BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

LUẬN VĂN THẠC SĨ KHOA HỌC

CÔNG NGHỆ MPLS VÀ ỨNG DỤNG TRONG MẠNG IP VPN

NGÀNH : ĐIỆN TỬ VIỄN THÔNG
MÃ SỐ:

NGUYỄN QUỲNH TRANG

Người hướng dẫn khoa học : TS. PHẠM NGỌC NAM

HÀ NỘI 2008

LỜI CAM ĐOAN

Kính gửi : Trung tâm Đào tạo và Bồi dưỡng sau Đại học
- Trường Đại học Bách khoa Hà nội

Tên tôi là : Nguyễn Quỳnh Trang

Sinh ngày: 12 – 03 – 1982

Học viên cao học khóa 2006 – 2008

Tôi xin cam đoan, toàn bộ kiến thức và nội dung trong bài luận văn của mình là các kiến thức tự nghiên cứu từ các tài liệu tham khảo trong và ngoài nước, không có sự sao chép hay vay mượn dưới bất kỳ hình thức nào để hoàn thành bản luận văn tốt nghiệp cao học chuyên ngành Điện tử Viễn thông.

Tôi xin chịu hoàn toàn trách nhiệm về nội dung của luận văn này trước Trung tâm Đào tạo và Bồi dưỡng sau Đại học – Trường Đại học Bách khoa Hà nội.

MỤC LỤC

TỪ VIẾT TẮT

ASIC	Application Specific Intergrated Circuits	Mạch tích hợp chuyên dụng
ATM	Asynchnorous Tranfer Mode	Truyền dẫn không đồng bộ
AToM	Any Transport over MPLS	Truyền tải qua MPLS
BGP	Border Gateway Protocol	Giao thức cổng biên
CE	Custome Edge	Biên phía khách hàng
CEF	Cisco Express Forwarding	Chuyển tiếp nhanh của Cisco
CoS	Class of Service	Cấp độ dịch vụ
CQ	Custom Queue	Hàng đợi tùy ý
CR	Constraint-based routing	Định tuyến ràng buộc
DiffServ	Differentiated Services	Dịch vụ khác biệt
DSCP	DiffServ Code Point	Mã điểm dịch vụ khác biệt
DS-TE	DiffServ-aware MPLS Traffic Engineering	Công nghệ điều khiển luồng MPLS quan tâm tới DiffiServ
E-LSR	Egress LER	LER biên ra
FEC	Forwarding Equivalency Class	Lớp chuyển tiếp tương đương
FTP	File Tranfer Protocol	Giao thức truyền file
GRE	Generic Routing Encapsulation	Đóng gói định tuyến chung
HDLC	High Data Link Control	Điều khiển kết nối dữ liệu tốc độ cao
IETF	Internet Engineering Task Force	Ủy ban tư vấn kỹ thuật Internet
IGP	Interior Gateway Protocol	Giao thức định tuyến trong phạm vi miền
I-LSR	Ingress LSR	LSR biên vào
IntServ	Integrated Services	Dịch vụ tích hợp

IP	Internet Protocol	Giao thức Internet
IS-IS	Intermediate System to Intermediate System Protocol	Giaot thức hệ thống trung gian tới hệ thống trung gian
LAN	Local Area Network	Mạng địa phương
LDP	Label Distribution Protocol	Giao thức phân phối nhãn
LER	Label Edge Router	Bộ định tuyến nhãn biên ra
LFIB	Label Forwarding Information Base	Cơ sở thông tin chuyển tiếp nhãn
LIB	Label Information Base	Bảng cơ sở dữ liệu nhãn
LSP	Label Switch Path	Tuyến chuyển mạch nhãn
LSR	Label Switch Router	Bộ định tuyến chuyển mạch nhãn
MAC	Media Access Control	Điều khiển truy nhập môi trường
MPLS	Multiprotool Label Switching	Chuyển mạch nhãn đa giao thức
MP-BGP	MPLS – border gateway Protocol	Đa giao thức cổng biên
OSPF	Open Shortest Path First	Giao thức OSPF
OUI	Organizationally Unique Identifier	Nhận dạng duy nhất tổ chức
PE	Provider Edge	Biên nhà cung cấp
PPP	Point-to-Point Protocol	Giao thức điểm - điểm
PQ	Priority Queue	Hàng đợi ưu tiên
PVC	Permanent Virtual Circuit	Mạch ảo cố định
QoS	Quanlity of Service	Chất lượng dịch vụ
RD	Route Distinguisher	Bộ phân biệt tuyến
RFC	Request for comment	Các tài liệu chuẩn do IETF đưa ra
RSVP	Resource Reservation Protocol	Giao thức dành sẵn tài nguyên

RT	Route Targets	Tuyến đích
SLA	Service Level Agreements	Thỏa thuận cấp độ dịch vụ
SP	Service Provider	Nhà cung cấp
SVC	Switch Virtual Connection	Chuyển mạch kết nối ảo
TCP	Tranmission Control Protocol	Giao thức điều khiển truyền dẫn
TDP	Tag Distribution Protocol	Giao thức phân phối tag
TE	Traffic Engineering	Kỹ thuật điều khiển lưu lượng
TTL	Time To Live	Thời gian sống
UDP	User Datagram Protocol	Giao thức UDP
UNI	User-to-Network Interface	Giao diện người dùng tới mạng
VC	Virtual Channel	Kênh ảo
VCI	Virtual Channel Identifier	Định danh kênh ảo
VoATM	Voice over ATM	Thoại qua ATM
VoIP	Voice over IP	Thoại qua IP
VP	Virtual Path	Tuyến ảo
VPI	Virtual Packet Indentifier	Định danh gói ảo
VPN	Virtual Pravite network	Mạng riêng ảo

DANH MỤC CÁC HÌNH VẼ

CHƯƠNG 1

CHƯƠNG 2

CHƯƠNG 3

CHƯƠNG 4

LỜI MỞ ĐẦU

Công nghệ MPLS (Multi Protocol Label Switching) được tổ chức quốc tế IETF chính thức đưa ra vào cuối năm 1997, đã phát triển nhanh chóng trên toàn cầu.

Công nghệ mạng riêng ảo MPLS VPN đã đưa ra một ý tưởng khác biệt hoàn toàn so với công nghệ truyền thống, đơn giản hóa quá trình tạo "đường hầm" trong mạng riêng ảo bằng cơ chế gán nhãn gói tin (Label) trên thiết bị mạng của nhà cung cấp. Thay vì phải tự thiết lập, quản trị, và đầu tư những thiết bị đắt tiền, MPLS VPN sẽ giúp doanh nghiệp giao trách nhiệm này cho nhà cung cấp – đơn vị có đầy đủ năng lực, thiết bị và công nghệ bảo mật tốt hơn nhiều cho mạng của doanh nghiệp.

Theo đánh giá của Diễn đàn công nghệ Ovum năm 2005, MPLS VPN là công nghệ nhiều tiềm năng, đang bước vào giai đoạn phát triển mạnh mẽ nhờ những tính năng ưu việt hơn hẳn những công nghệ truyền thống. Dự kiến cuối năm 2010, MPLS VPN sẽ dần thay thế hoàn toàn các công nghệ mạng truyền thống đã lạc hậu và là tiền đề tiến tới một hệ thống mạng băng rộng – Mạng thế hệ mới NGN (Next Generation Network).

Mạng truyền số liệu của EVNTelecom hiện này đang được triển khai dựa trên công nghệ chuyển mạch nhãn MPLS, với tính năng nổi trội MPLS/VPN đảm bảo an toàn thông tin, phục vụ ngày một tốt hơn cho nội bộ ngành điện, tiếp theo là nhằm cung cấp một cách đa dạng các loại dịch vụ cho người sử dụng.

Luận văn **"Công nghệ MPLS và ứng dụng trong mạng IPVPN"** đã nghiên cứu những kiến thức về công nghệ mạng riêng ảo MPLS/VPN và ứng dụng MPLS/VPN trong mạng EVNTelecom cung cấp dịch vụ mới IPVPN cho khách hàng.

Luận văn gồm 04 chương:

Chương 1: Tổng quan về công nghệ MPLS – Trình bày tổng quan về công nghệ chuyển mạch nhãn đa giao thức MPLS gồm khái niệm, ưu điểm và những ứng dụng của MPLS.

Chương 2: Công nghệ chuyển mạch MPLS – Trình bày những khái niệm cơ bản, các thành phần chính, cấu trúc và hoạt động của MPLS.

Chương 3: Mạng riêng ảo MPLS/VPN – bao gồm các khái niệm, các thành phần và hoạt động của MPLS/VPN.

Chương 4: Ứng dụng MPLS/VPN trong việc cung cấp dịch vụ IPVPN của EVNTelecom – trình bày tổng quan về mạng lõi và dịch vụ cho khách hàng IPVPN của mạng EVNTelecom.

Cuối cùng, để có được bản luận văn này, tôi xin bày tỏ lòng biết ơn sâu sắc tới gia đình, bạn bè, tới các thầy cô giáo của Trung tâm đào tạo và bồi dưỡng sau Đại Học, Khoa Điện tử - Viễn thông, Ban Giám hiệu Trường Đại học Bách Khoa Hà nội đã hết sức tạo điều kiện, động viên và truyền thụ các kiến thức bổ ích. Đặc biệt tôi xin gửi lời cám ơn chân thành đến thầy giáo – **T.S Phạm Ngọc Nam** cùng các đồng nghiệp tại Công ty Thông tin Viễn thông Điện lực đã tận tình giúp đỡ để tôi có thể hoàn thành tốt bài luận văn này.

CHƯƠNG 1
TỔNG QUAN VỀ CÔNG NGHỆ MPLS

Trong những năm gần đây MPLS (Multiprotocol Label Switching) phát triển rất nhanh. Nó trở thành công nghệ phổ biến sử dụng việc gắn nhãn vào các gói dữ liệu để chuyển tiếp chúng qua mạng. Chương này sẽ giúp chúng ta hiểu tại sao MPLS lại trở lên phổ biến trong thời gian ngắn như thế.

1.1 Giới thiệu về chuyển mạch đa giao thức (MPLS)

MPLS là một công nghệ kết hợp đặc điểm tốt nhất giữa định tuyến lớp ba và chuyển mạch lớp hai cho phép chuyển tải các gói rất nhanh trong mạng lõi (core) và định tuyến tốt mạng biên (edge) bằng cách dựa vào nhãn (label). MPLS là một phương pháp cải tiến việc chuyển tiếp gói trên mạng bằng cách gắn nhãn vào mỗi gói IP, tế bào ATM, hoặc frame lớp hai. Phương pháp chuyển mạch nhãn giúp các Router và các bộ chuyển mạch MPLS-enable ATM quyết định theo nội dung nhãn tốt hơn việc định tuyến phức tạp theo địa chỉ IP đích. MPLS cho phép các ISP cung cấp nhiều dịch vụ khác nhau mà không cần phải bỏ đi cơ sở hạ tầng sẵn có. Cấu trúc MPLS có tính mềm dẻo trong bất kỳ sự phối hợp với công nghệ lớp hai nào.

MPLS hỗ trợ mọi giao thức lớp hai, triển khai hiệu quả các dịch vụ IP trên một mạng chuyển mạch IP. MPLS hỗ trợ việc tạo ra các tuyến khác nhau giữa nguồn và đích trên một đường trục Internet. Bằng việc tích hợp MPLS vào kiến trúc mạng, các ISP có thể giảm chi phí, tăng lợi nhuận, cung cấp nhiều hiệu quả khác nhau và đạt được hiệu quả cạnh tranh cao.

Đặc điểm mạng MPLS:

- Không có MPLS API, cũng không có thành phần giao thức phía host.
- MPLS chỉ nằm trên các router.

- MPLS là giao thức độc lập nên có thể hoạt động cùng với giao thức khác IP như IPX, ATM, Frame Relay,…

- MPLS giúp đơn giản hoá quá trình định tuyến và làm tăng tính linh động của các tầng trung gian.

Phương thức hoạt động:

Thay thế cơ chế định tuyến lớp ba bằng cơ chế chuyển mạch lớp hai.MPLS hoạt động trong lõi của mạng IP. Các Router trong lõi phải enable MPLS trên từng giao tiếp. Nhãn được gắn thêm vào gói IP khi gói đi vào mạng MPLS. Nhãn được tách ra khi gói ra khỏi mạng MPLS. Nhãn (Label) được chèn vào giữa header lớp ba và header lớp hai. Sử dụng nhãn trong quá trình gửi gói sau khi đã thiết lập đường đi. MPLS tập trung vào quá trình hoán đổi nhãn (Label Swapping). Một trong những thế mạnh của kiến trúc MPLS là tự định nghĩa chồng nhãn (Label Stack).

Kỹ thuật chuyển mạch nhãn không phải là kỹ thuật mới. Frame relay và ATM cũng sử dụng công nghệ này để chuyển các khung (frame) hoặc các cell qua mạng. Trong Frame relay, các khung có độ dài bất kỳ, đối với ATM độ dài của cell là cố định bao gồm phần mào đầu 5 byte và tải tin là 48 byte. Phần mào đầu của cell ATM và khung của Frame Relay tham chiếu tới các kênh ảo mà cell hoặc khung này nằm trên đó. Sự tương quan giữa Frame relay và ATM là tại mỗi bước nhảy qua mạng, giá trị "nhãn" trong phần mào đầu bị thay đổi. Đây chính là sự khác nhau trong chuyển tiếp của gói IP. Khi một route chuyển tiếp một gói IP, nó sẽ không thay đổi giá trị mà gắn liền với đích đến của gói; hay nói cách khác nó không thay đổi địa chỉ IP đích của gói. Thực tế là các nhãn MPLS thường được sử dụng để chuyển tiếp các gói và địa chỉ IP đích không còn phổ biến trong MPLS nữa.

1.2 Lịch sử phát triển và các ưu điểm của MPLS

Các giao thức trước MPLS

Trước MPLS, giao thức WAN phổ biến nhất là ATM và Frame relay. Những mạng WAN có chi phí hiệu quả được xây dựng từ nhiều giao thức khác nhau. Cùng với việc bùng nổ mạng Internet, IP trở thành giao thức phổ biến nhất. IP ở khắp mọi nơi. VPN được tạo ra qua những giao thức WAN này. Khách hàng thuê những kết nối ATM và kết nối Frame relay hoặc sử dụng kênh truyền số liệu (kênh thuê riêng) và xây dựng mạng riêng của họ trên đó. Bởi vì những bộ định tuyến của nhà cung cấp cung cấp dịch vụ ở lớp 2 tới bộ định tuyến lớp 3 của khách hàng. Những kiểu mạng như vậy được gọi là mạng *overlay*. Hiện nay mạng Overlay vẫn được sử dụng nhưng rất nhiều khách hàng đã bắt đầu sử dụng dịch vụ MPLS VPN

1.2.1 Các lợi ích của MPLS

Phần này sẽ giới thiệu một cách ngắn gọn những lợi ích của việc sử dụng MPLS trong mạng. Những lợi ích này bao gồm:

- Việc sử dụng hạ tầng mạng thống nhất
- Ưu điểm vượt trội so với mô hình IP over ATM
- Giao thức cổng biên (BGP) – lõi tự do
- Mô hình peer to peer cho MPLS VPN
- Chuyển lưu lượng quang
- Điều khiển lưu lượng

Ta sẽ xem xét về lý do không có thực để chạy MPLS. Đây là lý do mà được xem hợp lý đầu tiên trong việc sử dụng MPLS nhưng nó không phải là lý do tốt để triển khai MPLS.

- Lợi ích không có thực (lợi ích về tốc độ):

Một trong những lý do đầu tiên đưa ra của giao thức trao đổi nhãn đó là sự cần thiết cải thiện tốc độ. Chuyển mạch gói IP trên CPU được xem như chậm

hơn so với chuyển mạch gói gán nhãn do chuyển mạch gói gán nhãn chỉ tìm kiếm nhãn trên cùng của gói. Một bộ định tuyến chuyển tiếp gói IP bằng việc tìm kiếm địa chỉ IP đích trong phần mào đầu IP và tìm kiếm kết nối tốt nhất trong bảng định tuyến. Việc tìm kiếm này phụ thuộc vào sự thực hiện của từng nhà cung cấp của bộ định tuyến đó. Tuy nhiên, bởi vì địa chỉ IP có thể là đơn hướng hoặc đa hướng (unicast hoặc multicast) và có 4 octet (1 octet = 1 ô 8 bit) nên việc tìm kiếm có thể rất phức tạp. Việc tìm kiếm phức tạp cũng có nghĩa là quyết định chuyển tiếp gói IP mất một thời gian.

Thời gian gần đây, các đường kết nối trên những bộ định tuyến có thể có băng thông lên tới 40 Gbps. Một bộ định tuyến mà có một vài đường link tốc độ cao không có khả năng chuyển mạch tất cả những gói IP mà chỉ sử dụng CPU để đưa ra quyết định chuyển tiếp. CPU tồn tại chủ yếu để sử dụng (điều khiển) bảng điều khiển.

Mặt phẳng điều khiển là một tập các giao thức để thiết lập một mặt phẳng dữ liệu hoặc mặt phẳng chuyển tiếp. Các thành phần chính của mặt phẳng điều khiển bao gồm giao thức định tuyến, bảng định tuyến và chức năng điều khiển khác hoặc giao thức báo hiệu được sử dụng để cung cấp mặt phẳng dữ liệu. Mặt phẳng dữ liệu là một đường chuyển tiếp gói qua bộ định tuyến hoặc bộ chuyển mạch. Sự chuyển mạch của các gói – hay mặt phẳng chuyển tiếp – hiện nay được thực hiện trên phần cứng được xây dựng riêng, hoặc thực hiện trên mạch tích hợp chuyên dụng (ASIC – Application specific intergrated circuits). Việc dùng ASIC trong mặt phẳng chuyển tiếp của bộ định tuyến dẫn đến những gói IP được chuyển mạch nhanh như các gói được dán nhãn. Do đó, nếu lý do duy nhất để đưa MPLS vào mạng là để tiếp tục thực hiện việc chuyển mạch các gói nhanh hơn qua mạng, đó chính là lý do ảo.

- Sử dụng hạ tầng mạng đơn hợp nhất

Với MPLS, ý tưởng là gán nhãn cho gói đi vào mạng dựa trên địa chỉ đích của nó hoặc tiêu chuẩn trước cấu hình khác và chuyển mạch tất cả lưu lượng qua hạ tầng chung. Đây là một ưu điểm vượt trội của MPLS. Một trong những lý do mà IP trở thành giao thức duy nhất ảnh hưởng lớn tới mạng trên toàn thế giới là bởi vì rất nhiều kỹ thuật có thể được chuyển qua nó. Không chỉ là dữ liệu (số liệu) chuyển qua IP mà còn cả thoại.

Bằng việc sử dụng MPLS với IP, ta có thể mở rộng khả năng truyền loại dữ liệu. Việc gắn nhãn vào gói cho phép ta mang nhiều giao thức khác hơn là chỉ có IP qua mạng trục IP lớp 3 MPLS-enabled, tương tự với những khả năng thực hiện được với mạng Frame Relay hoặc ATM lớp 2. MPLS có thể truyền IPv4, IPv6, Ethernet, điều khiển kết nối dữ liệu tốc độ cao (HDLC), PPP, và những kỹ thuật lớp 2 khác.

Chức năng mà tại đó bất kỳ khung lớp 2 được mang qua mạng đường trục MPLS được gọi là *Any Transport over MPLS (AToM)*. Những bộ định tuyến đang chuyển lưu lượng AToM không cần thiết phải biết tải MPLS; nó chỉ cần có khả năng chuyển mạch lưu lượng được dán nhãn bằng việc tìm kiếm nhãn trên đầu của tải. Về bản chất, chuyển mạch nhãn MPLS là một công thức đơn giản của chuyển mạch đa giao thức trong một mạng. Ta cần phải có bảng chuyển tiếp bao gồm các nhãn đến để trao đổi với nhãn ra và bước tiếp theo.

Tóm lại, AToM cho phép nhà cung cấp dịch vụ cung cấp dịch vụ ở cùng lớp 2 tới khách hàng như bất kỳ mạng khác. Tại cùng một thời điểm, nhà cung cấp dịch vụ chỉ cần một hạ tầng mạng đơn để có thể mang tất cả các loại lưu lượng của khách hàng.

1.2.2 Đặc điểm vượt trội của MPLS so với mô hình IP over ATM

Khi hợp nhất với chuyển mạch ATM, chuyển mạch nhãn tận dụng những thuận lợi của các tế bào ATM - chiều dài thích hợp và chuyển với tốc độ cao. Trong mạng đa dịch vụ chuyển mạch nhãn cho phép chuyển mạch BPX/MGX nhằm cung cấp dịch vụ ATM, Frame, Replay và IP Internet trên một mặt phẳng đơn trong một đường đi tốc độ cao. Các mặt phẳng (Platform) công cộng hỗ trợ các dịch vụ này để tiết kiệm chi phí và đơn giản hóa hoạt động cho nhà cung cấp đa dịch vụ. ISP sử dụng chuyển mạch ATM trong mạng lõi, chuyển mạch nhãn giúp các dòng Cisco, BPX8600, MGX8800, Router chuyển mạch đa dịch vụ 8540 và các chuyển mạch Cisco ATM giúp quản lí mạng hiệu quả hơn xếp chồng (overlay) lớp IP trên mạng ATM. Chuyển mạch nhãn tránh những rắc rối gây ra do có nhiều router ngang hàng và hỗ trợ cấu trúc phân cấp (hierarchical structure) trong một mạng của ISP.

- ***Sự tích hợp***: MPLS xác nhập tính năng của IP và ATM chứ không xếp chồng lớp IP trên ATM. MPLS giúp cho cơ sở hạ tầng ATM thấy được định tuyến IP và loại bỏ các yêu cầu ánh xạ giữa các đặc tính IP và ATM. MPLS không cần địa chỉ ATM và kỹ thuật định tuyến (như PNNI).
- ***Độ tin cậy cao hơn***: Với cơ sở hạ tầng ATM, MPLS có thể kết hợp hiệu quả với nhiều giao thức định tuyến IP over ATM thiết lập một mạng lưới (mesh) dịch vụ công cộng giữa các router xung quanh một đám mây ATM. Tuy nhiên có nhiều vấn đề xảy ra do các PCV link giữa các router xếp chồng trên mạng ATM. Cấu trúc mạng ATM không thể thấy bộ định tuyến. Một link ATM bị hỏng làm hỏng nhiều router-to-router link, gây khó khăn cho lượng cập nhật thông tin định tuyến và nhiều tiến trình xử lí kéo theo.
- ***Trực tiếp thực thi các loại dịch vụ***: MPLS sử dụng hàng đợi và bộ

đếm của ATM để cung cấp nhiều loại dịch vụ khác nhau. Nó hỗ trợ quyền ưu tiên IP và cấp dịch vụ CoS trên chuyển mạch ATM mà không cần chuyển đổi phức tạp sang các lớp ATM Forum Service.

- ***Hỗ trợ hiệu quả cho Mulicast và RSVP***: Khác với MPLS, xếp lớp IP trên ATM nảy sinh nhiều bất lợi, đặc biệt trong việc hỗ trợ các dịch vụ IP như IP muticast và RSVP (giao thức dành trước tài nguyên). MPLS hỗ trợ các dịch vụ này, kế thừa thời gian và công việc theo các chuẩn và khuyến khích tạo nên ánh xạ xấp xỉ của các đặc trưng IP&ATM
- ***Sự đo lường và quản lí VPN***: MPLS có thể tính được các dịch vụ IP VPN và rất dễ quản lí các dịch vụ VPN quan trọng để cung cấp các mạng IP riêng trong cơ sở hạ tầng của nó. Khi một ISP cung cấp dịch vụ VPN hỗ trợ nhiều VPN riêng trên một cơ sở hạ tầng đơn.Với một đường trục MPLS, thông tin VPN chỉ được xử lí tại một điểm ra vào. Các gói mang nhãn MPLS đi qua một đường trục và đến điểm ra đúng của nó. Kết hợp MPLS với MP- BGP (đa giao thức cổng biên) tạo ra các dịch vụ VNP dựa trên nền MPLS (MPLS-based VNP) dễ quản lí hơn với sự điều hành chuyển tiếp để quản lí phía VNP và các thành viên VNP, dịch vụ MPSL-based VNP còn có thể mở rộng để hỗ trợ hàng trăm nghìn VPN.
- ***Giảm tải trên mạng lõi***: Các dịch vụ VPN hướng dẫn cách MPLS hỗ trợ mọi thông tin định tuyến để phân cấp. Hơn nữa, có thể tách rời các định tuyến Internet khỏi lõi mạng cung cấp dịch vụ. Giống như dữ liệu VPN, MPSL chỉ cho phép truy suất bảng định tuyến Internet tại điểm ra vào của mạng. Với MPSL, kĩ thuật lưu lượng truyền ở biên của AS được gắn nhãn để liên kết với điểm tương ứng. Sự tách rời của định tuyến nội khỏi định tuyến Internet đầy đủ cũng giúp hạn

chế lỗi, ổn định và tăng tính bảo mật.

- ***Khả năng điều khiển lưu lượng***: MPLS cung cấp các khả năng điều khiển lưu lượng để sửng dụng hiệu quả tài nguyên mạng. Kỹ thuật lưu lượng giúp chuyển tải từ các phần quá tải sang các phần còn rỗi của mạng dựa vào điểm đích, loại lưu lượng, tải, thời gian,…

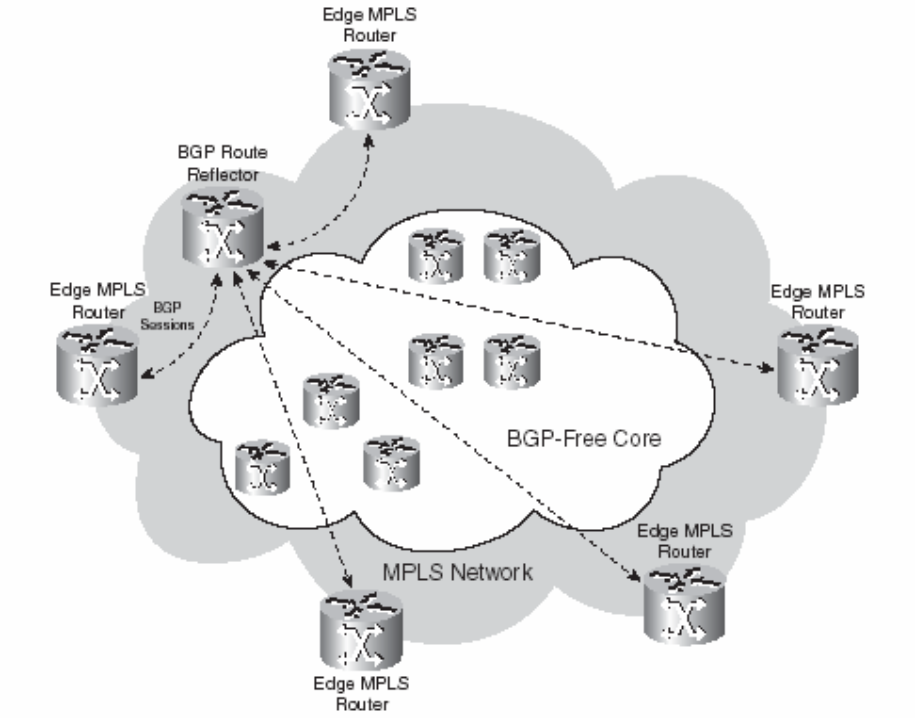
1.2.3 BGP – Free Core

Khi mạng IP của nhà cung cấp dịch vụ phải chuyển tiếp lưu lượng, mỗi bộ định tuyến phải tìm kiếm địa chỉ đích của gói. Nếu những gói được gửi tới đích nằm ngoài mạng của nhà cung cấp này, những tiền tố IP ngoài phải được thể hiện trong bảng định tuyến của mỗi bộ định tuyến. BGP mang tiền tố ngoài như là tiền tố của khách hàng hay tiền tố Internet. Có nghĩa là tất cả các bộ định tuyến trong mạng nhà cung cấp dịch vụ phải chạy BGP.

Tuy nhiên, MPLS cho phép chuyển tiếp những gói dựa trên tìm kiếm nhãn hơn là tìm kiếm địa chỉ IP. MPLS cho phép một nhãn được kết hợp với một bộ định tuyến vào hơn là với địa chỉ IP đích của gói. Nhãn này là thông tin được gán vào mỗi gói để thể hiện rằng tất cả bộ định tuyến trung gian tới bộ định tuyến biên vào mà nó phải chuyển tiếp tới. Bộ định tuyến lõi không cần thiết phải có thông tin để chuyển tiếp những gói dựa trên địa chỉ đích nữa. Do đó những bộ định tuyến lõi trong mạng nhà cung cấp dịch vụ không cần thiết chạy BGP.

Một bộ định tuyến tại biên của mạng MPLS vẫn cần xem xét (look at) địa chỉ IP đích của gói và do đó vẫn cần phải chạy BGP. Mỗi tiền tố BGP trên những bộ định tuyến MPLS ra có một địa chỉ IP bước nhảy tiếp theo BGP kết hợp với nó. Địa chỉ IP bước nhảy tiếp theo BGP là một địa chỉ IP của bộ định tuyến MPLS vào. Nhãn kết hợp với gói IP là nhãn mà kết hợp với địa chỉ IP bước nhảy tiếp theo BGP. Bởi vì tất cả các bộ định tuyến lõi chuyển tiếp gói

dựa trên nhãn MPLS được gán mà kết hợp với địa chỉ IP bước nhảy tiếp theo BGP, mỗi địa chỉ IP bước nhảy tiếp theo BGP của bộ định tuyến MPLS vào phải được tất cả những bộ định tuyến lõi biết đến. Bất kỳ giao thức định tuyến cổng trong (như giao thức OSPF hoặc IS-IS) có thể thực hiện nhiệm vụ này.



Hình 1- 1 Mạng lõi MPLS BGP free

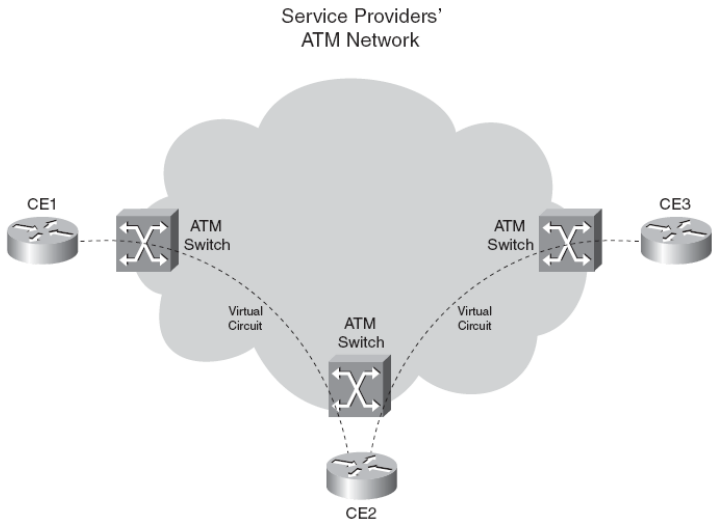
Một nhà cung cấp dịch vụ Internet (ISP) có 200 bộ định tuyến trong mạng lõi của nó cần phải chạy BGP trên tất cả 200 bộ định tuyến này. Nếu MPLS được bổ sung vào mạng thì chỉ những bộ định tuyến biên (khoảng 50 bộ định tuyến) cần thiết phải chạy BGP.

Hiện nay tất cả các bộ định tuyến trong mạng lõi đang thực hiện chuyển tiếp những gói được gắn nhãn, không phải tìm kiếm địa chỉ IP, do đó chúng ta phần nào bỏ bớt được các gánh nặng chạy BGP. Bởi vì bảng định tuyến Internet đầy đủ có thể có hơn 150.000 bộ định tuyến, việc chạy BGP trên tất cả bộ định tuyến là rất lớn. Các bộ định tuyến không bảng định tuyến Internet

đầy đủ cần ít dung lượng bộ nhớ. Ta có thể chạy bộ định tuyến lõi không cần kết hợp có BGP trên đó.

1.2.4 Luồng lưu lượng quang

Bởi vì chuyển mạch ATM hoặc Frame Relay chỉ đơn thuần ở Lớp 2, những bộ định tuyến kết nối qua chúng bởi các kênh ảo được tạo ra giữa chúng. Đối với bất kỳ một bộ định tuyến để chuyển lưu lượng trực tiếp tới một bộ định tuyến khác tại biên, một kênh ảo sẽ được tạo ra thẳng giữa chúng. Việc tạo ra những kênh ảo bằng tay này thường nhàm chán. Trong bất kỳ trường hợp này, nếu yêu cầu kết nối any – to – any giữa các site, cần thiết phải có mesh đầy đủ của những kênh ảo giữa các site, điều này làm tăng tính cồng kềnh mạng và tăng chi phí. Nếu các site chỉ kết nối với nhau như hình 1-2, lưu lượng từ CE1 tới CE3 phải đi qua CE2 trước.



Hình 1- 2 Non-Fully Meshed Overlay ATM Network

Kết quả là lưu lượng qua mạng đường trục ATM hai lần và đi đường vòng qua bộ định tuyến CE2. Khi sử dụng MPLS VPN như đưa ra trong phần trước, lưu lượng đổ trực tiếp – do đó tối ưu – giữa tất cả các kết cuối khách hàng. Đối với lưu lượng để di chuyển tối ưu giữa các kết cuối trong trường hợp của mô hình overlay VPN, tất cả các kết cuối phải được kết nối với nhau,

do đó yêu cầu có thiết kế dạng mesh đầy đủ của các đường kết nối hoặc các kênh ảo.

1.3 Ứng dụng của mạng MPLS

1.3.1 Mạng riêng ảo VPN

MPLS-VPN : Không giống như các mạng VPN truyền thống, các mạng MPLS-VPN không sử dụng hoạt động đóng gói và mã hóa gói tin để đạt được mức độ bảo mật cao. MPLS VPN sử dụng bảng chuyển tiếp và các nhãn "tags" để tạo nên tính bảo mật cho mạng VPN. Kiến trúc mạng loại này sử dụng các tuyến mạng xác định để phân phối các dịch vụ iVPN, và các cơ chế xử lý thông minh của MPLS VPN lúc này nằm hoàn toàn trong phần lõi của mạng.

Mỗi VPN được kết hợp với một bảng định tuyến - chuyển tiếp VPN (VRF) riêng biệt. VRF cung cấp các thông tin về mối quan hệ trong VPN của một site khách hàng khi được nối với PE router. Bảng VRF bao gồm thông tin bảng định tuyến IP (IP routing table), bảng CEF (Cisco Express Forwarding), các giao diện của forwarding table; các quy tắc, các tham số của giao thức định tuyến... Mỗi site chỉ có thể kết hợp với một và chỉ một VRF. Các VRF của site khách hàng mang toàn bộ thông tin về các "tuyến" có sẵn từ site tới VPN mà nó là thành viên.

Đối với mỗi VRF, thông tin sử dụng để chuyển tiếp các gói tin được lưu trong các IP routing table và CEF table. Các bảng này được duy trì riêng rẽ cho từng VRF nên nó ngăn chặn được hiện tượng thông tin bị chuyển tiếp ra ngoài mạng VPN cũng như ngăn chặn các gói tin bên ngoài mạng VPN chuyển tiếp vào các router bên trong mạng VPN. Đây chính là cơ chế bảo mật của MPLS VPN. Bên trong mỗi một MPLS VPN, có thể kết nối bất kỳ hai

điểm nào với nhau và các site có thể gửi thông tin trực tiếp cho nhau mà không cần thông qua site trung tâm.

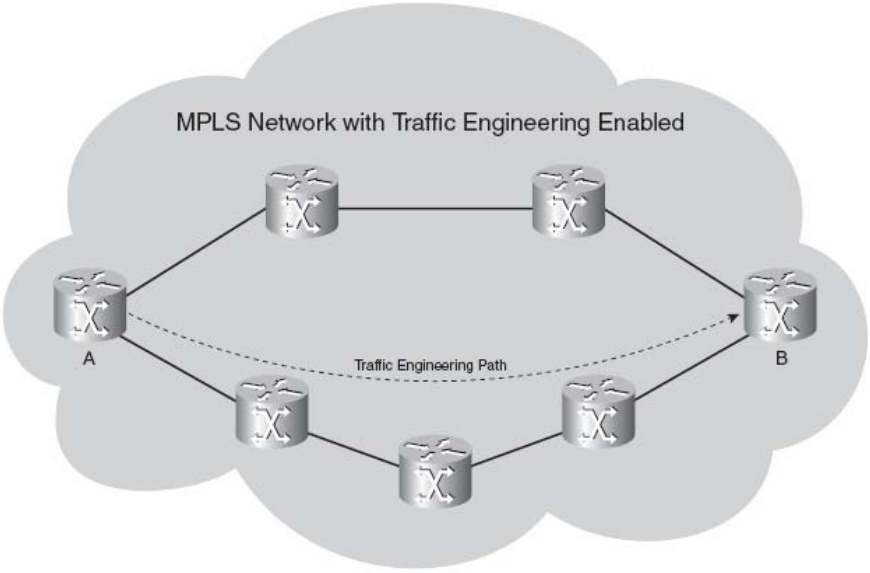
Ưu điểm đầu tiên của MPLS-VPN là không yêu cầu các thiết bị CPE thông minh. Vì các yêu cầu định tuyến và bảo mật đã được tích hợp trong mạng lõi. Chính vì thế việc bảo dưỡng cũng khá đơn giản, vì chỉ phải làm việc với mạng lõi. Trễ trong mạng MPLS-VPN là rất thấp, sở dĩ như vậy là do MPLS-VPN không yêu cầu mã hoá dữ liệu vì đường đi của VPN là đường riêng, được định tuyến bởi mạng lõi, nên bên ngoài không có khả năng thâm nhập và ăn cắp dữ liệu (điều này giống với FR).

Ngoài ra việc định tuyến trong MPLS chỉ làm việc ở lớp 2,5 chứ không phải lớp 3 vì thế giảm được một thời gian trễ đáng kể. Các thiết bị định tuyến trong MPLS là các Switch router định tuyến bằng phần cứng, vì vậy tốc độ cao hơn phần mềm như ở các router khác. Việc tạo Full mesh là hoàn toàn đơn giản vì việc tới các site chỉ cần dựa theo địa chỉ được cấu hình sẵn trong bảng định tuyến chuyển tiếp VPN (VEF).

1.3.2 Điều khiển lưu lượng trong MPLS

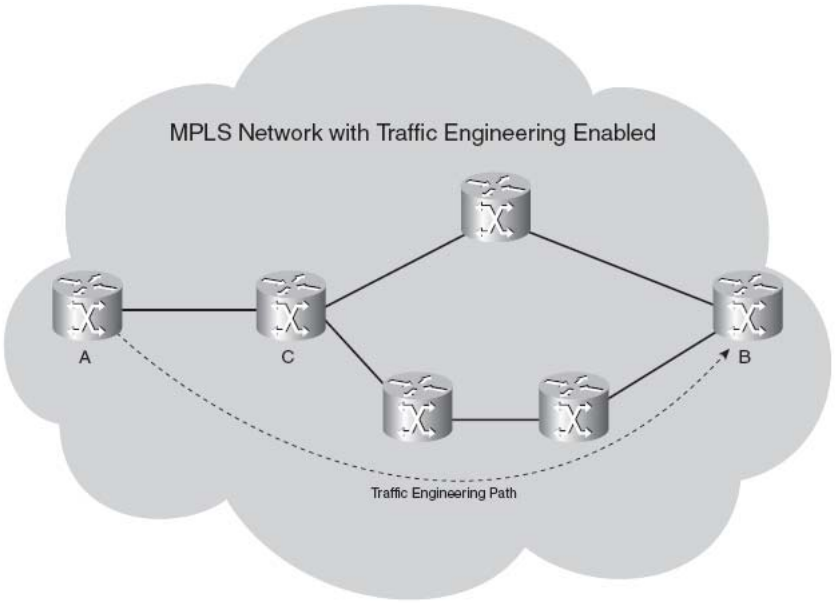
Ý tưởng cơ bản đằng sau việc điều khiển lưu lượng là để sử dụng tối ưu hạ tầng mạng, bao gồm các đường kết nối sử dụng không đúng mức, bởi vì chúng không thể thuộc các tuyến ưu tiên. Điều này có nghĩa là điều khiển lưu lượng phải cung cấp khả năng hướng lưu lượng qua mạng trên các tuyến đi khác nhau từ tuyến ưu tiên, đây là tuyến có chi phí thấp nhất được cung cấp bởi định tuyến IP. Tuyến chi phí thấp nhất là tuyến đường ngắn nhất như tính toán bởi giao thức định tuyến động. Với nhiệm vụ điều khiển lưu lượng trong mạng MPLS, ta có thể có lưu lượng mà được xác định cụ thể từ trước hoặc với chất lượng cụ thể của luồng dịch vụ từ điểm A đến điểm B dọc theo một tuyến (mà tuyến này khác với tuyến có chi phí thấp nhất). Kết quả là lưu

lượng có thể trải rộng hơn qua những đường kết nối có sẵn trong mạng và làm cho sử dụng nhiều đường kết nối không sử dụng đúng trong mạng. Hình 1-3 thể hiện ví dụ này.



Hình 1- 3 Điều khiển lưu lượng trong MPLS (ví dụ 1)

Như người điều hành mạng điều khiển lưu lượng MPLS, ta có thể hướng lưu lượng từ điểm A tới điểm B qua tuyến dưới (đây không phải là tuyến ngắn nhất giữa A và B – 4 bước so với 3 bước nhảy ở tuyến trên). Theo đúng nghĩa, ta có thể gửi lưu lượng qua các đường kết nối mà chúng có thể không được sử dụng nhiều. Ta có thể hướng lưu lượng trong mạng trên đường phía dưới bằng việc thay đổi ngôn ngữ giao thức định tuyến. Ví dụ hình 1-4.



Hình 1- 4 Điều khiển lưu lượng trong MPLS (ví dụ 2)

Nếu mạng này là mạng IP đơn thuần, ta có thể không có bộ định tuyến C chuyển lưu lượng dọc theo tuyến phía dưới bằng cách cấu hình một vài thứ trên bộ định tuyến A. Bộ định tuyến C quyết định để gửi lưu lượng trên tuyến trên hay tuyến dưới chỉ là do quyết định của chính nó. Nếu ta có thể điều khiển lưu lượng MPLS cho phép trên mạng này, ta cần có bộ định tuyến A gửi lưu lượng tới bộ định tuyến B dọc theo tuyến dưới. Điều khiển lưu lượng MPLS bắt buộc bộ định tuyến C chuyển tiếp lưu lượng A – B trên tuyến dưới. Điều này có thể thực hiện được trong MPLS do cơ chế chuyển tiếp nhãn. Bộ định tuyến đầu (head end router) (ở đây là bộ định tuyến A) của tuyến điều khiển lưu lượng là bộ định tuyến mà đưa ra tuyến đầy đủ để lưu lượng chuyển qua mạng MPLS. Bởi vì nó là bộ định tuyến đầu cuối (head end router) mà chỉ rõ tuyến, điều khiển lưu lượng cũng được nhắc đến (xem tham khảo – refer) tới như là dạng (form) của định tuyến nguồn cơ bản (*source – based routing*). Nhãn được dán (gắn) vào gói bởi bộ định tuyến đầu cuối (head end router) sẽ tạo nên luồng lưu lượng gói dọc theo tuyến đường mà do bộ định

tuyến đầu cuối chỉ rõ. Không có bộ định tuyến trung gian nào chuyển tiếp gói trên một tuyến khác.

Một ưu điểm vượt trội của việc sử dụng điều khiển lưu lượng MPLS là khả năng định tuyến lại nhanh (Fast ReRouting – FRR). FRR cho phép ta định tuyến lại lưu lượng có nhãn quanh một đường kết nối hoặc một bộ định tuyến mà trở thành không dùng được. Việc định tuyến lại lưu lượng xảy ra nhỏ hơn 50ms, mà nó nhanh như tiêu chuẩn hiện nay.

1.3.3 Chất lượng dịch vụ trong MPLS (QoS)

Chất lượng dịch vụ QoS chính là yếu tố thúc đẩy MPLS. So sánh với các yếu tố khác, như quản lý lưu lượng và hỗ trợ VPN thì QoS không phải là lý do quan trọng nhất để triển khai MPLS. Như chúng ta sẽ thấy dưới đây, hầu hết các công việc được thực hiện trong MPLS QoS tập trung vào việc hỗ trợ các đặc tính của IP QoS trong mạng. Nói cách khác, mục tiêu là thiết lập sự giống nhau giữa các đặc tính QoS của IP và MPLS, chứ không phải là làm cho MPLS QoS chất lượng cao hơn IP QoS.

Một trong những nguyên nhân để khẳng định MPLS đó là không giống như IP, MPLS không phải là giao thức xuyên suốt. MPLS không chạy trong các máy chủ, và trong tương lai nhiều mạng IP không sử dụng MPLS vẫn tồn tại. QoS mặt khác là đặc tính xuyên suốt của liên lạc giữa các LSR cùng cấp. Ví dụ, nếu một kênh kết nối trong tuyến xuyên suốt có độ trễ cao, độ tổn thất lớn, băng thông thấp sẽ giới hạn QoS có thể cung cấp dọc theo tuyến đó. Một cách nhìn nhận khác về vấn đề này là MPLS không thay đổi về căn bản mô hình dịch vụ IP. Các nhà cung cấp dịch vụ không bán dịch vụ MPLS, họ bán dịch vụ IP (hay dịch vụ Frame Relay hay các dịch vụ khác), và do đó, nếu họ đưa ra QoS thì họ phải đưa ra IP QoS (Frame Relay QoS, v.v) chứ không phải là MPSL QoS.

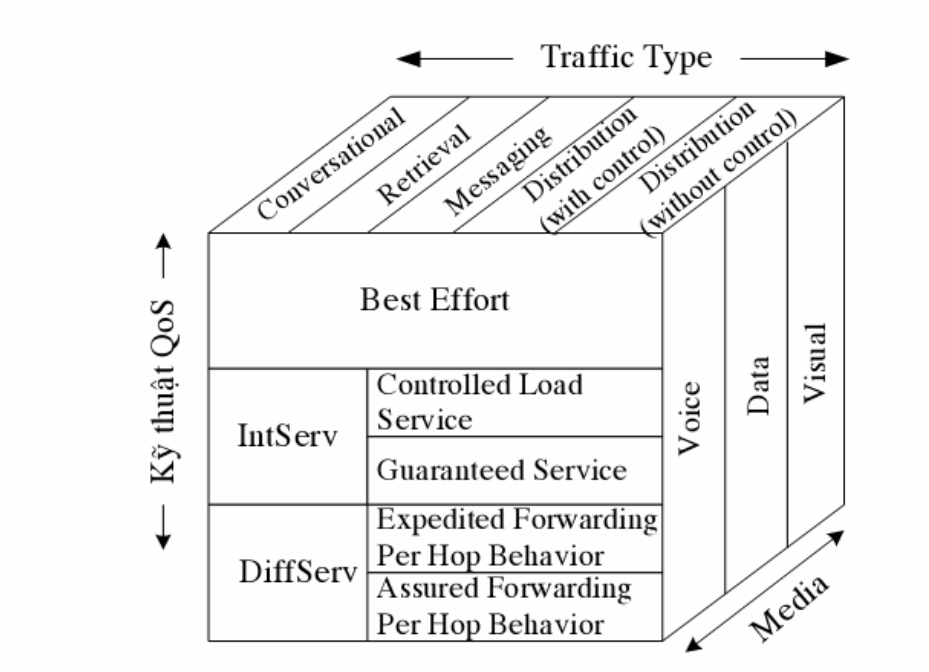
Điều đó không có nghĩa là MPLS không có vai trò trong IP QoS. Thứ nhất, MPLS có thể giúp nhà cung cấp đưa ra các dịch vụ IP QoS hiệu quả hơn. Thứ hai, hiện đang xuất hiện một số khả năng QoS mới hỗ trợ qua mạng sử dụng MPLS không thực sự xuyên suốt tuy nhiên có thể chứng tỏ là rất hữu ích, một trong số chúng là băng thông bảo đảm của LSP.

Chất lượng dịch vụ trở lên phổ biến trong những năm qua. Một vài mạng không có sự hạn chế về băng thông, do đó tắc nghẽn thường xuyên có khả năng xảy ra trong mạng. Qos là một phương tiện (means) để dành sự ưu tiên cho những lưu lượng quan trọng hơn những lưu lượng kém ưu tiên khác và đảm bảo rằng nó được vận chuyển qua mạng. IETF được thiết kế 2 cách để thực hiện QoS trong mạng IP: dịch vụ tích hợp (IntServ) và dịch vụ khác biệt (DiffServ).

- IntServ sử dụng giao thức báo hiệu giao thức dành trước tài nguyên (RSVP). Máy chủ báo hiệu cho mạng qua RSVP sự cần thiết QoS là cho luồng lưu lượng mà nó truyền.
- Việc đưa ra mô hình IntServ có vẻ như giải quyết được nhiều vấn đề liên quan đến QoS trong mạng IP. Tuy nhiên trong thực tế mô hình này đã không đảm bảo được QoS xuyên suốt (end to end). Đã có nhiều cố gắng nhằm thay đổi điều này nhằm đạt một mức QoS cao hơn cho mạng IP, và một trong những cố gắng đó là sự ra đời của DiffServ. DiffServsử dụng việc đánh dấu gói và xếp hàng theo loại để hỗ trợ dịch vụ ưu tiên qua mạng IP. Những bộ định tuyến tìm kiếm những bit để đánh dấu, xếp hàng, định hình, và thiết lập quyền ưu tiên (drop) của gói.
- Dịch vụ Best effort: Đây là dịch vụ phổ biến trên mạng Internet hay mạng IP nói chung. Các gói thông tin được truyền đi theo nguyên tắc "đến trước phục vụ trước" mà không quan tâm đến đặc tính lưu

lượng của dịch vụ là gì. Điều này dẫn đến rất khó hỗ trợ các dịch vụ đòi hỏi độ trễ thấp như các dịch vụ thời gian thực hay video. Cho đến thời điểm này, đa phần các dịch vụ được cung cấp bởi mạng Internet vẫn sử dụng nguyên tắc Best Effort này.

Ưu điểm lớn của DiffServ so với IntServ là mô hình DiffServ không cần giao thức báo hiệu. Mô hình IntServ sử dụng một giao thức báo hiệu mà phải chạy trên máy chủ và bộ định tuyến. Nếu mạng có hàng nghìn lưu lượng, những bộ định tuyến phải giữ thông tin trạng thái cho mỗi luồng lưu lượng truyền qua nó. Đây là một vấn đề lớn làm cho IntServ trở nên không phổ biến. Ví dụ tốt nhất cho QoS là lưu lượng VoIP. VoIP cần thiết được truyền tới đích trong thời gian thực, nếu không nó sẽ không còn dùng được. Do đó, QoS phải ưu tiên lưu lượng VoIP để đảm bảo nó được truyền trong một thời gian xác định. Để đạt được điều này, Cisco IOS đặt VoIP với mức ưu tiên cao hơn lưu lượng FTP hoặc HTTP và để đảm bảo rằng khi nghẽn mạch xảy ra, lưu lượng FTP hoặc HTTP sẽ bị đánh rớt trước VoIP.



Hình 1- 5 Các kỹ thuật QoS trong mạng IP

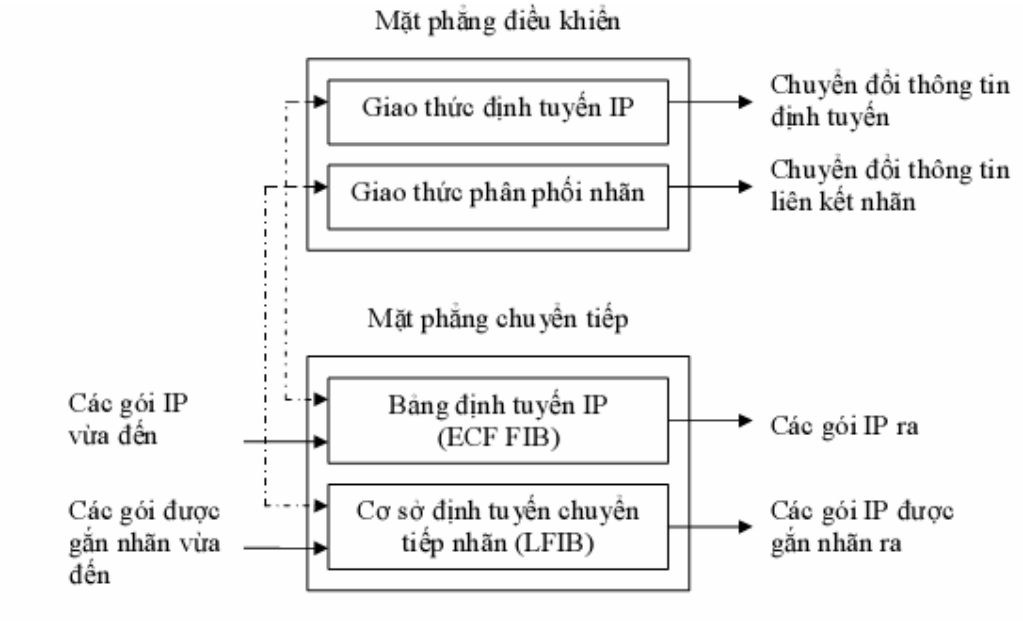
CHƯƠNG 2

CÔNG NGHỆ CHUYỂN MẠCH MPLS

MPLS viết tắt của Multiprotocol Label Switching chuyển mạch nhãn đa giao thức. Mặc dù tại thời điểm đầu chỉ có IPv4 là chuyển mạch nhãn, sau đó có thêm một vài giao thức nữa. Chuyển mạch nhãn chỉ ra rằng những gói được chuyển mạch không thuộc gói IPv4, IPv6 hoặc thậm chí là khung lớp 2 khi được chuyển mạch, nhưng chúng đều được dán nhãn. Phần quan trọng nhất trong MPLS là nhãn. Chương này sẽ giải thích nhãn để làm gì, sử dụng như thế nào và được phân phối trong mạng ra sao.

2.1 Cấu trúc của nút MPLS

Một nút của MPLS có hai mặt phẳng: mặt phẳng chuyển tiếp MPLS và mặt phẳng điều khiển MPLS. Nút MPLS có thể thực hiện định tuyến lớp ba hoặc chuyển mạch lớp hai. Hình sau mô tả cấu trúc cơ bản của một nút MPLS



Hình 2- 1 Cấu trúc một nút MPLS

2.1.1 Mặt phẳng chuyển tiếp (Forwarding plane):

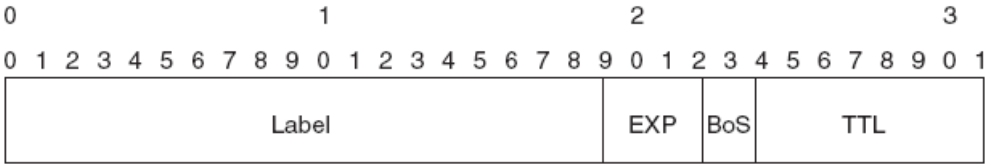
Mặt phẳng chuyển tiếp có trách nhiệm chuyển tiếp gói dựa trên giá trị chứa trong nhãn. Mặt phẳng chuyển tiếp sử dụng một cơ sở thông tin chuyển tiếp nhãn LFIB để chuyển tiếp các gói. Thuật toán mà được sử dụng bởi phần tử chuyển tiếp chuyển mạch nhãn sử dụng thông tin chứa trong LFIB như là các thông tin chứa trong giá trị nhãn. Mỗi nút MPLS có hai bảng liên quan đến việc chuyển tiếp là: cơ sở thông tin nhãn LIB và LFIB. LIB chứa tất cả các nhãn được nút MPLS cục bộ đánh dấu và ánh xạ của các nhãn này đến các nhãn được nhận từ láng giềng (MPLS neighbor) của nó. LFIB sử dụng một tập con các nhãn chứa trong LIB để thực hiện chuyển tiếp gói.

- **Nhãn MPLS**

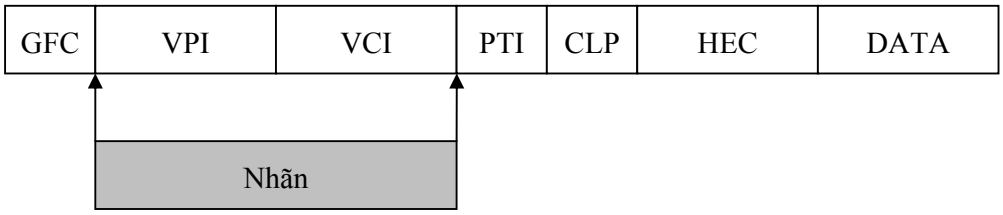
Một nhãn MPLS là một trường 32 bit cố định với cấu trúc xác định. Nhãn được dùng để xác định một FEC.

Đối với ATM, nhãn được đặt cả ở hoặc là trường VCI hoặc là VPI của mào đầu ATM. Tuy nhiên, nếu là khung trong Frame Relay, nhãn lại được đặt ở trường DLCI của mào đầu Frame Relay.

Kỹ thuật lớp 2 như Ethernet, Token Ring, FDDI, và kết nối point – to – point không thể tận dụng được trường địa chỉ lớp 2 của chúng để mang nhãn đi. Những kỹ thuật này mang nhãn trong những mào đầu đệm (shim). Mào đầu nhãn đệm được chèn thêm vào giữa lớp kết nối và lớp mạng, như hình sau đây . Việc sử dụng mào đầu nhãn đệm cho phép hỗ trợ MPLS trên hầu hết các kỹ thuật Lớp 2. Hình 2-2 chỉ ra cấu trúc của một nhãn MPLS.



ATM cell header



Shim header

Layer 2 header	Label	Layer 3 header	Layer 4 header	Data

Hình 2- 2 Cấu trúc của nhãn MPLS

Việc hộ trợ cho mào đầu đệm yêu cầu bộ định tuyến gửi có một đường dẫn để chỉ cho bộ định tuyến nhận biết rằng khung này chứa một mào đầu chèn thêm. Các kỹ thuật khác nhau sử dụng các cách khác nhau. Ethernet sử dụng giá trị ethertype 0x8848 và 0x8847 để chỉ sự có mặt của mào đầu chèn thêm. Giá trị Ethertype 0x8847 được sử dụng để chỉ ra rằng một khung đang mang gói unicast MPLS, và giá trị ethertype 0x8848 chỉ ra rằng khung đang mang gói multicast MPLS. Token ring và FDDI cũng sử dụng giá trị loại này như là một phần của mào đầu SNAP.

PPP sử dụng một Chương trình điều khiển mạng có chỉnh sửa (NCP – Network Control Program) được biết đến như là giao thức điều khiển MPLS (MPLS CP) và đánh dấu tất cả những gói chứa một mào đầu chèn thêm với 0x8281 trong trường giao thức PPP. Frame Relay sử dụng ID giao thức lớp mạng SNAP (NLP ID – Network Layer Protocol) và mà đầu SNAP được đánh dấu với giá trị dạng 0x8847 theo đó chỉ ra khung đang mang mào đầu chèn thêm. ATM sử dụng mào đầu SNAP với giá trị ethertype dang 0x8847 và 0x8848.

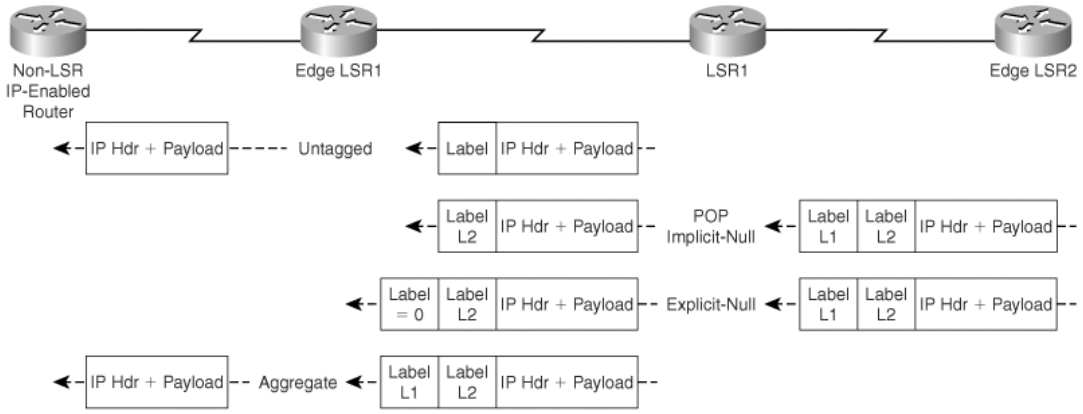
Nhãn MPLS chứa các trường sau:

- *Trường nhãn (label field)*: 20 bit đầu là giá trị của nhãn. Giá trị này nằm trong khoản từ 0 đến 220-1 hoặc 1048575. Tuy nhiên, 16 giá trị đầu tiên không được dùng để sử dụng; nó được sử dụng với những ý nghĩa đặc biệt.
- Các bit từ 20 đến 22 là 3 *bit thực nghiệm* (EXP – experimental). Những bit này chỉ được sử dụng trong chất lượng của dịch vụ (QoS); khi các gói MPLS xếp hàng có thể dùng các bit EXP tương tự như các bit IP ưu tiên (IP Precedence). Chú ý: Những bit được đặt tên là "thực nghiệm" là có lý do lịch sử. Trong quá khứ, không ai biết cách sử dụng những bit này.
- *Trường ngăn xếp* (stack field): 1 bit, bit 23 là bit cuối của ngăn xếp. Bit này sẽ được lập là 1 khi đây là nhãn cuối cùng của ngăn xếp, còn đối với các nhãn khác nó là 0 (bit BoS). Chồng nhãn là sự tập trung của những nhãn mà được đặt phía trên của gói. Chồng nhãn có thể chỉ gồm 1 nhãn, hoặc nhiều nhãn. Số lượng các nhãn (ở đây là trường 32 bit) mà ta có thể tìm thấy trong ngăn xếp là vô hạn, mặc dù ta ít khi nhìn thấy một ngăn xếp có bốn nhãn hoặc hơn.
- *Trường TTL*: Bit thứ 24 đến 31 là 8 bit sử dụng làm bit thời gian sống (Time to live TTL). Những TTL này có chức năng giống như TTL trong IP header. Nó được tăng lên 1 sau mỗi bước nhảy, và chức năng chính của nó là tránh một gói bị mắc kẹt trong vòng lặp định tuyến. Nếu vòng định tuyến xảy ra và không có TTL, thì vòng lặp gói là mãi mãi. Nếu TTL của một nhãn về 0 thì gói sẽ bị loại bỏ.

Chú ý: Nút ATM MPLS chỉ mang những nhãn trong trường VCI hoặc VPI/VCI của mào đầu ATM. Các trường EXP, Stack, TTL không được hỗ trợ. Tuy nhiên QoS và chức năng phát hiện loop vẫn có và có thể được thực

hiện khi sử dụng kỹ thuật ATM.

- **Các loại nhãn đặc biệt**
  - *Untagged*: gói MPLS đến được chuyển thành một gói IP và chuyển tiếp đến đích. Nó được dùng trong thực thi MPLS VPN.
  - *Nhãn Implicit-null hay POP*: Nhãn này được gán khi nhãn trên (top label) của gói MPLS đến bị bóc ra và gói MPLS hay IP được chuyển tiếp tới trạm kế xuôi dòng. Giá trị của nhãn này là 3 (trường nhãn 20 bit). Nhãn này được dùng trong mạng MPLS cho những trạm kế cuối.
  - *Nhãn Explicit-null*: được gán để giữ giá trị EXP cho nhãn trên (top label) của gói đến. Nhãn trên được hoán đổi với giá trị 0 và chuyển tiếp như một gói MPLS tới trạm kế xuôi dòng. Nhãn này sử dụng khi thực hiện QoS với MPLS.
  - *Nhãn Aggregate*: với nhãn này, khi gói MPLS đến nó bị bóc tất cả nhãn trong chồng nhãn ra để trở thành một gói IP và thực hiện tra cứu trong FIB để xác định giao tiếp ngõ ra cho nó.



Hình 2- 3 Các loại nhãn đặc biệt

- **Ngăn xếp nhãn**

Những bộ định tuyến MPLS tốt (capable) cần nhiều hơn 1 nhãn ở trên mỗi gói để định tuyến gói này trong mạng MPLS. Việc này được thực hiện bởi

việc đặt nhãn trong một ngăn xếp. Nhãn đầu tiên trong ngăn xếp được gọi là nhãn đỉnh và nhãn cuối cùng được gọi là nhãn đáy. Ở giữa ta có thể có nhiều nhãn. Hình 2-4 đưa ra cấu trúc của ngăn xếp nhãn.

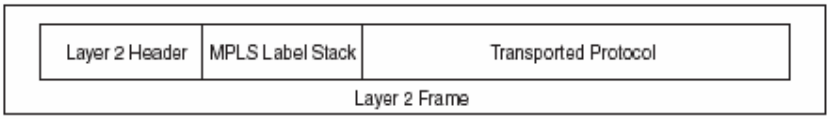
Hình 2- 4 Ngăn xếp nhãn

Trong ngăn xếp nhãn ở hình trên chỉ là rằng bit BoS là 0 đối với tất cả các nhãn, trừ nhãn đáy. Đối với nhãn đáy, bit BoS là 1.

Những ứng dụng thực tế của MPLS cần nhiều hơn 1 nhãn trong ngăn xếp nhãn để chuyển tiếp những gói được gán nhãn. Hai ví dụ ứng dụng của MPLS là MPLS VPN và AToM. Cả hai ứng dụng trên của MPLS đều đặt hai nhãn trong ngăn xếp. Trong các gói MPLS cơ bản, nhãn trên cùng xuất hiện ngay sau mào đầu lớp kết nối, và nhãn cuối cùng xuất hiện ngay trước mào đầu lớp mạng. Gói chuyển tiếp được thực hiện cùng với việc sử dụng giá trị nhãn của nhãn trên cùng trong ngăn xếp. Tuyến IP unicast không sử dụng ngăn xếp nhãn, nhưng MPLS VPN và điều khiển lưu lượng lại sử dụng ngăn xếp nhãn.

- **Mã hóa MPLS**

Ngăn xếp nhãn được đặt ở đâu? Ngăn xếp đặt trước gói lớp 3 – trước header của giao thức vận chuyển, nhưng sau header của lớp 2. Ngăn xếp MPLS thường được gọi là header đệm (shim header) bởi vị trí của nó.
Hình 2-4 thể hiện vị trí của ngăn xếp nhãn cho các gói được gán nhãn.



Có nhiều kiểu đóng gói mà lớp 2 có thể đáp ứng hoặc liên kết được có sự hỗ trợ của Cisco IOS như: PPP, HDLC, Ethernet ... Giả thiết rằng giao thức truyền tải là IPv4, và phương thức đóng gói đường link là PPP, lưu trữ nhãn hiện nay là sau header PPP nhưng trước header IPv4. Bởi vì ngăn xếp nhãn trong khung Lớp 2 được đặt trước header của Lớp 3 hoặc những giao thức truyền tải khác, ta có thể có những giá trị mới trong trường giao thức lớp kết nối dữ liệu, những giá trị này chỉ ra được phần tiếp theo của header lớp 2 sẽ là gói được dán nhãn MPLS. Trường giao thức lớp kết nối dữ liệu là một giá trị chỉ ra loại tải mà khung lớp 2 truyền đi. Bảng 2-1 chỉ ra tên và giá trị đối với trường nhận dạng giao thức (Protocol Identifier – PI) trong header lớp 2 đối với các loại đóng gói lớp 2 khác nhau.

Layer 2 Encapsulation Type	**Layer 2 Protocol Identifier name**	**Name Value (hex)**
PPP	PPP Protocol field	0281
Ethernet/802.3 LLC/SNAP encapsulation	Ethertype value	8847
HDLC	Protocol	8847
Frame Relay	NLPID (Network Level Protocol ID)	80

Bảng 2.1: Giá trị xác định giao thức MPLS cho các dạng đóng gói lớp 2

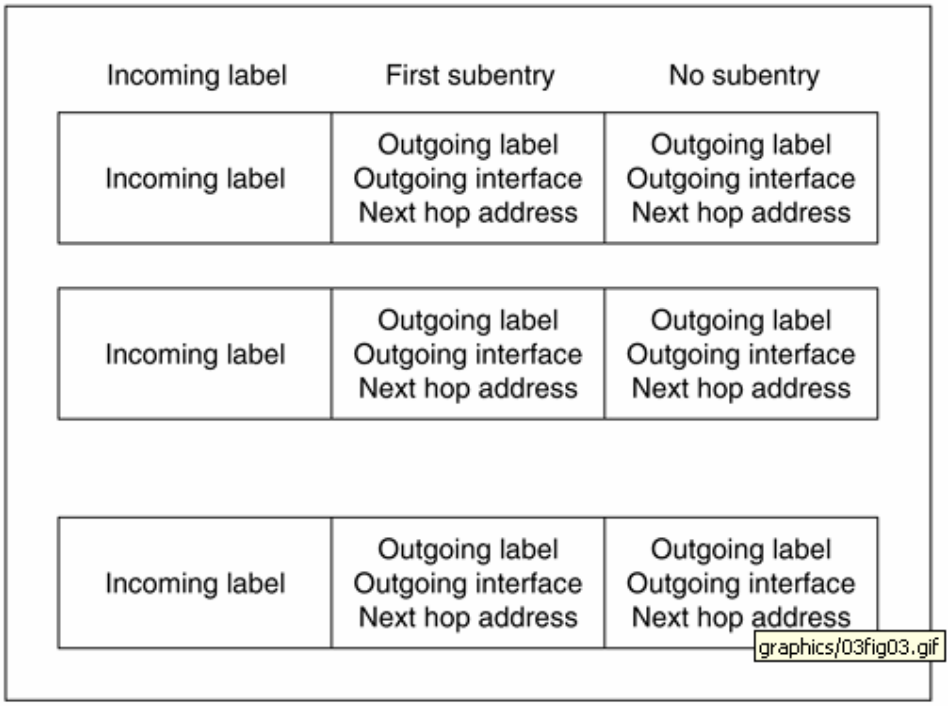
ATM không có mặt trong bảng 2-1 nói trên bởi vì nó sử dụng duy nhất cách đóng gói theo nhãn. Trong bảng trên, NLPID là 0x80, giá trị này cho biết header giao thức truy nhập mạng con (subnetwork Access Protocol SNAP)

đang được sử dụng. Header SNAP được sử dụng trong Frame Relay để cho bên nhận biết rằng Frame Relay đang sử dụng giao thức vận chuyển gì. Header SNAP bao gồm Nhận dạng duy nhất tổ chức (Organizationally Unique Identifier – OUI) của 0x000000 và dạng Ethernet là 0x8847 ở đây giao thức truyền tải là MPLS.

Giao thức truyền tải về mặt lý thuyết có thể không là gì hết; Cisco IOS hỗ trợ IPv4 và IPv6. Trong trường hợp AToM, ta sẽ thấy giao thức truyền tải có thể là bất kỳ giao thức phổ biến lớp 2 nào, như Frame Relay, PPP, HDLC, ATM và Ethernet.

- **Cơ sở thông tin chuyển tiếp nhãn (LFIB)**

LFIB được duy trì bởi một nút MPLS chứa một chuỗi các entry (mục nhập). Như hình dưới đây, mỗi đường nhập vào chứa một nhãn tới và một hoặc vài mục phụ. LFIB được lập bảng chứa các giá trị trong nhãn tới.



Hình 2- 5 ***Cấu trúc của LFIB***

Mỗi mục phụ bao gồm một nhãn ra, giao diện ra và địa chỉ nút nhảy tiếp theo. Các mục phụ với đường vào riêng biệt có thể giống hoặc khác nhãn vào. Chuyển tiếp Multicast yêu cầu mục phụ với đa nhãn ra, mà ở đó một nhãn vào được đưa đến tại một giao diện cần được gửi tới đa giao diện ra. Thêm vào gói ra, giao diện ra và thông tin bước nhảy tiếp theo, một đường vào trong bảng chuyển tiếp có thể bao gồm thông tin liên quan đến nguồn (resource) của gói có thể sử dụng, như hàng đợi ra mà gói phải được đặt vào.

Một nút MPLS có thể duy trì một bảng chuyển tiếp đơn, một bảng chuyển tiếp trên mỗi giao diện của nó hoặc là kết hợp cả hai. Trong trường hợp có nhiều bảng chuyển tiếp, chuyển tiếp gói được thực hiện bởi giá trị của nhãn tới cũng như giao diện vào mà ở đó gói đến.

- **Thuật toán chuyển tiếp gói:**

Chuyển mạch nhãn sử dụng thuật toán chuyển tiếp dựa trên việc trao đổi nhãn. Nút MPLS mà duy trì một LFIB đơn lấy giá trị nhãn từ trường nhãn tìm thấy trong gói tới và sử dụng giá trị này như chỉ số trong LFIB. Sau khi một nhãn tới match (khớp) được tìm thấy, nút MPLS thay thế nhãn này trong gói với một nhãn ra từ mục phụ và gửi gói qua giao diện ra cụ thể tới nút tiếp cụ thể theo bởi mục phụ. Nếu mục phụ chỉ ra một hàng đợi ra, nút MPLS đặt gói trong hàng đợi cụ thể.

Nếu nút MPLS duy trì nhiều LFIB cho mỗi giao diện của nó, nó sử dụng giao diện vật lý nơi gói đến để chọn một LFIB cụ thể phục vụ để chuyển tiếp gói. Thông thường, thuật toán chuyển tiếp sử dụng nhiều loại thuật toán để chuyển tiếp unicast, multicast và gói unicast với bit ToS được thiết lập. Tuy nhiên, MPLS chỉ sử dụng một thuật toán chuyển tiếp dựa trên trao đổi nhãn.

Một nút MPLS có thể lấy ra tất cả thông tin nó cần để chuyển tiếp nhãn cũng như để xác định tài nguyên dành riêng cần thiết bằng việc truy nhập bộ nhớ đơn. Tra cứu tốc độ cao và khả năng chuyển tiếp làm cho chuyển mạch

nhãn (label switching) thành kỹ thuật chuyển mạch có tính thực thi cao. MPLS cũng có thể được sử dụng để vận chuyển giao thức Lớp 3 khác như IPv6, IPX hoặc Apple Talk từ IPv4. Đặc tính này giúp MPLS có thể tương thích tốt với việc chuyển đổi các mạng từ IPv4 sang IPv6.

2.1.2 Mặt phẳng điều khiển (Control Plane):

Mặt phẳng điều khiển MPLS chịu trách nhiệm tạo ra và lưu trữ LFIB. Tất cả các nút MPLS phải chạy một giao thức định tuyến IP để trao đổi thông tin định tuyến IP với các nút MPLS khác trong mạng. Các nút MPLS enable ATM sẽ dùng một bộ điều khiển nhãn (LSC – Label Switch Controller) như router 7200, 7500 hoặc dùng một mô đun xử lý tuyến (RMP – Route Processor Module) để tham gia xử lý định tuyến IP.

Các giao thức định tuyến Link-state như OSPF và IS-IS là các giao thức được chọn vì chúng cung cấp cho mỗi nút MPLS thông tin của toàn mạng. Trong các bộ định tuyến thông thường, bảng định tuyến IP dùng để xây dựng bộ lưu trữ chuyển mạch nhanh (Fast switching cache) hoặc FIB – Cơ sở thông tin chuyển tiếp (dùng bởi CEF - Cisco Express Forwarding). Tuy nhiên với MPLS, bảng định tuyến IP cung cấp thông tin của mạng đích và tiền tố subnet sử dụng cho nhãn ghép (binding). Các giao thức định tuyến link-state như OSPF gửi thông tin định tuyến (flood) giữa một tập các router không nhất thiết liền kề nhau, trong khi thông tin liên kết nhãn (binding) chỉ được phân bố giữa các router liền kề bằng giao thức phân phối nhãn (LDP) hoặc TDP (Cisco's Proproetary Tag Distribution Protocol). Điều này làm giao thức định tuyến link – state không thích hợp với sự phân phối thông tin liên kết nhãn. Tuy nhiên sự mở rộng các giao thức định tuyến như PIM và BGP có thể được sử dụng để phân phối thông tin liên kết nhãn. Điều này làm cho việc phân phối thông tin liên kết nhãn phù hợp với việc phân phối thông tin định tuyến

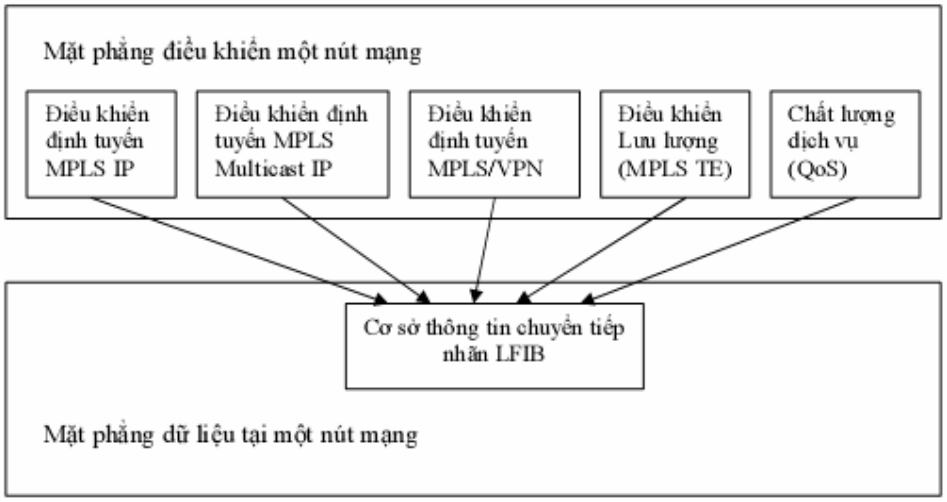
và tránh điều kiện ít xảy ra mà tại đó nút MPLS có thể nhận thông tin liên kết nhãn và không có thông tin định tuyến thích hợp. Nó cũng làm đơn giản hóa toàn bộ hệ thống vận hành bởi vì nó ngăn ngừa sự cần thiết của một giao thức riêng lẻ như LDP để phân phối thông tin nhãn ghép.

Những nhãn trao đổi với các nút MPLS liền kề được sử dụng để xây dựng LFIB. MPLS sử dụng một mô hình chuyển tiếp dựa trên trao đổi nhãn mà có thể được kết nối với một phạm vi các module điều khiển khác nhau. Mỗi module điều khiển chịu trách nhiệm đánh dấu, phân phối một tập các nhãn, cũng như chịu trách nhiệm dự trữ thông tin điều khiển khác có liên quan. Các giao thức cổng định tuyến trong phạm vi miền IGP được dùng để xác nhận khả năng đến được, sự liên kết và ánh xạ giữa FEC và địa chỉ trạm kế (next-hop address).

Thông tin liên kết nhãn chỉ được phân phối giữa các router nối trực tiếp với nhau bằng cách dùng giao thức phân phối LDP.

Các môđun điều khiển MPLS gồm:

- Định tuyến Unicast (Unicast Routing)
- Định tuyến Multicast (Multicast Routing)
- Kỹ thuật lưu lượng (Traffic Engineer)
- Mạng riêng ảo (VPN – Virtual private Network)
- Chất lượng dịch vụ (QoS – Quality of Service)



Hình 2- 6 Các thành phần mặt phẳng dữ liệu và mặt phẳng điều khiển của MPLS

2.2 Các phần tử chính của MPLS

2.2.1 LSR (label switch Router)

Thành phần cơ bản của mạng MPLS là thiết bị định tuyến chuyển mạch nhãn LSR. Thiết bị này thực hiện chức năng chuyển tiếp gói thông tin trong phạm vi mạng MPLS bằng thủ tục phân phối nhãn. Đó là khả năng cần thiết để hiểu được nhãn MPLS, nhận và truyền gói được gán nhãn trên đường liên kết dữ liệu. Có 3 loại LSR trong mạng MPLS:

- Ingress LSR – LSR vào nhận gói chưa có nhãn, chèn nhãn (ngăn xếp) vào trước gói và truyền đi trên đường kết nối dữ liệu.
- Egress LSR – LSR ra nhận các gói được gán nhãn, tách nhãn và truyền chúng trên đường kết nối dữ liệu. LSR ra và LSR vào là các LSR biên.
- LSR trung gian (intermediate LSR) – các LSR trung gian này sẽ nhận các gói có nhãn tới, thực hiện các thao tác trên nó, chuyển mạch gói và truyền gói đến đường kết nối dữ liệu đúng.

Bảng sau mô tả các hoạt động của nhãn:

Aggregate	Gỡ bỏ nhãn trên cùng trong ngăn xếp và thực hiện tra cứu ở Lớp 3
Pop	Gỡ bỏ nhãn trên cùng và truyền tải còn lại như là một gói IP được gán nhãn hoặc không được gán nhãn
Push	Thay nhãn trên cùng trong ngăn xếp với một tập nhãn
Swap	Thay nhãn trên cùng trong ngăn xếp với giá trị khác
Untag	Gở bỏ nhãn trên cùng và chuyển tiếp gói IP tới trạm IP kế tiếp.

LSR phải có khả năng lấy ra một hoặc nhiều nhãn (tách một hoặc nhiều nhãn từ phía trên của ngăn xếp nhãn) trước khi chuyển mạch gói ra ngoài. Một LSR cũng phải có khả năng gắn một hoặc nhiều nhãn vào gói nhận được. Nếu gói nhận được đã có sẵn nhãn, LSR đẩy một hoặc một vài nhãn lên trên ngăn xếp nhãn và chuyển mạch gói ra ngoài. Nếu gói chưa có nhãn, LSR tạo một ngăn xếp nhãn và gán nhãn lên gói. Một LSR phải có khả năng trao đổi nhãn. Nó có ý nghĩa rất đơn giản khi nó nhận được gói đã gán nhãn, nhãn trên cùng của ngăn xếp nhãn được trao đổi với nhãn mới và gói được chuyển mạch trên đường kết nối dữ liệu ra.

LSR mà gắn nhãn lên trên gói đầu tiên được gọi là LSR imposing (gắn) bởi vì nó là LSR đầu tiên đặt nhãn lên trên gói. Đây là một việc bắt buộc đối với một LSR vào. Một LSR mà tách tất cả các nhãn từ gói có dán nhãn trước khi chuyển mạch gói là một LSR Disposing (tách) hay là một LSR ra.

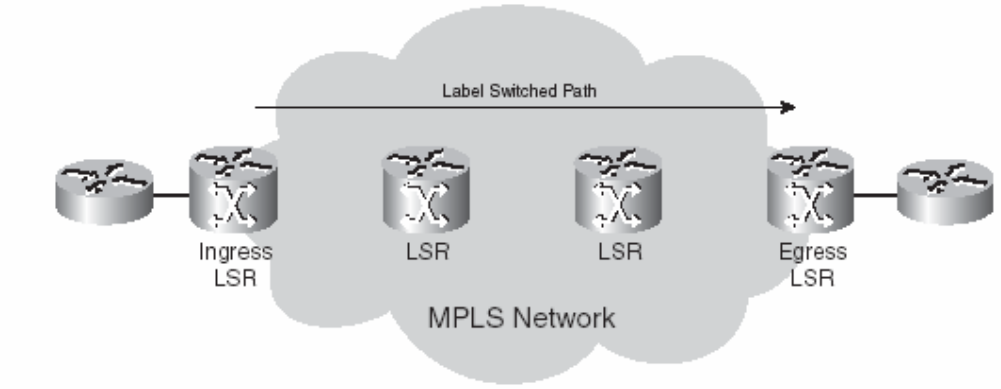
Trong MPLS VPN, các LSR ra và vào được biết đến như một bộ định tuyến cung cấp biên (PE). LSR trung gian được biết đến như là bộ định tuyến của nhà cung cấp. Bộ định tuyến PE và P trở lên phổ biến đến nỗi nó thường xuyên được sử dụng khi mạng MPLS không chạy MPLS VPN.

LER (label edge Router)

Bộ định tuyến nhãn ở biên mạng (LER) là thiết bị hoạt động ở ranh giới giữa mạng MPLS và mạng truy cập. LER hỗ trợ nhiều cổng nối đến các mạng khác nhau như ATM, Frame Relay, Ethernet để chuyển tiếp các lưu lượng vào trong mạng MPLS và phân phối lưu lượng này trở lại các mạng truy cập ở đầu ra.

2.2.2 LSP (label switch Path)

Đường chuyển mạch nhãn là một tập hợp các LSR mà chuyển mạch một gói có nhãn qua mạng MPLS hoặc một phần của mạng MPLS. Về cơ bản, LSP là một đường dẫn qua mạng MPLS hoặc một phần mạng mà gói đi qua. LSR đầu tiên của LSP là một LSR vào, ngược lại LSR cuối cùng của LSP là một LSR ra. Tất cả các LSR ở giữa LSR vào và ra chính là các LSR trung gian. Trong hình 2-5 dưới đây, mũi tên ở trên cùng chỉ hường bởi vì đường chuyển mạch nhãn là đường theo một phương hướng duy nhất. Luồng của các gói có nhãn trong một hướng khác – từ phải sang trái – giữa cùng các LSR biên sẽ là một LSP khác.

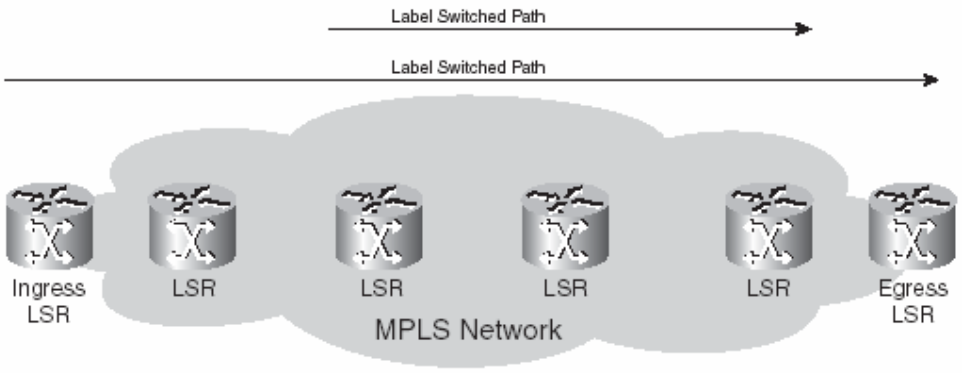


Hình 2- 7 Ví dụ về một LSP qua mạng MPLS

LSR vào của một LSP không nhất thiết phải là bộ định tuyến đầu tiên gán nhãn vào gói. Gói có thể đã được gán nhãn bởi các LSR trước đó. Đây là

trường hợp này là một LSP xếp lồng (ghép), hay là có một LSP trong một LSP khác.

Trong hình 2-8, ta có thể thấy LSP mà trải rộng toàn bộ độ rộng mạng MPLS. Một LSP khác bắt đầu tại LSR thứ ba và kết thúc ở trước LSR cuối cùng.Do đó, khi một gói đi vào LSP thứ hai trên cổng LSR vào của nó (có nghĩa là LSR thứ ba), nó đã thực sự được dán nhãn. LSR vào của LSP nested (ghép) sau đó gán một nhãn thứ hai lên trên gói. Ngăn xếp nhãn của gói trên LSP thứ hai bây giờ đã có 2 nhãn. Nhãn trên cùng sẽ phụ thuộc vào LSP nested (ghép), và nhãn dưới cùng sẽ phụ thuộc vào LSP mà trải rộng hết toàn bộ mạng MPLS. Đường hầm điều khiển lưu lượng dự phòng là một ví dụ cho LSP nested (ghép)



Hình 2- 8 Mô hình LSP Nested

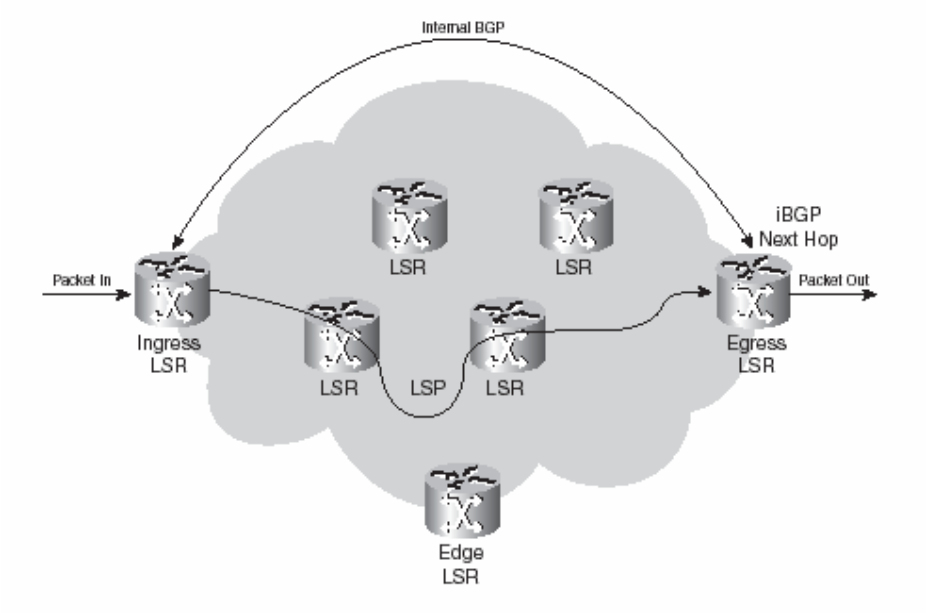
2.2.3 FEC (Forwarding Equivalence Class)

Lớp chuyển tiếp tương đương (FEC) là một nhóm hoặc luồng các gói được chuyển tiếp dọc theo cùng một tuyến và được xử lý theo cùng một cách chuyển tiếp. Tất cả các gói cùng thuộc một FEC sẽ có nhãn giống nhau. Tuy nhiên, không phải tất cả các gói có cùng nhãn đều thuộc cùng một FEC, bởi vì giá trị EXP của chúng có thể khác nhau; phương thức chuyển tiếp khác nhau và nó có thể phụ thuộc vào FEC khác nhau.

Bộ định tuyến mà quyết định gói nào thuộc một FEC nào chính là LSR biên vào. Đây là logic vì LSR biên vào sắp xếp và dán nhãn vào gói. Sau đây là một vài ví dụ về FEC:

- Những gói với địa chỉ IP đích lớp 3 khớp (match) với một tiền tố nào đó
- Gói truyền multicast thuộc nhóm nào đó.
- Gói với cùng phương thức chuyển tiếp, dựa trên thứ tự ưu tiên hoặc trường điểm mã DiffServ IP (DSCP)
- Khung lớp 2 chuyển qua MPLS nhận được trên một VC hoặc một giao diện LSR biên vào và truyền trên một VC hoặc giao diện trên LSR biên ra.
- Những gói với địa chỉ đích IP lớp 3 mà thuộc một tập tiền tố BGP Giao thức cổng biên, tất cả với cùng BGP bước tiếp theo.

Ví dụ cuối cùng của FEC là một sự quan tâm đặc biệt. Tất cả các gói trên LSR biên vào mà địa chỉ IP đích chỉ tới một tập các tuyến BGP trong bảng định tuyến – tất cả cùng địa chỉ bước nhảy tiếp theo BGP – thuộc cùng một FEC. Điều này có nghĩa tất cả các gói đi vào trong mạng MPLS có được một nhãn tùy thuộc vào bước nhảy BGP tiếp theo là gì. Hình 2-9 đưa ra ví dụ mạng MPLS tại đó tất cả các LSR biên chạy BGP trong (iBGP).



Hình 2- 9 Mạng MPLS chạy iBGP

Địa chỉ IP đích của tất cả các gói IP mà đi vào LSR vào sẽ được tìm thấy trong bảng chuyển tiếp IP. Tất cả những địa chỉ này lại phụ thuộc vào một tập hợp các tiền tố mà chúng được tìm thấy trong mạng định tuyến như là tiền tố BGP (BGP Prefixes). Rất nhiều tiền tố BGP trong bảng định tuyến có cùng một địa chỉ bước nhảy BGP tiếp theo, cụ thể là một LSR ra. Tất cả các gói với một địa chỉ IP đích, mà sự tra cứu IP trong bảng định tuyến đệ quy tới cùng địa chỉ bước nhảy BGP tiếp theo, sẽ được nối tới cùng một FEC. Như đã nói ở trên, tất cả các gói mà thuộc cùng một FEC có cùng nhãn được gán bởi LSR vào.

2.3 Các giao thức sử dụng trong MPLS

2.3.1 Phân phối nhãn

Nhãn đầu tiên được gán trên một LRS vào và nhãn này sẽ thuộc một LSP. Tuyến đi của gói qua mạng MPLS được quy định (bound) bởi một LSP. Sự thay đổi chính trong quá trình chuyển tiếp là nhãn trên cùng trong ngăn xếp nhãn được trao đổi tại mỗi bước nhảy. LSR vào sẽ gắn một hoặc nhiều nhãn

lên gói. LSR trung gian sẽ thực hiện việc trao đổi nhãn trên cùng (nhãn đi vào) của gói nhận được (gói đã được gán nhãn) với một nhãn khác (nhãn đi ra) và truyền gói trên đường kết nối ra. LSR ra của LSP sẽ lấy toàn bộ nhãn của LSP này và chuyển tiếp gói.

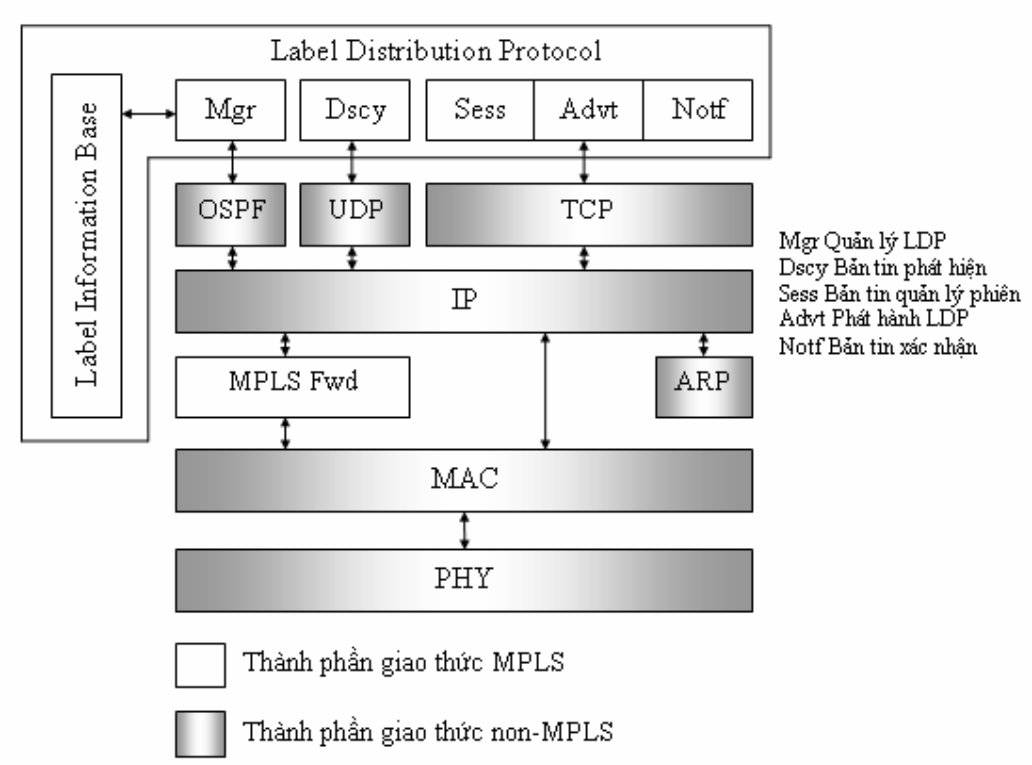
Xem xét ví dụ về mặt phẳng IPv4 trên MPLS, đây là ví dụ đơn giản nhất về mạng MPLS. Mặt phẳng IPv4 – trên MPLS là một mạng mà bao gồm một số các LSR chạy giao thức cổng trong IGP (ví dụ tuyến mở ngắn nhất OSPF, IS – IS, và giao thức định tuyến cổng trong nâng cao EIGRP). LSR vào tìm kiếm địa chỉ IPv4 đích của gói, gán nhãn, và chuyển tiếp gói. LSR tiếp theo (và bất kỳ LSR trung gian khác) nhận gói trao đổi nhãn nhận với nhãn gửi, và chuyển tiếp gói. LSR ra tách nhãn và chuyển tiếp gói IPv4 không có nhãn trên đường kết nối ra. Để thực hiện việc này, những LSR liền kề phải đồng ý với nhãn sử dụng cho mỗi tiền tố IGP. Do đó, mỗi LSR trung gian phải có khả năng tính toán để thực hiện việc trao đổi nhãn gửi và nhãn nhận cho nhau. Điều này có nghĩa là ta cần phải có một kỹ thuật để báo cho bộ định tuyến biết nhãn nào được sử dụng khi chuyển tiếp gói. Giữa mỗi cặp bộ định tuyến liền kề là những nhãn nội bộ. Đối với những bộ định tuyến liền kề để đồng ý những nhãn mà sử dụng cho tiền tố nào,giữa chúng cần có một vài mẫu giao tiếp; nếu không, những bộ định tuyến sẽ không biết nhãn gửi nào cần nối với nhãn nhận nào. Do đó cần thiết phải có giao thức phân phối nhãn.

- **Phân phối nhãn với LDP**

Giao thức phân phối nhãn được nhóm nghiên cứu MPLS của IETF xây dựng và ban hành dưới tên RFC 3036. Phiên bản mới nhất được công bố năm 2001 đưa ra những định nghĩa và nguyên tắc hoạt động của giao thức LDP.

Giao thức phân phối nhãn được sử dụng trong quá trình gán nhãn cho các gói thông tin yêu cầu. Giao thức LDP là giao thức điều khiển tách biệt được các LSR sử dụng để trao đổi và điều phối quá trình gán nhãn/FEC. Giao thức này

là tập hợp các thủ tục trao đổi các bản tin cho phép các LSR sử dụng giá trị nhãn thuộc FEC nhất định để truyền các gói thông tin.



Hình 2- 10 Quan hệ giữa các LDP với các giao thức khác.

Một kết nối TCP được thiết lập giữa các LSR đồng cấp để đảm bảo các bản tin LDP được truyền một cách trung thực theo đúng thứ tự. Các bản tin LDP có thể xuất phát từ trong bất cứ một LSR (điều khiển đường chuyển mạch nhãn LSP độc lập) hay từ LSR biên lối ra (điều khiển LSP theo lệnh) và chuyển từ LSR phía trước đến LSR bên cạnh phía sau. Việc trao đổi các bản tin LDP có thể được khởi phát bởi sự xuất hiện của luồng số liệu đặc biệt, bản tin lập dự trữ RSVP hay cập nhật thông tin định tuyến. Khi một cặp LSR đã trao đổi bản tin LDP cho một FEC nhất định thì một đường chuyển mạch LSP từ đầu vào đến đầu ra được thiết lập sau khi mối LSR ghép nhãn đầu vào với nhãn đầu ra tương ứng trong LIB của nó.

- **Các tính chất cơ bản của giao thức phân phối nhãn LDP**

LDP có các tính chất cơ bản như sau:

- Cung cấp cơ chế nhận biết LSR cho phép các LSR ngang cấp tìm kiếm nhau và thiết lập kết nối.
- Định nghĩa bốn lớp bản tin:
  - Các bản tin DISCOVERY
  - Các bản tin ADJCAENCY, để giải quyết vấn đề khởi tạo, duy trì, hủy bỏ các phiên giữa hai LSR.
  - Các bản tin LABEL ADVERTISEMENT, giải quyết thông báo, yêu cầu, thu hồi và loại bỏ kết hợp nhãn.
  - Các bản tin NOTIFICATION, sử dụng để cung cấp các thông tin trợ giúp và thông tin lỗi tín hiệu.
- Chạy trên TCP cung cấp phương thức phân phối bản tin đáng tin cậy (ngoại trừ các bản tin DISCOVERY)
- Thiết kế cho phép khả năng mở rộng dễ dàng, sử dụng các bản tin được xác định như một tập hợp các đối tượng mã hóa TLV (kiểu, độ dài, giá trị).

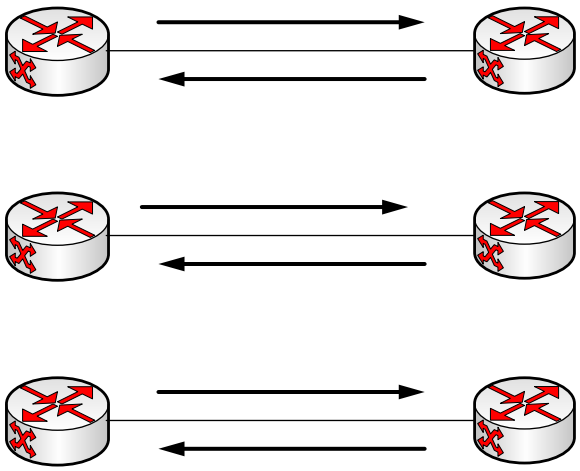
Mã hóa TLV nghĩa là mỗi đối tượng bao gồm một trường kiểu biểu thị về loại đối tượng chỉ định, một trường độ dài thông báo độ dài của đối tượng và một trường giá trị phụ thuộc vào trường kiểu. Hai trường đầu tiên có độ dài cố định và được đặt tại vị trí đầu tiên của đối tượng cho phép dễ dàng thực hiện việc loại bỏ kiểu đối tượng mà nó không nhận ra. Trường giá trị có một đối tượng có thể gồm nhiều đối tượng mã hóa TLV hơn.

- **Thủ tục phát hiện LSR lân cận**

Thủ tục phát hiện LSR lân cận của LDP chạy trên UDP và thực hiện như sau:

- Một LSR định kỳ gửi đi bản tin HELLO tới các cổng UDP đã biết trong tất cả các bộ định tuyến trong mạng con của nhóm multicast.

- Tất cả các LSR tiếp nhận bản tinh HELLO này trên cổng UDP. Như vậy, tại một thời điểm nào đó LSR sẽ biết được tất cả các LSR khác mà nó có kết nối trực tiếp.
- Khi LSR nhận biết được địa chỉ của LSR khác bằng cơ chế này thì nó sẽ thiết lập kết nối TCP đến LSR đó.
- Khi đó phiên LDP được thiết lập giữa 2 LSR. Phiên LDP là phiên hai chiều nghĩa là mỗi LSR ở hai đầu kết nối đều có thể yêu cầu và gửi liên kết nhãn.



Hình 2- 11 Thủ tục phát hiện LSR lân cận

Trong trường hợp các LSR không kết nối trực tiếp trong một mạng con (subnet) người ta sử dụng một cơ chế bổ sung như sau:

LSR định kỳ gửi bản tin HELLO đến cổng UDP đã biết tại địa chỉ IP xác định được khai báo khi lập cấu hình. Đầu nhận bản tin này có thể trả lời lại bằng bản tin HELLO khác truyền một chiều ngược lại đến LSR gửi và việc thiết lập các phiên LDP được thực hiện như trên.

Thông thường trường hợp này hay được áp dụng khi giữa 2 LSR có một nhãn LSP cho điều khiển lưu lượng và nó yêu cầu phải gửi các gói có nhãn qua đường LSP đó.

T

- **Giao thức truyền tải tin cậy**

Việc quyết định sử dụng TCP để truyền các bản tin LDP là một vấn đề cần xem xét. Yêu cầu về độ tin cậy là rất cần thiết: nếu việc liên kết nhãn hay yêu cầu liên kết nhãn được truyền một cách không tin cậy thì lưu lượng cũng không được chuyển mạch theo nhãn. Một vấn đề quan trọng nữa đó là thứ tự các bản tin phải bảo đảm đúng. Như vậy liệu việc sử dụng TCP để truyền LDP có bảo đảm hay không và có nên xây dựng luôn chức năng truyền tải này trong bản thân LDP hay không?

Việc xây dựng các chức năng bảo đảm độ tin cậy trong LDP không nhất thiết phải thực hiện toàn bộ các chức năng của TCP trong LDP mà chỉ cần dừng lại ở những chức năng cần thiết nhất ví dụ như chức năng điều khiển tránh tắc nghẽn được coi là không cần thiết trong LDP... Tuy nhiên việc phát triển thêm các chức năng đảm bảo độ tin cậy trong LDP cũng có nhiều vấn đề cần xem xét ví dụ như các bộ định thời cho các bản tin ghi nhận và không ghi nhận, trong trường hợp sử dụng TCP chỉ cần 1 bộ định thời của TCP cho toàn phiên LDP.

Thiết kế một giao thức truyền tải tin cậy là một vấn đề nan giải. Đã có rất nhiều cố gắng để cải thiện TCP nhằm làm tăng độ tin cậy của giao thức truyền tải. Tuy nhiên vấn đề hiện nay vẫn chưa rõ ràng và TCP vẫn được sử dụng cho truyền tải LDP.

- **Các bản tin LDP**

Có 4 dạng bản tin cơ bản sau đây:

- Bản tin Initialization
- Bản tin KeepAlive
- Bản tin Label Mapping
- Bản tin Release
  - Bản tin Lable Withdrawal

- Bản tin Request
- Bản tin Request Abort.

o *Dạng bản tin Initialization*

Các bản tin thuộc loại này gửi đi khi bắt đầu một phiên LDP giữa 2 LSR để trao đổi các tham số, các tùy chọn cho phiên. Các tham số này bao gồm:

- Chế độ phân bổ nhãn
- Các giá trị bộ định thời
- Phạm vi các nhãn sử dụng trong kênh giữa 2 LSR đó.

Cả 2 LSR đều có thể gửi các bản tin Initialization và LSR nhận sẽ trả lời bằng KeepAlive nếu các tham số được chấp nhận. Nếu có một tham số nào đó không được chấp nhận LSR trả lời thông báo có lỗi và phiên kết thúc.

o *Dạng bản tin KeepAlive*

Các bản tin KeepAlive được gửi định kỳ khi không có bản tin nào được gửi để đảm bảo cho mỗi thành phần LDP biết rằng thành phần LDP khác đang hoạt động tốt. Trong trường hợp không xuất hiện bản tin KeepAlive hay một số bản tin khác của LDP trong khoảng thời gian nhất định thì LSR sẽ xác định đối phương hoặc kết nối bị hỏng và phiên LDP bị dừng.

o *Dạng bản tin Label Mapping*

Các bản tin Label Mapping được sử dụng để quảng bá liên kết giữa FEC (Prefix địa chỉ) và nhãn. Bản tin Label Withdrawal thực hiện quá trình ngược lại: nó được sử dụng để xóa bỏ liên kết vừa thực hiện. Bản tin này được sử dụng khi có sự thay đổi trong cấu hình LSR làm tạm dừng việc chuyển nhãn các gói trong FEC đó.

o *Dạng bản tin Label Release*

Bản tin này được sử dụng bởi LSR khi nhận được chuyển đổi nhãn mà nó không cần thiết nữa. Điều đó thường xảy ra khi LSR giải phóng nhận thấy nút tiếp theo cho FEC đó không phải là LSR quảng bá liên kết nhãn/FEC đó.

Trong chế độ hoạt động gán nhãn theo yêu cầu từ phía trước, LSR sẽ yêu cầu gán nhãn từ LSR lân cận phía trước sử dụng bản tin Label Request. Nếu bản tin Label Request cần phải hủy bỏ trước khi được chấp nhận (do nút kế tiếp trong FEC yêu cầu đã thay đổi), thì LSR yêu cầu sẽ loại bỏ yêu cầu với bản tin Label Request Abort.

- **Các chế độ phân phối nhãn**

Chúng ta đã biết một số chế độ hoạt động trong việc phân phối nhãn như: không yêu cầu phía trước, theo yêu cầu phía trước, điều khiển LSP theo lệnh hay độc lập, duy trì tiên tiến hay bảo thủ. Các chế độ này được thỏa thuận bởi LSR trong quá trình khởi tạo phiên LDP.

Khi LSR hoạt động ở chế độ duy trì bảo thủ, nó sẽ chỉ giữ những giá trị Nhãn/FEC mà nó cần tại thời điểm hiện tại. Các chuyển đổi khác được giải phóng. Ngược lại trong chế độ duy trì tiên tiến. LSR giữ tất cả các chuyển đổi mà nó được thông báo ngay cả khi một số không được sử dụng tại thời điểm hiện tại. Hoạt động của chế độ này như sau:

- LSR1 gửi gắn kết nhãn vào một số FEC đến một trong các LSR lân cận (LSR 2) nó cho FEC đó.
- LSR2 nhận thấy LSR1 hiện tại không phải là nút tiếp theo đối với FEC đó và nó không thể sử dụng gắn kết này cho mục đích chuyển tiếp tại thời điểm hiện tại nhưng nó vẫn lưu việc gắn kết này lại.
- Tại thời điểm nào đó sau này có sự xuất hiện thay đổi định tuyến và LSR 1 trở thành nút tiếp theo của LSR2 đối với FEC đó thì LSR2 sẽ cập nhật thông tin trong bảng định tuyến tương ứng và có thể chuyển tiếp các gói có nhãn đến LSR1 trên tuyến mới của chúng. Việc này được thực hiện một cách tự động mà không cần đến báo hiệu LDP hay quá trình phân bổ nhãn mới.

Ưu điểm lớn nhất của chế độ duy trì tiên tiến đó là khả năng phản ứng nhanh hơn khi có sự thay đổi định tuyến. Nhược điểm lớn nhất là lãng phí bộ nhớ và nhãn. Điều này đặc biệt quan trọng và có ảnh hưởng rất lớn đối với những thiết bị lưu trữ bảng định tuyến trong phần cứng như ATM – LSR. Thông thường chế độ duy trì bảo thủ nhãn được sử dụng trong các ATM – LSR.

2.3.2 Giao thức đặt trước tài nguyên

Sau khi đã xem xét những thành phần chính trong cấu trúc dịch vụ tích hợp, phần này chúng ta sẽ tập trung vào giao thức báo hiệu RSVP là giao thức báo hiệu đóng vai trò rất quan trọng trong MPLS. RSVP là giao thức cho phép các ứng dụng thông báo các yêu cầu về QoS với mạng và mạng sẽ đáp ứng bằng những thông báo thành công hoặc thất bại. RSVP phải mang các thông tin sau:

- Thông tin phân loại, nhờ nó mà các luồng lưu lượng với các yêu cầu QoS cụ thể có thể được phân biệt trong mạng. Thông tin này bao gồm địa chỉ IP phía gửi và phía nhận, số cổng UDP.
- Chỉ tiêu kỹ thuật của luồng lưu lượng và các yêu cầu QoS, theo khuôn dạng TSpec và RSpec, bao gồm các dịch vụ yêu cầu (có bảo đảm hoặc tải điều khiển)

Rõ ràng là RSVP phải mang những thông tin này từ các máy chủ tới tất cả các tổng đài chuyển mạch và các bộ định tuyến dọc theo đường truyền từ bộ gửi đến bộ nhận, vì vậy tất cả các thành phần mạng này phải tham gia vào việc đảm bảo các yêu cầu QoS của ứng dụng.

RSVP mang các thông tin trong hai loại bản tin cơ bản là: PATH và RESV. Các bản tin PATH truyền từ bộ gửi tới một hoặc nhiều bộ nhận có chứa TSpec và các thông tin phân loại do bộ gửi cung cấp. Một lý do cho

phép có nhiều bộ nhận là RSVP được thiết kế để hỗ trợ multicast. Một bản tin PATH bao giờ cũng được gửi tới một địa chỉ được gọi là *địa chỉ phiên*, nó có thể là địa chỉ unicast hoặc multicast. Chúng ta thường xem phiên đại diện cho một ứng dụng đơn, nó được xác nhận bằng một địa chỉ đích và số cổng đích sử dụng riêng cho ứng dụng. Trong phần tiếp theo chúng ta sẽ thấy rằng không có lý do nào để xem xét một phiên theo cách hạn chế như vậy.

Khi bộ nhận nhận được bản tin PATH, nó có thể gửi bản tin RESV trở lại cho bộ gửi. Bản tin RESV xác nhận phiên có chứa thông tin về số cổng dành riêng và RSpec xác nhận mức QoS mà bộ nhận yêu cầu. Nó cũng bao gồm một vài thông tin xem xét những bộ gửi nào được phép sử dụng tài nguyên đang được cấp phát. Hình 2-12 biểu diễn trình tự bản tin trao đổi giữa bộ gửi và nhận. Ở đây chúng ta lưu ý rằng các cổng dành riêng là đơn công. Nếu cần sử dụng các cổng dành riêng song công (ví dụ như phục vụ cho thoại truyền thống) thì phải có các bản tin bổ sung theo chiều ngược lại. Cũng chú ý rằng các bản tin được nhận và chuyển tiếp bởi tất cả các bộ định tuyến dọc theo đường truyền thông tin, do đó việc cấp phát tài nguyên có thể được thực hiện tại tất cả các nút mạng cần thiết.

Khi các cổng dành được thiết lập, các bộ định tuyến nằm giữa bộ gửi và bộ nhận sẽ xác định các gói tin thuộc cổng dành riêng nào nhờ việc kiểm tra năm trường trong phần mào đầu của IP và giao thức truyền tải đó là: địa chỉ đích, số cổng đích, số giao thức (ví dụ UDP), địa chỉ nguồn và cổng nguồn. Chúng ta gọi tập các gói tin được nhận dạng theo cách này là ***luồng dành riêng***. Các gói tin trong luồng dành riêng thường bị khống chế (đảm bảo cho luồng không phát sinh lưu lượng vượt quá so với thông báo trong TSpec) và xếp vào hàng đợi để phù hợp với yêu cầu về QoS. Ví dụ một cách để có dịch vụ bảo đảm là sử dụng các hàng đợi có trọng số (WFQ), ở đây mỗi cổng dành riêng khác nhau được xem như một luồng đối với các hàng đợi, và trọng số

được ấn định cho mỗi luồng phù hợp với tốc độ dịch vụ yêu cầu trong RSpec của nó.

Đối với các luồng unicast thì RSVP là khá đơn giản. Nó trở nên phức tạp hơn trong môi trường multicast, bởi vì có thể có rất nhiều bộ phận dành riêng cổng cho một phiên đơn và các bộ phận khác nhau có thể yêu cầu các mức QoS khác nhau. Hiện nay MPLS chủ yếu tập trung vào các ứng dụng unicast của RSVP, chúng ta sẽ không đi sâu vào khía cạnh multicast của RSVP.

Điểm cuối cùng phải chú ý về RSVP: đây là giao thức "trạng thái mềm". Đặc tính để phân biệt giao thức trạng thái mềm với các giao thức khác là trạng thái sẽ tự động hết hiệu lực sau một thời gian trừ khi nó được refresh liên tục theo chu kỳ. Điều đó có nghĩa RSVP sẽ định kỳ gửi đi các bản tin PATH và RESV để làm tươi các cổng dành riêng. Nếu chúng không được gửi trong một khoảng thời gian xác định thì các cổng dành riêng tự động bị hủy bỏ.

Hình 2- 12 Thủ tục báo hiệu trong RSVP

- **MPLS hỗ trợ RSVP**

Trong phần này chúng ta chỉ tập trung vào vai trò của RSVP trong mạng MPLS về khía cạnh hỗ trợ QoS.

Mục tiêu đầu tiên của việc bổ sung hỗ trợ RSVP vào MPLS là cho phép các LSR dựa vào việc phân loại gói tin theo nhãn chứ không phải theo mào đầu IP nhận biết các gói tin thuộc các luồng của cổng dành riêng. Nói cách khác, cần phải tạo và kết hợp phân phối giữa các luồng và các nhãn cho các

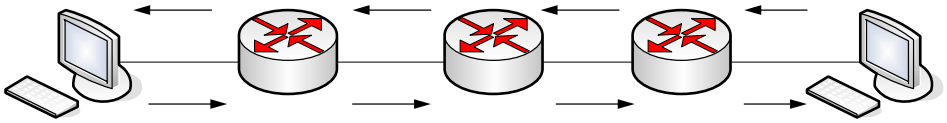
luồng có các cổng dành riêng RSVP như là một trường hợp riêng khác của FEC.

Điều này trở nên khá dễ dàng để kết hợp các nhãn với các luồng dành riêng trong RSVP, ít nhất là với unicast. Chúng ta định nghĩa một đối tượng RSVP mới là đối tượng LABEL được mang trong bản tin RSVP RESV. Khi một LSR muốn gửi bản tin RESV cho một luồng RSVP mới, LSR cấp phát một nhãn từ trong tập nhãn rỗi, tại một lối vào trong LFIB của nó với nhãn lối vào được đặt cho nhãn cấp phát, và gửi đi bản tin RESV có chứa nhãn này trong đối tượng LABEL. Chú ý là các bản tin RESV truyền từ bộ nhận tới bộ gửi là dưới dạng cấp phát nhãn xuôi.

Khi nhận được bản tin RESV chứa đối tượng LABEL, một LSR thiết lập LFIB của nó với nhãn này là nhãn lối ra. Sau đó nó cấp phát một nhãn để sử dụng như là nhãn lối vào và chèn nó vào bản tin RESV trước khi gửi nó đi. Rõ ràng là, khi các bản tin RESV truyền lên LSR ngược thì LSP được thiết lập dọc theo tuyến đường. Cũng chú ý là, khi các nhãn được cung cấp trong các bản tin RESV, mỗi LSR có thể dễ dàng kết hợp các tài nguyên QoS phù hợp với LSP. Hình 2-13 minh họa quá trình trao đổi này. Trong trường hợp này chúng ta giả sử các máy chủ không tham dự vào việc phân phối nhãn. LSR R3 cấp phát nhãn 5 cho cổng dành riêng này và thông báo nó với R2. R2 cấp phát nhãn 9 cũng cho cổng dành riêng này và thông báo nó với R1. Bây giờ đã có một LSP cho luồng dành riêng từ R1 đến R3. Khi các gói tin tương ứng với cổng dành riêng này (ví dụ gói tin gửi từ H1 tới H2 với số cổng nguồn, đích thích hợp và số giao thức giao vận thích hợp) tới R1, R1 phân biệt nó bằng các thông tin mào đầu IP và lớp truyền tải để tạo ra QoS thích hợp cho cổng dành riêng ví dụ như đặc điểm và hàng đợi các gói tin trong hàng đợi lối ra. Nói cách khác, nó thực hiện các chức năng của một bộ định tuyến tích hợp dịch vụ sử dụng RSVP. Hơn nữa, R1 đưa mào đầu nhãn vào

các gói tin và chèn giá trị nhãn lối ra là 9 trước khi gửi chuyển tiếp gói tin tới R2.

Khi R2 nhận gói tin mang nhãn 9, nó tìm kiếm nhãn đó trong LFIB và tìm tất cả các trạng thái liên quan đến QoS để xem kiểm soát luồng, xếp hàng đợi gói tin, v.v.. như thế nào. Điều này tất nhiên không cần kiểm tra mào đầu lớp IP hay lớp truyền tải. Sau đó R2 thay thế nhãn trên gói tin với một nhãn lối ra từ LFIB của nó (mang giá trị 5) và gửi gói tin đi.



Hình 2- 13 Nhãn phân phối trong bản tin RESV

Lưu ý rằng, do việc tạo ra nhãn kết hợp được điều khiển bởi các bản tin RSVP vì vậy việc kết hợp được điều khiển như trong các môi trường khác của MPLS. Cũng chú ý là đây cũng là một ví dụ chứng tỏ việc mang thông tin kết hợp nhãn trên một giao thức có sẵn không cần một giao thức riêng như LDP.

Một kết quả thú vị của việc thiết lập một LSP cho một luồng với cổng dành riêng RSVP là chỉ có một bộ định tuyến đầu tiên trong LSP mà trong ví dụ trên là R1 liên quan tới việc xem liệu các gói tin thuộc luồng dành riêng nào. Điều này cho phép RSVP được áp dụng trong môi trường MPLS theo cách mà nó không thể thực hiện được trong mạng IP truyền thống. Theo quy ước, các cổng dành riêng RSVP có thể tạo chỉ cho những luồng ứng dụng riêng lẻ, tức là những luồng được xác định nhờ năm trường mào đầu như mô tả phía trước. Tuy nhiên, có thể đặt cấu hình R1 để lựa chọn các gói tin dựa trên một số các tiêu chuẩn. Ví dụ R1 có thể lấy tất cả các gói tin có cùng một tiền tố ứng với một đích và đẩy chúng vào LSP. Vì vậy thay vì có một LSP

RESV
Nhãn =9
R1
H1 PATH

cho mỗi luồng ứng dụng riêng, một LSP có thể cung cấp QoS cho nhiều luồng lưu lượng. Một ứng dụng của khả năng này là có thể cung cấp "đường ống" với băng thông đảm bảo từ một Site của một công ty lớn đến một Site khác, thay vì phải sử dụng đường thuê bao riêng giữa các Site này. Khả năng này cũng hữu ích cho mục đích điều khiển lưu lượng, ở đây một lưu lượng lớn cần được gửi dọc theo các LSP với băng thông đủ để tải lượng.

Để hỗ trợ một vài cách sử dụng tăng cường của RSVP, MPLS định nghĩa một đối tượng RSVP mới có thể mang trong bản tin PATH là: đối tượng LABEL_REQUEST. Đối tượng này thực hiện hai chức năng. Thứ nhất, nó được sử dụng để thông báo cho một LSR tại phía cuối của LSP gửi RESV trở về để thiết lập LSP. Điều này hữu ích cho việc thiết lập các LSR site – to – site. Thứ hai, khi LSP được thiết lập cho một tập các gói tin, không chỉ là một luồng ứng dụng riêng, đối tượng chứa một trường để xác định giao thức lợp cao hơn sẽ sử dụng LSP. Trường này được sử dụng giống như ethertype hoặc tương tự như mã đế phân kênh để xác định giao thức lớp cao hơn (IPv4, IPX, v.v...), vì vậy sẽ không có trường phân kênh trong mào đầu MPLS nữa. Do vậy, một LSP có thể cần được thiết lập cho mỗi giao thức lớp cao hơn nhưng ở đây không giới hạn những giao thức nào được hỗ trợ. Đặc biệt, không yêu cầu các gói tin mang trong LSP được thiết lập sử dụng RSVP phải là các gói tin IP.

- **RSVP và khả năng mở rộng**

Một trong những điều chắc chắn về RSVP là nó có thể chịu tổn thất về khả năng mở rộng ở một mức nào đấy. Trong thực tế, đặc tính này không chính xác hoàn toàn. RSVP khởi đầu được thiết kế để hỗ trợ dự trữ tài nguyên cho các luồng ứng dụng riêng và đây là nhiệm vụ với những thách thức về khả năng mở rộng vốn có.

Chính xác thì khả năng mở rộng là gì? Nói chung thuật ngữ này được sử

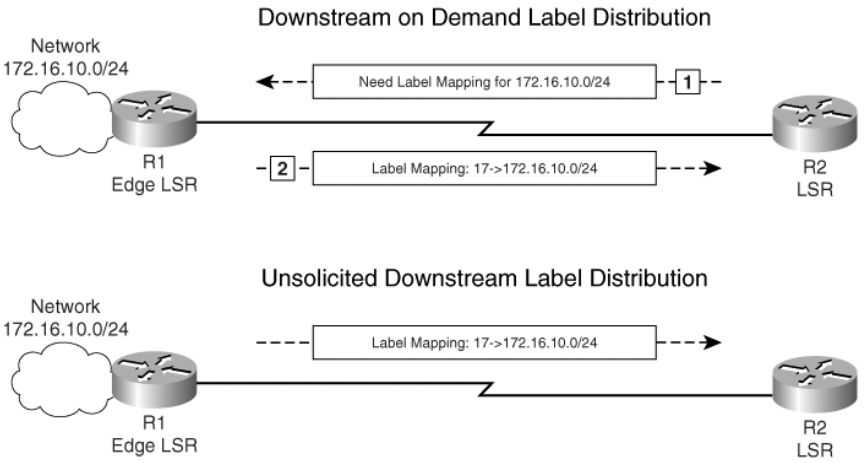
dụng để chỉ giới hạn sử dụng tài nguyên tăng nhanh như thế nào khi mạng lớn hơn. Ví dụ trong mạng IP quy mô lớn như mạng xương sống nhà cung cấp dịch vụ Internet, chúng ta có thể quan tâm đến liệu một bảng định tuyến sẽ chiếm bộ nhớ của bộ định tuyến lớn đến mức nào, khả năng bộ xử lý và băng thông liên kết. Vì thế, bảng định tuyến tăng chậm hơn nhiều so với số người sử dụng kết nối vào mạng.

Dự trữ tài nguyên cho các luồng ứng dụng riêng rõ ràng là ảnh hưởng xấu đến khả năng mở rộng. Chúng ta có thể cho rằng mỗi người sử dụng sẽ dự trữ tài nguyên tại một vài tốc độ trung bình, vì thế số tài nguyên dự trữ được tạo ra qua mạng lớn có khả năng tăng nhanh bằng số người sử dụng của mạng. Điều này sẽ dẫn đến chi phí lớn nếu mỗi bộ định tuyến phải lưu trữ trạng thái và tiến trình một vài bản tin cho mỗi tài nguyên dự trữ cho luồng ứng dụng riêng.

Nói tóm lại, sẽ chính xác hơn nếu nói rằng mức dự trữ tài nguyên cho các luồng ứng dụng là kém hơn so với RSVP. Sự khác nhau này đặc biệt quan trọng khi chúng ta xem xét rằng RSVP không những đòi hỏi cho việc dự trữ tài nguyên cho các luồng ứng dụng riêng mà còn dự trữ tài nguyên cho lưu lượng tổng hợp.

Trong một miền MPLS, một nhãn gán tới một địa chỉ (FIB) đích được phân phối tới các láng giềng ngược dòng sau khi thiết lập session. Việc kết nối giữa mạng cụ thể với nhãn cục bộ và một nhãn trạm kế (nhận từ router xuôi dòng) được lưu trữ trong LFIB và LIB. MPLS dùng các phương thức phân phối nhãn như sau:

- Yêu cầu xuôi dòng (Downstream on demand).
- Tự nguyện xuôi dòng (Unsolicited downstream).



Hình 2- 14 Phương thức phân phối nhãn

CHƯƠNG 3

MẠNG RIÊNG ẢO MPLS VPN

3.1 Giới thiệu về MPLS VPN

3.1.1 Định nghĩa VPN

Ngày nay, một công ty có trụ sở phân tán ở nhiều nơi. Để kết nối các máy tính tại các vị trí này, công ty đó cần có một mạng thông tin. Mạng đó là mạng riêng với ý nghĩa là nó chỉ được công ty đó sử dụng. Mạng đó là mạng riêng cũng với ý nghĩa là kế hoạch định tuyến và đánh địa chỉ trong mạng đó độc lập với việc định tuyến và đánh địa chỉ của các mạng khác. Mạng đó là một mạng ảo với ý nghĩa là các phương tiện được sử dụng để xây dựng mạng này có thể không dành riêng cho công ty đó mà có thể chia sẻ dùng chung với các công ty khác. Các phương tiện cần thiết để xây dựng mạng này được cung cấp bởi người thứ ba được gọi là nhà cung cấp dịch vụ VPN. Các công ty sử dụng mạng được gọi là các khách hàng VPN. Các công ty cung cấp dịch vụ VPN gọi là SP (services Provider).

VPN có thể được sử dụng để mở rộng phạm vi của một Intranet. Bởi vì, Intranet thường được sử dụng để trao đổi thông tin một cách độc quyền và ta không muốn những thông tin này được truyền bá trên Internet. Tuy nhiên trong nhiều trường hợp, các văn phòng công ty trên diện rộng có nhu cầu chia sẻ thông tin và những người sử dụng từ xa muốn truy cập vào Intranet thông qua Internet. VPN sẽ cho phép kết nối vào Intranet một cách an toàn và không lo ngại bị lộ thông tin. Có thể coi kết nối loại này như là Extranet. Điểm khác nhau giữa hai trường hợp Intranet và Extranet đó là câu hỏi ai là người đặt ra các chính sách của mạng VPN, trong trường hợp mạng Intranet thì đó là một công ty còn trong trường hợp mạng Extranet thì đó là một nhóm công ty.

Sử dụng ví dụ trên về cơ sở dữ liệu khách hàng, rất dễ hiểu là làm thế nào

mà VPN có thể mở rộng khả năng ứng dụng của Intranet. Giả sử tất cả các nhân viên bán hàng của công ty đang đi công tác hoặc là làm việc tại nhà. Họ có thể sử dụng Internet để truy cập vào các WebServer chứa những thông tin về khách hàng. VPN cung cấp kết nối đảm bảo an toàn giữa máy tính của nhân viên và WebServer chứa CSDL và mã hóa dữ liệu. VPN cho phép khả năng sử dụng linh hoạt đối với bất cứ dịch vụ mạng nào được sử dụng một cách an toàn thông qua Internet.

Đặc tính chủ yếu của một mạng riêng là lưu lượng khách hàng được tách riêng với cơ sở hạ tầng bên dưới và từ các khách hàng mà cùng chia sẻ cơ sở hạ tầng đó. Sự tách biệt thể hiện ở hai khía cạnh:

- Tách biệt về topology (Topological Isolation): nghĩa là các khách hàng có thể đưa vào bất cứ không gian địa chỉ và định tuyến nào họ lựa chọn. Một vấn đề phổ biến sử dụng cho các mạng riêng là địa chỉ IP sử dụng không thực sự là duy nhất (mang tính tổng thể) và sẽ xảy ra va chạm với người khác sử dụng cùng địa chỉ đó hiện hữu trên mạng Internet.
- Tách biệt về thời gian (Temporal Isolation): Nghĩa là dịch vụ mạng riêng chỉ phụ thuộc vào các đặc tính của lưu lượng khách hàng đó.

Tạo ra mạng riêng ảo yêu cầu các cơ chế cho phép một cơ sở hạ tầng chung (ví dụ, một tập hợp các liên kết và các router) được chia sẻ trong khi vẫn làm cho các khách hàng tin rằng họ được đảm bảo sự riêng tư. Các kỹ thuật chẳng hạ *IP tunneling* qua một backbone IP có thể hỗ trợ sự tách biệt về topology, nhưng IP backbone vẫn cần thiết được đảm bảo băng thông khả dụng xác định và độ trễ đầu cuối đến đầu cuối cho các IP tunnel khác nhau.

Có nhiều mô hình kết nối các Site với nhau. Nó có thể là kết nối dạng mắt lưới hoặc cũng có thể là kết nối hình sao qua Hub. Một ví dụ khác về cấu hình kết nối giữa các Site thuộc hai hoặc nhiều nhóm là các Site trong mỗi nhóm

được kết nối với nhau dạng mắt lưới còn các Site trong các nhóm khác nhau được kết nối gián tiếp thông qua một Site cụ thể.

VPN là một cách mô phỏng mạng riêng trên một mạng công cộng như Internet. Nó được gọi là ảo bởi vì nó phụ thuộc vào việc sử dụng các kết nối ảo, đó là những kết nối tạm thời gồm các gói được định tuyến trên nhiều máy tính trên Internet theo một cấu trúc đặc biệt. Các kết nối ảo đảm bảo an ninh được thiết lập giữa các máy tính, giữa các mạng, giữa mạng và máy tính.

Sử dụng Internet cho truy cập từ xa sẽ tiết kiệm được chi phí. Ta có thể quay số ở bất cứ đâu chỉ cần tại đó ISP có điểm truy nhập POP. Nếu ISP có các điểm POP mang tính quốc gia thì đối với mạng LAN sẽ chỉ là các cuộc gọi nội hạt. Một vài ISP có thể có các mở rộng quốc tế hoặc có sự thỏa thuận với các ISP khác. Việc lựa chọn ISP sẽ rẻ hơn đối với việc truy cập từ xa với những người sử dụng roaming.

VPN được thiết lập giữa các router tại hai chi nhánh của công ty thông qua Internet. Hơn nữa, VPN cho phép hợp nhất các kết nối Internet và WAN vào một router và một đường truyền, điều này giúp tiết kiệm chi phí thiết bị và hạ tầng cơ sở viễn thông.

3.1.2 Mô hình Overlay VPN và Peer to Peer VPN

VPN được giới thiệu như là một một mạng riêng mà sử dụng trên hạ tầng chung. Một mạng riêng yêu cầu tất cả các đầu cuối khách hàng có thể kết nối với nhau và hoàn toàn riêng biệt đối với các mạng VPN khác. Mạng VPN thường là một công ty và có một vài điểm kết cuối kết nối qua hạ tầng của nhà cung cấp dịch vụ chung.

Dựa vào sự tham gia của mình trong việc định tuyến cho khách hàng Nhà cung cấp dịch vụ có thể triển khai hai mô hình VPN chính để cung cấp dịch vụ VPN cho khách hàng.

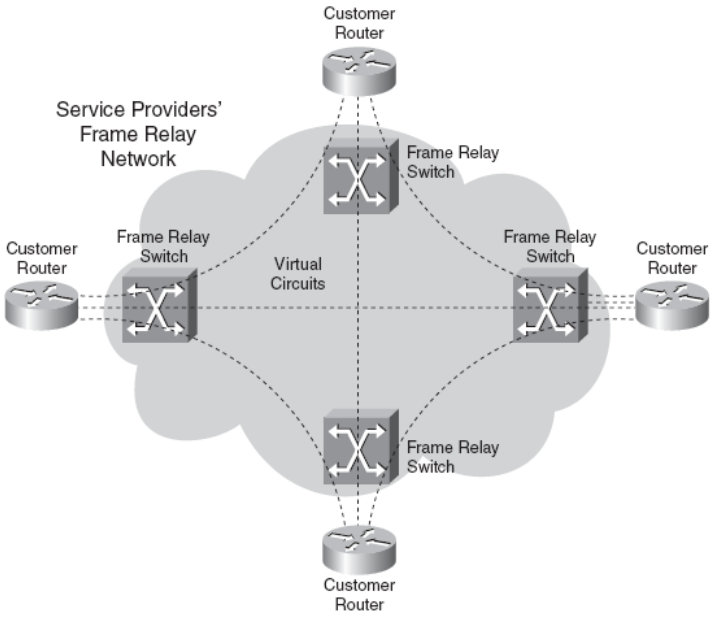
- Mô hình Overlay VPN
- Mô hình Peer to Peer VPN

- **Mô hình Overlay VPN**

Trong mô hình overlay VPN, nhà cung cấp dịch vụ cung cấp một kết nối điểm – điểm hoặc kênh ảo từ bên này sang bên kia mạng của họ giữa các bộ định tuyến của khách hàng. Như vậy, mô hình Overlay VPN cung cấp cho khách hàng các mạng riêng, nhà cung cấp không thể tham gia vào việc định tuyến khách hàng. Các nhà cung cấp dịch vụ chỉ vận chuyển dữ liệu qua các kết nối point-to-point ảo. Nếu mạch ảo là cố định, sẵn sàng cho khách hàng sử dụng mọi lúc thì được gọi là mạch ảo cố định PVC. Nếu mạch ảo được thiết lập theo yêu cầu (on-demand) thì được gọi là mạch ảo chuyển đổi. Hạn chế chính của mô hình Overlay là các mạch ảo của các site khách hàng kết nối dạng full mesh (ngoại trừ triển khai dạng hub-and-spoke hay partial hub-and-spoke). Nếu có N site khách hàng thì tổng số lượng mạch ảo cần thiết cho việc tối ưu định tuyến là N(N-1)/2.

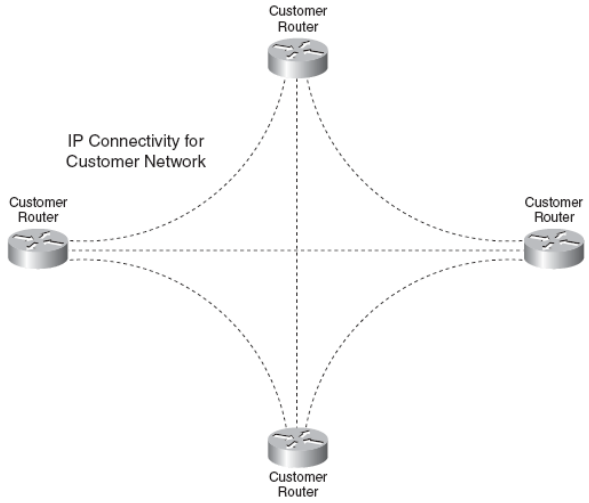
Ban đầu Overlay VPN được thực thi bởi SP để cung cấp các kết nối lớp 1 (physical layer) như Ghép kênh phân chia theo thời gian (TDM), E1, E3, SONET, và đường kết nối SDH, hay mạch chuyển vận lớp 2 (dữ liệu dạng frame hoặc cell) giữa các site khách hàng bằng cách sử dụng các thiết bị Frame Relay hay ATM switch làm PE (ví dụ lớp 2 là các kênh ảo được tạo bởi X.25, ATM hoặc Frame Relay). Do đó nhà cung cấp dịch vụ không thể nhận biết được việc định tuyến ở phía khách hàng.

Hình 3-1 chỉ ra một ví dụ về mạng overlay trên Frame Relay. Trong mạng của nhà cung cấp dịch vụ là những bộ chuyển mạch Frame Relay mà thiết lập những kênh ảo giữa những bộ định tuyến của khách hàng trên biên của mạng Frame relay.



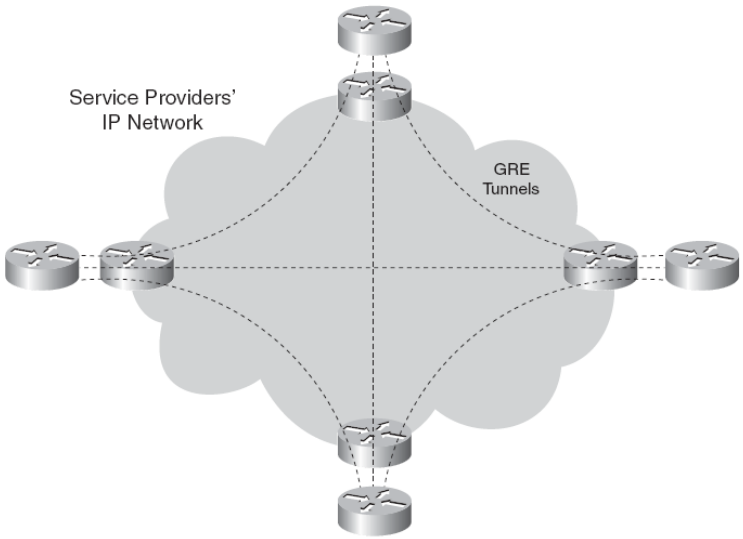
Hình 3- 1 Mô hình mạng Overlay trên Frame relay

Sau đó, Overlay VPN thực thi các dịch vụ qua IP (lớp 3) với các giao thức định đường hầm như L2TP, GRE, và IPSec. Tuy nhiên, dù trong trường hợp nào thì mạng của nhà cung cấp vẫn trong suốt đối với khách hàng, và các giao thức định tuyến chạy trực tiếp giữa các router của khách hàng.



Hình 3- 2 Mạng Overlay - Customer Routing Peering

Phần lớn những đường hầm (tunnel) hay được sử dụng để xây dựng mạng overlay trên IP là những đường hầm đóng gói định tuyến chung (GRE - generic routing encapsulation). Những đường hầm đóng gói lưu lượng với header GRE và header IP. Header GRE và một số chỉ tiêu khác chỉ ra giao thức vận chuyển nào đang được sử dụng. Header IP thường được sử dụng để định tuyến gói qua mạng nhà cung cấp dịch vụ. Hình 3-3 chỉ ra ví dụ về mạng overlay với đường hầm GRE, một trong những ưu điểm của đường hầm GRE là nó có thể định tuyến lưu lượng khác hơn lưu lượng IP.

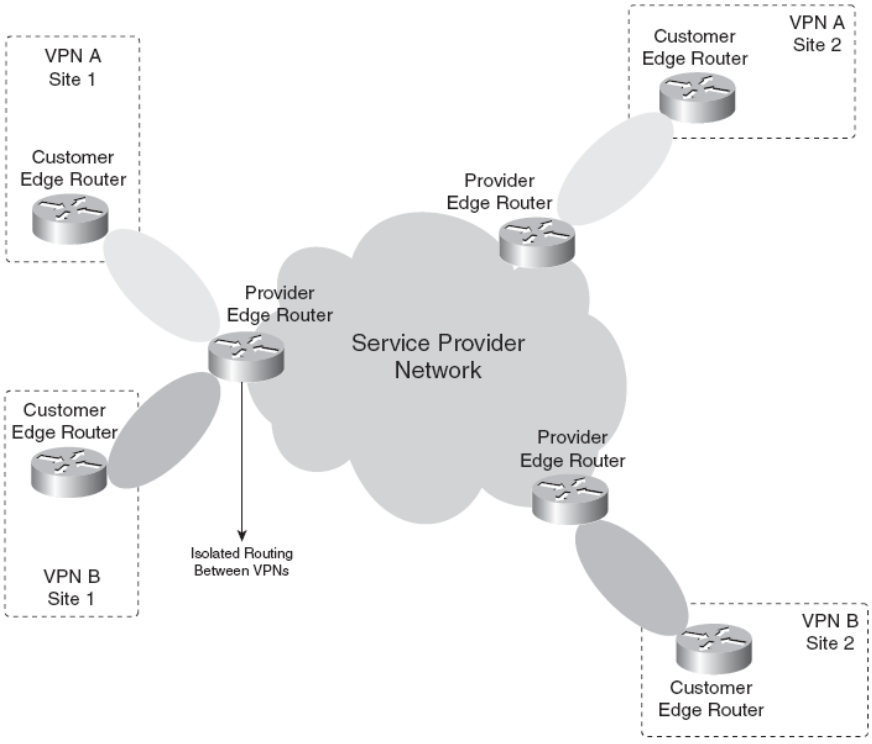


Hình 3- 3 Đường hầm GRE trên mạng overlay

- **Mô hình Peer – to – Peer**

Mô hình ngang cấp (peer-to-peer) được phát triển để khắc phục nhược điểm của mô hình Overlay và cung cấp cho khách hàng cơ chế vận chuyển tối ưu qua SP backbone. Trong mô hình này, những bộ định tuyến của nhà cung cấp dịch vụ vận chuyển dữ liệu của khách hàng qua mạng, nhưng nó cũng tham gia vào việc định tuyến của khách hàng. Nói một cách khác, những bộ định tuyến của nhà cung cấp dịch vụ sẽ ngang hàng với bộ định tuyến của khách hàng tại Lớp 3. Trong mô hình peer-to-peer, thông tin định tuyến được

trao đổi giữa các router khách hàng và các router của nhà cung cấp dịch vụ, dữ liệu của khách hàng được vận chuyển qua mạng lõi của nhà cung cấp. Thông tin định tuyến của khách hàng được mang giữa các router trong mạng của nhà cung cấp (P và PE), và mạng khách hàng (các CE router). Mô hình này không yêu cầu tạo ra mạch ảo. Quan sát hình trên ta thấy, các CE router trao đổi tuyến với các router PE trong SP domain. Thông tin định tuyến của khách hàng được quảng bá qua SP backbone giữa các PE và P và xác định được đường đi tối ưu từ một site khách hàng đến một site khác. Việc phát hiện các thông tin định tuyến riêng của khác hàng đạt được bằng cách thực hiện lọc gói tại các router kết nối với mạng khách hàng. Địa chỉ IP của khách hàng do nhà cung cấp kiểm soát. Tiến trình này xem như là thực thi các PE peer-topeer chia sẻ (shared PE peer-to-peer).

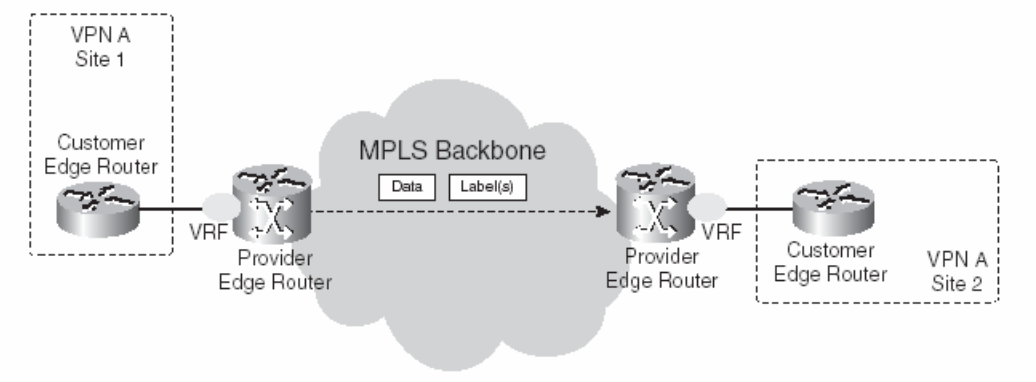


Hình 3- 4 Đưa ra khái niệm của mô hình VPN ngang hàng.

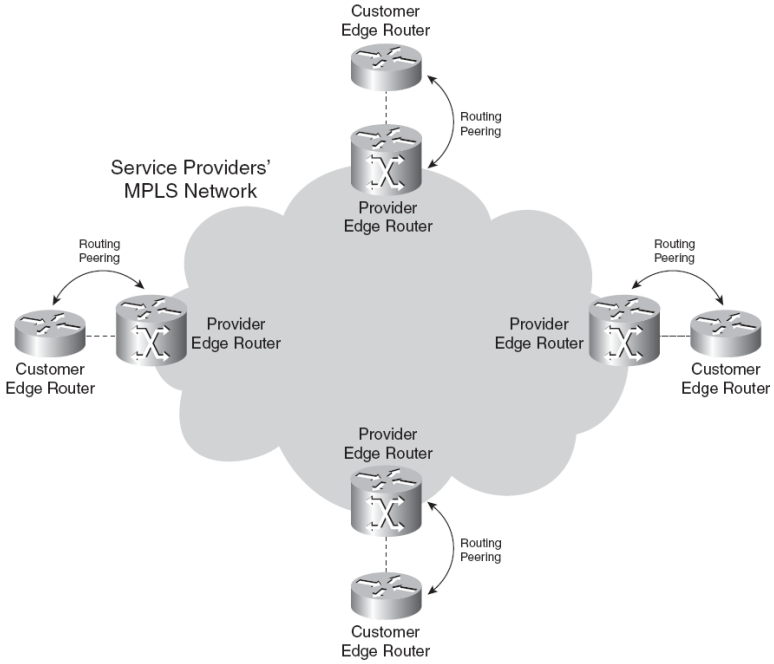
Trước khi MPLS ra đời, mô hình peer – to – peer VPN có thể thiết lập bằng cách tạo ra định tuyến ngang cấp IP giữa bộ định tuyến của khách hàng và của nhà cung cấp. Mô hình VPN cũng yêu cầu tính cá nhân (riêng biệt) và cách ly giữa các khách hàng khác nhau. Ta cũng có thể thiết lập bằng cách cấu hình bộ lọc gói (danh sách truy nhập) để điều khiển dữ liệu tới và đi từ bộ định tuyến của khách hàng. Một cách khác để thực hiện được định hình thức cá nhân là cấu hình những bộ lọc định tuyến để thông báo định tuyến hoặc dừng định tuyến từ việc thông báo tới bộ định tuyến của khách hàng. Hoặc ta có thể thực hiện tất cả các phương thức trên cùng một lúc.

Trước khi MPLS trở nên phổ biến, mô hình trùng lặp overlay VPN đã được triển khai nhiều hơn mô hình peer – to – peer VPN. Mô hình peer – to – peer VPN yêu cầu nhiều từ phía nhà cung cấp bởi vì khi thêm một khách hàng yêu cầu rất nhiều sự thay đổi cấu hình tại rất nhiều site. MPLS VPN là một ứng dụng của MPLS mà nó tạo ra mô hình peer – to – peer VPN dễ dàng hơn để thực hiện. Bây giờ việc thêm vào hoặc bỏ ra một điểm cuối khách hàng dễ dàng hơn trong việc cấu hình và do đó yêu cầu ít thời gian và sự cố gắng hơn. Với MPLS VPN, một bộ định tuyến khách hàng (được gọi là bộ định tuyến khách hàng biên - CE) ngang cấp với Lớp IP với ít nhất một bộ định tuyến của nhà cung cấp dịch vụ (được gọi là bộ định tuyến nhà cung cấp biên - PE).

Tính cá nhân (private) trong mạng MPLS VPN đạt được bởi việc sử dụng khái niệm của chuyển tiếp định tuyến ảo (VRF) và thực tế dữ liệu được chuyển tiếp trong mạng đường trục như là những gói được dán nhãn. VRF đảm bảo rằng thông tin định tuyến từ các khách hàng khác nhau được giữ riêng biệt, và MPLS trên mạng đường trục đảm bảo những gói được chuyển tiếp dựa trên thông tin nhãn và không phải là thông tin trên mào đầu IP. Hình 3-5 đưa ra khái niệm về VRF và gói dán nhãn chuyển tiếp trên mạng đường trục mà đang sử dụng công nghệ MPLS VPN.



Hình 3- 5 MPLS VPN với VRF



Hình 3- 6 Định nghĩa mô hình peer to peer ứng dụng trong MPLS VPN

Việc thêm một kết cuối khách hàng có nghĩa là trên bộ định tuyến PE, chỉ ngang hàng với bộ định tuyến CE, phải được thêm vào. Ta không gặp nhiều rắc rối trong việc tạo ra nhiều kênh ảo như với mô hình overlay (overlay) hoặc với những cấu hình bộ lọc gói hoặc những bộ lọc định tuyến với mô hình peer – to – peer VPN qua mạng IP. Đây chính là ưu điểm của MPLS VPN cho nhà cung cấp dịch vụ.

Phần lớn nhà cung cấp dịch vụ sử dụng mạng hub – and – spoke, một số lại sử dụng mạng meshed đầy đủ quanh mạng đường trục của nhà cung cấp. Số còn lại sử dụng một vài tính năng của cả 2. Khách hàng sẽ được nhiều lợi ích nhất của MPLS VPN khi khách hàng sử dụng mạng Mesh đầy đủ. Hình 3-1 chỉ ra mạng mesh đầy đủ của khách hàng quanh mạng Frame Relay, và so sánh với cùng khách hàng mà sử dụng MPLS VPN trong hình 3-6. Trong hình 3-1 mỗi bộ định tuyến biên khách hàng tương đương (ngang hàng) với *n-1* bộ định tuyến biên của các khách hàng khác – trong đó *n* là tổng số các bộ định tuyến biên khách hàng. Một lợi ích khách của nhà cung cấp dịch vụ là chỉ cần cung cấp đường kết nối giữa bộ định tuyến PE và CE. Với mô hình overlay, nhà cung cấp dịch vụ cần phải cung cấp đường kết nối hoặc những kênh ảo giữa các điểm (site). Điều này dễ dự đoán lưu lượng hơn và băng thông yêu cầu tại mỗi điểm (site) hơn là dự đoán mô hình lưu lượng hoàn chỉnh giữa tất cả các điểm cuối khách hàng.

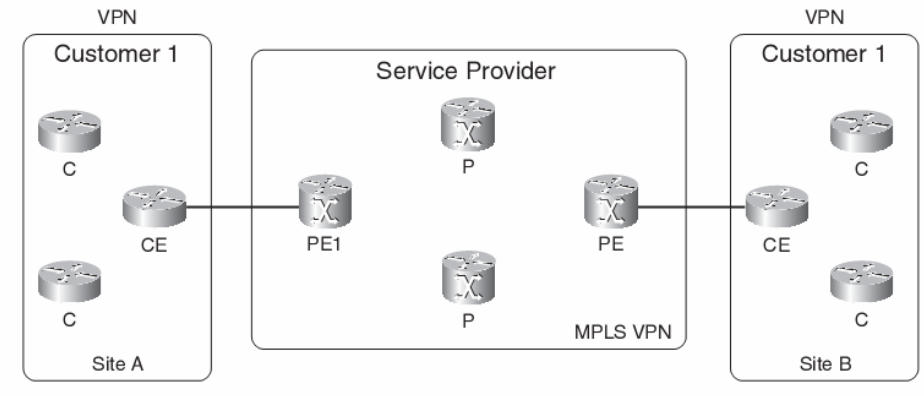
Những nhược điểm của mô hình peer – to – peer VPN so với mô hình overlay VPN.:

- Khách hàng phải chia sẻ trách nhiệm định tuyến với nhà cung cấp dịch vụ.
- Yêu cầu phải có thêm thiết bị biên của nhà cung cấp.

Nhược điểm đầu tiên là khách hàng phải có một định tuyến ngang hàng với nhà cung cấp dịch vụ. Khách hàng không thể kiểm soát (điều khiển) mạng end to end trên lớp 3 và theo định tuyến IP, như với mô hình overlay. Nhược điểm thứ hai là của nhà cung cấp dịch vụ. Gánh nặng của nhà cung cấp dịch vụ chính là việc phải trang bị thêm thiết bị biên – bộ định tuyến PE. Nhà cung cấp dịch vụ phải có trách nhiệm và định tuyến hội tụ của mạng khách hàng bởi vì các bộ định tuyến PE phải có khả năng mang tất cả bộ định tuyến của nhiều khách hàng trong khi cung cấp định tuyến hội tụ kịp thời.

3.1.3 Mô hình mạng MPLS VPN

Nhà cung cấp dịch vụ đang cung cấp hạ tầng công cộng chung cho khách hàng.



Hình 3- 7 Biểu đồ tổng quan về MPLS VPN

PE là bộ định tuyến biên của nhà cung cấp. Bộ PE kết nối trực tiếp với bộ định tuyến biên CE của khách hàng tại lớp 3. Bộ định tuyến P là bộ định tuyến không kết nối trực tiếp với bộ định tuyến của khách hàng. Trong khi thực hiện, cả hai bộ định tuyến P và PE đều chạy MPLS. Điều này có nghĩa là chúng phải có khả năng phân phối nhãn giữa chúng và chuyển tiếp những gói được gán nhãn.

Bộ định tuyến CE cũng kết nối trực tiếp với PE tại lớp 3. Bộ định tuyến khách hàng C không kết nối trực tiếp với PE. Bộ định tuyến CE không cần thiết phải chạy MPLS. Bởi vì cả CE và PE đều tương tác tại lớp 3, giữa chúng phải có một giao thức định tuyến (hoặc định tuyến tĩnh). Bộ định tuyến CE chỉ ngang hàng với một PE. Nếu CE là multihomed (đa điểm), nó có thể ngang hàng với nhiều PE. Bộ định tuyến CE không thể ngang hàng với bất kỳ bộ định tuyến CE của các site khác qua mạng nhà cung cấp dịch vụ, như với mô hình overlay. Tên mô hình peer to peer xuất phát từ thực tế là CE và PE là ngang hàng với nhau ở lớp 3.

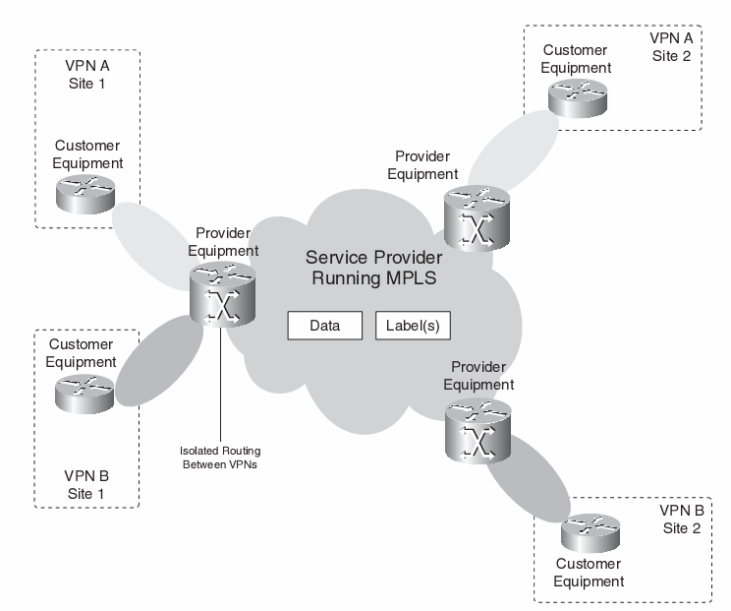
Chữ P trong VPN viết tắt của Private. Theo đó, khách hàng của nhà cung cấp dịch vụ được phép có lược đồ địa chỉ IP của chính họ. Có nghĩa là họ có thể đăng ký địa chỉ IP nhưng cũng là địa chỉ IP dành riêng hoặc thậm chí là địa chỉ IP mà nó cũng được sử dụng bởi khách hàng khác mà những khách hàng này đang kết nối tới cùng nhà cung cấp dịch vụ (như là địa chỉ IP trùng lắp). Nếu gói được chuyển tiếp như gói IP trong mạng của nhà cung cấp, nó có thể gây ra lỗi, bởi vì bộ định tuyến P có thể bị nhầm lẫn. Nếu lược đồ địa chỉ IP cá nhân và địa chỉ IP trùng lắp không được cho phép, thì tất cả khách hàng phải sử dụng một dải địa chỉ duy nhất. Trong trường hợp này, gói có thể được chuyển tiếp qua mạng bởi việc tìm kiếm địa chỉ IP đích trên mỗi bộ định tuyến trong mạng của nhà cung cấp dịch vụ. Điều này có nghĩa là P và PE phải có bảng định tuyến hoàn chỉnh của tất cả khách hàng. Nó sẽ là một bảng định tuyến rất lớn. Giao thức định tuyến mà có dung lượng lớn có khả năng mang số lượng lớn tuyến là Giao thức cổng biên (BGP). Tất cả các P và PE đều chạy BGP trong (i BGP) giữa chúng. Tuy nhiên, đây không phải là lược đồ VPN, bởi vì nó không riêng biệt tới khách hàng.

Một giải pháp khác đó là các P và PE có một bảng định tuyến riêng cho mỗi khách hàng. Một vài quá trình của một giao thức định tuyến (một thực thi trên VPN) có thể đang chạy trên tất cả bộ định tuyến để phân phối tuyến VPN. Mỗi lần một VPN được thêm vào trong mạng, một quy trình định tuyến mới phải được thêm vào trong mỗi bộ định tuyến P. Hơn nữa, nếu gói IP đi vào một một bộ định tuyến P, làm thế nào để P xác định được gói đó thuộc VPN nào có thể tìm ra bảng định tuyến riêng cho gói đó để chuyển tiếp đúng gói. Nếu gói là một gói IP, điều này là không thể. Ta có thể thêm vào một trường trong gói IP để chỉ ra rằng gói IP này thuộc VPN nào. Sau đó bộ định tuyến P có thể chuyển tiếp gói IP này bằng cách xem trường thêm vào này và

địa chỉ IP đích. Một lần nữa, tất cả bộ định tuyến P phải có thêm các kiến thức về trường thêm vào này.

Một giải pháp nữa là bộ định tuyến P hoàn toàn không có kiến thức về VPN. Sau đó P không cần có thêm gánh nặng về việc có phải có các thông tin của tuyến VPN. Ta có thể thực hiện điều này bằng việc sử dụng MPLS. Gói IP của khách hàng được gắn nhãn trong mạng của nhà cung cấp dịch vụ để đạt được VPN riêng đối với mỗi khách hàng. Hơn nữa, bộ định tuyến P không cần phải có bảng định tuyến của khách hàng nữa bằng việc sử dụng hai nhãn MPLS. Do đó, P không cần thiết chạy BGP. Xem thêm phần BGP Free core để hiểu thêm. Tuyến VPN chỉ được biết tại các PE. Thông thường, những hiểu biết VPN chỉ được thể hiện trên bộ định tuyến biên của mạng MPLS VPN.

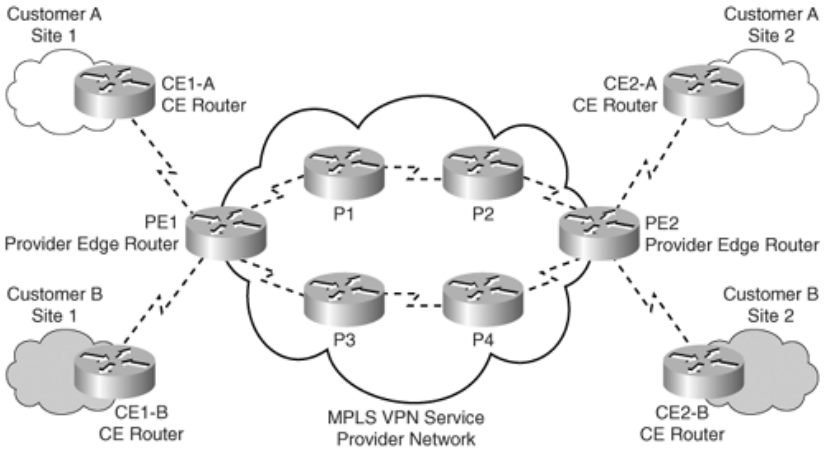
Hình 3-8 đưa ra mô hình của MPLS VPN: gói chuyển mạch nhãn trong mạng của nhà cung cấp dịch vụ và bộ định tuyến PE.



Hình 3- 8 Mô hình MPLS VPN

Trong kiến trúc mạng MPLS VPN, các router biên mang thông tin định tuyến khách hàng, cung cấp định tuyến tối ưu cho lưu lượng giữa các site của

khách hàng. Mô hình MPLS-based VPN cũng giúp cho khách hàng sử dụng không gian địa chỉ trùng lắp (overlapping address spaces), không giống như mô hình peer-to-peer truyền thống trong việc định tuyến lưu lượng khách hàng yêu cầu nhà cung cấp phải gán địa chỉ IP riêng cho mỗi khách hàng (hoặc khách hàng phải thực hiên NAT) để tránh trùng lắp không gian địa chỉ. MPLS VPN là một dạng thực thi đầy đủ của mô hình peer-to-peer; MPLS VPN backbone và các site khách hàng trao đổi thông tin định tuyến lớp 3, và dữ liệu được chuyển tiếp giữa các site khách hàng sử dụng MPLS-enable SP IP backbone. Miền (domain) MPLS VPN, giống như VPN truyền thống, gồm mạng của khách hàng và mạng của nhà cung cấp. Mô hình MPLS VPN giống với mô hình router PE dành riêng (dedicated PE router model) trong các dạng thực thi VPN ngang cấp peer-to-peer VPN. Tuy nhiên, thay vì triển khai các router PE khác nhau cho từng khách hàng, lưu lượng khách hàng được tách riêng trên cùng router PE nhằm cung cấp khả năng kết nối vào mạng của nhà cung cấp cho nhiều khách hàng. Các thành phần của một MPLS VPN được trình bày trong hình sau:



Hình 3- 9 Các thành phần của MPLS VPN

- Mạng khách hàng – thường là miền điều khiển của khách hàng gồm các thiết bị hay các router trải rộng trên nhiều site của cùng một khách hàng. Các router CE – là những router trong mạng khách hàng giao

tiếp với mạng của nhà cung cấp. Ở hình trên, mạng khách hàng của CustomerA gồm các router CE1-A, CE2-A và các thiết bị trong Site 1 và Site 2 của CustomerA. Các router CE của Customer A là CE1-A và CE2-A, và router CE của Customer B là CE1-B và CE2-B.

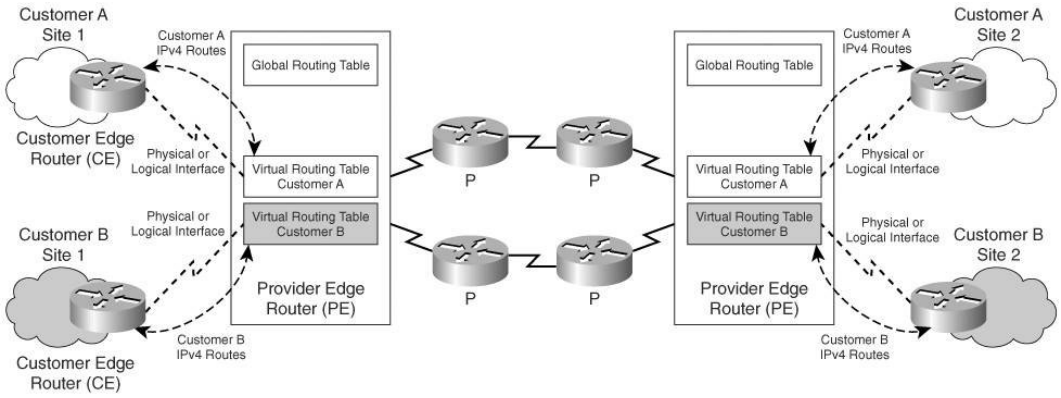
- Mạng của nhà cung cấp – miền thuộc điều khiển của nhà cung cấp gồm các router biên (edge) và lõi (core) để kết nối các site thuộc vào các khách hàng trong một hạ tầng mạng chia sẻ. Các router PE – là các router trong mạng của nhà cung cấp giao tiếp với router biên của khách hàng. Các router P – router trong lõi của mạng, giao tiếp với các router lõi khác hoặc router biên của nhà cung cấp. Trong hình trên, mạng của nhà cung cấp gồm các router PE1, PE2, P1, P2, P3, và P4. PE1 và PE2 là router biên của nhà cung cấp trong miền MPLS VPN cho khách hàng A và B. Router P1, P2, P3 và P4 là các router nhà cung cấp (provider router).

Mô hình định tuyến MPLS VPN

MPLS VPN giống như mô hình mạng ngang cấp với router dành riêng. Từ một router CE, chỉ cập nhật IPv4, dữ liệu được chuyển tiếp đến router PE. CE không cần bất kỳ một cấu hình riêng biệt nào cho phép nó tham gia vào miền MPLS VPN. Yêu cầu duy nhất trên CE là một giao thức định tuyến (hay tuyến tĩnh(static)/tuyến ngầm định (default)) cho phép nó trao đổi thông tin định tuyến IPv4 với các router PE. Trong mô hình MPLS VPN, router PE thực hiện rất nhiều chức năng. Trước tiên nó phải phân tách lưu lượng khách hàng nếu có nhiều hơn một khách hàng kết nối tới nó. Vì thế, mỗi khách hàng được gắn với một bảng định tuyến độc lập. Định tuyến qua SP backbone thực hiện bằng một tiến trình định tuyến trong bảng định tuyến toàn cục.

Router P cung cấp chuyển mạch nhãn giữa các router biên của nhà cung cấp và không biết đến các tuyến VPN. Các router CE trong mạng khách hàng

không nhận biết được các router P và do đó cấu trúc mạng nội bộ của mạng SP trong suốt đối với khách hàng. Hình sau mô tả chức năng của router PE.



Hình 3- 10 Chức năng của router PE

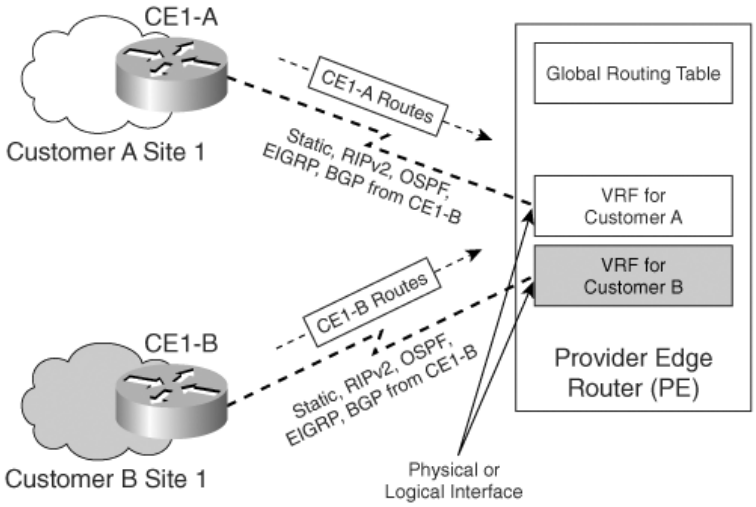
3.2 Các thành phần chính của kiến trúc MPLS VPN

Để thực hiện được MPLS VPN, ta cần xây dựng một số khối cơ bản trên PE. Những khối này là: VRF, RD – route Distinguisher (bộ phân biệt tuyến), RT – route targets (tuyến đích), sự ánh xạ tuyến qua MP-BGP và chuyển tiếp gói được gắn nhãn.

3.2.1 VRF - Virtual Routing and Forwarding Table

Khách hàng được phân biệt trên router PE bằng các bảng định tuyến ảo (virtual routing tables) hoặc các instance, còn được gọi là VRF. Thực chất nó giống như duy trì nhiều router riêng biệt cho các khách hàng kết nối vào mạng của nhà cung cấp. Chức năng của VRF giống như một bản định tuyến toàn cục, ngoại trừ việc nó chứa mọi tuyến liên quan đến một VPN cụ thể. VRF cũng chứa một bảng chuyển tiếp CEF cho VRF riêng biệt (VRF- specific CEF forwarding table) tương ứng với bảng CEF toàn cục xác định các yêu cầu kết nối và các giao thức cho mỗi site khách hàng kết nối trên một router PE. VRF xác định bối cảnh (context) giao thức định tuyến tham gia vào một VPN cụ thể cũng như giao tiếp trên router PE cục bộ tham gia vào VPN, nghĩa là sử

dụng VRF. Giao tiếp tham gia vào VRF phải hỗ trợ chuyển mạch CEF.Một VRF có thể gồm một giao tiếp (logical hay physical) hoặc nhiều giao tiếp trên một router. VRF chứa một bảng định tuyến IP tương ứng với bảng định tuyến IP toàn cục, một bảng CEF, liệt kê các giao tiếp tham gia vào VRF, và một tập hợp các nguyên tắc xác định giao thức định tuyến trao đổi với các router CE (routing protocol contexts). VRF còn chứa các định danh VPN (VPN identifier) như thông tin thành viên VPN (RD và RT). Hình sau cho thấy chức năng của VRF trên một router PE thực hiện tách tuyến khách hàng.



Hình 3- 11 Chức năng của VRF

Cisco IOS hỗ trợ các giao thức định tuyến khác nhau như những tiến trình định tuyến riêng biệt (OSPF, EIGRP,…) trên router. Tuy nhiên, một số giao thức như RIP và BGP, IOS chỉ hỗ trợ một instance của giao thức định tuyến. Do đó, thực thi định tuyến VRF bằng các giao thức này phải tách riêng hoàn toàn các VRF với nhau. Bối cảnh định tuyến (routing context) được thiết kế để hỗ trợ các bản sao của cùng giao thức định tuyến VPN PE-CE. Các bối ảnh định tuyến này có thể được thực thi như các tiến trình riêng biệt (OSPF), hay như nhiều instance của cùng một giao thức định tuyến (BGP, RIP, …). Nếu nhiều instance của cùng một giao thức định tuyến được sử dụng thì mỗi

instance có một tập các tham số của riêng nó.

Hiện tại, Cisco IOS hỗ trợ RIPv2, EIGRP, BGPv4 (nhiều instance), và OSPFv2 (nhiều tiến trình) được dùng cho VRF để trao đổi thông tin định tuyến giữa CE và PE.

Chú ý: các giao tiếp VRF có thể là luận lý (logical) hoặc vật lý (physical) nhưng mỗi giao tiếp chỉ được gán với một VRF.

Trong mô hình MPLS VPN, router PE phân biệt các khách hàng bằng VRF. Tuy nhiên, thông tin này cần được mang theo giữa các router PE để cho phép truyền dữ liệu giữa các site khách hàng qua MPLS VPN backbone. Router PE phải có khả năng thực thi các tiến trình cho phép các mạng khách hàng kết nối vào có không gian địa chỉ trùng lắp (overlapping address spaces). Router PE học các tuyến này từ các mạng khách hàng và quảng bá thông tin này bằng mạng trục chia sẻ của nhà cung cấp (shared provider backbone). Điều này thực hiện bằng việc kết hợp với RD trong bảng định tuyến ảo (virtual routing table) trên một router PE. Ta có thể tạo VRF trên PE với lệnh ***ip vrf*** .Ta sử dụng lệnh ***ip vrf forwarding*** để gán một giao diện PE – CE trên PE tới VRF. Ta cũng có thể gán một giao diện tới một VRF duy nhất, nhưng cũng có thể gán nhiều giao diện tới cùng một VRF. Sau đó PE sẽ tự động tạo một bảng VRF và CEF. Bảng định tuyến VRF không giống với bảng định tuyến thông thường trong Cisco IOS trừ khi nó được sử dụng cho một tập VPN site duy nhất và hoàn toàn riêng biệt với tất cả các bảng định tuyến khác. Sau đây là ví dụ cấu hình VRF cho VRF *cust-one*.

```
!
ip vrf cust-one
   rd  1:1
   route-target export 1:1
   route-target import 1:1
!
Interface Serial15/1
   ip vrf forwarding cust-one
   ip address 10.10.4.1 255.255.255.0
!
sydney#show ip route vrf cust-one
Routing Table: cust-one
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
    10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
B       10.10.2.0/24 [200/0] via 10.200.254.2, 00:31:04
C       10.10.4.0/24 is directly connected, Serial5/1
C       10.10.4.2/32 is directly connected, Serial5/1
B       10.10.100.1/32 [200/1] via 10.200.254.2, 00:31:04
```

```
B       10.10.100.3/32 [20/0] via 10.10.4.2, 00:13:29
sydney#show ip cef vrf cust-one
Prefix              Next Hop            Interface
0.0.0.0/0           no route
0.0.0.0/32          receive
10.10.2.0/24        10.200.214.1        POS0/1/0
10.10.4.0/24        attached            Serial5/1
10.10.4.0/32        receive
10.10.4.1/32        receive
10.10.4.2/32        attached            Serial5/1
10.10.4.255/32      receive
10.10.100.1/32      10.200.214.1        POS0/1/0
```

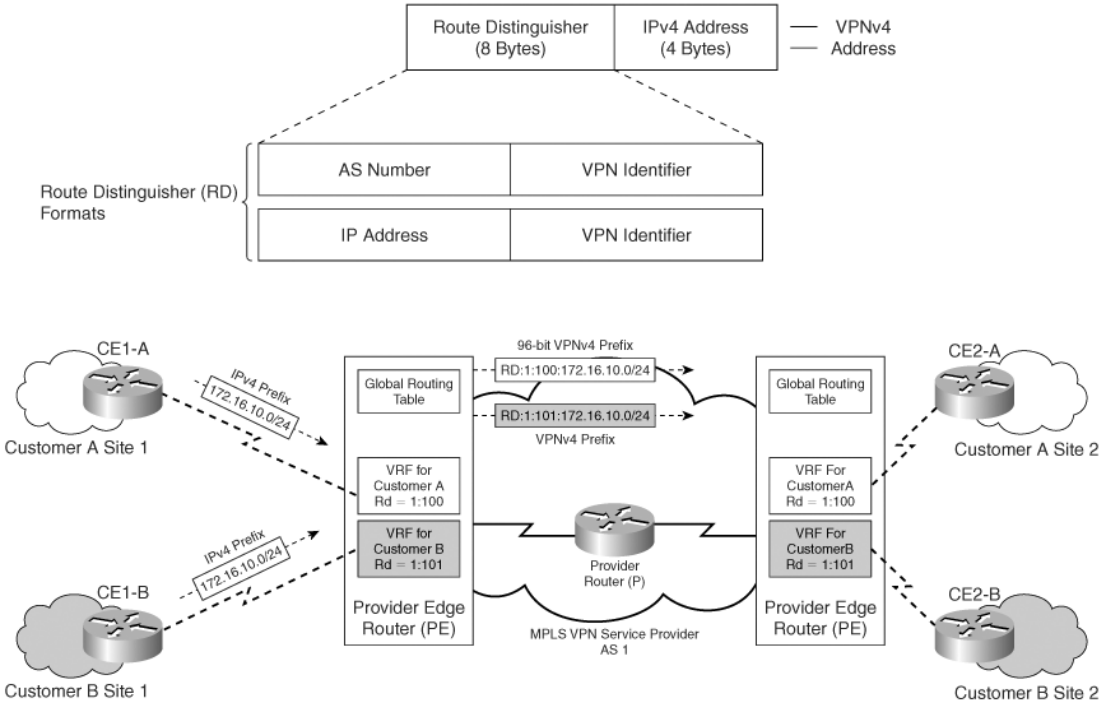
Chú ý: trong Cisco IOS, CEF chỉ là phương thức chuyển mạch hỗ trợ cho chuyển tiếp gói IP từ giao diện VRF. Thông thường, CEF phải được cho phép toàn cục trên tất cả PE và tất cả các giao diện VRF.

3.2.2 RD – Route Distinguisher

Là một định danh 64-bit duy nhất, thêm vào trước 32-bit địa chỉ tuyến được học từ router CE tạo thành địa chỉ 96-bit duy nhất có thể được chuyển vận giữa các router PE trong miền MPLS. Do đó chỉ duy nhất một RD được cấu hình cho 1 VRF trên router PE. Địa chỉ 96 bit cuối cùng (tổng hợp của 32-bit địa chỉ khách hàng và 64-bit RD) được gọi là một địa chỉ VPNv4.

Địa chỉ VPNv4 trao đổi giữa các router PE trong mạng nhà cung cấp. RD có thể có hai định dạng: dạng địa chỉ IP hoặc chỉ số AS. Giá trị 64 bit có thể có 2 định dạng: *ASN:nn* hoặc *IP-address:nn* (ở đây nn là một số). Trong đó định dạng *ASN:nn* được sử dụng nhiều hơn (ở đây *ASN* viết tắt của số hệ thống tự trị - autonomous system number). RD được sử dụng để tránh trường hợp tuyến IPv4 của một khách hàng trùng với tuyến IPv4 của khách hàng khác. Nếu tiền tố IPv4 10.1.1.0/24 và RD 1:1, tiền tố vpnv4 sẽ là 1:1:10.1.1.0/24.

Một khách hàng có thể sử dụng các RD khác nhau cho cùng một tuyến IPv4. Khi một VPN site được kết nối tới 2 PE, tuyến từ VPN có thể có 2 RD khác nhau, phụ thuộc vào PE nào mà tuyến nhận được. Mỗi tuyến IPv4 có thể có 2 RD khác nhau và có 2 tuyến vpnv4 hoàn toàn khác nhau. Điều này cho phép BGP nhìn thấy chúng như là các tuyến khác nhau và áp dụng một chính sách khác nhau cho mỗi tuyến. Hình bên dưới cho thấy hai khách hàng có địa chỉ mạng giống nhau, 172.16.10.0/24, được phân biệt nhờ vào các giá trị RD khác nhau, 1:100 và 1:101, ưu tiên quảng bá địa chỉ VPNv4 trên router PE.



Hình 3- 12 Ví dụ về RD

Giao thức dùng để trao đổi các tuyến VPNv4 giữa các PE là multiprotocol BGP (MP- BGP). IGP yêu cầu duy trì iBGP (internal BGP) khi thực thi MPLS VPN. Do đó, PE phải chạy một IGP cung cấp thông tin NLRI cho iBGP nếu cả hai PE cùng trong một AS. Hiện tại, Cisco hỗ trợ cả OSPFv2 và ISIS trong mạng nhà cung cấp như là IGP. MP-BGP cũng chịu trách nhiệm

chỉ định nhãn VPN. Khả năng mở rộng là lý do chính chọn BGP làm giao thức mang thông tin định tuyến khách hàng. Hơn nữa, BGP cho phép sử dụng địa chỉ VPNv4 trong môi trường MPLS VPN với dãy địa chỉ trùng lắp cho nhiều khách hàng.

Một phiên làm việc MP-BGP giữa các PE trong một BGP AS được gọi là MP-iBGP session và kèm theo các nguyên tắc thực thi của iBGP liên quan đến thuộc tính của BGP (BGP attributes). Nếu VPN mở rộng ra khỏi phạm vi một AS, các VPNv4 sẽ trao đổi giữa các AS tại biên bằng MP-eBGP session.
Cấu hình một RD

```
sydney#conf  t
Enter configuration commands, one per line.  End with CNTL/Z.
sydney(config)#ip  vrf  ?
  WORD  VPN Routing/Forwarding instance name
sydney(config)#ip vrf cust-one
sydney(config-vrf)#rd  ?
ASN:nn or IP-address:nn  VPN Route Distinguisher
sydney(config-vrf)#rd  1:1
```

3.2.3 RT – Route targets

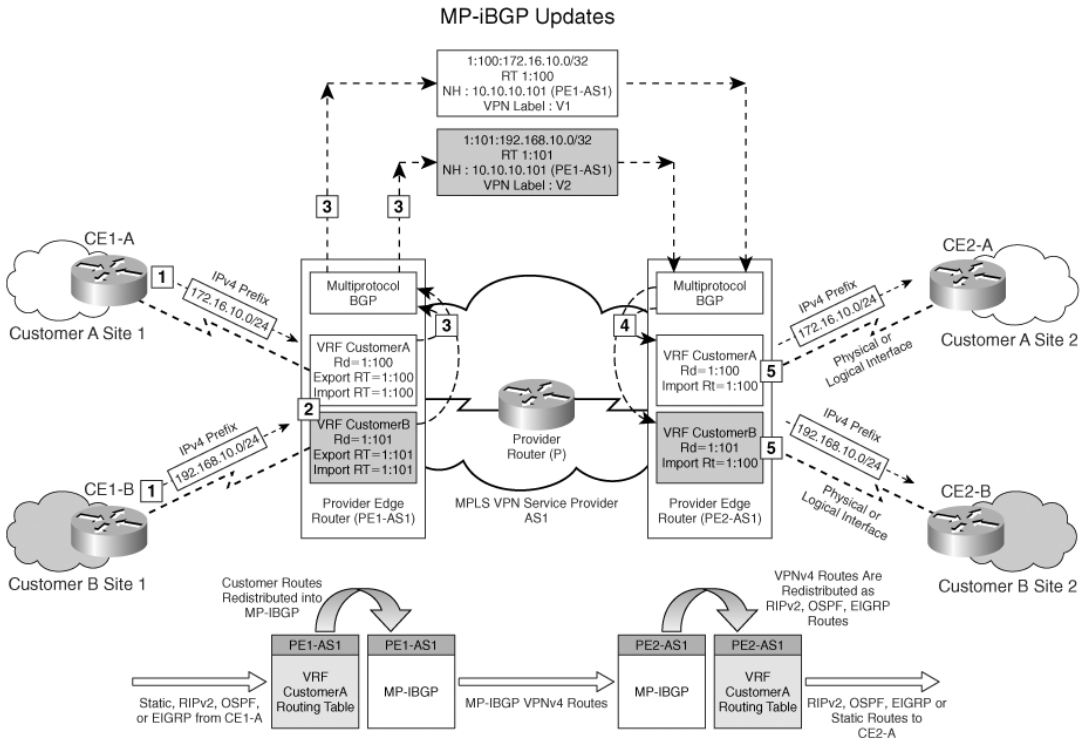
Nếu RD chỉ được sử dụng cho riêng một VPN, việc giao tiếp giữa các site của các VPN khác nhau trở nên khó giải quyết. Một site của công ty A không có khả năng trao đổi kết nối với một site của Công ty B bởi vì RD không nối với nhau (không khớp nhau). Khái niệm nhiều site của Công ty A có khả năng kết nối trao đổi với nhiều Site của Công ty B được gọi là extranet VPN. Và việc kết nối trao đổi giữa các site trong cùng Công ty A được gọi là Intranet VPN. Việc giao tiếp giữa các site được điều khiển bởi một chức năng khác của MPLS VPN gọi là RT – route target. RT là một thuộc tính mở rộng của BGP, nó chỉ ra những tuyến nào nên được nhập từ MP-BGP trong VRF. RT được thực thi bởi các thuộc tính mở rộng BGP sử dụng 16 bit cao của

BGP ecxtended community (64 bit) mã hóa với một giá trị tương ứng với thành viên VPN của site cụ thể. Khi một tuyến VPN học từ một CE chèn vào VPNv4 BGP, một danh sách các thuộc tính community mở rộng cho VPN router target được kết hợp với nó.

- Export RT dùng để xác định thành viên VPN và được kết lớp với mỗi VRF. Export RT được nối thêm vào địa chỉ khách hàng khi chuyển thành địa chỉ VPNv4 bởi PE và quảng bá trong các cập nhật MP-BGP. Export RT có nghĩa là tuyến vpnv4 xuất nhận một thuộc tính mở rộng – đó chính là RT – được cấu hình dưới *ip vrf* trên PE, khi tuyến được phân phối lại từ bảng định tuyến VRF trong MP-BGP.
- Import RT kết hợp với mỗi VRF và xác định các tuyến VPNv4 được thêm vào VRF cho khách hàng cụ thể. Định dạng của RT giống như giá trị RD. Import RT có nhĩa là tuyến vpnv4 nhân được từ MP-BGP được kiểm tra lại khớp thuộc tính mở rộng – đó là RT – với một cái khác trong việc cấu hình. Nếu kết quả là khớp, tiền tố này được đặt vào bảng định tuyến VRF như một tuyến IPv4. Nếu kết quả không khớp, tiền tố này sẽ bị đẩy ra.

Sự tương tác của RT và giá trị RD trong MPLS VPN domain khi cập nhật được chuyển thành cập nhật MP-BGP như hình sau.

Câu lệnh để cấu hình RT trong VRF là **route-target{import | export | both}** *route-target-ext-community*. Từ khóa *both* được dùng để chỉ cả import và export.



Hình 3- 13 Ví dụ về RT

Khi thực thi các cấu trúc mạng VPN phức tạp (như: extranet VPN, Internet access VPNs, network management VPN,…) sử dụng công nghệ MPLS VPN thì RT giữ vai trò nòng cốt. Một địa chỉ mạng có thể được kết hợp với một hoặc nhiều export RT khi quảng bá qua mạng MPLS VPN. Như vậy, RT có thể kết hợp với nhiều site thành viên của nhiều VPN.

Các tiến trình xảy ra trong suốt quá trình quảng bá tuyến ở hình trên như sau: Mạng 172.16.10.0/24 được nhận từ CE1-A, tham gia vào VRF CustomerA trên PE1- AS1. PE1 kết hợp một giá trị RD 1:100 và một giá trị export RT 1:100 khi cấu hình cho VRF trên router PE1-AS1. Các tuyến học từ CE1-A được phân phối vào tiến trình MP-BGP trên PE1-AS1 với prefix 172.16.10.0/24 và thêm vào đầu giá trị RD 1:100 và nối thêm export RT 1:100 để gửi đi địa chỉ VPNv4 khi tham gia cập nhật MP- iBGP giữa các PE. Nhãn VPN (3 byte) được gán cho mỗi địa chỉ học từ các tiến trình của CE kết nối trong một VRF từ tiến trình MP-BGP của PE. MP-BGP chạy trong

miền MPLS của nhà cung cấp dịch vụ nên mang theo địa chỉ VPNv4 (Ipv4 + RD) và BGP RT.

Lưu ý: RT là cấu hình bắt buộc trong một MPLS VPN cho mọi VRF trên một router, giá trị RT có thể được dùng để thực thi trên cấu trúc mạng VPN phức tạp, trong đó một site có thể tham gia vào nhiều VPN. Giá trị RT còn có thể dùng để chọn tuyến nhập vào VRF khi các tuyến VPNv4 được học trong các cập nhật MP-iBGP. Nhãn VPN chỉ được hiểu bởi egress PE (mặt phẳng dữ liệu) kết nối trực tiếp với CE quảng bá mạng đó. Các trạm kế (next hop) phải được học từ IGP khi thực thi MPLS VPN chứ không phải quảng cáo từ tiến trình BGP. Trong hình trên nhãn VPN được mô tả bằng trường V1 và V2. Cập nhật MP-BGP được nhận bởi PE2 và tuyến được lưu trữ trong bảng VRF tương ứng cho Customer A dựa trên nhãn VPN. Các tuyến MP-BGP nhận được được phân phối vào các tiến trình định tuyến VRF PE-CE, và tuyến được quảng bá tới CE2-A. Các thuộc tính commynity BGP mở rộng khác như SoO (site of origin) có thể dùng chủ yếu trong quảng bá cập nhật MP-iBGP. Thuộc tính SoO được dùng để xác định site cụ thể từ tuyến học được của PE và ứng dụng trong việc chống vòng lặp tuyến (routing loop) vì nó xác định được nguồn của site nên có thể ngăn việc quảng cáo lại mạng cho site đã gửi quảng cáo đó. SoO xác định duy nhất một site từ một tuyến mà PE học được. SoO cho phép lọc lưu lượng dựa trên site mà lưu lượng đó xuất phát. Khả năng lọc của SoO giúp quản trị lưu lượng MPLS VPN và chống vòng lặp tuyến xảy ra trong cấu trúc mạng hỗn hợp và phức tạp, các site khách hàng trong đó có thể xử lý các kết nối qua MPLS VPN backbone như các kết nối cửa sau (backdoor link) giữa các site.

Khi thực thi một MPLS VPN, mọi VPN site thuộc vào một khách hàng có thể liên lạc với mọi site trong cùng miền của khách hàng đó được gọi là VPN đơn giản hay intranet VPN. RT có thể được sử dụng để thực hiện cấu trúc

VPN phức tạp, các site của một khách hàng có thể truy cập đến site của các khách hàng khác. Dạng thực thi này được gọi là extranet VPN. Các biến thể của extranet VPN như network management VPN, central services VPN và Internet access VPN có thể được triển khai.

Address family là một khái niệm quan trọng trong hoạt động của MP-BGP cho phép chuyển vận các tuyến VPNv4 với các thuộc tính community mở rộng. Theo RFC 2283 "Multiprotocol Extensions for BGP-4", BGPv4 chỉ có khả năng mang thông tin định tuyến thuộc vào IPv4. BGP-4 có thể mang thông tin của nhiều giao thức lớp mạng. BGP-4 hỗ trợ định tuyến cho nhiều giao thức lớp mạng, BGP-4 phải đăng ký (account) một giao thức lớp mạng cụ thể liên quan đế một trạm kế (next hop) như NLRI (network layer reachability information). Hai thuộc tính mới được thêm vào của BGP là MP_REACH_NLRI (Multiprotocol Reachable NLRI) và MP_UNREACH_NLRI (Multiprotocol Unreachable NLRI). MP_REACH_NLRI mang một tập các đích đến được (reachable destination) với thông tin trạm kế được dùng để chuyển tiếp cho các đích đến này. MP_UNEACH_NLRI mang một tập các đích không đến được. Cả hai thuộc tính này là optional và nontransitive. Vì thế, một BGP speaker không hỗ trợ tính năng đa giao thức này sẽ bỏ qua thông tin được mang trong các thuộc tính này và sẽ không chuyển nó đến các BGP speaker khác.

Một address family là một giao thức lớp mạng được định nghĩa. Một định danh họ địa chỉ (AFI – address family identifier) mang một định danh của giao thức lớp mạng kết hợp với địa chỉ mạng trong thuộc tính đa giao thức của BGP. AFI cho các giao thức lớp mạng được xác định trong RFC 1700, 'Assigned Numbers'.

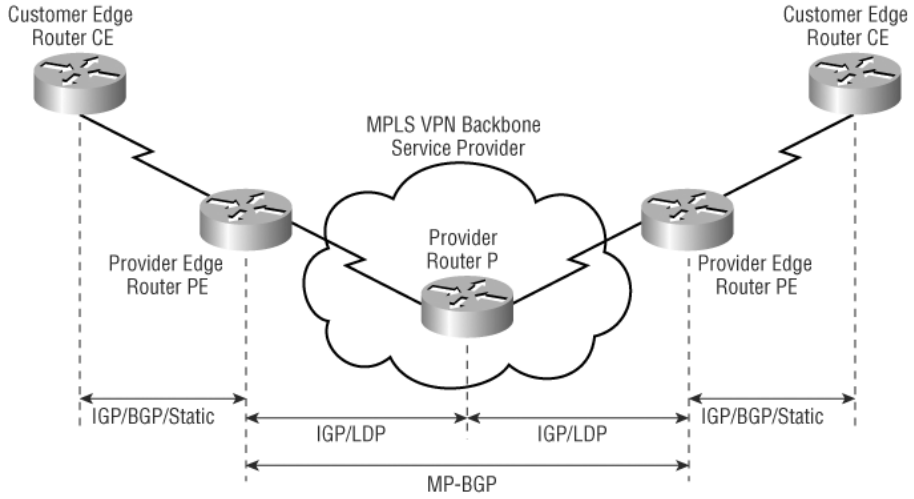
PE thực chất là một LER biên (Edge LSR) và thực hiện tất cả chức năng của một Edge LSR. PE yêu cầu LDP cho việc gán và phân phối nhãn cũng

như chuyển tiếp các gói được gắn nhãn. Cộng thêm các chức năng của một Edge LSR, PE thực thi một giao thức định tuyến (hay định tuyến tĩnh) với các EC trong một bảng định tuyến ảo (virtual routing table) và yêu cầu MP-BGP quảng bá các mạng học được từ CE như các VPNv4 trong MP-iBGP đến các PE khác bằng nhãn VPN.

Router P cần chạy một IGP (OSPF hoặc ISIS) khi MPLS cho phép chuyển tiếp các gói được gán nhãn (mặt phẳng dữ liệu – data plane) giữa các PE. IGP quảng bá các NLRI đến các P và PE để thực thi một MP—iBGP session giữa các PE (mặt phẳng điều khiển – control plane). LDP chạy trên các router P để gán và phân phối nhãn.

3.2.4 Hoạt động của mặt phẳng điều khiển MPLS VPN

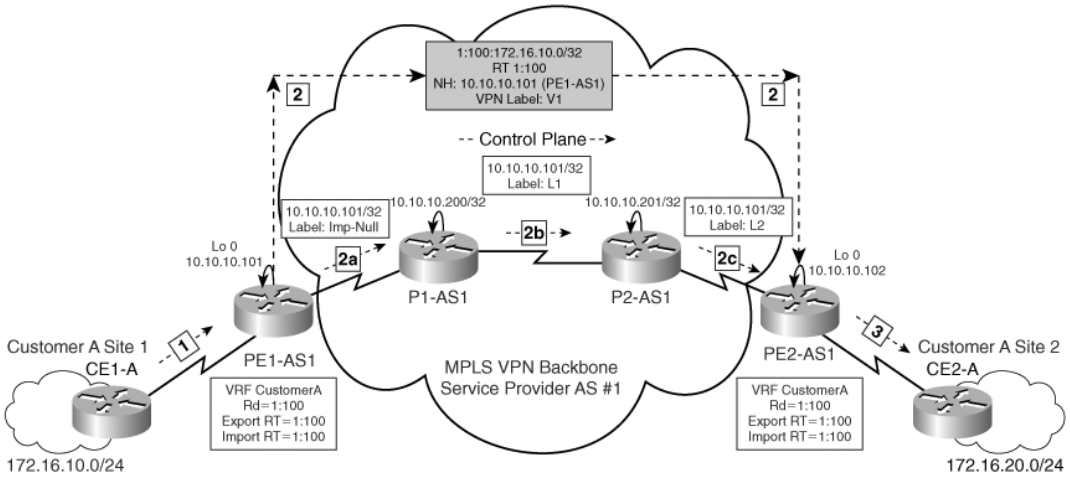
Mặt phẳng điều khiển trong MPLS VPN chứa mọi thông tin định tuyến lớp 3 và các tiến trình trao đổi thông tin của các IP prefix được gán và phân phối nhãn bằng LDP. Mặt phẳng dữ liệu thực hiện chức năng chuyển tiếp các gói IP được gán nhãn đến trạm kế để về đích. Hình sau cho thấy sự tương tác của các giao thức trong mặt phẳng điều khiển của MPLS VPN.



Hình 3- 14 Sự tương tác giữa các giao thức trong mặt phẳng điều khiển

Các router CE được kết nối với các PE, và một IGP, BGP, hay tuyến tĩnh (static route) được yêu cầu trên các CE cùng với các PE để thu thập và quảng cáo thông tin NLRI. Trong MPLS VPN backbone gồm các router P và PE, một IGP kết hợp với LDP được sử dụng giữa các PE và P. LDP dùng để phân phối nhãn trong một MPLS domain. IGP dùng để trao đổi thông tin NLRI, ánh xạ (map) các NLRI này vào MP- BGP. MP-BGP được duy trì giữa các PE trong một miền MPLS VPN và trao đổi cập nhật MP-BGP.

Các gói từ CE đến PE luôn được quảng bá như các gói Ipv4. Hoạt động của mặt phẳng điều khiển MPLS VPN như hình sau:



Hình 3- 15 Hoạt động của mặt phẳng điều khiển MPLS VPN

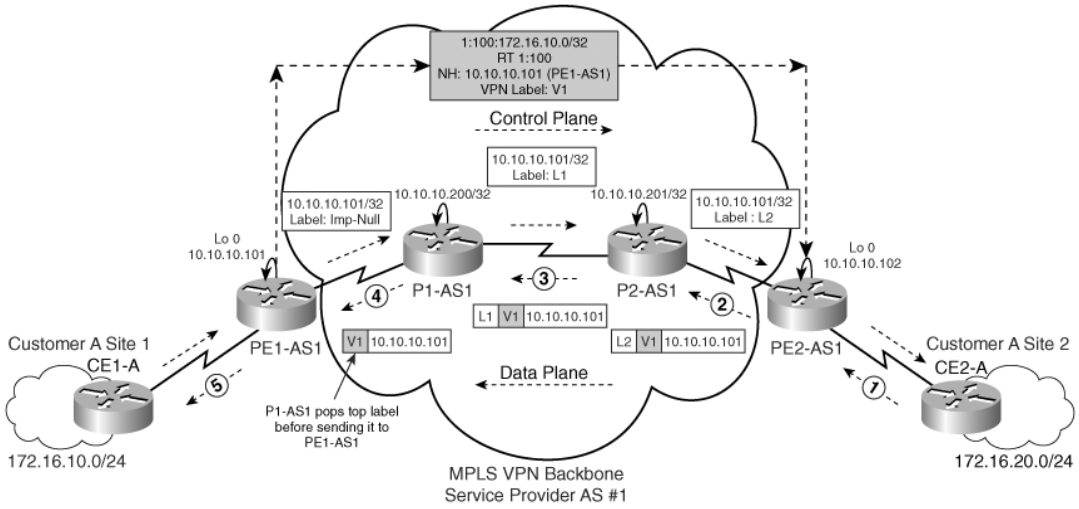
Sau đây là các bước hoạt động của mặt phẳng điều khiển MPLS VPN (minh họa bằng hình trên): Cập nhật Ipv4 cho mạng 172.16.10.0 được nhận bởi egress PE (mặt phẳng dữ liệu). PE1-AS1 nhận và vận chuyển tuyến Ipv4, 172.16.10.0/24, đến một tuyến VPNv4 gắn với RD 1:100, SoO, va RT 1:100 dựa trên cấu hình VRF trên PE1-AS1. Nó định vị một nhãn VPNv4 V1 tới cập nhật 172.16.10.0/24 và viết lại thuộc tính trạm kế cho dja chỉ 10.10.10.101 của loopback0 trên PE1-AS1. Sự quảng bá nhãn cho 10.10.10.101/32 tù PE1-AS1 tới PE2-AS2 nhanh chóng được thay thế ngay khi mạng MPLS VPN của nhà cung cấp được thiết lập và thực hiện quảng bá VPNv4 trong mạng. Các

bước sau thực hiện tiến trình quảng bá nhãn cho 10.10.10.101/32:

- Router PE2-AS1 yêu cầu một nhãn cho 10.10.10.101/32 sử dụng LDP ánh xạ nhãn yêu cầu từ láng giềng xuôi dòng (downstream neighbor) của nó, P1- AS1. PE1-AS1 xác định một nhãn implicit-null cho 10.10.10.101/32, chỉnh sửa mức trong LFIB liên quan đến 10.10.10.101/32, và gửi đến P1-AS1 bằng LDP reply.
- P1-AS1 sử dụng nhãn implicit-null nhận được từ PE1-AS1 làm giá trị nhãn xuất (outbound label) của nó, xác định một nhãn (L1) cho 10.10.10.101/32, và sửa mức trong LFIB cho 10.10.10.101/32. Sau đó P1-AS1 gửi giá trị nhãn này đến P2-AS1 bằng LDP reply.
- P2-AS1 dùng nhãn L1 làm giá trị nhãn xuất, xác định nhãn L2 cho 10.10.10.101/32, và sửa mức trong LFIB cho 10.10.10.101/32. Sau đó P2-AS1 gửi giá trị nhãn này đến PE2-AS1 bằng LDP reply. PE1-AS1 có cấu hình VRF để nhân các tuyến với RT 1:100 nên chuyển cập nhật VPNv4 thanh Ipv4 và chèn tuyến trong VRF cho Customer A. Sau đó nó quảng bá tuyến này tới CE2-A.

3.2.5 Hoạt động của mặt phẳng dữ liệu MPLS VPN

Việc chuyển tiếp trong mạng MPLS VPN đòi hỏi phải dùng chồng nhãn (label stack). Nhãn trên (top lable) được gán và hoán đổi (swap) để chuyển tiếp gói dữ liệu đi trong lõi MPLS. Nhãn thứ hai (nhãn VPN) được kết hợp với VRF ở router PE để chuyển tiếp gói đến các CE. Hình sau mô tả các bước trong chuyển tiếp dữ liệu khách hàng của mặt phẳng dữ liệu từ một site khách hàng CE2-A tới CE1-A trong hạ tầng mạng của SP.



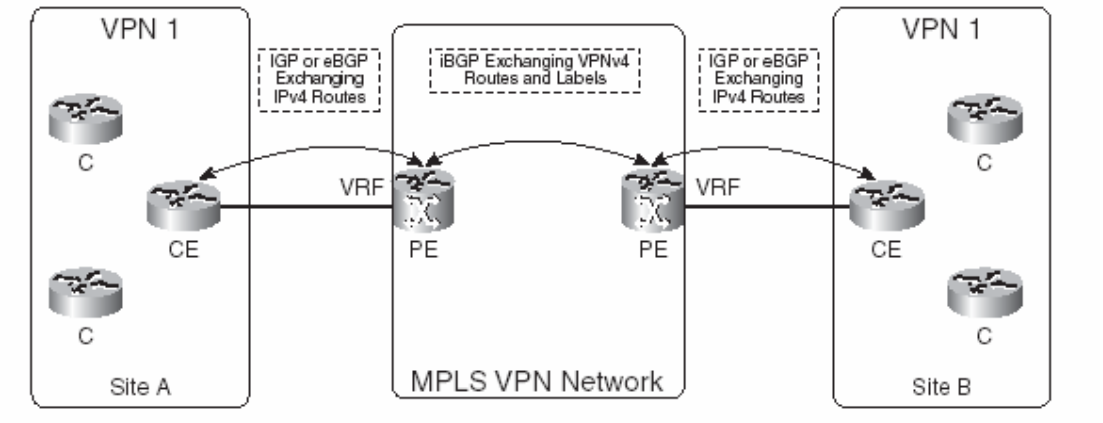
Hình 3- 16 Các bước chuyển tiếp trong mặt phẳng dữ liệu

Khi dữ liệu được chuyển tiếp tới một mạng cụ thể dọc theo mạng VPN qua lõi MPLS, chỉ có nhãn trên (top lable) trong chồng nhãn bị hoán đổi (swap) khi gói đi qua backbone. Nhãn VPN vẫn giữ nguyên và được bóc ra khi đến router PE ngõ ra (egress)/xuôi dòng(downstream). Mạng gắn với một giao tiếp ngõ ra thuộc vào một VRF cụ thể trên router phụ thuộc vào giá trị của nhãn VPN.

Sau đây là những bước trong việc chuyển tiếp của mặt phẳng dữ liệu minh họa cho hình trên: CE2-A tạo ra một gói dữ liệu với địa chỉ nguồn 172.16.20.1 và đích là 172.16.10.1. PE2-AS1 nhận gói dữ liệu, thêm vào nhãn VPN V1 và nhãn LDP L2 rồi chuyển tiếp gói đến P2-AS1. P2-AS1 nhận gói dữ liệu và chuyển đổi (swap) nhãn LDP L2 thành L1. P1-AS1 nhận gói dữ liệu và bóc (pop) nhãn trên (top label) ra vì nó nhận một ánh xạ nhãn implicit-null cho 10.10.10.101/32 từ PE1-AS1. Kết quả, gói được gán nhãn (nhãn VPN la V1) được chuyển tiếp đến PE1-AS1. PE1-AS1 bóc nhãn VPN V1 ra và chuyển tiếp gói dữ liệu dến CE1-A nơi có địa chỉ mạng 172.16.10.0 được định vị.

3.2.6 Định tuyến VPNv4 trong mạng MPLS VPN

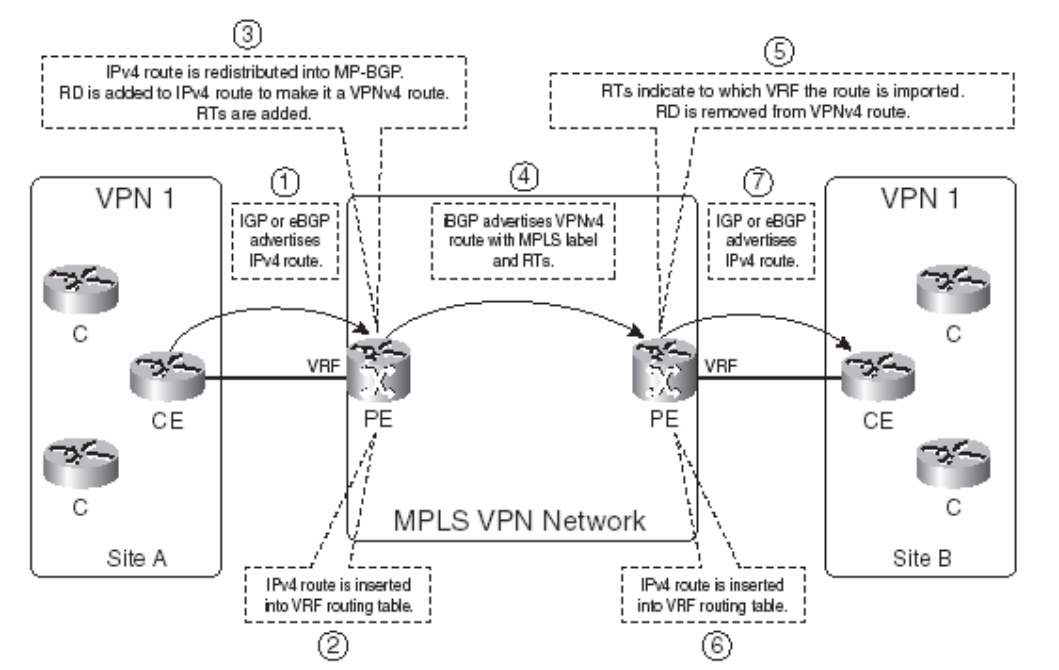
VRF tách riêng khách hàng trên bộ định tuyến PE, nhưng làm thế nào để tiền tố được vận chuyển qua mạng của nhà cung cấp dịch vụ? bởi vì, nhiều khả năng, số lượng lớn các tuyến – có thể là một trăm nghìn – được vận chuyển qua. BGP là một ứng cử viên bởi vì nó là giao thức định tuyến tĩnh và proven có thể mang rất nhiều tuyến. Chỉ thấy rằng BGP là giao thức định tuyến cơ bản để mang bảng định tuyến Internet hoàn chỉnh. Bởi vì tuyến VPN của khách hàng được thực hiện duy nhất bằng cách thêm RD vào mỗi tuyến IPv4 – chuyển nó thành tuyến VPNv4 – tất cả các tuyến khách hàng có thể được vận chuyển an toàn qua mạng MPLS VPN.



Hình 3- 17 Sự truyền tuyến trong mạng MPLS VPN

Bộ định tuyến PE nhận tuyến IPv4 từ bộ định tuyến CE qua giao thức cổng trong (IGP – Interior Gateway Protocol) hoặc BGP ngoài (external BGP – eBGP). Những tuyến IPv4 từ site VPN được đặt vào trong bảng định tuyến VRF. VRF được sử dụng phụ thuộc vào VRF mà được cấu hình trên giao diện trên bộ định tuyến PE tới bộ định tuyến CE. Những tuyến này được nối với RD mà được chỉ định tới VRF. Do đó, chúng trở thành tuyến VNPv4, tuyến này sau đó được đưa vào MP – BGP. BGP quan tâm đến sự phân phối những tuyến VPNv4 tới tất cả các bộ định tuyến PE trong mạng MPLS VPN. Trên

bộ định tuyến PE, những tuyến VPNv4 được tách RD và đưa vào bảng định tuyến VRF như tuyến IPv4. Tuyến VNPv4, sau khi được tách bỏ RD, có được đưa vào bảng VRF hay không còn phụ thuộc vào RT có cho phép truy nhập vào VRF hay không. Những tuyến IPv4 sau đó được quảng bá tới các bộ định tuyến CE qua giao thức IGP hoặc eBGP (giao thức chạy giữa bộ định tuyến PE và CE). Hình sau mô tả các bước trong sự truyền tuyến từ CE đến CE trong mạng MPLS VPN.



Hình 3- 18 Sự truyền tuyến trong mạng MPLS VPN step by step

Bởi vì nhà cung cấp dịch vụ mà đang chạy mạng MPLS VPN chạy BGP trong hệ thống tự trị, iBGP đang chạy giữa các bộ định tuyến PE.

Sự truyền từ eBGP – giao thức chạy giữa PE và CE – tới MP –iBGP trong mạng MPLS VPN và ngược lại là tự động và không cần cấu hình thêm. Tuy nhiên việc phân phối lại của MP – iBGP trong IGP mà hiện đang chạy giữa PE và CE là không tự động. Ta phải cấu hình phân phối lại lẫn nhau giữa MP-iBGP và IGP.

3.2.7 Chuyển tiếp gói trong mạng MPLS VPN

Như đã nói trong phần trước, những gói không thể được chuyển tiếp như gói IP đơn thuần giữa các site. Bộ định tuyến P không thể chuyển tiếp chúng bởi vì nó không có thông tin VRF từ mỗi site. MPLS không thể giải quyết vấn đề này bởi dán nhãn vào gói. Bộ định tuyến P sau đó phải có thông tin chuyển tiếp đúng cho nhãn để chuyển tiếp gói. Cách chung nhất là cấu hình giao thức phân phối nhãn (LDP) giữa tất cả các bộ định tuyến P và PE nên tất cả các lưu lượng IP là chuyển mạch nhãn giữa chúng. Ta cũng có thể sử dụng giao thức RSVP mở rộng cho điều khiển lưu lượng (TE) khi thực thi MPLS TE, nhưng LDP là phương thức chung nhất cho MPLS VPN. Gói IP sau đó được chuyển tiếp nhãn với một nhãn từ bộ định tuyến PE vào tới bộ định tuyến PE ra. Bộ định tuyến P không bao giờ phải thực hiện việc tìm kiếm địa chỉ IP đích. Đây là cách để các gói được chuyển mạch giữa các bộ định tuyến PE vào và ra. Những nhãn này được gọi là nhãn IGP, bởi vì nó là nhãn phải có trong tiền tố IPv4 trong bảng định tuyến toàn cục của bộ định tuyến P và PE, và IGP của mạng nhà cung cấp dịch vụ quảng bá nó.

Làm thế nào để bộ định tuyến PE biết được gói nào thuộc VRF nào. Thông tin này không có trong mào đầu IP, và nó không thể được nhận lấy từ nhãn IGP, bởi vì đây chỉ được sử dụng để chuyển tiếp gói qua mạng của nhà cung cấp dịch vụ. Giải pháp ở đây là thêm một nhãn khác trong chồng nhãn MPLS. Nhãn này sẽ chỉ ra gói nào thuộc VRF. Do đó tất cả các gói của khách hàng được chuyển tiếp với 2 nhãn: nhãn IGP như là nhãn trên cùng và nhãn VPN như là nhãn dưới cùng. Nhãn VPN phải được đặt trên bộ định tuyến PE vào để chỉ ra bộ định tuyến PE ra nào mà gói thuộc VRF đó. Làm thế nào để bộ định tuyến PE ra báo hiệu tới bộ định tuyến PE vào mà nhãn được sử dụng cho tiền tố VRF? Bởi MP – BGP thực sự được sử dụng để quảng bá tiền tố

VPNv4, nó cũng báo hiệu nhãn VPN (được biết đến nhãn BGP) mà được kết nối với tiền tố VPNv4.

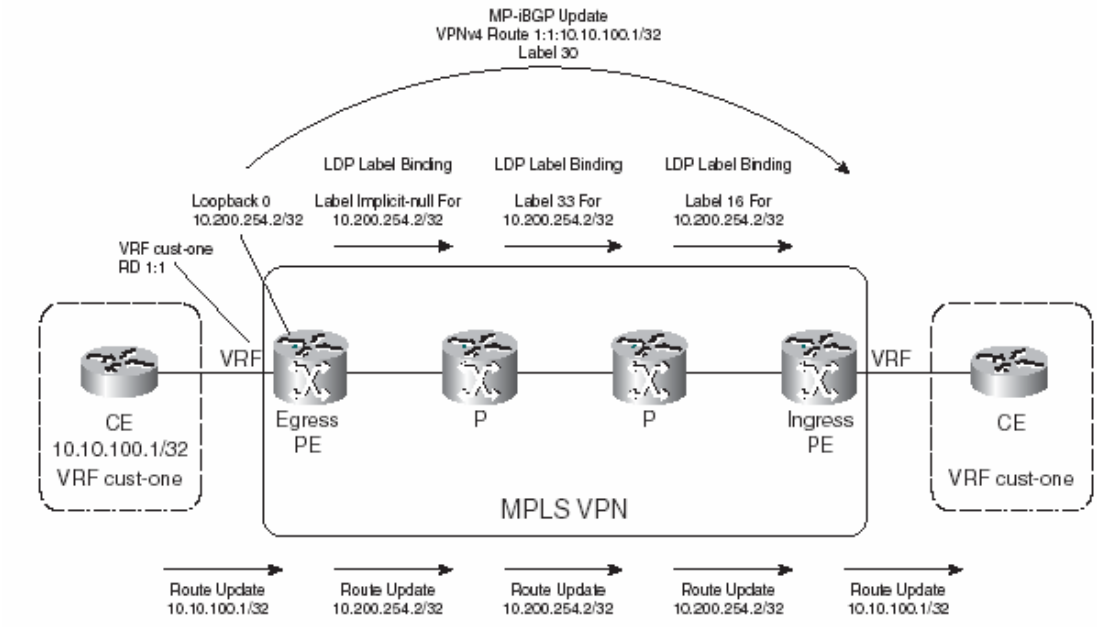
Chú ý: Thực sự thì khái niệm có một nhãn VPN chỉ ra gói nào thuộc VRF cũng không thực sự đúng. Nó có thể đúng trong vài trường hợp, nhưng đa số là không. Nhãn VPN thường chỉ ra nút tiếp theo mà gói được chuyển tiếp tới trên bộ định tuyến PE ra. Do đó, mục đích của nó là để chỉ bộ định tuyến CE đúng như bước tiếp theo của gói.

Nói tóm lại, lưu lượng VRF – to – VRF có 2 nhãn trong mạng MPLS VPN. Nhãn trên cùng là nhãn IGP và được phân phối bởi LDP hoặc RSVP cho TE giữa tất cả các bộ định tuyến P và PE hop by hop. Nhãn dưới cùng là nhãn VPN mà được quảng bá bởi MP – iBGP từ PE đến PE. Những bộ định tuyến P sử dụng nhãn IBG để chuyển tiếp gói tới bộ định tuyến PE ra tương ứng. Bộ định tuyến PE ra sử dụng nhãn VPN để chuyển tiếp gói IP tới bộ định tuyến CE tương ứng.

Hình sau đây mô tả việc chuyển tiếp gói trong mạng MPLS VPN. Gói đi vào bộ định tuyến PE trên giao diện VRF như là gói IPv4. Nó được chuyển tiếp qua mạng MPLS VPN với hai nhãn. Bộ định tuyến P chuyển tiếp nhãn bằng việc tìm kiếm tại nhãn trên cùng. Nhãn trên cùng được trao đổi với nhau tại mỗi bộ định tuyến P. Những nhãn này được tách ra tại bộ định tuyến PE và gói được chuyển tiếp như một gói IPv4 trên giao diện VRF tới bộ định tuyến CE. Bộ định tuyến CE tương ứng được tìm thấy bởi việc tìm kiếm nhãn VPN.

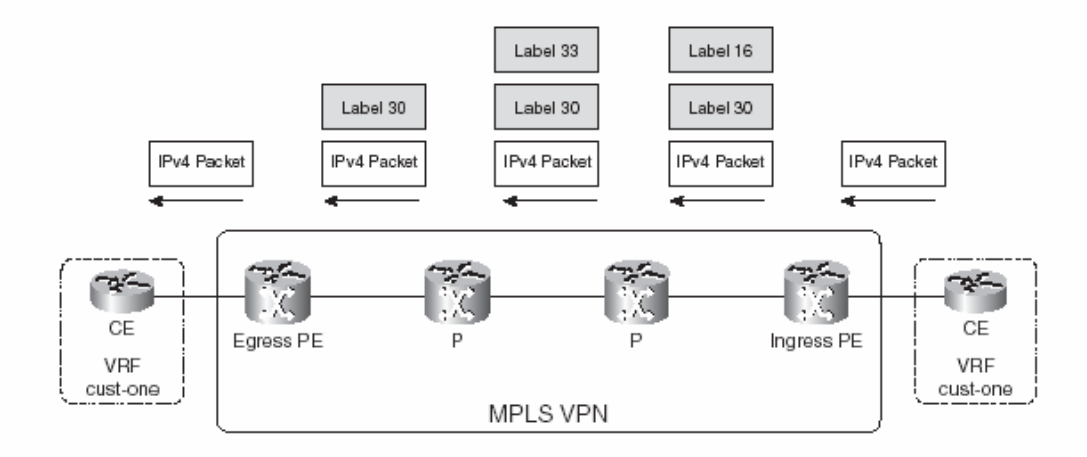
Trong phần này ta sẽ xem xét về sự sống của gói IP vì nó đi ngang qua mạng đường trục MPLS VPN từ một địa điểm của khách hàng tới một địa điểm khác. Đầu tiên phải xét đến những khối xây dựng cơ bản của MPLS VPN. Giữa các PE cần có đa giao thức iBGP, giao thức này sẽ phân phối tuyến vpnv4 và nhãn VPN kết hợp. Giữa các bộ PE và P cần thiết phải có một giao thức phân phối nhãn. Ở đây là giả thiết rằng giao thức phân phối nhãn này là

LDP. Giữa các bộ định tuyến PE và CE cần thiết phải có một giao thức định tuyến để chạy và đặt những tuyến của khách hàng vào trong bảng định tuyến VRF trên PE. Cuối cùng,những bộ định tuyến này cần được phân bố trong MP-iBGP và ngược lại. Hình 3-19 và 3-20 giúp ta hiểu rõ hơn về vấn đề này. Hình 3-26 chỉ tuyến quảng bá của vpnv4 và nhãn từ PE ra tới PE vào và sự quảng bá của tuyến IGP – biểu diễn bước nhảy tiếp theo BGP của PE ra – và nhãn tới PE vào. Địa chỉ bước nhảy tiếp theo BGP trên PE ra là 10.200.254.2/32, mà một IGP quảng bá tới PE vào. Nhãn cho tuyến IGP được quảng bá hop by hop bởi LDP. Tuyến IPv4 của khách hàng 10.10.100.1/32 được quảng bá bởi giao thức định tuyến PE – CE từ CE tới PE ra. PE ra thêm RD 1:1, chuyển nó vào trong tuyến vpnv4 1:1:10.10.100/32, và gửi nó đến PE vào với nhãn 30 qua iBGP đa giao thức.



Hình 3- 19 Sự sống của một gói IPv4 qua mạng đường trục MPLS VPN tuyến và quảng bá nhãn.

Hình 3-20 đưa ra ví dụ về một gói với địa chỉ IP đích 10.10.100.1 đang được chuyển tiếp với 2 nhãn như được quảng bá trong hình 3-26.



Hình 3- 20 Đời sống của gói IPv4 qua mạng đường trục MPLS VPN: chuyển tiếp gói

Khi một gói IP đi vào ingress PE từ CE, PE vào sẽ tìm kiếm địa chỉ IP đích trong bảng CEF, VRF *cust-one*. PE vào tìm VRF đúng bằng việc tìm tại giao diện gói vào bộ định tuyến PE, và với bảng VRF mà giao diện này liên kết tới. Các mục vào (entry) cụ thể trong bảng CEF VRF thường thể hiện rằng có 2 nhãn cần thiết được thêm vào.

Chú ý: Khi PE vào và PE ra được kết nối trực tiếp, các gói sẽ chỉ có một nhãn duy nhất – nhãn VPN. Đầu tiên, PE vào gắn nhãn VPN 30 – như được quảng bá bởi BGP cho tuyến vpnv4. Nó trở thành nhãn cuối. Sau đó, PE vào gắn nhãn IGP như nhãn trên cùng. Nhãn này là nhãn mà liên kết với tuyến IGP /32 cho địa chỉ IP bước nhảy tiếp theo BGP. Đây thường là địa chỉ IP của giao diện loopback trên PE ra. Nhãn này được quảng bá hop by hop giữa các bộ định tuyến P cho tới khi nó tới được PE ra. Mỗi bước nhảy thay đổi giá trị của nhãn. Nhãn IGP mà được gắn bởi PE vào là nhãn 16.

Gói IPv4 đi ra khỏi PE vào với 2 nhãn trên của nó. Nhãn trên cùng – nhãn iGP cho PE ra – được hoán đổi tại mỗi bước nhảy. Nhãn này đặt gói IPv4

VPN tới đúng PE ra. Thông thường, bởi vì đây là hoạt động mặc định trong Cisco IOS – hoạt động PHP được đặt giữa bộ định tuyến P cuối cùng và PE ra. Do đó, nhãn IBP được gỡ ra trên bộ định tuyến P cuối cùng và gói đi vào trong bộ PE ra chỉ với một nhãn VPN trong ngăn xếp nhãn. Bộ PE ra tìm kiếm nhãn VPN trong LFIB và đưa ra quyết định chuyển tiếp. Bởi vì nhãn đi ra (outgoing label) là nhãn số (*No label*), ngăn xếp nhãn còn lại bị gỡ bỏ và gói được chuyển tiếp như gói IP tới bộ định tuyến CE. Bộ PE ra không phải thực hiện việc tra cứu địa chỉ IP đích trong mào đầu IP nếu nhãn ra (outgoing label) là nhãn số (*No label*). Thông tin bước nhảy đúng tiếp theo được tìm thấy bởi sự tìm kiếm nhãn VPN trong LFIB. Chỉ khi nhãn ra là *Aggreate*, bộ PE ra phải thực hiện việc tra cứu IP trong bảng CEF VRF sau khi tra cứu nhãn trong LFIB.

Các ví dụ sau đây cho thấy nhãn được quảng bá bởi LDP và MP-iBGP và việc sử dụng của chúng trong bảng CEF VRF và LFIB. Những nhãn này tương ứng với những nhãn trong hình 3-19 và 3-20.

Ví dụ: Bảng VRF CEF Cust-one trên PE vào

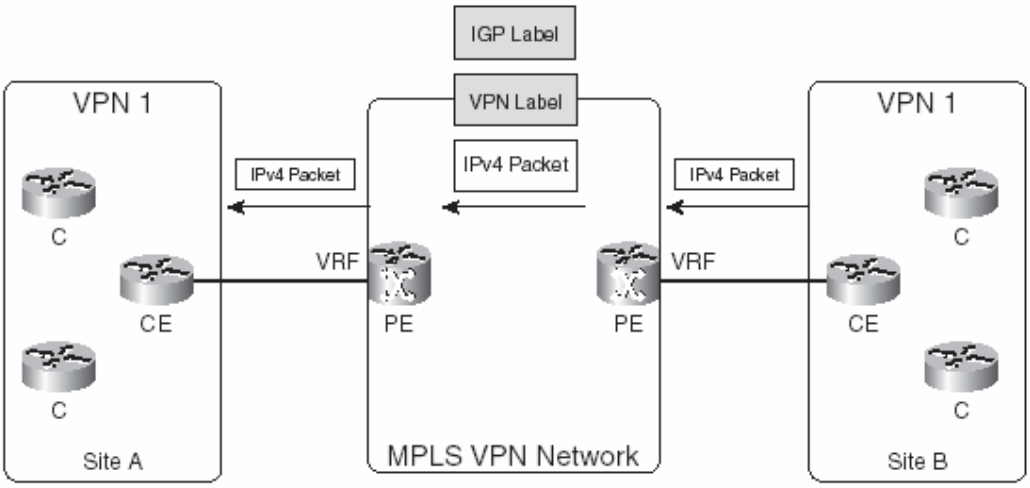
```
Ingress-PE#show ip cef vrf cust-one 10.10.100.1 255.255.255.255 detail
10.10.100.1/32, epoch 0
recursive via 10.200.254.2 label 30
nexthop 10.200.214.1 POS0/1/0 label 16
```

Ví du: tuyến Vpnv4 trên PE vào

```
Ingress-PE#show ip bgp vpnv4 rd 1:1 10.10.100.1
BGP routing table entry for 1:1:10.10.100.1/32, version 81
Paths: (1 available, best #1, table cust-one)
Not advertised to any peer
Local
10.200.254.2 (metric 3) from 10.200.254.2 (10.200.254.2)
Origin incomplete, metric 1, localpref 100, valid, internal, best
Extended Community: RT:1:1,
mpls labels in/out nolabel/30
```

Ví dụ: LFIB Entry trên PE ra

Egress-PE#**show mpls forwarding-table labels 30**					
Local Label	Outgoing Label or VC	Prefix or Tunnel Id	Bytes Label Switched	Outgoing interface	Next Hop
30	No Label	10.10.100.1/32[V]	0	Et0/1/2	10.10.2.1



Hình 3- 21 Chuyển tiếp gói trong mạng MPLS VPN

CHƯƠNG 4

ỨNG DỤNG CỦA MPLS TRONG VIỆC CUNG CẤP DỊCH VỤ IPVPN CỦA EVNTELECOM

Nắm bắt xu thế phát triển của công nghệ thông tin và viễn thông, lưu lượng mạng công cộng chạy trên mạng sẽ dần chuyển sang các ứng dụng của giao thức IP và có xu hướng chuyển về mô hình IP VPN. Từ năm 2004, EVNTelecom đã đưa mạng NGN đầy đủ vào sử dụng với hai tổng đài điện thoại tại Hà Nội và Hồ Chí Minh. Mạng NGN này dựa trên hạ tầng truyền dẫn IP, được xây dựng bởi các bộ định tuyến Juniper.

EVNTelecom hiện đang triển khai các hệ thống cung cấp dịch vụ viễn thông công cộng như: dịch vụ VoIP – 179, dịch vụ Internet, dịch vụ cho thuê cổng quốc tế qua trạm vệ tinh, dịch vụ kênh thuê riêng quốc tế và trong nước và đặc biệt là dịch vụ điện thoại cố định không dây dựa trên công nghệ CDMA 2000 1x-450Mhz. Với hệ thống mạng đường trục đã sẵn sàng cho kết nối EVNTelecom đang dần chiếm thị phần trong lĩnh vực cung cấp dịch vụ VoIP – 179 và dịch vụ thuê kênh riêng. EVNTelecom đã có 2 mạng đường trục Bắc – Nam tốc độ cao. Đây là những đường trục quan trong, để kết nối 3 khu vực Bắc – Trung – Nam, sử dụng công nghệ SDH với băng thông lên tới 10Gbps (sẵn sàng nâng cấp lên công nghệ DWDM).

Trong thời gian tới, EVNTelecom sẽ giới thiệu hệ thống đường trục thứ 3 đưa vào vận hành với dung lượng lên tới 40Gbps sử dụng công nghệ DWDM. Ngoài ra, EVNTelecom đã thiết lập PoP tại hầu hết các tỉnh của Việt Nam. Sau đó EVNTelecom sẽ tiếp tục xây dựng những PoP mới nhằm cải thiện chất lượng của dịch vụ.

Hiện nay, EVNTelecom có một trung tâm vận hành mạng để điều khiển mạng truyền dẫn và mạng IP với chức năng hỗ trợ và xử lý sự cố 24/24. Bên

cạnh đó, EVNTelecom cũng có những trung tâm vận hành tại Bắc, Trung và Nam để điều hành mạng nội hạt. Công nghệ MPLS/VPN là một sự thay đổi của công nghệ IPoA truyền thống (IP over ATM). Do đó, mạng IP của EVNTelecom có cả những ưu điểm của kỹ thuật ATM (như tốc độ cao, mềm dẻo linh hoạt, controllable current...) và những tính năng mới của công nghệ IP trong những năm qua. Mạng IP của EVNTelecom có thể cung cấp tất cả các dịch vụ: Internet (ISP,IXP), Internet CDMA, Intertnet qua CATV, mạng NGN, UIN (unified Intelligent Network)....

EVNTelecom đã đưa ra mô hình cung cấp dịch vụ MPLS/VPN cho khách hàng với những ưu điểm của MPLS:

- Riêng biệt và bảo mật
- Độc lập với mạng khách hàng
- Linh hoạt và ổn định
- Khả năng quản lý hiệu quả, đơn giản.
- Mạng khách hàng có thể sử dụng địa chỉ IP private.
- Chi phí thuê kênh rẻ, nhất là trong việc kết nối điểm – đa điểm, hoặc đa điểm – đa điểm.

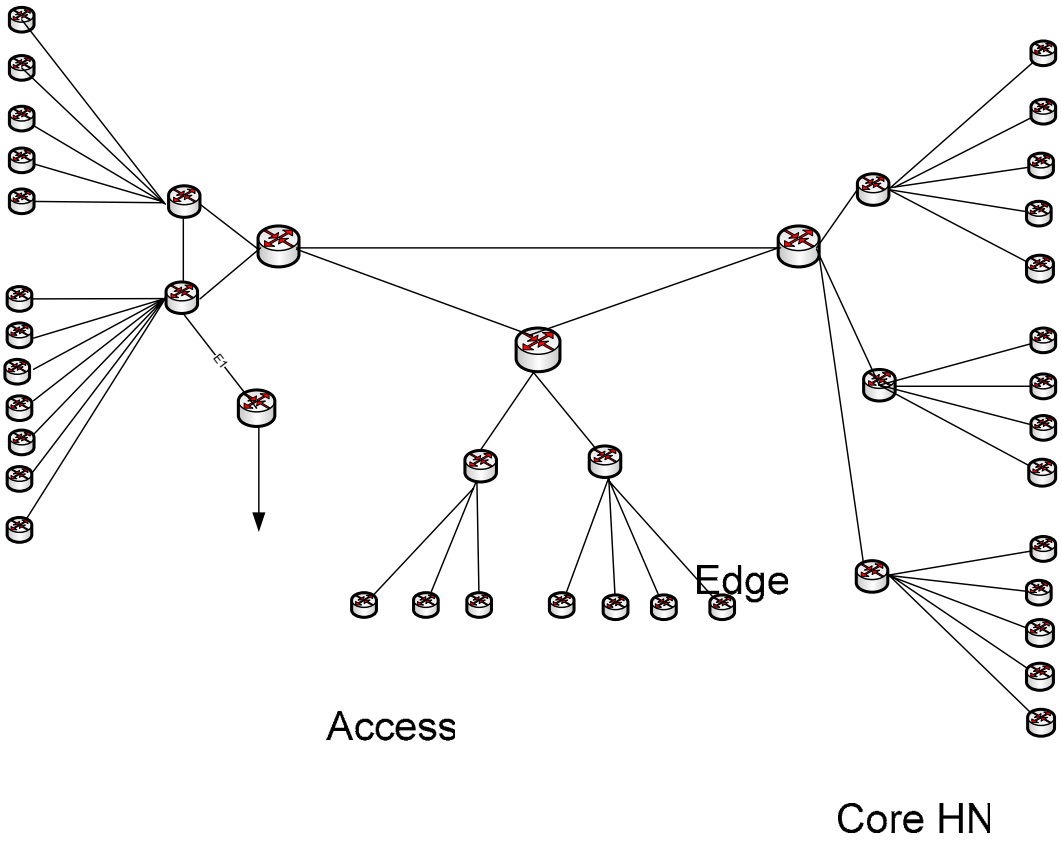
4.1 Ứng dụng MPLS trong mạng IP core của EVNTelecom

- Các thiết bị BRAS, Edge, Core Router đều hỗ trợ MPLS
- Tất cả các thiết bị BRAS, Edge, Core Router đều thuộc một hãng.
- Hiện phần hạ tầng mạng IP core đã sử dụng MPLS
- Có hệ thống quản lý VPN center
- Không cần đầu tư thêm cho hệ thống core.

Hiện tại các thiết bị BRAS, Edge, Core Router đều là của hãng Juniper và tất cả đều hỗ trợ MPLS nên chúng đều có khả năng đáp ứng được dịch vụ MPLS VPN. Mặt khác toàn bộ các thiết bị này đều thuộc một hãng nne chúng được quản lý và hưởng một giải pháp chung để cung cấp dịch vụ VPN. Phần mềm có khả năng đáp ứng tính năng VPN center giúp việc khai báo và quản lý các site của khách hàng một cách dễ dàng hơn.
Do các thiết bị từ BRAS đến core đều hỗ trợ MPLS nên đối với mạng core không cần phải đầu tư thêm thiết bị đã hoàn toàn có thể đáp ứng được việc cung cấp dịch vụ MPLS VPN.

Cấu trúc mạng của EVNTelecom là cấu trúc Client – Server (chủ - tớ). Hiện nay EVNTelecom đang sử dụng nền tảng quản lý mạng: hệ thống TNMS của Siemens, hệ thống ONMS của Lucent, ZONME 300, hệ thống T2000 của Huawei.

Cấu trúc IP của EVNTelecom bao gồm 3 lớp: Core, Egde và Access. Những bộ định tuyến Core được thiết lập tại Hà Nội, Đà Nẵng và Tp Hồ Chí Minh. Bộ định tuyến Edge được thiết lập tại Hà Nội, Đà Nẵng, Cần Thơ và Tp Hồ Chí Minh. Còn bộ định tuyến Access được thiết lập tại các văn phòng thông tin của EVNTelecom (EVNTelecom’s Information Departments) tại tất cả các tỉnh. Như hình 4.1sau đây:



Hình 4- 1 Mô hình mạng IP của EVNTelecom

Trong đó chức năng chính của các thành phần như sau:

- CORE có nhiệm vụ kết nối và Forward data trên mạng lõi.
- Edge là bộ đệm giữa access và core, gom tất cả các lưu lượng từ các access về rồi chuyển mạch lên core theo đúng tuyến VPN.
- Access thì kết nối trực tiếp xuống khách hàng thông qua các phương thức của nhà cung cấp như ADSL, cable, FTTH hoặc leasedline. Access bao gồm BRAS, DSLAM, CMTS. Router POP là access

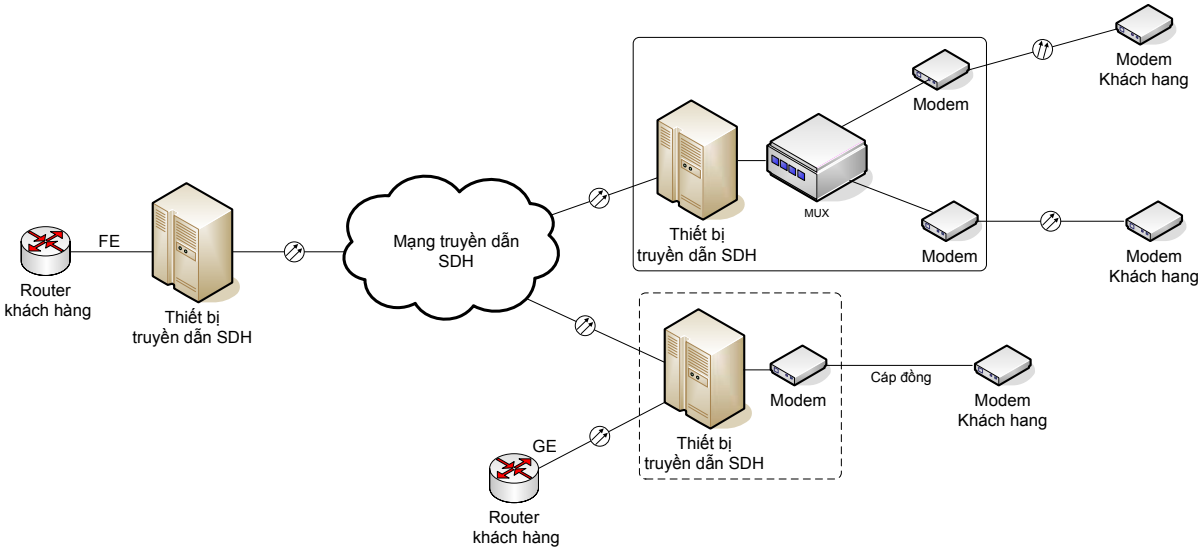
BRAS (Broadband Remote Access Server) là một phần tử mạng có chức năng tập hợp và điều khiển các phiên truy nhập của thuê bao. BRAS còn có chức năng quản lý và tính cước các thuê bao truy nhập internet.

4.1.1 Dịch vụ kênh thuê riêng leased line

Dịch vụ thuê kênh riêng Lease Line của EVNTelecom hay còn gọi là E-Line cung cấp cho khách hàng tại Hà Nội dựa trên mạng truyền dẫn SDH nội hạt.

Dung lượng của mỗi kênh E-Line thường không lớn hơn 2Mb/s. Do đó giải pháp được lựa chọn là khách hàng kết nối bằng các modem cáp quang hoặc cáp đồng vào mạng SDH của EVNTelecom. Mỗi khách hàng sẽ được cung cấp một kênh E1 trên mạng SDH. Đối với những khách hàng thuê một chùm kênh thì sẽ được bổ sung thêm thiết bị ghép kênh DACS.

Đối với những khách hàng thuê kênh riêng tốc độ cao như STM1, STM4, GE… thì giải pháp được đưa ra là lắp đặt thiết bị truyền dẫn SDH tại khách hàng để kết nối vào mạng truyền dẫn.



Hình 4- 2 Sơ đồ kết nối dịch vụ leased line

4.1.2 Dịch vụ IP VPN

Để đáp ứng nhu cầu của các doanh nghiệp trong việc xây dựng hệ thống mạng riêng có quy mô lớn tại Việt Nam cũng như đi quốc tế, EVNTelecom đã cung cấp dịch vụ mạng IP VPN. Đây là một dịch vụ mạng có thể dùng cho

các ứng dụng khác nhau, cho phép việc trao đổi thông tin một cách an toàn bằng nhiều lựa chọn kết nối với nhiều tính năng nổi trội như: Kết nối trực tiếp giữa các điểm bất kỳ (Any – to – Any Connectivity); nhiều lựa chọn công nghệ kết nối (Choice of Access Technology; tích hợp dữ liệu, thoại và video (Data, Voice and Video Conver-gence); độ bảo mật cao (High Network Privacy); dễ sử dụng (Easy of Operation).

Dịch vụ IP VPN của EVNTelecom cung cấp cho khách hàng dựa trên nền hạ tầng mạng IP chia sẻ nhưng vẫn đảm bảo được tính riêng tư của dữ liệu. EVNTelecom đã triển khai mạng NNI với đối tác nước ngoài nhằm mục đích mở rộng dịch vụ IP VPN đi quốc tế.

Dung lượng của mỗi kênh IP VPN thường không lớn hơn 2Mbps. Do đó giải pháp được lựa chọn là khách hàng kết nối bằng các modem cáp quang vào điểm kết nối (Access) của EVNTelecom. Hiện nay EVNTelecom đã triển khai mạng NNI với dung lượng ban đầu là 2xE1s với đối tác nước ngoài nhằm mục đích cung cấp dịch vụ IPVPN đi quốc tế. Trong thời gian tới, EVNTelecom sẽ tăng dung lượng lên 4xE1s.

- **Dịch vụ nhiều ưu điểm**

Sử dụng dịch vụ này, tất cả các địa điểm trong mạng có thể liên hệ trực tiếp với nhau chỉ với một kết nối vật lý duy nhất tại mỗi điểm, không dùng Leased line hay PVC. Điều này làm cấu trúc mạng trở nên đơn giản và cho phép các doanh nghiệp mở rộng mạng một cách nhanh chóng không cần thiết kế lại mạng hay làm gián đoạn hoạt động của mạng.

Với các công nghệ quản lý chất lượng dịch vụ (QoS) chuẩn, tất cả các ứng dụng dữ liệu, thoại và video có thể chạy trên một mạng IP riêng, không cần có các mạng riêng rẽ hay các thiết bị chuyên dùng. Hệ thống bảo mật có sẵn trong mạng sử dụng công nghệ chuyển mạch nhãn đa giao thức (Multi-Protocol Label Switching – MPLS) cho phép phân tách luồng dữ liệu của mỗi

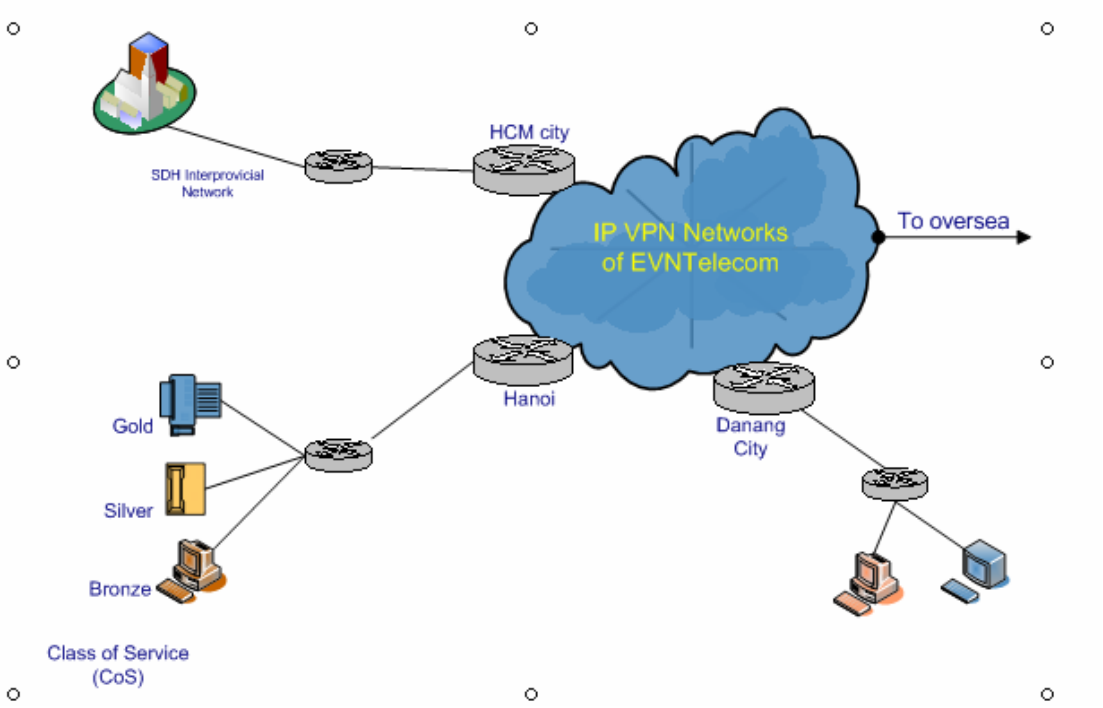
khách hàng ra khỏi Internet cũng như các khách hàng khác. Mức độ bảo mật tương đương các dịch vụ lớp 2 như X.25, frame relay và ATM. IP VPN còn hạn chế yêu cầu đối với người dùng trong việc thực hiện các công việc phức tạp như thiết kế mạng, cấu hình bộ định tuyến, do vậy giảm rất nhiều chi phí vận hành.

- **Những ứng dụng phù hợp với nhiều đối tượng khách hàng**

Khi sử dụng dịch vụ, khách hàng sẽ truyền file, dịch vụ thư tín điện tử, chia sẻ tài nguyên trên mạng (file hoặc máy in), cơ sở dữ liệu, Web nội bộ, truyền ảnh, các ứng dụng ERP, các ứng dụng thiết kế kỹ thuật; truy nhập Internet và sử dụng các dịch vụ trên nền mạng này như một khách hàng Internet trực tiếp bình thường; các ứng dụng về âm thanh, hình ảnh trong mạng riêng của khách hàng (khách hàng có khả năng thiết lập một tổng đài PBX sử dụng công nghệ IP và có thể gọi trong phạm vi mạng nội bộ của mình).Ngoài ra khách hàng có thể ứng dụng nhiều dịch vụ cao hơn như: Hội thảo qua mạng MPLS VPN, hosting...

Dịch vụ VPN phù hợp với đối tượng khách hàng là các đơn vị hoạt động trong lĩnh vực ngân hàng, bảo hiểm, hàng hải...; các văn phòng đại diện các công ty nước ngoài đặt tại Việt Nam liên quan đến viễn thông, tin học; các doanh nghiệp sản xuất có chi nhánh ở nước ngoài trong các khu công nghiệp, khu chế xuất, doanh nghiệp sản xuất; các khu công nghệ phần mềm, các đơn vị sản xuất phần mềm; các cá nhân thuộc một trong các đơn vị kể trên có nhu cầu sử dụng dịch vụ và các cơ quan Chính phủ, các Bộ, các Tổng công ty.

Để sử dụng được dịch vụ, khách hàng cần đáp ứng đầy đủ các thiết bị như: Modem NTU, Router, đường kết nối truyền dẫn trực tiếp với mạng MPLS VPN, modem gián tiếp, line thoại, máy tính với các truy nhập gián tiếp.



Hình 4- 3 Sơ đồ kết nối dịch vụ IPVPN

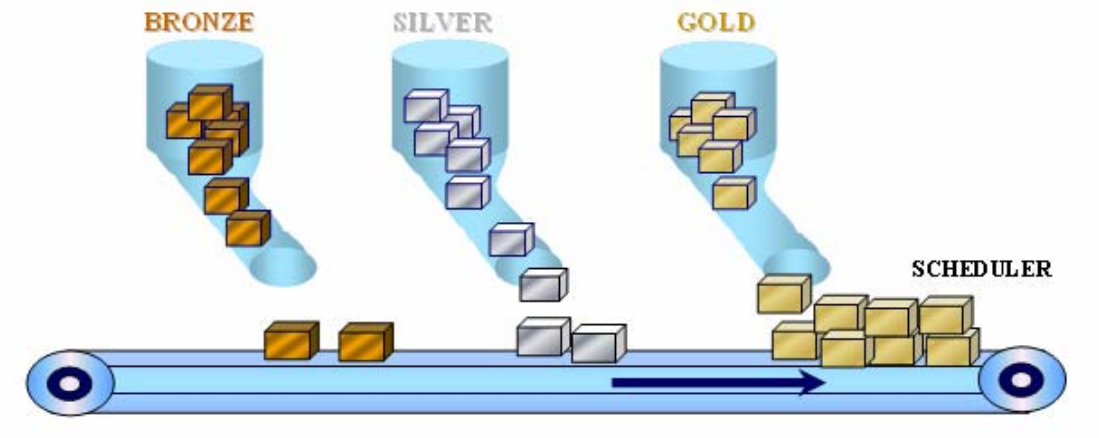
EVNTelecom đảm bảo kết nối IP giữa các site của khách hàng, hỗ trợ kết nối điểm – điểm, điểm – đa điểm, đa điểm – đa điểm.

4.2 Chất lượng dịch vụ mạng EVNTelecom

Các cấp dịch vụ (CoS – Classes of Services) truyền gói trong mạng

- *Gói Vàng*: 99.9% một tháng. Mức độ ưu tiên cao nhất dùng để truyền các ứng dụng yêu cầu độ trễ thấp ví dụ như voice, video.
- *Gói Bạc*: 99.5% một tháng. Lưu lượng ổn định theo yêu cầu với độ trễ và mất gói theo cam kết như các dịch vụ SAP, ERP và những giao dịch tài chính khác.
- *Gói Đồng*: 99.0% một tháng. Lưu lượng không ổn định áp dụng cho các dịch vụ như Email, Intranet hoặc lưu lượng Internet.

Tùy thuộc vào khách hàng lựa chọn gói dịch vụ nào mà mức độ ưu tiên trên đường truyền sẽ khác nhau. Hình 4-4 mô tả mức độ ưu tiên giữa các gói trong mạng:



Giá trị ToS	Class
0	Bronze
3	Silver
5	Gold

Hình 4- 4 Mức ưu tiên giữa các gói dịch vụ của EVNTelecom

- Độ trễ gói trong mạng:

Độ trễ toàn trình "Delay": trễ quá mức từ đầu cuối đến đầu cuối khiến cuộc đàm thoại bất tiện và mất tự nhiên. Mỗi thành phần trong tuyến truyền dẫn: máy phát, mạng lưới, máy thu đều tham gia làm tăng độ trễ. ITU-TG.114 khuyến cáo độ trễ tối đa theo một hướng là 150ms để đảm báo thoại có chất lượng cao. Dưới đây là thông số trễ gói trong mạng mà EVNTelecom cam kết cung cấp cho khách hàng đối với các kênh cấp trong khu vực.

Region	Class of Service (CoS)		
	GOLD	SILVER	BRONZE
IP Precedence	5	3	0
Intra-Asia (Tier1)	<= 110ms	<= 120ms	<= 130ms

Để phân biệt được các lớp dịch vụ khác nhau thì bộ CE chịu trách nhiệm

đánh dấu bit ToS/Differv cho các lớp dịch vụ khác nhau của lưu lượng khi lưu lượng đi vào PE. Sau đó PE sẽ sao chép những bit ToS/Differv tương ứng vào bit EXP MPLS và chuyển tiếp gói vào mạng MPLS

- Khả năng cấp dịch vụ - Service Availability

Khả năng cấp dịch vụ được xác định như là khả năng của trao đổi gói IP của một khách hàng với mạng EVNTelecom. Hiện nay EVNTelecom cam kết cấp cho khách hàng 99.99% trong một tháng.

- Độ trễ pha "Jitter":

Định lượng độ trễ trên mạng đối với từng gói khi đến máy thu. Các gói được phát đi một cách đều đặn từ Gateway bên trái đến được Gateway bên phải ở các thời khoản không đều Jitter quá lớn sẽ làm cho cuộc đàm thoại đứt quãng và khó hiểu. Jitter được tính trên thời gian đến của các gói kế tiếp nhau. Bộ đệm jitter được dùng để giảm tác động "trồi sụt" của mạng và tạo ra dòng gói đến đều đặn hơn ở máy thu.

- Độ mất gói "packet Loss":

Có thể xảy ra theo cụm hoặc theo chu kỳ do mạng bị nghẽn liên tục. Mất gói theo chu kỳ đến 5-10% số gói phát ra có thể làm chất lượng thoại xuống cấp đáng kể. Từng cụm gói bị mất không thường xuyên cũng khiến đàm thoại gặp khó khăn.

Các thông số này (độ truyền gói - packet delivery, độ trễ, khả năng cấp dịch vụ - service availability) được đo bằng cách lấy trung bình của những mẫu đo trong một tháng giữa các PoP VPN trong cùng một khu vực hoặc giữa các khu vực.

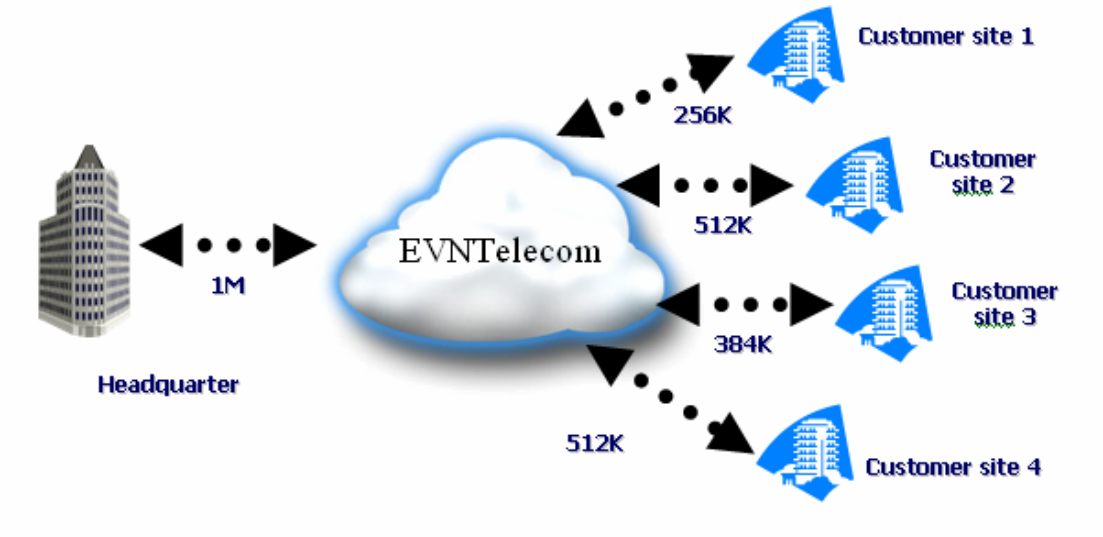
Chú ý: QoS có áp dụng cho giao diện ngoài cua CE, EVNTelecom sẽ áp dụng các dạng lưu lượng cho lưu lượng CoS và thông báo tới CE thông lượng lớn nhất của giao diện giữa PE và CE trong trường hợp băng thông IPVPN yêu cầu của khách hàng không tương ứng với kết nối vật lý.

Các đặc trưng yêu cầu

Tên tính năng	Yêu cầu của ANC	Khả năng hỗ trợ của EVNTelecom
Phân đoạn nội hạt của giao diện hỗ trợ	Các dạng khác nhau của dịch vụ này: • n x 64k • Kênh trắng DS1, DS3 • SONET OC3 STM1 • SONET OC12STM4 • E1 • E3 • ATM (DS-3 / OC-3) • Fast Ethernet • Gigabit Ethernet • Others	Các dạng khác nhau của dịch vụ này: • n x 64k • SDH STM1 • E1 • E3 • Fast Ethernet • Gigabit Ethernet
phương thức đóng gói kênh	Hỗ trợ đóng gói: • Cisco HDLC • Frame Relay • ATM • PPP • Ethernet • Others	Hỗ trợ đóng gói: • Cisco HDLC • PPP • Ethernet • PPP
Hỗ trợ định tuyến Layer-VPNT giữa PE và CE	Hỗ trợ Layer-3 VPN : • BGP-4 • Static • OSPF	Hỗ trợ Layer-3 VPN: • BGP • Static • OSPF

	• RIPv2 • EIGRP • Others	• RIPv2 • Others
Cước phí	Phí hàng tháng = cước thuê cổng + băng thông thực sự sử dụng	Phí hàng tháng = cước phí của cổng
CoS	ANC đưa ra 5 mức CoS	EVNTel đưa ra 4 mức CoS
Internet Access	Khả năng truy nhập Internet sử dụng đường kết nối vật lý đơn.	Hỗ trợ truy nhập Internet sử dụng đường kết nối vật lý đơn.

Hình 4-5 dưới đây đưa ra các ví dụ về việc cung cấp dịch vụ IP VPN cho khách hàng kết nối theo kiểu điểm – đa điểm.



Hình 4- 5 Kết nối IP VPN điểm – đa điểm

Hình 4-6 và 4-7 sau đây đưa ra ví dụ về việc kết nối giữa 4 địa điểm khách hàng với nhau và so sánh giữa dịch vụ IPVPN và IPLC trong trường hợp yêu

cầu kết nối này.

Hình 4- 6 Kết nối giữa 4 điểm khách hàng dựa trên giải pháp của IPLC

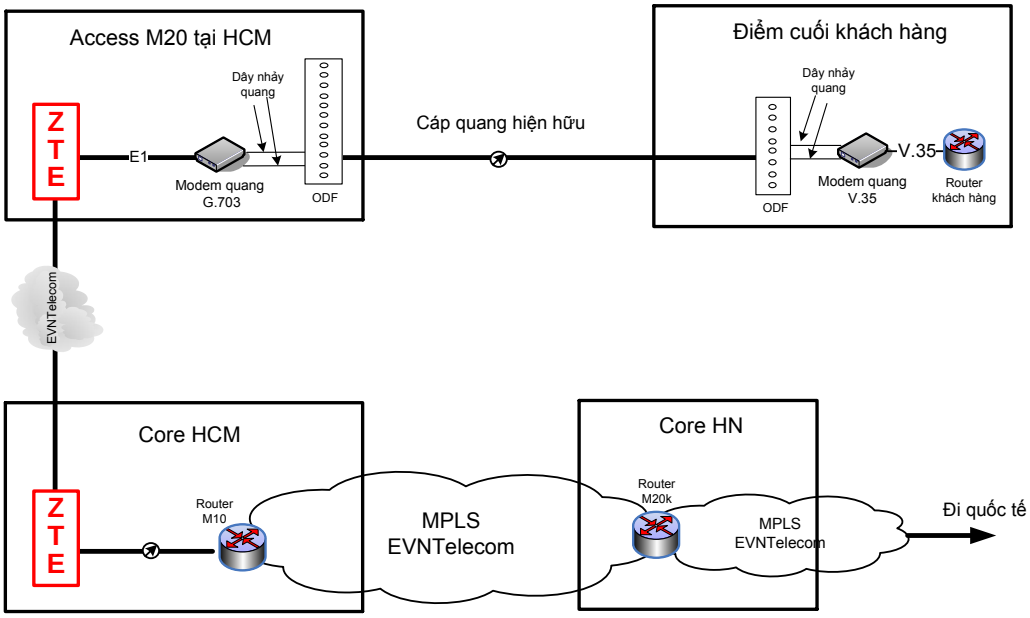
Dịch vụ IPLC kết nối giữa 4 điểm tạo thành một mạng full – mesh, giá thành cao hơn rất nhiều và khó vận hành quản lý.

Với dịch vụ IP VPN việc kết nối giữa 4 điểm trở nên đơn giản và giá thành rẻ.

Hình 4- 7 Kết nối giữa 4 điểm khách hàng dựa trên giải pháp của IPVPN

4.3 Giới thiệu về việc cấp kênh tới khách hàng

Khách hàng yêu cầu kênh truyền tốc độ 256K từ Tp Hồ Chí Minh đi Hong Kong, với CoS là Silver.



Hình 4- 8 Sơ đồ kết nối của khách hàng kết nối tới mạng EVNTelecom

Subject: Fresenius IPVPN [HGC-EVN] (HK, Vietnam)
Date: 3 Sept 2008

Carrier	EVN	HGC
Order Number	PM (M)	08-IP-VPN00254
HGC IB Ref No.	PM (M)	S00003261
Circuit ID	VF800039Z005	VF800039W001
Customer Name	Fresenius- Kabi Asia Pacific Ltd.	Fresenius Netcare Gmbh
PoP City	Vietnam (EVN)	Hong Kong
Local Loop Provider (if any)	EVN	HGC
Local Loop circuit ID (if any)	(TBA)	VF800039W001
Orer Type	IPVPN	IPVPN
Billing Type	N/A	N/A
Port No.	PM (O)	PM (O)
Port Speed	256K	T1
PE Router WAN IP Address	192.168.177.81 / 30	192.168.230.1 / 30
CE Router WAN IP Address	192.168.177.82 / 30	192.168.230.2 / 30
PE-CE Routing Protocol	BGP	BGP

PE-CE Encapsulation	PPP	PPP
Customer LAN IP Prefix and Subnet Mask	Customer AS number : 65141 EVN AS number : 24086	Customer AS number : 65205 HGC AS number : 9304
QoS	100% Silver	100% Silver
Electrical Interface	V.35	V.35
Order Issue Date	8-Aug-08	8-Aug-08
Customer Request Date	8-Sep-08	8-Sep-08
ITMC Test Date	TBA	TBA
End-2-End Test Date	TBA	TBA

4.4 Khó khăn trong việc cung cấp MPLS VPN

Việc cung cấp dịch vụ MPLS VPN của EVNTelecom cũng gặp nhiều khó khăn như:

- Các thiết bị BRAS và mạng Access không thuộc quyền quản lý của EVNTelecom
- Vẫn đang xây dựng quy trình cung cấp dịch vụ.
- Chưa có chính sách về giá cước dịch vụ đầy đủ.
- Nhân lực chưa đủ để đáp ứng được việc cung cấp dịch vụ đang ngày càng được khách hàng sử dụng nhiều.

Không như dịch vụ Leased line là dịch vụ ở Lớp 1, chúng ta chỉ cung cấp đường truyền vật lý cho khách hàng. Dịch vụ MPLS VPN diễn ra ở "lớp 2.5" và lớp 3 nên việc cung cấp dịch vụ sẽ phức tạp và khó khăn hơn. Ngoài việc thiết lập đường truyền vật lý, còn phải cấu hình các thiết bị Router trên mạng từ đầu cuối đến đầu cuối (cấu hình các lớp trên) để cung cấp dịch vụ cho khách hàng.

Ngoài ra do MPLS vẫn là công nghệ mới đối với khách hàng, do đó khách hàng vẫn chưa có sự hiểu biết nhất định nên việc thuyết phục sử dụng gặp nhiều khó khăn.

Chưa có đủ nhân lực làm chủ công nghệ để có thể chuẩn đoán, gỡ rối, ứng cứu khi có sự cố đối với khách hàng (đây là dịch vụ lớp cao nên việc chuẩn đoán, gỡ rối, ứng cứu khác hoàn toàn với việc xử lý thông tin của leased line).

Trong bối cảnh EVNTelecom đang tham gia tích cực và nhanh chóng vào thị trường viễn thông công cộng, tận dụng triệt để cơ sở hạ tầng viễn thông hiện có của ngành điện để nhanh chóng triển khai hàng loạt các dự án trước tiên phục vụ ngày một tốt hơn cho nội bộ ngành điện, tiếp theo là cung cấp một cách đa dạng các loại hình dịch vụ cho người sử dụng. Việc triển khai dịch vụ IPVPN với 03 tổng đài đặt tại 3 vùng, đã thiết lập một hệ thống mạng lõi đủ mạnh tiến đến mục tiêu đưa EVNTelecom trở thành một trong 3 nhà cung cấp dịch vụ viễn thông mạnh tại Việt Nam.

KẾT LUẬN VÀ KIẾN NGHỊ

Công nghệ MPLS (Multiprotocol Label Switching) là kết quả phát triển của nhiều công nghệ chuyển mạch IP (IP Switching) sử dụng cơ chế hoán đổi nhãn như của ATM để tăng tốc độ truyền gói tin mà không cần thay đổi các giao thức định tuyến IP. MPLS là một công nghệ chuyển mạch IP có nhiều triển vọng. Với tính chất cơ cấu định tuyến của mình, MPLS có khả năng nâng cao chất lượng dịch vụ của mạng IP truyền thống. Bên cạnh đó, thông lượng của mạng sẽ được cải thiện một cách rõ rệt. Đây là xu hướng tất yếu của mạng truyền dẫn trong quá trình triển khai và xây dựng mạng NGN ở Việt Nam.

Hướng phát triển của đề tài

Trong công nghệ mới ngày nay, mạng truyền dẫn quang đang dần chiếm lĩnh vị trí số một. Mạng truyền dẫn quang có dung lượng cao, nhưng để giảm chi phí trên một đơn vị băng thông thì cần đến sự kết hợp của hai công nghệ: mạng Quang và IP. Sự kết hợp của công nghệ IP và Quang sẽ mang lại sự phát triển về dung lượng, khả năng mở rộng và sự linh hoạt. Sự kết hợp IP và Quang đáp ứng yêu cầu cho các nhà cung cấp dịch vụ:

- Bổ sung công nghệ Quang cho nền tảng IP.
- Tiếp tục tích hợp IP và dữ liệu trên nền tảng Quang.
- Phát triển một mức quản lý thống nhất, dựa trên tiêu chuẩn để đẩy mạnh hơn nữa việc triển khai và tăng cường hiệu quả mạng IP và Quang
- Củng cố những công cụ quản lý mạng sử dụng cho các thành phần IP và Quang

Cùng với chuyển mạch IP, chuyển mạch Quang cũng đang được cải tiến cùng với sự phát triển của **MPLS tổng quát** (GMPLS – General MPLS)

GMPLS mở rộng sự ảnh hưởng của việc điều khiển MPLS vượt ngoài thiết bị định tuyến và chuyển mạch ATM, đến những thiết bị lớp vật lý như thiết bị kết nối chéo quang và thiết bị TDM truyền thống như các bộ ghép kênh xen kẽ SONET. GMPLS cung cấp tín hiệu thông minh và phần điều khiển định tuyến để cung ứng một cách năng động các tài nguyên quang để cung cấp tính bền vững của hệ thống sử dụng các kỹ thuật bảo vệ và phục hồi.

Trong môi trường quang, khái niệm nhãn được "tổng quát hóa" để bao gồm các đối tượng trong các môi trường phân chia theo thời gian, tần số và không gian. Ví dụ, trong môi trường chuyển mạch TDM (SONET/SDH), các khe thời gian đều có nhãn. Trong chuyển mạch không gian (cổng vào ingress và cổng ra egress) như trong đấu nối chéo quang các cổng đều có nhãn. Trong ghép kênh phân chia theo bước sóng WDM, các bước sóng đều có nhãn. Đó là lý do mở rộng MPLS trong môi trường quang được gắn với chữ "Tổng quát". Thay vì hoán chuyển các nhãn ở mỗi Router, STS (khe của SONET), bước sóng (quang) hoặc sợi cáp quang, nó được hoán chuyển tại mỗi chỗ đấu nối chéo quang. Như vậy, tuyễn chuyển mạch nhãn trong GMPLS là một tuyến quang được thiết lập bằng thủ tục tín hiệu GMPLS.

Mạng thông minh đang được định nghĩa là một tiêu chuẩn mở, theo các yêu cầu được chỉ ra trong tiêu chuẩn Mạng truyền tải chuyển mạch tự động ASTN (Automatic Switched Transport Network) của ITU mà gần đây đã được chấp nhận như G.807. Những dịch vụ này cho phép thay đổi mạng quang tĩnh ngày nay thành mạng năng động cho khách hàng và giảm chi phí cung cấp cho các nhà khai thác mạng. GMPLS là cơ chế lý tưởng cho giao diện chuyển tín hiệu ASTN giữa khách hàng và mạng, trong phạm vi mạng giữa các mạng quang.

Trong mạng chuyển mạch gói hiện nay, cấu hình bị giới hạn bởi các liên kết quang đã được thiết lập từ trước. Lớp mạng gói không thể thiết lập

được các tuyến quang một cách độc lập để đáp ứng được theo sự yêu cầu băng rộng. Nếu những yêu cầu về lưu lượng mới xuất hiện, có thể đưa ra yêu cầu cho nhà cung cấp mạng quang về việc băng rộng bổ sung mà điều này cần phải có kế hoạch thực hiện trước (nhiều ngày). Khi sử dụng dịch vụ ASTN, các kết nối có thể tiến hành với nhiều mức độ về khả năng lưu trữ, phù hợp với mức chất lượng dịch vụ QoS mạng gói.

Do nhiều tính năng khác biệt, GMPLS làm cho mạng Internet quang nhanh hơn và thông minh hơn, giảm thời gian cung cấp hàng tháng xuống còn hàng giây cho dung lượng mạng quang. Việc sử dụng NUNI quang hỗ trợ các khách hàng IP và đa dịch vụ, khả năng kết nối năng động với lớp mạng quang được quản lý có hiệu năng cao hơn và đem lại lợi nhuận cao cho mạng VPN quang. GMPLS là điểm mấu chốt cho việc tích hợp của cả mạng quang cũng như mạng toàn quang sau này.

Hướng nghiên cứu GMPLS là một hướng mở cho công nghệ chuyển mạch nhãn đa giao thức MPLS đã được đề cập trong bài luận văn tốt nghiệp.

TÀI LIỆU THAM KHẢO

Tiếng Việt

1. Trần Thị Tố Uyên, *Chuyển mạch nhãn đa giao thức*, VnPro – Cisco Authorized Training Center.

Tiếng Anh

1. Cisco Systems 2003,USA,*Implementting Cisco (MPLS) v2.0*.
2. Jim Guichard, Ivan Pepelnjak, Jeff Apcar (June 06,2003), *MPLS and VPN Architectures*, Volumer II, Cisco Press
3. Joseph M.Soricelli (2004),*Juniper Networks Certified Internet Specialist,*SYBEX Inc., 1151 Marina Village Parkway, Alameda, CA 94501,pp.767-876.
4. Luc De Ghein (November 2006), *MPLS fundamentals,* Cisco Press.
5. Rosel et al (March 2000), *Multiprotocol Label Switching Architechture.*
6. Vivek Alwayn (September 25,2001), *Advanced MPLS Design and Implementation*, Cisco Press, 201 West 103rd Street Indianapolis, IN 46290 USA,pp.78-150.
7. Multiprotocol Label Switching. http://www.iec.org Web Tutorials.
8. MPLS VPN, http://www.cisco.com Web Technology Document.