explicit path và không có dynamic. Để giải quyết vấn đề này ta cấu hình một dynamic path option với số cao hơn explicit path. Như vậy khi protected link xảy ra lỗi, head end sẽ sử dụng dynamic path option và tái định tuyến tunnel.

Để cấu hình backup tunnel ta sử dụng câu lệnh sau trên protected link **mpls traffic-eng backup-path**. Ta cấu hình một explicit path từ PLR đến next hop router. Tại head end của protected tunnel ta qui định cho nó sử dụng backup khi link xảy ra lỗi với câu lệnh **tunnel mpls traffic-eng fast-reroute**. Traffic thông thường không sử dụng backup tunnel vì thế nó không nên có cấu hình autoroute announce.

### 2.5.2.2 FRR-node Protection

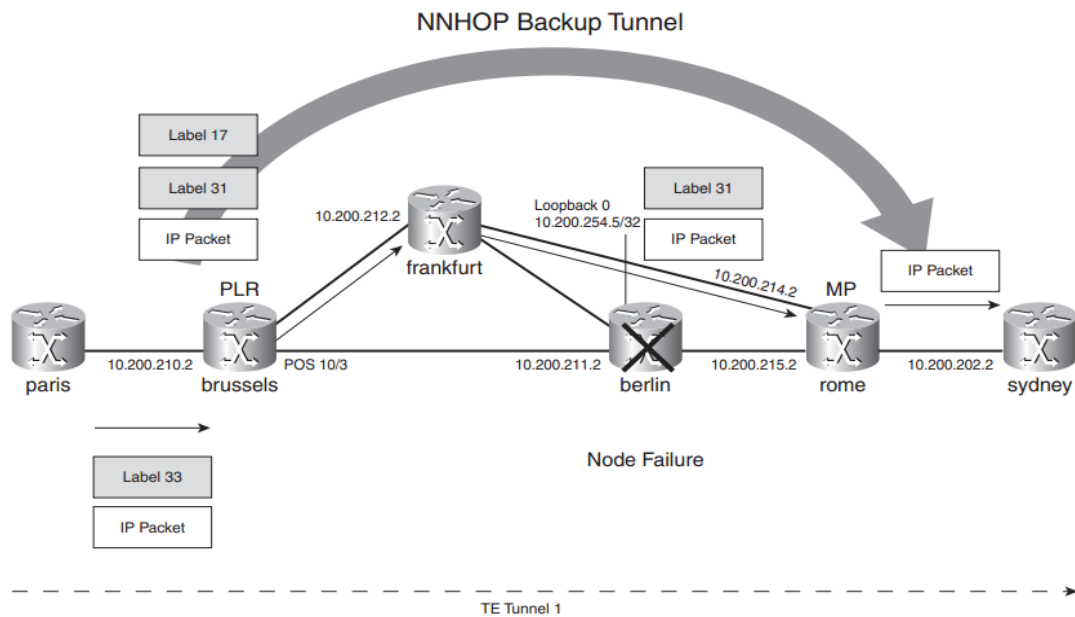
Với node protection ta không bảo vệ một link mà là cả một router. Nó hoạt động dựa một next next hop backup tunnel. Một NNHOP backup tunnel không phải là một tunnel đến next hop router của PLR nhưng đi đến router phía sau protected router. Ta dùng câu lệnh **tunnel mpls traffic-eng fast-reroute node-protect** tại head end của TE tunnel, nó sẽ set flag về 0x10 trong Session attribute của PATH để chứng tỏ nó muốn node protection.



Hình 2.8: Node Protection

Hai vấn đề làm node protection có một chút phức tạp. Vấn đề thứ nhất là packet không còn đi đến NHOP LSR mà là NNHOP LSR. Như vậy PLR phải biết được nhãn để sử dụng cho NNHOP backup tunnel để packet đi đến NNHOP có nhãn giống như khi backup tunnel chưa được sử dụng. Để giải quyết việc này, nhãn được quảng bá trong một label subobject trong trường RRO ở RESV từ NNHOP đến PLR. Khi gói tin đi vào PLR từ LSP tái định tuyến, PLR sẽ chuyển nhãn vừa đến và đưa nhãn đó vào NNHOP backup tunnel. Vấn đề thứ hai là backup tunnel phải tránh router kia biết được là đang trong tình trạng tái định tuyến. ERO trong PATH vẫn giữ địa chỉ của

router được bảo vệ, mặc dù không đi qua nó. PLR sẽ gửi gói PATH đó vào NNHOP tunnel để đảm bảo mọi việc hoạt động bình thường.



Hình 2.9: Node Protection Active

## 2.6 Tổng kết

Chương 2 nêu ra được các tính năng, giao thức, cơ chế hoạt động của MPLS – TE:

- Điều khiển lưu lượng: Sử dụng các tunnel để điều chỉnh, cân tải lưu lượng giữa các đường truyền mạng, đảm bảo tận dụng tài nguyên mạng với hiệu suất cao, tránh các trường hợp nghẽn đường truyền làm ảnh hưởng dịch vụ.
- Chọn đường đi chất lượng tốt nhất: Tính toán được các thuộc tính vật lý của đường truyền (delay, jitter,...) để chọn đường đi tốt nhất.
- Khả năng hội tụ cao: Có cơ chế dự phòng tốt, đảm bảo hội tụ nhanh khi có vấn đề xảy ra trên đường truyền, giúp cho không bị gián đoạn dịch vụ trong quá trình truyền lưu lượng.

# Chương 3: Thiết lập thử nghiệm mạng MPLS-TE trên thiết bị mạng thật

## 3.1 Mục đích

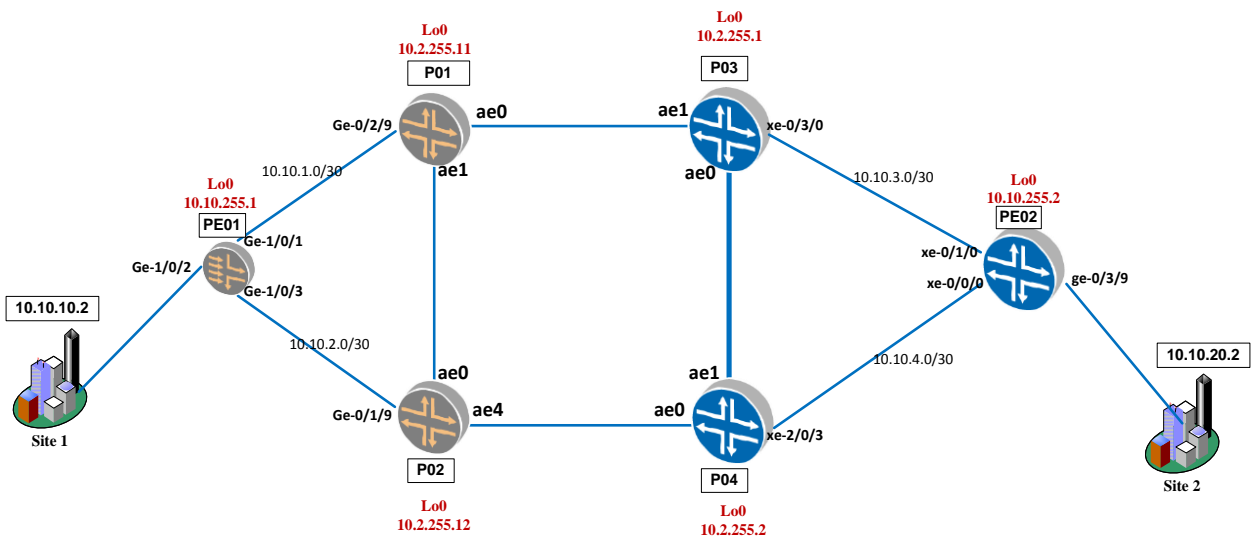
Demo MPLS TE trên hệ thống mạng thật:

- So sánh hiệu suất giữa hệ thống mạng sử dụng MPLS-TE và IP thuần.
- Kết hợp QoS cấp phát băng thông động.

## 3.2 Phương pháp thực hiện

- Xây dựng sơ đồ kết nối các nút router mạng.
- Cấu hình MPLS TE cho các router trong miền MPLS.
- Sử dụng máy đo truyền lưu lượng để kiểm nghiệm các bài mô phỏng.

## 3.3 Mô hình thực thể

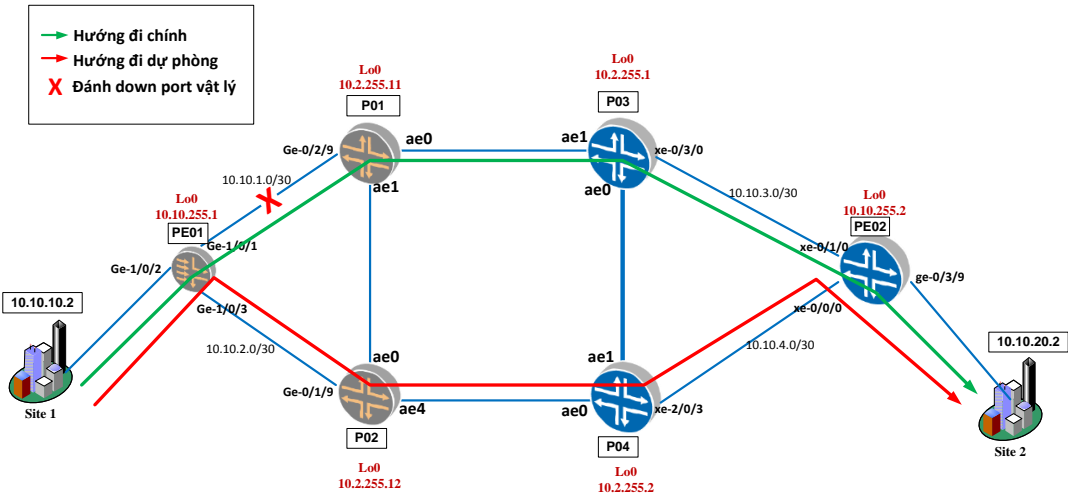


Hình 3.1: Mô hình chi tiết cho cấu hình mô phỏng MPLS TE

- Miền MPLS bao gồm các nút mạng:
  - o Edge LSR: PE01 và PE02, dòng thiết bị Juniper ACX2100.
  - o LSR Core: P01, P02, P03 và P04, dòng thiết bị Juniper MX480 và MX104.
  - o Site 1 và Site 2 là máy đo để truyền lưu lượng IXA.

### 3.3.1 So sánh hiệu suất giữa hệ thống mạng sử dụng MPLS-TE và IP thuần

## So sánh hội tụ giữa hệ thống mạng sử dụng MPLS-TE và IP thuần



Thực hiện truyền lưu lượng từ Site 1 đến Site 2, sau đó thực hiện đánh down một kết nối trên đường truyền và kiểm tra tính hội tụ:

- T1: Đường truyền sử dụng IP thuần.
- T2: Đường truyền sử dụng MPLS-TE.

Hình 3.2: Mô hình đo thời gian hội tụ giữa MPLS-TE và IP

### Cách thực hiện:

- Truyền lưu lượng 1000 packets/s từ Site 1 đến Site 2, sau đó đánh down kết nối từ PE01 đến P01.

Transmit State	Suspend	Tx Port	Configured Frame Size	Applied Frame Size	Frame Rate	Rx Ports	Flow Group Name	Tx port type
1		Ethernet - 004	Fixed: 1000	Fixed: 1000	1000 fps	Ethernet - 003;	PE1-PE2-EndpointSet-1 - Flow Group 0001	Ethernet

Hình 3.3: Máy đo truyền lưu lượng vào hệ thống mạng

- Trên máy đo IXA sẽ cho thấy kết quả rút gói để xác định thời gian hội tụ, ví dụ: Rút 100 packets thì thời gian hội tụ là 100 ms.

Kết quả đo trong 2 trường hợp:

- Trường hợp 1: Đường truyền sử dụng IP thuần, mạng không chạy MPLS-TE:
  - o Show route Site 2 trước thực hiện học qua OSPF (IP thuần):

```
[edit groups TEST-LAB1 logical-systems PE01]
juniper@SRT05# run show route 10.10.20.2 logical-system PE01
inet.0: 26 destinations, 26 routes (26 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
10.10.20.0/24      *[OSPF/10] 00:00:05, metric 65637
                  > to 10.10.1.1 via ge-1/0/1.0
[edit groups TEST-LAB1 logical-systems PE01]
juniper@SRT05#
```

Hình 3.4: Bảng định tuyến để thấy Site 1 qua Site 2 bằng định tuyến IP

- Rớt 1033 packets -> mạng hội tụ trong 1033 ms:

	Tx Port	Rx Port	Traffic Item	Tx Frames	Rx Frames	Frames Delta	Loss %
1	Ethernet - 004	Ethernet - 003	PE1-PE2	265,871	264,838	1,033	0.389

Hình 3.5: Kết quả hội tụ mạng IP thuần trên máy đo

- Trường hợp 2: Đường truyền sử dụng MPLS-TE:
  - Show route Site 2 trước thực hiện học qua LSP của MPLS-TE:

```

juniper@SRT05> show route 10.10.20.2 logical-system PE01
inet.0: 25 destinations, 27 routes (25 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
10.10.20.0/24      *[RSVP/7/1] 00:00:04, metric 65535
                   > to 10.10.2.1 via ge-1/0/3.0, label-switched-path PE01_TO_PE02_SITE1
                   [OSPF/10] 00:00:04, metric 65646
                   > to 10.10.2.1 via ge-1/0/3.0
inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
10.10.20.0/24      *[RSVP/7/1] 00:00:04, metric 65535
                   > to 10.10.2.1 via ge-1/0/3.0, label-switched-path PE01_TO_PE02_SITE1
juniper@SRT05>

```

Hình 3.6: Bảng định tuyến để thấy Site 1 qua Site 2 bằng định tuyến MPLS-TE

- Rớt 353 packets -> mạng hội tụ trong 352 ms:

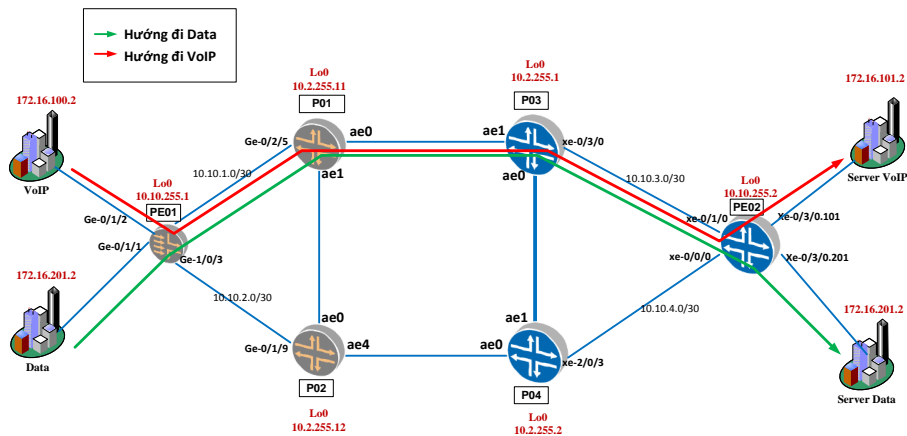
	Tx Port	Rx Port	Traffic Item	Tx Frames	Rx Frames	Frames Delta	Loss %
1	Ethernet - 004	Ethernet - 003	PE1-PE2	39,874	39,521	353	0.885

Hình 3.7: Kết quả hội tụ mạng MPLS-TE trên máy đo

**Kết luận:** Mạng sử dụng MPLS-TE sẽ có thời gian hội tụ (khôi phục dịch vụ) khi có sự cố mạng nhanh hơn nhiều lần so với mạng chỉ chạy IP thuần (353 ms so với 1033 ms).

### 3.3.2 Kết hợp QoS đảm bảo chất lượng dịch vụ và cấp phát băng thông động

## Kết hợp QoS cấp phát băng thông động và đảm bảo chất lượng dịch vụ



Đường truyền từ PE01 đến PE02 có băng thông 1Gb: Cấp cho tunnel phục vụ VoIP 500Mb, QoS High và tunnel phục vụ Data 500Mb, QoS low.

- T1: VoIP chỉ dùng 100Mb, còn dư 400Mb, Data dùng 800Mb, thiếu 300Mb, nhưng VoIP còn dư thì sẽ sử dụng cho Data.
- T2: VoIP cần sử dụng lên 400Mb, VoIP sẽ được sử dụng lên 400Mb, Data sẽ còn lại 600Mb được cấp. (đo thời gian VoIP lấy lại BW đã cho mượn)
- T3: VoIP sử dụng 400Mb, Data sử dụng 800Mb, lúc này đường truyền nghẽn -> VoIP sẽ được ưu tiên hơn và không bị drop, Data sẽ bị drop.

Hình 3.8: Mô hình đo QoS cấp phát băng thông động và đảm bảo chất lượng dịch vụ

### Cách thực hiện:

- Thiết lập kết nối từ site VoIP và Data đến server qua 2 LSP VoIP và Data:

```

juniper@SRT02# show routing-options
static {
  route 172.16.101.0/30 {
    lsp-next-hop VoIP;
  }
  route 172.16.201.0/30 {
    lsp-next-hop Data;
  }
}

[edit groups TEST-LAB1]
juniper@SRT02# run show route 172.16.101.0/30

inet.0: 23 destinations, 26 routes (23 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

172.16.101.0/30    *[Static/5] 00:12:30
                  > to 10.10.1.1 via ge-0/2/3.0, label-switched-path VoIP
                  [OSPF/10] 00:12:39, metric 11100
                  > to 10.10.1.1 via ge-0/2/3.0

[edit groups TEST-LAB1]
juniper@SRT02# run show route 172.16.201.0/30

inet.0: 23 destinations, 26 routes (23 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

172.16.201.0/30  *[Static/5] 00:12:34
                  > to 10.10.1.1 via ge-0/2/3.0, label-switched-path Data
                  [OSPF/10] 00:12:43, metric 11100
                  > to 10.10.1.1 via ge-0/2/3.0

[edit groups TEST-LAB1]
juniper@SRT02# |
    
```

Hình 3.9: Bảng định tuyến thể hiện đường đi VoIP và Data qua MPLS-TE

- Cấu hình QoS cho VoIP 500Mb, Data 500Mb:

```

[edit groups TEST-LAB1]
juniper@SRT02# show class-of-service schedulers
S_AF4 {
    transmit-rate 500m;
    priority low;
}
S_AF3 {
    transmit-rate 500m;
    priority low;
}

[edit groups TEST-LAB1]
juniper@SRT02# show class-of-service interfaces
ge-0/2/3 {
    scheduler-map SCH_MAP;
}
ge-0/1/2 {
    unit 0 {
        forwarding-class AF3;
    }
}
ge-0/1/1 {
    unit 0 {
        forwarding-class AF4;
    }
}

[edit groups TEST-LAB1]
juniper@SRT02# |

```

Hình 3.10: Cấu hình QoS cấp băng thông động và độ ưu tiên

- Trên máy đo IXA sẽ thực hiện truyền lưu lượng từ site VoIP, Data đến 2 server VoIP và Data.

#### Kết quả đo trong 3 trường hợp:

- **Trường hợp 1:** Lưu lượng VoIP 100Mb (interface ge-0/1/2), Data 700Mb (interface ge-0/1/1),:

SRT02		Seconds: 126		Time: 08:36:33	
Interface	Link	Input bytes	(bps)	output bytes	(bps)
lsq-0/0/0	Up	0	(0)	0	(0)
ge-0/1/0	Down	256	(0)	10764	(0)
ge-0/1/1	Up	199881102266	(700000000)	14230	(0)
ge-0/1/2	Up	196510244420	(100000000)	14558	(0)
ge-0/1/3	Down	0	(0)	0	(0)
ge-0/1/4	Down	0	(0)	0	(0)
ge-0/1/5	Down	0	(0)	0	(0)
ge-0/1/6	Down	0	(0)	0	(0)
ge-0/1/7	Down	0	(0)	0	(0)
ge-0/2/0	Down	0	(0)	0	(0)
ge-0/2/1	Down	0	(0)	0	(0)
ge-0/2/2	Down	0	(0)	0	(0)
ge-0/2/3	Up	374310	(1392)	198353507642	(803201248)
dsc	Up	0	(0)	0	(0)
em0	Up	6111125	(0)	6019874	(0)
fxp0	Up	4487648	(0)	1443524	(0)
gre	Up	0	(0)	0	(0)
ipip	Up	0	(0)	0	(0)
irb	Up	0	(0)	0	(0)
lo0	Up	4192	(0)	4192	(0)
lsi	Up	0	(0)	0	(0)
mtun	Up	0	(0)	0	(0)
pimd	Up	0	(0)	0	(0)

Bytes=b, Clear=c, Delta=d, Packets=p, Quit=q or ESC, Rate=r, Up=^U, Down=^D

Hình 3.11: Bảng thông luồng VoIP và Data truyền vào mạng

→ Khi VoIP không sử dụng hết 500Mb được cấp thì Data có thể mượn để sử dụng.

- **Trường hợp 2:** Data đang truyền 800Mb thì VoIP cần truyền 400Mb:
  - o Voip lấy lại băng thông đã cho mượn

```

Interface: xe-0/2/0.101, Enabled, Link is up
Flags: SNMP-Traps 0x4000
Encapsulation: ENET2
VLAN-Tag [ 0x8100.101 ]
Local statistics:
  Input bytes: 348
  Output bytes: 848
  Input packets: 5
  Output packets: 16
Remote statistics:
  Input bytes: 84 (0 bps)
  Output bytes: 138886952728 (392784984 bps)
  Input packets: 3 (0 pps)
  Output packets: 141432745 (49998 pps)
Traffic statistics:
  Input bytes: 432
  Output bytes: 138886953576
  Input packets: 8
  Output packets: 141432761
Protocol: inet, MTU: 1500, Flags: None

```

Next='n', Quit='q' or ESC, Freeze='f', Thaw='t', Clear='c', Interface='i'

Hình 3.12: Bảng thông VoIP tăng lên khi VoIP cần lấy lại băng thông

- VoIP lấy lại băng thông đã cho mượn và truyền được lên 400Mb.

```

Interface: xe-0/2/0.201, Enabled, Link is up
Flags: SNMP-Traps 0x4000
Encapsulation: ENET2
VLAN-Tag [ 0x8100.201 ]
Local statistics:
  Input bytes: 348
  Output bytes: 2918
  Input packets: 5
  Output packets: 61
Remote statistics:
  Input bytes: 84 (0 bps)
  Output bytes: 172874021828 (566210760 bps)
  Input packets: 3 (0 pps)
  Output packets: 176042795 (72073 pps)
Traffic statistics:
  Input bytes: 432
  Output bytes: 172874024746
  Input packets: 8
  Output packets: 176042856
Protocol: inet, MTU: 1500, Flags: None

```

Next='n', Quit='q' or ESC, Freeze='f', Thaw='t', Clear='c', Interface='i'

Hình 3.13: Bảng thông Data giảm xuống khi VoIP cần lấy lại băng thông

- Data lúc này phải trả lại băng thông đã mượn và còn lại 600Mb để truyền.
  - o Data truyền 800Mb thì VoIP truyền 400Mb, trường hợp này đường truyền bị nghẽn:



The screenshot shows a network configuration window with two traffic items: DATA and VoIP. Below, the 'Flow Statistics' table shows the following data:

Tx Port	Rx Port	Traffic Item	Frames	Bytes	Packets	Discards
1 1G-Port1	10GE LAN - P1	VoIP	688,848	688,844	4	0.001
2 1G-Port4	10GE LAN - P1	DATA	15,817,132	15,432,368	384,764	2.433

Hình 3.14: Độ rớt gói của VoIP và Data khi đường truyền nghẽn

- ➔ VoIP vẫn đảm bảo băng thông và không bị rớt gói, Data bị rớt gói nhiều do không đủ băng thông cung cấp.
- ➔ Lúc VoIP lấy lại băng thông cho mượn để truyền từ 100Mb lên 400Mb thì bị rớt 4 gói tin.

**Kết luận:**

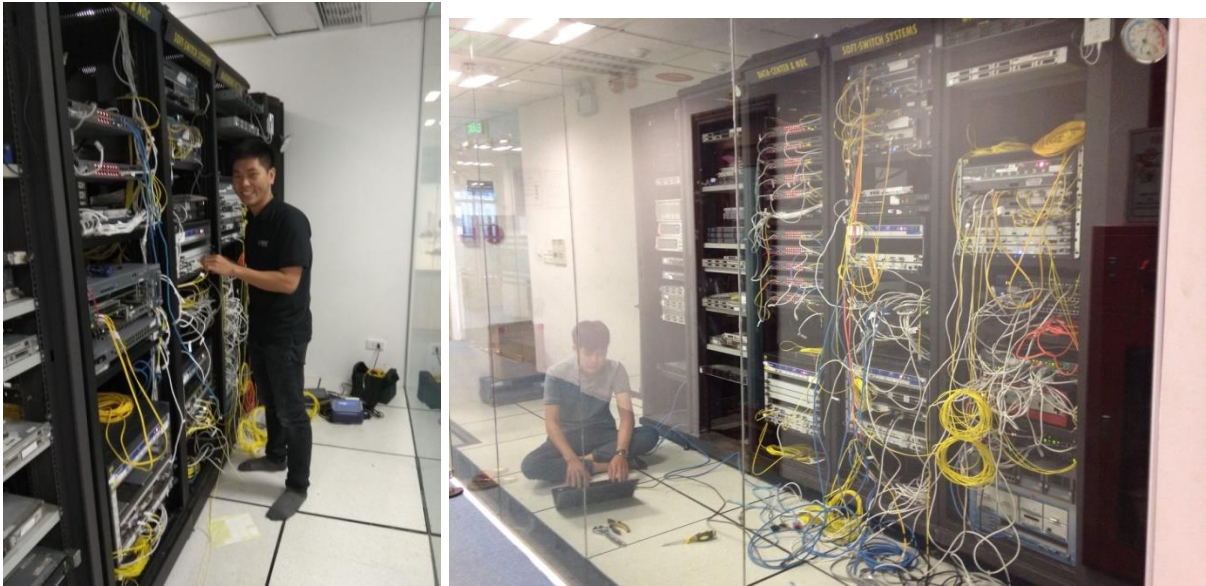
- Khi áp dụng QoS thì băng thông sẽ được cấp phát động, các tunnel có thể sử dụng băng thông của tunnel khác chưa sử dụng và khi tunnel khác cần sử dụng thì sẽ lấy lại.
- Trong khi nghẽn đường truyền thì các lưu lượng vượt quá băng thông cho phép sẽ bị rớt gói, còn các dịch vụ lưu lượng trong ngưỡng cho phép thì sẽ đảm bảo dịch vụ.

**3.4 Môi trường thực nghiệm**

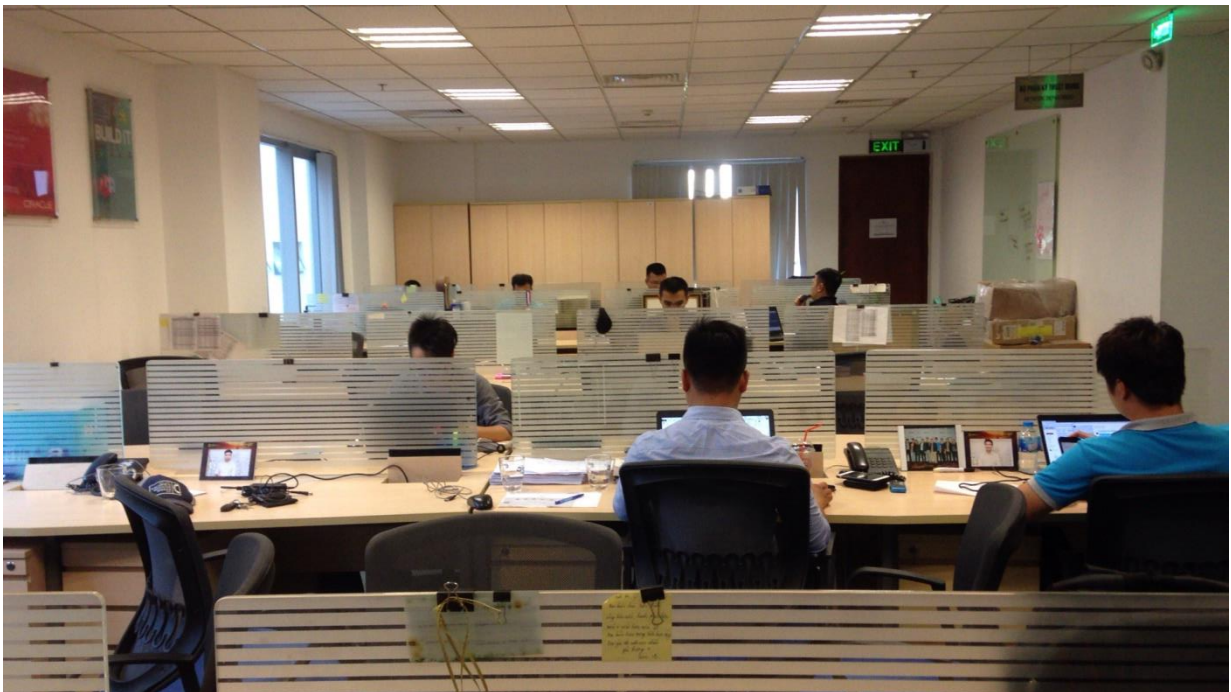
Các thiết bị dùng để thực nghiệm thuộc Công ty SVTech, công ty chuyên cung cấp các thiết bị mạng và server cho các nhà cung cấp dịch vụ viễn thông lớn ở Việt Nam (Viettel, FPT, MobilePhone, VinaPhone, CMC,...).



Hình 3.15: Công ty SVTech



Hình 3.16: Phòng LAB thiết bị mạng



Hình 3.17: Không gian làm việc của kỹ sư SVTech

# Chương 4: Kết luận

## 4.1 Vấn đề đặt ra

### 4.1.1 Tối ưu hiệu suất sử dụng tài nguyên mạng

Việc sử dụng IGP trong mạng sẽ xảy ra hiện tượng chia tải không đều giữa các kết nối trong mạng, có những kết nối bị nghẽn băng thông trong khi các kết nối khác có hiệu suất sử dụng thấp.

### 4.1.2 Đảm bảo chất lượng đường truyền

- Dịch vụ được truyền trên đường truyền có chất lượng dịch vụ tốt nhất (delay, jitter,...thấp, băng thông đảm bảo).
- Khi xảy ra sự cố đường truyền chính thì không bị gián đoạn dịch vụ.

## 4.2 Ứng dụng của MPLS-TE

### 4.2.1 Điều khiển lưu lượng

- Sử dụng các tunnel để điều chỉnh, cân tải lưu lượng giữa các đường truyền mạng, đảm bảo tận dụng tài nguyên mạng với hiệu suất cao, tránh các trường hợp nghẽn đường truyền làm ảnh hưởng dịch vụ.
- MPLS - TE hỗ trợ điều khiển từng loại lưu lượng khác nhau đi trên các tuyến đường khác nhau trong hệ thống mạng, ứng dụng để lái các loại dịch vụ quan trọng như VoIP qua các đường truyền có chất lượng tốt nhằm đảm bảo chất lượng dịch vụ.

### 4.2.2 Chọn đường đi chất lượng tốt nhất và đảm bảo chất lượng dịch vụ

- Tính toán được các thuộc tính vật lý của đường truyền (delay, jitter,...) để chọn đường đi tốt nhất.
- Kết hợp QoS đảm bảo chất lượng dịch vụ quan trọng khi xảy ra nghẽn đường truyền.

### 4.2.3 Khả năng hội tụ cao

- Có cơ chế dự phòng tốt, đảm bảo hội tụ nhanh khi có vấn đề xảy ra trên đường truyền, giúp cho không bị gián đoạn dịch vụ trong quá trình truyền lưu lượng.

## 4.3 Kết quả đạt được

Chứng minh bằng thử nghiệm trên thiết bị thật các vấn đề:

- Mạng sử dụng MPLS-TE có thời gian hội tụ đưa mạng về trạng thái ổn định nhanh hơn nhiều lần so với mạng chỉ sử dụng IP thuần (MPLS-TE hội tụ 353ms so với IP là 1033ms).
- Điều khiển lưu lượng theo đường đi mong muốn để tối ưu sử dụng tài nguyên mạng.
- Kết hợp QoS đảm bảo chất lượng dịch vụ và cấp phát băng thông động để sử dụng hiệu quả băng thông đường truyền.

## 4.4 Đề xuất cải tiến

### 4.4.1 Giám sát lưu lượng các tunnel dành riêng cho từng dịch vụ, khách hàng

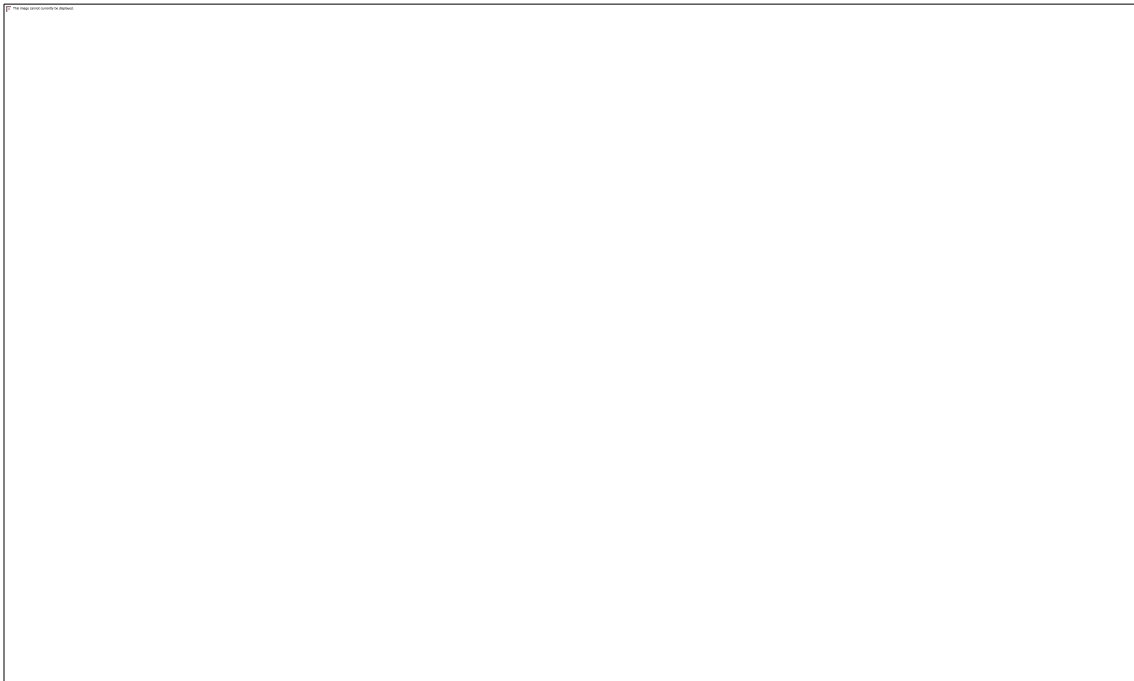
Cách thực hiện:

- Sử dụng công cụ giám sát áp dụng giao thức SNMP (Simple Network Management Protocol) để lấy thông tin lưu lượng trên từng tunnel dựa vào giá trị OID.
- Vẽ ra biểu đồ theo dõi lưu lượng theo thời gian thực (theo chu kỳ khoảng 5 phút).
- Ví dụ sử dụng SNMP để giám sát lưu lượng tunnel trên thiết bị Cisco:

OID:

```
target .1.3.6.1.2.1.31.1.1.1.6.65 {
    bits 64;
    table ifInOctets_3299;
    id 4486051;
    speed 9000000000000;
    descr "tunnel-te1 - 65 (IGW01_TO_PECD-HLC-01)";
};
target .1.3.6.1.2.1.31.1.1.1.10.65 {
    bits 64;
    table ifOutOctets_3299;
    id 4486051;
    speed 9000000000000;
    descr "tunnel-te1 - 65 (IGW01_TO_PECD-HLC-01)";
};
```

Biểu đồ giám sát lưu lượng:



Hình 4.1: Biểu đồ giám sát băng thông interface tunnel

**Lợi ích:**

- Kết hợp với giám sát lưu lượng các kết nối vật lý trên mạng để linh hoạt trong việc điều chỉnh đường đi, tối ưu hiệu suất sử dụng tài nguyên mạng.

- Dựa vào kết quả giám sát lưu lượng của từng tunnel đang chạy trên kết nối chính để tính toán băng thông trên hướng dự phòng cần phải dự trữ để đảm bảo dịch vụ trong trường hợp sự cố lỗi kết nối chính.
- Theo dõi băng thông tunnel để phát hiện sớm sự cố ảnh hưởng dịch vụ khi có hiện tượng tụt giảm băng thông bất thường.

#### **4.4.2 Kết hợp QoS đảm bảo chất lượng dịch vụ và cấp phát băng thông động**

##### **Cách thực hiện:**

- Đánh dấu các giá trị QoS cho các tunnel của các dịch vụ.
- Cấu hình QoS với các độ ưu tiên và băng thông tương ứng cho các tunnel của các dịch vụ khác nhau, đảm bảo các dịch vụ quan trọng luôn được ưu tiên cao hơn.
- Chuyển tiếp lưu lượng tương ứng từng dịch vụ vào các tunnel.

##### **Lợi ích:**

- Tối ưu việc sử dụng tài nguyên băng thông đường truyền: Trong trường hợp một tunnel không sử dụng hết băng thông được ưu tiên thì các tunnel khác có thể mượn để sử dụng, khi tunnel cần sử dụng thì sẽ được trả lại băng thông tunnel khác đã mượn.
- Đảm bảo chất lượng cho các dịch vụ quan trọng có độ ưu tiên cao: Trong trường hợp băng thông đường truyền bị nghẽn thì các dịch vụ có QoS cao sẽ luôn được đảm bảo băng thông.

# TÀI LIỆU THAM KHẢO

## Tiếng Việt

1. Trần Công Hùng (2009), Chuyển mạch nhãn đa giao thức MPLS, Nhà xuất bản Thông Tin và Truyền Thông.
2. <https://vi.wikipedia.org/>

## Tiếng Anh

3. Luc De Ghein (2007), MPLS Fundamentals, Cisco Press 800 East 96th Street Indianapolis.
4. Traffic Engineering with MPLS, By Eric Osborne CCIE #4122, Ajay Simha CCIE #2970.
5. Cisco Systems Learning (2006), Implementing Cisco MPLS, Cisco Systems.