ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

TRẦN VĂN TIẾN

CÁC GIẢI PHÁP CHO MẠNG RIÊNG ẢO KIỂU SITE-TO-SITE DÙNG GIAO THỨC MPLS

LUẬN VĂN THẠC SỸ CÔNG NGHỆ THÔNG TIN

Hà Nội – 2016

ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

TRẦN VĂN TIẾN

CÁC GIẢI PHÁP CHO MẠNG RIÊNG ẢO KIỂU SITE-TO-SITE DÙNG GIAO THỨC MPLS

Ngành: Công nghệ thông tin

Chuyên ngành: Truyền dữ liệu và mạng máy tính

Mã số: Thí điểm

LUẬN VĂN THẠC SỸ CÔNG NGHỆ THÔNG TIN

NGƯỜI HƯỚNG DẪN KHOA HỌC:

PGS.TS. NGUYỄN ĐÌNH VIỆT

Hà Nội – 2016

LỜI CAM ĐOAN

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

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

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

Học viên

Trần Văn Tiến

LỜI CẢM ƠN

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

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

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

Hà Nội, tháng 11 năm 2016

Học viên

Trần Văn Tiến

MỤC LỤC

DANH MỤC HÌNH VẼ

DANH MỤC TỪ VIẾT TẮT

Viết tắt	Tiếng Anh	Tiếng Việt
AF	Assured Forwarding	Chuyển tiếp bảo đảm
AH	Authentication Header	Tiêu đề cho xác thực
ATM	Asynchronous Transfer Mode	Phương thức truyền dẫn không đồng bộ
AS	Autonomous System	Hệ thống tự trị
BGP	Border Gateway Protocol	Giao thức cổng đường biên
CBWFQ	Class-Base Weighted Fair Queuing	Hàng đợi công bằng có trọng số dựa trên cơ sở lớp
CE	Customer Edge	Bộ định tuyến biên khách hàng
CHAP	Challenge Handshake Authentication Protocol	Giao thức xác thực bắt tay kiểu thách đố
CoS	Class of Service	Lớp dịch vụ
DES	Data Encryption Standard	Chuẩn mã hóa dữ liệu
DSCP	Differentiated Service Code Point	Điểm mã dịch vụ phân biệt
EF	Expedited Forwarding	Chuyển tiếp nhanh
ESP	Encapsulating Security Payload	Phương thức đóng gói bảo mật tải tin
FEC	Forwarding Equivalence Class	Lớp chuyển tiếp tương đương
FIB	Forwarding Information Base	Cơ sở dữ liệu chuyển tiếp
IETF	Internet Engineering Task Force	Tổ chức chuyên trách về kỹ thuật Internet
IGP	Interior Gateway Protocol	Giao thức định tuyến nội vùng
IKE	Internet Key Exchange	Phương thức trao đổi khóa Internet
IPSec	Internet Protocol Security	Giao thức IP bảo mật
ISP	Internet Service Provider	Nhà cung cấp dịch vụ
L2TP	Layer 2 Tunnel Protocol	Giao thức đường hầm lớp 2
LAN	Local Area Network	Mạng cục bộ
LDP	Label Distribution Protocol	Giao thức phân phối nhãn

LER	Label Edge Router	Router chuyển mạch nhãn biên
LFIB	Label Forwarding Information Base	Cơ sở dữ liệu nhãn chuyển tiếp
LIB	Label Information Base	Cơ sở dữ liệu nhãn
LLQ	Low-latency Queueing	Hàng đợi có độ trễ thấp
LSP	Label Switched Path	Đường chuyển mạch nhãn
LSR	Label Switching Router	Router chuyển mạch nhãn
MD5	Message-Digest Algorithm	Thuật toán mã hóa MD5
MPLS	Multiprotocol Label Switching	Chuyển mạch nhãn đa giao thức
MPPE	Microsoft Point to Point Encryption	Phương pháp mật mã hóa điểm điểm của Microsoft
NAS	Network Access Server	Máy phục vụ truy cập mạng
OSPF	Open Shortest Path First	Giao thức tìm đường ngắn nhất
PAP	Password Authentication Protocol	Giao thức xác thực mật khẩu
PE	Provider Edge Router	Bộ định tuyến biên của nhà cung cấp
PPP	Point to Point Protocol	Giao thức điểm điểm
PPTP	Point-to-Point Tunneling Protocol	Giao thức đường hầm điểm điểm
PQ	Priority Queue	Hàng đợi ưu tiên
PSTN	Public Switched Telephone Network	Mạng điện thoại công cộng
QoS	Quality of Service	Chất lượng dịch vụ
RAS	Remote Access Server	Máy chủ truy cập từ xa
RD	Route Distinguisher	Định tuyến phân biệt
RED	Random Early Detection	Phương pháp phát hiện sớm ngẫu nhiên
RSVP	Resource Reservation Protocol	Giao thức dành riêng tài nguyên
SHA	Secure Hash Algorithm	Thuật toán băm bảo mật
VC	Virtual Circuit	Mạch ảo
VPN	Virtual Private Network	Mạng riêng ảo
VRF	Virtual Routing and Forwrding	Bảng định tuyến và chuyển tiếp ảo

DANH MỤC CÁC BẢNG

MỞ ĐẦU

MPLS VPN là một lựa chọn mới cho cho mạng diện rộng WAN. Nó đang ngày càng được trở nên phổ biến trong nền công nghiệp viễn thông. Các khách hàng doanh nghiệp đang dần dần hướng tới những nhà cung cấp dịch vụ có triển khai ứng dụng MPLS VPN. Lý do chính cho sự thay đổi này nằm ở việc MPLS có khả năng cung cấp sẵn các tính năng bảo mật và các kết nối đa điểm tới đa điểm. QoS là một thành phần rất quan trọng trong các mạng khách hàng. Mạng doanh nghiệp thường có nhiều loại lưu lượng như thoại, hình và dữ liệu đi qua một hạ tầng mạng duy nhất.

Trong luận văn này tôi sẽ trình bày nghiên cứu của mình về các vấn đề của QoS (trễ, biến thiên trễ, mất gói…) trong môi trường MPLS VPN. Nó sẽ là cơ sở để nhà cung cấp dịch vụ và khách hàng duy trì một chất lượng dịch vụ ổn định cho các lưu lượng hình, tiếng, dữ liệu… chạy qua môi trường này.

Để đạt được chất lượng dịch vụ từ điểm đầu tới điểm cuối một cách ổn định, nhà cung cấp dịch vụ và khách hàng doanh nghiệp phải làm việc với nhau một cách chặt chẽ đồng thời chia sẻ các chính sách giống nhau bởi vì nhà cung cấp dịch vụ tham gia vào định tuyến của khách hàng trong môi trường MPLS VPN. Chúng ta sẽ sử dụng mô hình chất lượng dịch vụ DiffServ cho môi trường MPLS VPN. Đồng thời chúng ta cũng sẽ lựa chọn một mô hình 4,5 hoặc 6 lớp dịch vụ cho nhà cung cấp dịch vụ và khách hàng để triển khai thử nghiệm.

Trong phần cuối tôi sẽ tiến hành thử nghiệm chất lượng dịch vụ (độ mất gói, trễ, biến thiên trễ…) từ điểm đầu tới điểm cuối. Sau đó chúng ta sẽ so sánh kết quả của các tham số trên khi áp dụng và khi không áp dụng mô hình chất lượng dịch vụ DiffServ trong mạng MPLS VPN. Chúng ta sẽ thấy rõ ràng trong phần kết quả khi sử dụng mô hình chất lượng dịch vụ DiffServ các tham số trễ, mất gói, biến thiên trễ sẽ tăng khi dữ liệu trong mạng tăng lên. Tuy nhiên sau khi áp dụng mô hình chất lượng dịch vụ DiffServ các tham số trên sẽ không bị ảnh hưởng khi tăng lưu lượng dữ liệu trong mạng và cung cấp một mức chất lượng dịch vụ ổn định.

CHƯƠNG 1. TỔNG QUAN VỀ MẠNG RIÊNG ẢO – VPN

VPN có thể được hiểu như là mạng kết nối các site khách hàng đảm bảo an ninh trên cơ sở hạ tầng mạng chung cùng với các chính sách điều khiển truy cập và bảo mật như một mạng riêng. Tuy được xây dựng trên cơ sở hạ tầng có sẵn của mạng công cộng nhưng VPN lại có được các tính chất của một mạng cục bộ như khi sử dụng các đường kênh thuê riêng. Chương này sẽ trình bày từ những nguyên lý cơ bản nhất trong hoạt động trao đổi thông tin của các mạng truyền thông.

1.1 Mạng Internet và kiến trúc giao thức mạng Internet

1.1.1 Sự ra đời mạng Internet

Tiền thân của mạng Internet ngày nay là mạng ARPANET. Cơ quan quản lý dự án nghên cứu phát triển ARPA thuôc bộ quốc phòng Mỹ liên kết 4 địa điểm đầu tiên vào tháng 7 năm 1969 gồm: Viện nghiên cứu Stanford, Đại học California, Los Angeles, Đại học Utah và Đại học California, Santa Barbara. Đó chính là mạng liên khu vực (Wide Area Network - WAN) đầu tiên được xây dựng.

Thuật ngữ Internet lần đầu xuất hiện vào khoảng năm 1974. Lúc đó mạng vẫn được gọi là ARPANET. Năm 1983, giao thức TCP/IP chính thức được coi như một chuẩn đối với ngành quân sự Mỹ và tất cả các máy tính nối với ARPANET phải sử dụng chuẩn mới này. Năm 1984, ARPANET được chia ra thành hai phần: phần thứ nhất vẫn được gọi là ARPANET, dành cho việc nghiên cứu và phát triển; phần thức hai được gọi là MILNET, là mạng dùng cho các mục đích quân sự

Giao thức TCP/IP ngày càng thể hiện rõ các điểm mạnh của nó, quan trọng nhất là khả năng liên kết các mạng khác với nhau một cách dễ dàng. Chính điều này cùng với các chính sách mở cửa đã cho phép các mạng dùng cho nghiên cứu và thương mại kết nối được với ARPANET, thúc đẩy việc tạo ra một siêu mạng (Supernetwork). Năm 1980, ARPANET được đánh giá là mạng trụ cột của Internet. Mốc lịch sử quan trọng của Internet được xác lập vào giữa thập nhiên 1980 khi tổ chức khoa học quốc gia Mỹ NSF thành lập mạng liên kết các trung tâm máy tính lớn với nhau gọi là NSFNET. Nhiều doanh nghiệp đã chuyển từ ARPANET sang NSFNET và do đó sau gần 20 năm hoạt động, ARPANET không còn hiệu quả đã ngừng hoạt động vào khoảng năm 1990.

Sự hình thành mạng xương sống của NSFNET và những mạng vùng khác đã tạo ra một môi trường thuận lợi cho sự phát triển của mạng Internet. Tới năm 1995, NSFNET thu lại thành một mạng nghiên cứu còn Internet thì vẫn tiếp tục phát triển.

Với khả năng kết nối mở như vậy, Internet đã trở thành một mạng lớn nhất trên thế giới, mạng của các mạng, xuất hiện trong mọi lĩnh vực thương mại, chính trị, quân sự, nghiên cứu, giáo dục, văn hóa, xã hội… Cũng từ đó, các dịch vụ trên Internet không ngừng phát triển tạo ra cho nhân loại một thời kỳ mới: kỷ nguyên thương mại điện tử trên Internet.

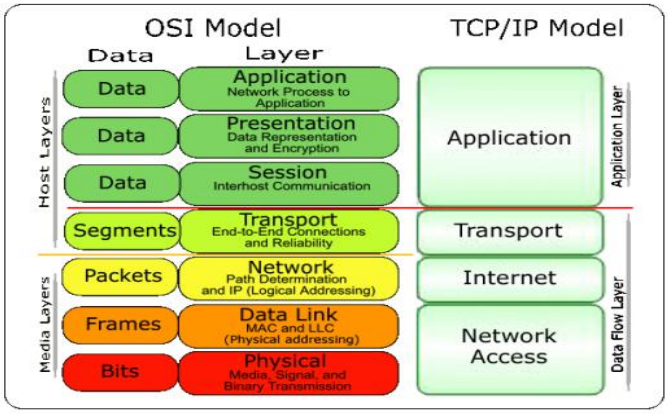
Đến năm 1997 Internet chính thức xuất hiện tại Việt Nam. [11]

1.1.2 Kiến trúc giao thức mạng Internet

Đầu những năm 1980 một bộ giao thức mới được đưa ra làm giao thức chuẩn cho mạng ARPANET và các mạng của DoD mang tên DARPA Internet protocol suite,

thường được gọi là bộ giao thức TCP/IP hay gọi tắt là TCP/IP. Bộ giao thức này cũng được sử dụng cho các hệ thống sử dụng Unix. Bộ giao thức cốt lõi TCP/IP và yếu tố phi tập trung của nó đã mang lại sự thành công cho ARPANET và INTERNET ngày nay.

So sánh mô hình OSI và TCP/IP



Hình 1 - 1 So sánh kiến trúc mô hình OSI và TCP/IP

Khi triển trúc tiêu chuẩn OSI xuất hiện thì TCP/IP đã trên con đường phát triển. Xét một cách chặt chẽ, TCP/IP và OSI không liên quan tới nhau. Nói cách khác mô hình TCP/IP được đưa ra bởi các nhà sản xuất thương mại. Tuy nhiên, hai mô hình này có những mục tiêu giống nhau và do đó sự tương tác giữa các nhà thiết kế tiêu chuẩn nên 2 mô hình xuất hiện những điểm tương thích. Cũng chính vì thế, các thuật ngữ của OSI thường được áp dụng cho TCP/IP. Cả OSI và TCP/IP là các tiêu chuẩn xây dựng mô hình mạng. [4]

1.2 Mạng cục bộ LAN

1.2.1 Mạng LAN và các đặc điểm chính

1.2.1.1 Khái niệm

Mạng cục bộ LAN (Local Area Network) là hệ thống truyền thông tốc độ cao được thiết kế để kết nối các máy tính và các thiết bị xử lý dữ liệu khác cùng hoạt động với nhau trong một khu vực địa lý nhỏ như ở một tầng của tòa nhà hoặc một tòa nhà… Tên gọi "mạng cục bộ" được xem xét từ quy mô của mạng. Tuy nhiên đó không phải là đặc tính duy nhất của mạng cục bộ nhưng trên thực tế, quy mô của mạng quyết định nhiều đặc tính và công nghệ của mạng

1.2.1.2 Đặc điểm của mạng cục bộ

Mạng cục bộ có những đặc điểm chính sau: [1]

- Mạng cục bộ có quy mô nhỏ, thường là bán kính dưới vài km. Đặc điểm này cho phép không cần dùng các thiết bị dẫn đường với các mối liên hệ phức tạp
- Mạng cục bộ thường được sở hữu của một tổ chức. Điều này dường như có vẻ ít quan trọng nhưng trên thực tế đó là điều khá quan trọng để việc quản lý mạng có hiệu quả

- Mạng cục bộ có tốc độ cao và ít lỗi. Trên mạng rộng tốc độ nói chung chỉ đặt vài Kbit/s. Còn tốc độ thông thường trên mạng cục bộ là 10, 100, 1000 Mb/s. Xác suất lỗi rất thấp

1.2.1.3 Các đặc tính kỹ thuật của LAN

- **Đường truyền**: là thành phần quan trọng của một mạng máy tính, là phương tiện dùng để truyền các tín hiệu điện tử giữa các máy tính. Các tín hiệu điện tử đó chính là các thông tin, dữ liệu được biểu thị dưới dạng các xung nhị phân (ON_OFF), mọi tín hiệu truyền giữa các máy tính với nhau đều thuộc sóng điện từ, tùy theo tần số mà ta có thể dựng các đường truyền vật lý khác nhau. Các máy tính được kết nối với nhau bởi các loại cáp truyền: cáp đồng trục, cáp xoắn đôi…
- **Chuyển mạch**: Là đặc trưng kỹ thuật chuyển tín hiệu giữa các nút trong mạng, các nút mạng có chức năng hướng thông tin tới đích nào đó trong mạng. Trong mạng nội bộ, phần chuyển mạch được thực hiện thông qua các thiết bị chuyển mạch như HUB, Switch…
- **Kiến trúc mạng**: Kiến trúc mạng máy tính thể hiện cách nối các máy tính với nhau và tập các quy tắc, quy ước mà tất cả các thực thể tham gia truyền thông trên mạng phải tuân theo để đảm bảo cho mạng hoạt động tốt. Người ta thường nhắc đến hai vấn đề trong kiến trúc mạng là topo mạng (Network topology) và giao thức mạng (Network protocol)
    - *Network Topology*: Cách két nối các máy tính với nhau về mặt hình học mà ta gọi là topo mạng. Một số loại cơ bản là: hình sao, hình bus, hình vòng…
    - *Network Protocol:* Tập hợp các quy ước truyền thông giữa các thực thể truyền thông mà ta gọi là giao thức của mạng. Các giao thức thường gặp là: TCP/IP, NETBIOS, IPX/SPX…
- **Kỹ thuật truy cập đường truyền** (Medium Access Control - MAC): Chỉ ra cách thức mà các host trong mạng LAN sử dụng để truy cập và chia sẻ đường truyền mạng. MAC sẽ quản trị việc truy cập đến đường truyền trong LAN và cung cấp cơ sở cho việc định danh các tính trong mạng LAN theo chuẩn IEEE. [5]

1.2.1.4 Phân loại và một số công nghệ mạng LAN phổ biến

IEEE là tổ chức đi tiên phong trong lĩnh vực chuẩn hóa mạng cục bộ với dự án IEEE 802 nổi tiếng và được triển khai từ những năm 1980 và kết quả là hàng loại chuẩn thuộc họ 802.x ra đời, tạo nền tảng quan trọng cho việc thiết kế và cài đặt mạng nội bộ trong thời gian qua. Có thể kể đến một số chuẩn trong họ 802 như: IEEE 801.1: High Level Interface; IEEE 802.2: Logical Link Control (LLC), IEEE 802.3: CSMA/CD là chuẩn đặc tả một mạng cục bộ dựa trên mạng Ethernet nổi tiếng do Digital, Intel và Xerox hợp tác phát triển từ năm 1990; IEEE 802.11: Wireless LAN…

Một số công nghệ LAN phổ biến:

- Ethernet (802.3) đã dễ dàng trở thành công nghệ mạng LAN thành công nhất trong 30 năm qua. Được phát triển từ giữa thập kỷ 1970s bởi các nhà nghiên

cứu tại Xerox Palo Alto Research Center (PARC), Ethernet là một ví dụ thực tiễn của loại mạng cục bộ sử dụng giao thức CSMA/CD. Các công nghệ Ethernet phổ biến là 100BASE-T, 10BASE-T…

1.2.2 Mạng LAN không dây và các đặc điểm chính

1.2.2.1 Khái niệm

WLAN (Wireless LAN) là một loại mạng máy tính nhưng việc kết nối giữa các thành phần trong mạng không sử dụng các loại cáp như một mạng thông thường, môi trường truyền thông của các thành phần trong mạng là không khí. Các thành phần trong mạng sử dụng sóng điện từ để truyền thông với nhau.

Công nghệ WLAN lần đầu xuất hiện vào cuối năm 1990, khi những nhà sản xuất giới thiệu những sản phẩm hoạt động trong băng tần 900Mhz. Những giải pháp này cung cấp tốc độ truyền dữ liệu 1Mpbs, thấp hơn nhiều so với tốc độ 10Mpbs của hầu hết các mạng sử dụng cáp hiện thời.

Năm 1997, IEEE đã phê chuẩn sự ra đời của chuẩn 802.11 và cũng được biết với tên gọi WIFI (Wireless Fidelity) cho các mạng WLAN. Chuẩn 802.11 hỗ trợ ba phương pháp truyền tín hiệu trong đó có bao gồm phương pháp truyền tín hiệu vô tuyền ở tần số 2.4Ghz.

Năm 1999, IEEE lại tiếp tục thông qua hai sự bổ sung cho 802.11 là các chuẩn 802.11a và 802.11b. Và những thiết bị WLAN dựa trên chuẩn 802.11b đã nhanh chóng trở thành công nghệ không dây vượt trội có thể truyền dữ liệu lên tới 11Mbps.

Năm 2003, IEEE tiếp tục công bố thêm sự cải tiến là chuẩn 802.11g mà có thể truyền nhận ở cả hai băng tần 2.4Ghz và 5Ghz đồng thời nâng tốc độ truyền lên tới 54Mbps

1.2.2.2 Phân loại

Một số loại mạng không dây phổ biến: [1]

- ***WLAN (Wireless Local Area Network):*** nổi bật là công nghệ Wifi với nhiều chuẩn mở rộng khác nhau thuộc họ gia đình 802.11 (a, b, g, n…) hiện nay mới nhất là 802.11ac. Tốc độ dao động từ 10 -> 300 Mpbs. Mạng WLAN được triển khai trong phạm vị hẹp (<500m)
- ***WWAN (Wireless Wide Area Network):*** tên gọi khác là mạng tế bào. Sử dụng các công nghệ như GSM, GPRS, CDMA, HSDPA, LTE… Tốc độ vào khoảng 10 – 384 Mbps tầm phủ sóng xa. Hệ thống triển khai trên phạm vi rộng trên toàn khu vực hoặc xuyên quốc gia
- ***WMAN (Wireless Personal Area Network):*** là mạng được tạo bởi các sóng vô tuyến ngắn (vài mét) giữa các thiết bị như smartphone, đồng hồ, tai nghe, điều khiển từ xa… với máy tính. Tốc độ vào khoảng 1Mbps tầm phủ sóng ngắn ví dụ công nghệ Bluetooth

1.2.2.3 Ưu nhược điểm

a) Ưu điểm

- *Sự tiện lợi*: Mạng không dây cũng như hệ thống mạng thông thường. Nó cho phép người dùng truy xuất tài nguyên mạng ở bất kỳ nơi đâu trong khu vực được triển khai. Với sự gia tăng của người sử dụng các máy tính xách tay đó là một điều thuận lợi
- *Khả năng di động*: Với sự phát triển của các mạng không dây công cộng, người dùng có thể truy cập Internet bất kỳ nơi đâu. Chẳng hạn ở các quán Café, người dùng có thể truy cập Internet miễn phí không dây
- *Hiệu quả:* Người dùng có thể duy trì kết nối mạng khi họ đi từ nơi này đến nơi khác
- *Triển khai:* Việc thiết lập hệ thống mạng không dây ban đầu chỉ cần ít nhất 1 Access Point. Với mạng dùng dây thì sẽ gặp khó khăn trong việc triển khai cáp ở nhiều vị trí trong nhà
- *Khả năng mở rộng:* Mạng không dây có thể đáp ứng tức thì khi gia tăng số lượng người dùng. Với hệ thống mạng dùng cpas thì phải gắn thêm cáp

b) Nhược điểm

- *Bảo mật:* Môi trường kết nối không dây là không khí nên khả năng bị tấn công cao
- *Phạm vi:* Một mạng chuẩn 802.11g với các thiết bị chuẩn chỉ có thể hoạt động trong phạm vi khoảng vài chục mét. Để đáp ứng với khoảng cách rộng hơn thì cần mua thêm Repeater hay Access point gây tốn kém
- *Độ tin cậy:* Vì sư dụng sóng vô tuyến để truyền thông nên việc bị nhiễu, tín hiệu bị giảm do tác động của các thiết bị khác (lò vi sóng…) là không tránh khỏi. Làm giảm đáng kể hiệu quả hoạt động của mạng
- *Tốc độ:* Tốc độ của mạng không dây (1 – 125 Mbps) rất chậm so với mạng sử dụng cáp (100Mpbs đến hàng Gbps)

Có thể thấy rằng mạng WLAN (đặc biệt chuẩn 802.11) – một trong những mang phổ biến nhất và sử dụng nhiều nhất trong họ 802.x vẫn có những đặc điểm giống với mạng LAN như có quy mô nhỏ được sở hữu bởi một tổ chức nào đó và do đó thường được áp dụng một số chính sách quản trị, chia sẻ tài nguyên…Đây là mạng được đề cập chủ yếu trong luận văn.

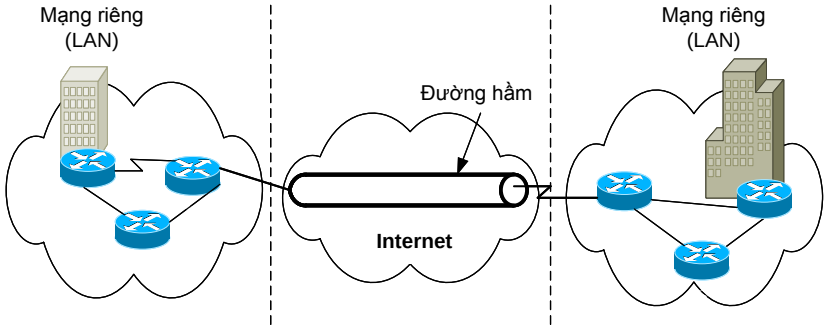
1.3 Mạng riêng ảo – VPN

1.3.1 Khái niệm

Mạng riêng ảo được định nghĩa như là một mạng kết nối các site khách hàng đảm bảo an ninh trên cơ sở hạ tầng mạng chung cùng với các chính sách điều khiển truy nhập và bảo mật như một mạng riêng. Tuy được xây dựng trên cơ sở hạ tầng sẵn có của mạng công cộng nhưng VPN lại có được các tính chất của một mạng cục bộ như khi sử dụng các đường kênh thuê riêng

Tính "riêng" của VPN thể hiện ở chỗ dữ liệu truyền luôn được giữ bí mật và chỉ có thể truy nhập bởi những người sử dụng được trao quyền. Mạng riêng ảo sử dụng các phương pháp mã hóa để bảo vệ dữ liệu. Dữ liệu ở đầu ra của một mạng được mã hóa rồi chuyển vào mạng công cộng như các dữ liệu khác để truyền tới đích và sau đó được giải mã tại phía thu. Dữ liệu đã mật mã có thể coi như được truyền trong một

đường hầm bảo mật từ nguồn tới đích. Cho dù một kẻ tấn công có thể nhìn thấy dữ liệu đó trên đường truyền thì cũng không có khả năng đọc được vì nó đã được mật mã. Hình 1-2 minh họa mạng riêng ảo sử dụng cơ sở hạ tầng mở và phân tán của Internet cho việc truyền dữ liệu giữa các site.



Hình 1 - 2 Mô hình kết nối VPN

Ví dụ về giao thức sử dụng trong việc mã hóa để đảm bảo an toàn là IPSec. Đó là một tiêu chuẩn cho mã hóa cũng như xác thực các gói IP tại tầng mạng. IPSec hỗ trợ một tập hợp các giao thức mật mã với hai mục đích: an ninh mạng và thay đổi các khóa mật mã. Nhiều hãng đã nhanh chóng phát triển và cung cấp các dịch vụ IPSec VPN Server và IPSec VPN Client. Kết nối trong VPN là kết nối động, nghĩa là không được gắn cứng và tồn tại như một kết nối thực khi lưu lượng mạng chuyển qua. Kết nối này có thể thay đổi và thích ứng với nhiều môi trường khác nhau. Khi có yêu cầu kết nối thì nó được thiết lập và duy trì giữa những điểm đầu cuối. [3]

1.3.2 Các chức năng và đặc điểm của VPN

1.3.2.1 Chức năng

VPN cung cấp ba chức năng chính là ***tính xác thực (Authentication), tính toàn vẹn (Integrity)*** và ***tính bảo mật (Confidentiality)***

> ***Tính xác thực:*** Để thiết lập một kết nối VPN thì trước hết cả hai phía phải xác thực lẫn nhau để khẳng định mình đang trao đổi thông tin với người mình mong muốn chứ không phải là một người khác

Tính toàn vẹn: Đảm bảo dữ liệu không bị thay đổi hay có bất kỳ sự xáo trộn nào trong quá trình truyền dẫn

Tính bảo mật: Người gửi có thể mã hóa các gói dữ liệu trước khi truyền qua mạng công cộng và dữ liệu sẽ được giải mã ở phía thu. Bằng cách làm như vậy, không một ai có thể truy cập thông tin mà không được phép. Thậm chí nếu có lấy được thì cũng không đọc được

1.3.2.2 Ưu điểm

Mạng riêng ảo mang lại lợi ích thực sự và tức thời cho các công ty. Nó không chỉ giúp đơn giản hóa việc trao đổi thông tin giữa các nhân viên làm việc ở xa, người dùng lưu động, mở rộng Intranet đến từng văn phòng, chi nhánh, thậm chí triển khai Extranet đến tận khách hàng và các đối tác chủ chốt mà còn cho phép giảm chi phí rất

nhiều so với việc mua thiết bị và đường truyền cho mạng WAN riêng. Những lợi ích trực tiếp và gián tiếp mà VPN mạng lại bao gồm: tiết kiệm chi phí, tính linh hoạt, khả năng mở rộng…

Tiết kiệm chi phí

Việc sử dụng VPN sẽ giúp các công ty giảm được chi phí đầu tư và chi phí thường xuyên. Tổng giá thành của việc sở hữu một mạng VPN sẽ được thu nhỏ, do chỉ phải trả ít hơn cho việc thuê băng thông đường truyền, các thiết bị mạng đường trục và duy trì hoạt động của hệ thống. Nhiều số liệu cho thấy, giá thành cho việc kết nối LAN-to-LAN giảm từ 20 tới 30% so với việc sử dụng đường thuê riêng truyền thống, còn đối với việc truy cập từ xa giảm từ 60 tới 80%

Tính linh hoạt

Tính linh hoạt ở đây không chỉ thể hiện trong quá trình vận hành khai thác mà còn thực sự mềm dẻo đối với yêu cầu sử dụng. Khách hàng có thể sử dụng nhiều kiểu kết nối khác nhau để kết nối các văn phòng nhỏ hay các đối tượng di động. Nhà cung cấp dịch vụ VPN có thể cho phép nhiều sự lựa chọn kết nối cho khách hàng: modem 56 kbit/s, ISDN 128 kbit/s, xDSL, E1,…

Khả năng mở rộng

Do VPN được xây dựng dựa trên cơ sở hạ tầng mạng công cộng nên bất cứ ở nơi nào có mạng công cộng (như Internet) đều có thể triển khai VPN. Ngày nay mạng Internet có mặt ở khắp nơi nên khả năng mở rộng của VPN rất dễ dàng. Một văn phòng ở xa có thể kết nối một cách khá đơn giản đến mạng của công ty bằng cách sử dụng đường dây điện thoai hay đường thuê bao số DSL.

Khả năng mở rộng còn thể hiện ở chỗ, khi một văn phòng hay chi nhánh yêu cầu băng thông lớn thì nó có thể được nâng cấp dễ dàng. Ngoài ra, cũng có thể dễ dàng gỡ bỏ VPN khi không có nhu cầu.

Giảm thiểu các hỗ trợ kỹ thuật

Việc chuẩn hóa trên một kiểu kết nối từ đối tượng di động đến một POP của ISP và việc chuẩn hóa các yêu cầu về bảo mật đã làm giảm thiểu nhu cầu về nguồn hỗ trợ kỹ thuật cho mạng VPN. Ngày nay, khi mà các nhà cung cấp dịch vụ đảm nhiệm việc hỗ trợ mạng nhiều hơn thì những yêu cầu hỗ trợ kỹ thuật đối với người sử dụng ngày càng giảm

Giảm thiểu các yêu cầu về thiết bị

Bằng việc cung cấp một giải pháp truy nhập cho các doanh nghiệp qua đường Internet, VPN yêu cầu về thiết bị ít hơn và đơn giản hơn nhiều so với việc bảo trì các modem riêng biệt, các card tương thích cho thiết bị đầu cuối và các máy chủ truy nhập từ xa. Một doanh nghiệp có thể thiết lập các thiết bị khách hàng cho một môi trường chẳng hạn như T1 hay E1, phần còn lại của kết nối được thực hiện bởi ISP

Đáp ứng các nhu cầu thương mại

Đối với các thiết bị và công nghệ viễn thông mới thì những vấn đề cần quan tâm là chuẩn hóa, các khả năng quản trị, mở rộng và tích hợp mạng, tính kế thừa, độ tin cậy và hiệu suất hoạt động, đặc biệt là khả năng thương mại của sản phẩm.

Các sản phẩm dịch vụ VPN tuân theo chuẩn chung hiện nay, một phần là để đảm bảo khả năng làm việc của sản phẩm nhưng có lẽ quan trọng hơn là để sản phẩm của nhiều nha cung cấp khác nhau có thể làm việc với nhau

1.3.2.3 Nhược điểm

Sự rủi ro an ninh

Một mạng riêng ảo thường rẻ và hiệu quả hơn so với giải pháp sử dụng kênh thuê riêng. Tuy nhiên, nó cũng tiềm ẩn nhiều rủi ro an ninh khó lường trước. Mặc dù hầu hết các nhà cung cấp dịch vụ VPN quảng cáo rằng giải pháp của họ là đảm bảo an toàn, sự an toàn đó không bao giờ là tuyệt đối. Cũng có thể làm cho mạng riêng ảo khó phá hoại hơn bằng cách bảo vệ tham số của mạng một cách thích hợp, song điều này lại ảnh hưởng đến giá thành của dịch vụ.

Độ tin cậy và sự thực thi

VPN sử dụng phương pháp mã hoá để bảo mật dữ liệu, và các hàm mật mã phức tạp có thể dẫn đến lưu lượng tải trên các máy chủ là khá nặng. Nhiệm vụ của người quản trị mạng là quản lí tải trên máy chủ bằng cách giới hạn số kết nối đồng thời để biết máy chủ nào có thể điều khiển. Tuy nhiên, khi số người cố gắng kết nối tới VPN đột nhiên tăng vọt và phá vỡ hết quá trình truyền tin, thì chính các nhân viên quản trị này cũng không thể kết nối được vì tất cả các cổng của VPN đều bận. Điều đó chính là động cơ thúc đẩy người quản trị tạo ra các khoá ứng dụng làm việc mà không đòi hỏi VPN. Chẳng hạn thiết lập dịch vụ proxy hoặc dịch vụ Internet Message Access Protocol (IMAP) để cho phép nhân viên truy nhập e-mail từ nhà hay trên đường.

Vấn đề lựa chọn giao thức

Việc lựa chọn giữa IPSec hay SSL/TLS hoặc một vài giao thức khác là một vấn đề khó quyết định, cũng như viễn cảnh sử dụng chúng như thế nào cũng khó có thể nói trước. Dễ thấy là là SSL/TLS có thể làm việc thông qua một tường lửa dựa trên bảng biên dịch địa chỉ NAT, còn IPSec thì không. Nhưng nếu cả hai giao thức làm việc qua tường lửa thì sẽ không dịch được địa chỉ.

IPSec mã hoá tất cả các lưu lượng IP truyền tải giữa hai máy tính, còn SSL/TLS thì đặc tả một ứng dụng. SSL/TLS dùng các hàm mã hoá không đối xứng để thiết lập kết nối và nó bảo vệ hiệu quả hơn so với dùng các hàm mã hoá đối xứng.

Trong các ứng dụng trên thực tế, người quản trị có thể quyết định kết hợp và ghép các giao thức để tạo ra sự cân bằng tốt nhất cho sự thực thi và độ an toàn của mạng. Ví dụ, các client có thể kết nối tới một Web server thông qua tường lửa dùng đường dẫn an toàn của SSL/TLS, Web server có thể kết nối tới một dịch vụ ứng dụng dùng IPSec, và dịch vụ ứng dụng có thể kết nối tới một cơ sở dữ liệu thông qua các tường lửa khác cũng dùng SSL

1.3.3 Các mô hình VPN

[3] Có hai mô hình triển khai VPN là: dựa trên khách hàng (Customer-based) và dựa trên mạng (Network-based). Mô hình dựa trên khách hàng còn được gọi là *mô hình chồng lấn (overlay)*, trong đó VPN được cấu hình trên các thiết bị của khách hàng và sử dụng các giao thức đường hầm xuyên qua mạng công cộng. Nhà cung cấp dịch vụ sẽ bán các mạch ảo giữa các site của khách hàng như là đường kết nối thuê riêng (leased line).

Mô hình dựa trên mạng còn được gọi là mô hình ngang hàng hay *ngang cấp (peer-to-peer)*, trong đó VPN được cấu hình trên các thiết bị của nhà cung cấp dịch vụ và được quản lý bởi nhà cung cấp dịch vụ. Nhà cung cấp dịch vụ và khách hàng trao đổi thông tin định tuyến lớp 3, sau đó nhà cung cấp sẽ sắp đặt dữ liệu từ các site khách hàng vào đường đi tối ưu nhất mà không cần có sự tham gia của khách hàng

1.3.3.1 Mô hình chồng lấn

Mô hình VPN chồng lấn ra đời từ rất sớm và được triển khai bằng nhiều công nghệ khác nhau. Ban đầu, VPN được xây dựng bằng cách sử dụng các đường thuê riêng để cung cấp kết nối giữa khách hàng ở nhiều vị trí khác nhau. Khách hàng mua dịch vụ đường thuê riêng của nhà cung cấp. Các đường thuê này được thiết lập giữa các site của khách hàng cần kết nối và là đường dành riêng cho khách hàng

Khi Frame Relay ra đời, nó được xem như là một công nghệ hỗ trợ tốt cho VPN vì đáp ứng được yêu cầu kết nối cho khách hàng như dịch vụ đường thuê riêng. Điểm khác là ở chỗ khách hàng không được cung cấp các đường dành riêng, mà sẽ sử dụng một đường chung nhưng được chỉ định sử dụng các mạch ảo. Các mạch ảo này đảm bảo lưu lượng cho mỗi khách hàng là riêng biệt. Mạch ảo có thể gồm mạch ảo cố định PVC và mạch ảo chuyển mạch SVC

Cung cấp mạch ảo cho khách hàng nghĩa là nhà cung cấp dịch vụ đã xây dựng một đường hầm riêng cho lưu lượng khách hàng truyền qua mạng dùng chung của nhà cung cấp dịch vụ. Khách hàng thiết lập phiên liên lạc giữa các thiết bị phía khách hàng CPE qua kênh ảo. Giao thức định tuyến chạy trực tiếp giữa các bộ định tuyến khách hàng thiết lập mối quan hệ cận kề và trao đổi thông tin định tuyến với nhau. Nhà cung cấp dịch vụ không hề biết đến thông tin định tuyến của khách hàng. Nhiệm vụ của nhà cung cấp dịch vụ trong mô hình này chỉ là đảm bảo vận chuyển dữ liệu điểm-điểm giữa các site của khách hàng mà thôi.

VPN chồng lấn còn được triển khai dưới dạng đường hầm. Sự thành công của công nghệ IP đã thúc đẩy các nhà cung cấp dịch vụ triển khai VPN qua IP. Nếu khách hàng nào muốn xây dựng mạng riêng của họ qua Internet thì có thể dùng giải pháp này vì chi phí thấp. Bên cạnh lý do kinh tế, mô hình đường hầm còn đáp ứng cho khách hàng việc bảo mật dữ liệu. Hai công nghệ VPN đường hầm phổ biến là IPSec (IP Security) và GRE (Generic Routing Encapsulation).

Các cam kết về QoS trong mô hình VPN chồng lấn thường là cam kết về băng thông tối đa (đỉnh) trên một VC. Giá trị này được gọi là CIR (Committed Information

Rate). Băng thông có thể sử dụng được trên một kênh ảo gọi là PIR (Peak Information Rate). Việc cam kết băng thông được thực hiện thông qua các thống kê của dịch vụ lớp 2 nhưng lại phụ thuộc vào chiến lược của nhà cung cấp. Điều này có nghĩa là tốc độ cam kết không thật sự được bảo đảm. Thường thì nhà cung cấp có thể đảm bảo tốc độ nhỏ nhất MIR (Minimum Information Rate).

Cam kết về băng thông cũng chỉ là cam kết cho hai điểm trong mạng khách hàng. Nếu không có ma trận lưu lượng đầy đủ cho tất cả các lớp lưu lượng thì thật khó có thể thực hiện cam kết này cho khách hàng trong mô hình chồng lấn. Và thật khó để cung cấp nhiều lớp dịch vụ vì nhà cung cấp dịch vụ không thể phân biệt được lưu lượng ở giữa mạng. Vấn đề này có thể được khắc phục bằng cách tạo ra nhiều kết nối (full-mesh), như trong mạng Frame Relay hay ATM có các PVC giữa các site khách hàng. Tuy nhiên, kết nối đầy đủ thường làm tăng thêm chi phí của mạng.

Mô hình VPN chồng lấn có ưu điểm là dễ thực hiện, theo quan điểm của cả khách hàng và nhà cung cấp dịch vụ. Trong mô hình này nhà cung cấp dịch vụ không tham gia vào định tuyến lưu lượng khách hàng. Nhiệm vụ của họ là vận chuyển dữ liệu điểm-điểm giữa các site của khách hàng. Việc đánh dấu điểm tham chiếu giữa nhà cung cấp dịch vụ và khách hàng sẽ cho phép quản lý dễ dàng hơn.

Mô hình chồng lấn thích hợp cho các mạng không cần độ dự phòng với ít site trung tâm và nhiều site ở đầu xa, nhưng lại khó quản lý nếu như cần nhiều kết nối kiểu mắt lưới. Việc cung cấp nhiều VC đòi hỏi phải có sự hiểu biết cặn kẽ về loại lưu lượng giữa các site, mà điều này thường không thật sự thích hợp. Ngoài ra, khi thực hiện mô hình này với các công nghệ lớp 2 thì sẽ tạo ra một lớp mới không cần thiết đối với các nhà cung cấp hầu hết chỉ dựa trên IP, và như vậy làm tăng thêm chi phí hoạt động của mạng.

1.3.3.2 Mô hình ngang hàng

Để khắc phục các hạn chế của mô hình VPN chồng lấn và tối ưu hóa việc vận chuyển dữ liệu qua mạng đường trục, mô hình VPN ngang hàng đã ra đời. Với mô hình này nhà cung cấp dịch vụ sẽ tham gia vào hoạt động định tuyến của khách hàng. Bộ định tuyến biên mạng nhà cung cấp PE (Provider Edge) thực hiện trao đổi thông tin định tuyến trực tiếp với bộ định tuyến của khách hàng CE (Customer Edge).

Đối với mô hình VPN ngang hàng, việc định tuyến trở nên đơn giản hơn (nhìn từ phía khách hàng) khi bộ định tuyến khách hàng chỉ trao đổi thông tin định tuyến với một hoặc một vài bộ định tuyến biên nhà cung cấp PE. Trong khi ở mô hình VPN chồng lấn, số lượng bộ định tuyến lân cận có thể gia tăng với số lượng lớn. Ngoài ra, do nhà cung cấp dịch vụ biết cấu hình mạng của khách hàng nên có thể thiết lập định tuyến tối ưu cho lưu lượng giữa các site khách hàng.

Việc cung cấp băng thông cũng đơn giản hơn bởi vì khách hàng chỉ phải quan tâm đến băng thông đầu vào và ra ở mỗi site mà không cần phải quan tâm đến toàn bộ lưu lượng từ site này đến site kia như trong mô hình VPN chồng lấn. Khả năng mở rộng trong mô hình VPN ngang hàng dễ dàng hơn vì nhà cung cấp dịch vụ chỉ cần thêm vào một site và thay đổi cấu hình trên bộ định tuyến PE. Trong mô hình chồng

lấn, nhà cung cấp dịch vụ phải tham gia vào toàn bộ tập hợp các kênh ảo VC từ site này đến site khác của VPN khách hàng.

Hạn chế của mô hình VPN ngang hàng là nhà cung cấp dịch vụ phải đáp ứng được định tuyến khách hàng cho đúng và đảm bảo việc hội tụ của mạng khách hàng khi có lỗi liên kết. Ngoài ra, bộ định tuyến P của nhà cung cấp dịch vụ phải mang tất cả các tuyến của khách hàng.

1.3.4 Phân loại VPN và ứng dụng

[3]Mạng riêng ảo VPN cung cấp nhiều khả năng ứng dụng khác nhau. Yêu cầu cơ bản đối với VPN là phải điều khiển được quyền truy nhập của khách hàng, các nhà cung cấp dịch vụ cũng như các đối tượng bên ngoài khác. Dựa vào hình thức ứng dụng và những khả năng mà mạng riêng ảo mang lại, có thể phân chúng thành hai loại như sau:

- VPN truy cập từ xa (Remote Access VPN)
- VPN điểm tới điểm (Site-to-Site VPN)

Trong đó VPN điểm tới điểm lại được chia thành hai loại:

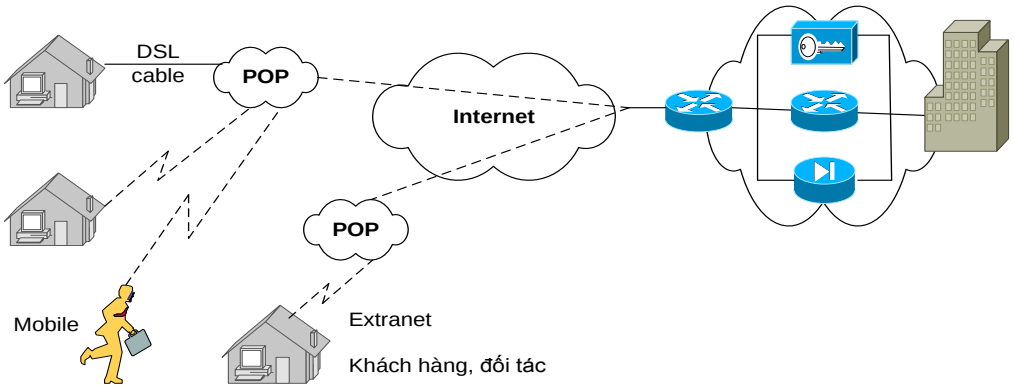
- VPN cục bộ (Intranet VPN)
- VPN mở rộng (Extranet VPN)

1.3.4.1 VPN truy cập từ xa

Các VPN truy nhập từ xa cung cấp khả năng truy nhập từ xa cho người sử dụng (hình 1-3). Tại mọi thời điểm, các nhân viên hay chi nhánh văn phòng di động có thể sử dụng các phần mềm VPN để truy nhập vào mạng của công ty thông qua gateway hoặc bộ tập trung VPN (bản chất là một server). Giải pháp này vì thế còn được gọi là giải pháp client/server. VPN truy nhập từ xa là kiểu VPN điển hình nhất, bởi vì chúng có thể được thiết lập vào bất kể thời điểm nào và từ bất cứ nơi nào có mạng Internet.

VPN truy nhập từ xa mở rộng mạng công ty tới những người sử dụng thông qua cơ sở hạ tầng chia sẻ chung, trong khi những chính sách mạng công ty vẫn duy trì. Chúng có thể dùng để cung cấp truy nhập an toàn cho những nhân viên thường xuyên phải đi lại, những chi nhánh hay những bạn hàng của công ty. Những kiểu VPN này được thực hiện thông qua cơ sở hạ tầng công cộng bằng cách sử dụng công nghệ ISDN, quay số, IP di động, DSL hay công nghệ cáp và thường yêu cầu một vài kiểu phần mềm client chạy trên máy tính của người sử dụng.

Một vấn đề quan trọng là việc thiết kế quá trình xác thực ban đầu để đảm bảo yêu cầu được xuất phát từ một nguồn tin cậy. Thường thì giai đoạn ban đầu này dựa trên cùng một chính sách về bảo mật của công ty. Chính sách này bao gồm một số qui trình kỹ thuật và các ứng dụng chủ, ví dụ như Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+), …



Hình 1 - 3 Mô hình truy cập VPN từ xa

Các ưu điểm của VPN truy nhập từ xa so với các phương pháp truy nhập từ xa truyền thống là:

- VPN truy cập từ xa không cần sự hỗ trợ của nhân viên mạng bởi vì quá trình kết nối từ xa được các ISP thực hiện
- Giảm được các chi phí cho kết nối từ khoảng cách xa bởi vì các kết nối khoảng cách xa được thay thế bởi các kết nối cục bộ thông qua mạng Internet
- Cung cấp dịch vụ kết nối giá rẻ cho những người sử dụng ở xa
- Do kết nối truy nhập là nội bộ nên các modem kết nối hoạt động ở tốc độ cao hơn so với cách truy nhập khoảng cách xa

Mặc dù có nhiều ưu điểm nhưng mạng VPN truy nhập từ xa vẫn còn những nhược điểm cố hữu đi cùng như:

- VPN truy nhập từ xa không hỗ trợ các dịch vụ đảm bảo QoS
- Nguy cơ bị mất dữ liệu cao do các gói có thể không được phân phát đến nơi hoặc bị mất
- Do thuật toán mã hóa phức tạp nên kích thước tiêu đề gói tin giao thức tăng một cách đáng kể

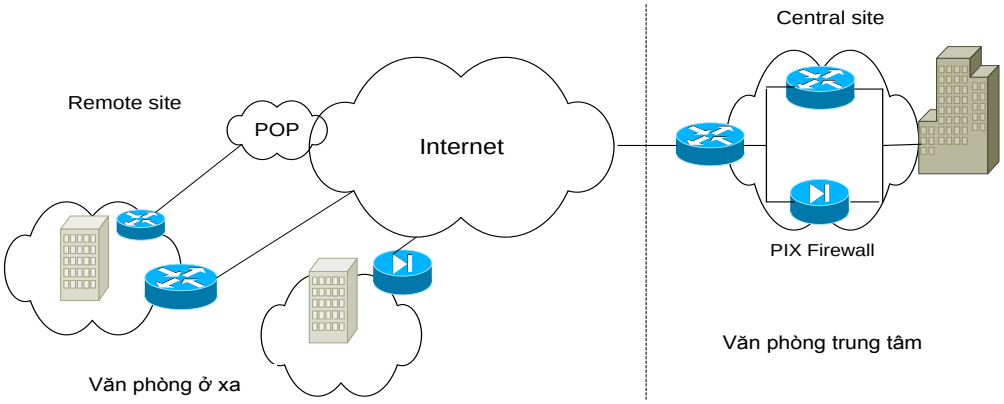
1.3.4.2 VPN điểm tới điểm

VPN điểm tới điểm (Site-to-Site hay LAN-to-LAN) là giải pháp kết nối các hệ thống mạng ở những nơi khác nhau với mạng trung tâm thông qua VPN. Trong tình huống này, quá trình xác thực ban đầu cho người sử dụng sẽ là quá trình xác thực giữa các thiết bị. Các thiết bị này hoạt động như Cổng an ninh (Security Gateway), truyền lưu lượng một cách an toàn từ Site này đến Site kia. Các thiết bị định tuyến hay tường lửa với hỗ trợ VPN đều có khả năng thực hiện kết nối này. Sự khác nhau giữa VPN truy nhập từ xa và VPN điểm tới điểm chỉ mang tính tượng trưng. Nhiều thiết bị VPN mới có thể hoạt động theo cả hai cách này.

VPN điểm tới điểm có thể được xem như một VPN cục bộ hoặc mở rộng xét từ quan điểm quản lý chính sách. Nếu hạ tầng mạng có chung một nguồn quản lý, nó có thể được xem như VPN cục bộ. Ngược lại, nó có thể được coi là mở rộng. Vấn đề truy nhập giữa các điểm phải được kiểm soát chặt chẽ bởi các thiết bị tương ứng.

VPN cục bộ

VPN cục bộ là một dạng cấu hình tiêu biểu của VPN điểm tới điểm, được sử dụng để bảo mật các kết nối giữa các địa điểm khác nhau của một công ty (hình 1-4). Nó liên kết trụ sở chính, các văn phòng, chi nhánh trên một cơ sở hạ tầng chung sử dụng các kết nối luôn được mã hoá bảo mật. Điều này cho phép tất cả các địa điểm có thể truy nhập an toàn các nguồn dữ liệu được phép trong toàn bộ mạng của công ty.



Hình 1 - 4 Mô hình VPN cục bộ

VPN cục bộ cung cấp những đặc tính của mạng WAN như khả năng mở rộng, tính tin cậy và hỗ trợ cho nhiều kiểu giao thức khác nhau với chi phí thấp nhưng vẫn đảm bảo tính mềm dẻo. Những ưu điểm chính của giải pháp VPN cục bộ bao gồm:

- Các mạng cục bộ hay diện rộng có thể được thiết lập thông qua một hay nhiều nhà cung cấp dịch vụ
- Giảm được số nhân viên kỹ thuật hỗ trợ trên mạng đối với những nơi xa
- Do kết nối trung gian được thực hiện thông qua Internet nên nó có thể dễ dàng thiết lập thêm một liên kết ngang hàng mới
- Tiết kiệm chi phí từ việc sử dụng đường hầm VPN thông qua Internet kết hợp với các công nghệ chuyển mạch tốc độ cao

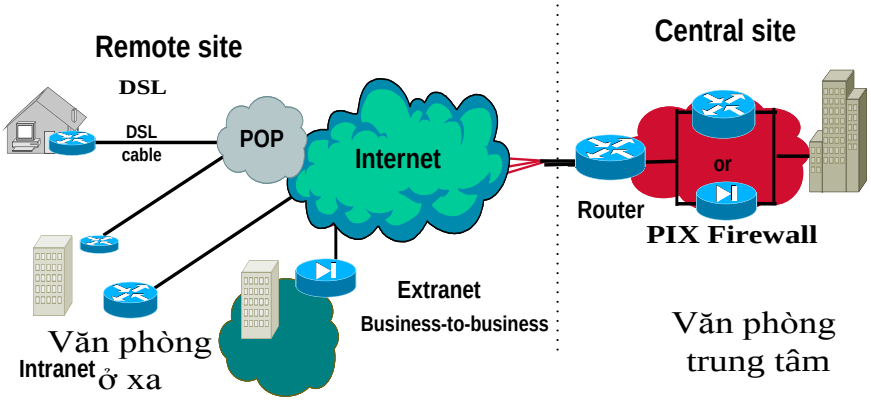
Tuy nhiên giải pháp mạng cục bộ dựa trên VPN cũng có những nhược điểm đi cùng như:

- Do dữ liệu truyền "ngầm" qua mạng công cộng như Internet nên vẫn còn những mối đe dọa về mức độ bảo mật dữ liệu và chất lượng dịch vụ (QoS)
- Khả năng các gói dữ liệu bị mất trong khi truyền dẫn vẫn còn khá cao
- Trường hợp cần truyền khối lượng lớn dữ liệu như đa phương tiện với yêu cầu tốc độ cao và đảm bảo thời gian thực là thách thức lớn trong môi trường Internet

VPN mở rộng

VPN mở rộng được cấu hình như một VPN điểm tới điểm, cung cấp đường hầm bảo mật giữa các khách hàng, nhà cung cấp và đối tác thông qua một cơ sở hạ tầng mạng công cộng (hình 1-5). Kiểu VPN này sử dụng các kết nối luôn được bảo

mật và nó không bị cô lập với thế giới bên ngoài như các trường hợp VPN cục bộ hay truy nhập từ xa.



Hình 1 - 5 Mô hình VPN mở rộng

Giải pháp VPN mở rộng cung cấp khả năng điều khiển truy nhập tới những nguồn tài nguyên mạng cần thiết để mở rộng tới những đối tượng kinh doanh. Sự khác nhau giữa VPN cục bộ và VPN mở rộng là sự truy nhập mạng được công nhận ở một trong hai đầu cuối của VPN.

Những ưu điểm chính của mạng VPN mở rộng bao gồm:

- Chi phí cho VPN mở rộng thấp hơn nhiều so với các giải pháp kết nối khác để cùng đạt được một mục đích như vậy
- Dễ dàng thiết lập, bảo trì và thay đổi đối với các mạng đang hoạt động
- Do VPN mở rộng được xây dựng trên mạng Internet nên có nhiều cơ hội trong việc cung cấp dịch vụ và chọn lựa giải pháp phù hợp với các nhu cầu của từng công ty
- Các kết nối Internet được nhà cung cấp dịch vụ Internet bảo trì nên có thể giảm được số lượng nhân viên kỹ thuật hỗ trợ mạng, và do vậy giảm được chi phí vận hành của toàn mạng

Bên cạnh những ưu điểm trên, giải pháp VPN mở rộng cũng còn những nhược điểm đi cùng như:

- Vấn đề bảo mật thông tin khó khăn hơn trong môi trường mở rộng như vậy, và điều này làm tăng nguy cơ rủi ro đối với mạng cục bộ của công ty
- Khả năng mất mát dữ liệu trong khi truyền qua mạng công cộng vẫn tồn tại
- Việc truyền khối lượng lớn dữ liệu với yêu cầu tốc độ cao và thời gian thực vẫn còn là một thách thức lớn cần giải quyết

1.3.4.3 Ứng dụng VPN

Cả VPN truy nhập từ xa và VPN điểm tới điểm đều cung cấp giải pháp để xây dựng mạng riêng ảo cho doanh nghiệp. Các công ty có thể mở rộng mạng ra những nơi mà trước đây không thể mở rộng. Trong nhiều ứng dụng, VPN cho phép tiết kiệm chi phí một cách đáng kể. Thay vì cần nhiều kết nối đến cùng trụ sở chính, giải pháp VPN tích hợp lưu lượng vào một kết nối duy nhất, tạo ra cơ hội để giảm chi phí cả bên trong và bên ngoài doanh nghiệp.

Mạng Internet hiện nay là một hạ tầng tốt, cho phép doanh nghiệp thay đổi mạng của họ theo nhiều chiều hướng. Đối với các công ty lớn có thể dễ dàng nhận thấy rằng các kết nối WAN qua kênh thuê riêng là rất tốn kém và đang dần được thay thế bởi kết nối VPN. Đối với dịch vụ truy nhập từ xa, thay vì dùng các đường kết nối tốc độ chậm hoặc các dịch vụ kênh thuê riêng đắt tiền, người sử dụng bây giờ đã có thể được cung cấp các dịch vụ truy nhập tốc độ cao với giá thành rẻ. Ngoài ra, những người dùng cơ động cũng có thể tận dụng các kết nối tốc độ cao Ethernet trong các khách sạn, sân bay hay nơi công cộng để phục vụ cho công việc của mình một cách hiệu quả. Chỉ riêng yếu tố cắt giảm chi phí cuộc gọi đường dài trong trường hợp này cũng đã là một lý do rất thuyết phục để sử dụng VPN.

Một trong những lợi ích khác của VPN là giúp các công ty có thể triển khai nhiều ứng dụng mới trên nền thương mại điện tử (e-Commerce) một cách nhanh chóng. Tuy nhiên, trong trường hợp này một vài yếu tố cũng cần phải được xem xét một cách cẩn thận. Các trở ngại chính của Internet là bảo mật, chất lượng dịch vụ, độ tin cậy và khả năng quản lý.

1.4 Kết luận chương

Các kỹ thuật mạng được trình bày ở chương này là cơ sở hạ tầng cho việc truyền thông và là nền tảng của các công nghệ mạng dựa trên IP như MPLS hay các mạng riêng ảo (VPN). Chương này cũng trình bày những khái niệm cơ bản về VPN, các chức năng và đặc điểm của VPN, từ đó làm cơ sở phân loại VPN và đưa ra các thuận lợi cũng như khó khăn khi sử dụng các loại hình VPN khác nhau.

CHƯƠNG 2. CÁC GIAO THỨC ĐƯỜNG HẦM

[7] Có thể nói đường hầm là một trong những khái niệm nền tảng của VPN. Giao thức đường hầm thực hiện việc đóng gói dữ liệu với các phần tiêu đề tương ứng để truyền qua mạng Internet. Trong chương này giới thiệu về các giao thức đường hầm phổ biến đang tồn tại hiện nay và sử dụng cho VPN trên nền IP bao gồm PPTP, L2TP, IPSec.

2.1 Giới thiệu các giao thức đường hầm

Các giao thức đường hầm là nền tảng của công nghệ VPN. Có nhiều giao thức đường hầm khác nhau và việc sử dụng giao thức nào liên quan đến các phương pháp xác thực và mã hóa đi kèm. Các giao thức đường hầm phổ biến gồm:

- *Giao thức chuyển tiếp lớp 2* (L2F – Layer Two Forwarding)
- *Giao thức đường hầm điểm tới điểm* (PPTP – Point to Point Tunneling Protocol)
- *Giao thức đường hầm lớp 2* (L2TP – Layer Two Tunneling Protocol)
- *Giao thức bảo mật IP* (IPSec – Internet Protocol Security)

L2F và PPTP đều được phát triển dựa trên giao thức PPP (Point to Point Protocol). PPP là một giao thức truyền thông nối tiếp lớp 2, có thể sử dụng để đóng gói dữ liệu liên mạng IP và hỗ trợ đa giao thức lớp trên. Giao thức L2F do Cisco phát triển độc lập, còn PPTP là do nhiều công ty hợp tác phát triển. Trên cơ sở L2F và PPTP, IETF đã phát triển giao thức đường hầm L2TP. Hiện nay các giao thức PPTP và L2TP được sử dụng còn giao thức L2F hầu như không còn được dùng

Trong các giao thức đường hầm nói trên, IPSec là giải pháp tối ưu về mặt an ninh dữ liệu. Nó hỗ trợ các phương pháp xác thực và mật mã mạnh nhất. Ngoài ra, IPSec còn có tính linh hoạt cao, không bị ràng buộc bởi bất cứ thuật toán xác thực hay mật mã nào. IPSec có thể sử dụng đồng thời cùng với các giao thức đường hầm khác để tăng tính an toàn cho hệ thống. Tuy nhiên để tận dụng khả năng đảm bảo an ninh dữ liệu của IPSec thì cần phải sử dụng cơ sở hạ tầng khóa công khai PKI (Pulic Key Infrastructure) phức tạp để giải quyết các vấn đề như chứng thực số hay chữ ký số

Khác với IPSec, các giao thức PPTP và L2TP là các chuẩn đã được hoàn thiện, nên sản phẩm hỗ trợ chúng tương đối phổ biến. PPTP có thể triển khai với một hệ thống mật khẩu đơn giản mà không cần sử dụng PKI. Ngoài ra, PPTP và L2TP còn có một số ưu điểm khác so với IPSec như khả năng hỗ trợ đa giao thức lớp trên

2.2 Giao thức đường hầm điểm tới điểm – PPTP

Giao thức đường hầm điểm tới điểm được đưa ra đầu tiên bởi một nhóm các công ty được gọi là PPTP Forum. Ý tưởng cơ sở của giao thức này là tách các chức năng chung và riêng của truy nhập từ xa, lợi dụng cơ sở hạ tầng Internet sẵn có để tạo kết nối bảo mật giữa người dùng ở xa (client) và mạng riêng. Người dùng ở xa chỉ việc quay số tới nhà cung cấp dịch vụ Internet địa phương là có thể tạo đường hầm bảo mật tới mạng riêng của họ.

Giao thức PPTP được xây dựng dựa trên chức năng của PPP, cung cấp khả năng quay số truy nhập tạo ra một đường hầm bảo mật thông qua Internet đến site đích.

PPTP sử dụng giao thức đóng gói định tuyến chung GRE được mô tả lại để đóng và tách gói PPP. Giao thức này cho phép PPTP mềm dẻo xử lý các giao thức khác không phải IP như IPX, NETBEUI.

2.2.1 Hoạt động của PPTP

PPP đã trở thành giao thức truy nhập vào Internet và các mạng IP rất phổ biến hiện nay. Làm việc ở lớp liên kết dữ liệu trong mô hình OSI, PPP bao gồm các phương thức đóng, tách gói cho các loại gói dữ liệu khác nhau để truyền nối tiếp. PPP có thể đóng các gói IP, IPX, NETBEUI và truyền đi trên kết nối điểm-điểm từ máy gửi đến máy nhận.

PPTP đóng gói các khung dữ liệu của giao thực PPP vào các IP datagram để truyền qua mạng IP (Internet hoặc Intranet). PPTP dùng một kết nối TCP (gọi là kết nối điều khiển PPTP) để khởi tạo, duy trì, kết thúc đường hầm, và một phiên bản của giao thức GRE để đóng gói các khung PPP. Phần tải tin của khung PPP có thể được mật mã và/hoặc nén.

PPTP sử dụng PPP để thực hiện các chức năng:

- Thiết lập và kết thúc kết nối vật lý
- Xác thực người dùng
- Tạo các gói dữ liệu PPP

PPTP giả định tồn tại một mạng IP giữa PPTP client (VPN client sử dụng PPTP) và PPTP server (VPN server sử dụng PPTP). PPTP client có thể được nối trực tiếp qua việc quay số tới máy chủ truy nhập mạng NAS để thiết lập kết nối IP. Khi một kết nối PPP được thiết lập thì người dùng thường đã được xác thực. Đây là giai đoạn tuỳ chọn trong PPP, tuy nhiên nó luôn luôn được cung cấp bởi các ISP.

Việc xác thực trong quá trình thiết lập kết nối dựa trên PPTP sử dụng các cơ chế xác thực của kết nối PPP. Các cơ chế xác thực đó có thể là:

- *EAP (Extensible Authentication Protocol)* – Giao thức xác thực mở rộng
- *CHAP (Challenge Handshake Authentication Protocol)* – Giao thức xác thực đòi hỏi bắt tay
- *PAP (Password Authentication Protocol)* – Giao thức xác thực mật khẩu

Với PAP mật khẩu được gửi qua kết nối dưới dạng văn bản đơn giản và không có bảo mật. CHAP là một giao thức xác thực mạnh hơn, sử dụng phương thức bắt tay ba chiều. CHAP chống lại các vụ tấn công quay lại bằng cách sử dụng các giá trị thách đố (Challenge Value) duy nhất và không thể đoán trước được.

PPTP cũng thừa hưởng việc mật mã và/hoặc nén phần tải tin của PPP. Để mật mã phần tải tin PPP có thể sử dụng phương thức mã hoá điểm tới điểm MPPE (Microsoft Point to Point Encryption). MPPE chỉ cung cấp mật mã mức truyền dẫn, không cung cấp mật mã đầu cuối đến đầu cuối. Nếu cần sử dụng mật mã đầu cuối đến đầu cuối thì có thể sử dụng IPSec để mật mã lưu lượng IP giữa các đầu cuối sau khi đường hầm PPTP đã được thiết lập.

Sau khi PPP thiết lập kết nối, PPTP sử dụng các quy luật đóng gói của PPP để đóng các gói truyền trong đường hầm. Để tận dụng ưu điểm của kết nối tạo ra bởi PPP, PPTP định nghĩa hai loại gói là điều khiển và dữ liệu, sau đó gán chúng vào hai kênh riêng là kênh điều khiển và kênh dữ liệu. PPTP phân tách các kênh điều khiển và kênh và kênh dữ liệu thành luồng điều khiển với giao thức TCP và luồng dữ liệu với giao thức IP. Kết nối TCP tạo giữa máy trạm PPTP (client) và máy chủ PPTP (server) được sử dụng để truyền thông báo điều khiển.

Các gói dữ liệu là dữ liệu thông thường của người dùng. Các gói điều khiển được gửi theo chu kỳ để lấy thông tin về trạng thái kết nối và quản lý báo hiệu giữa ứng dụng khách PPTP và máy chủ PPTP. Các gói điều khiển cũng được dùng để gửi các thông tin quản lý thiết bị, thông tin cấu hình giữa hai đầu đường hầm.

Kênh điều khiển được yêu cầu cho việc thiết lập một đường hầm giữa máy trạm và máy chủ PPTP. Máy chủ PPTP là một server sử dụng giao thức PPTP với một giao diện nối với Internet và một giao diện khác nối với Intranet, còn phần mềm client có thể nằm ở máy người dùng từ xa hoặc tại máy chủ của ISP.

2.2.2 Duy trì đường hầm bằng kết nối điều khiển PPTP

Kết nối điều khiển PPTP là kết nối giữa địa chỉ IP của máy trạm PPTP (có cổng TCP được cấp phát động) và địa chỉ IP của máy chủ PPTP (sử dụng cổng TCP dành riêng 1723). Kết nối điều khiển PPTP mang các bản tin điều khiển và quản lí được sử dụng để duy trì đường hầm PPTP. Các bản tin này bao gồm PPTP Echo-Request và PPTP Echo-Reply định kỳ để phát hiện các lỗi kết nối giữa máy trạm và máy chủ PPTP. Các gói của kết nối điều khiển PPTP bao gồm tiêu đề IP, tiêu đề TCP, bản tin điều khiển PPTP và tiêu đề, phần đuôi của lớp liên kết dữ liệu (hình 2-1).

Tiêu đề liên kết dữ liệu	Tiêu đề IP	Tiêu đề TCP	Bản tin điều khiển PPTP	Phần đuôi liên kết dữ liệu

Hình 2 - 1 Gói dữ liệu kết nối điều khiển PPTP

2.2.3 Đóng gói dữ liệu đường hầm PPTP

Đóng gói khung PPTP và GRE

Dữ liệu đường hầm PPTP được đóng gói thông qua nhiều mức. Hình 2-2 là cấu trúc dữ liệu đã được đóng gói.

Tiêu đề liên kết dữ liệu	Tiêu đề IP	Tiêu đề GRE	Tiêu đề PPP	Tải PPP được mã hoá (IP, IPX, NETBEUI)	Phần đuôi liên kết dữ liệu

Hình 2 - 2 Đóng gói dữ liệu đường hầm PPTP

Phần tải của khung PPP ban đầu được mật mã và đóng gói với tiêu đề PPP để tạo ra khung PPP. Khung PPP sau đó được đóng gói với phần tiêu đề của phiên bản giao thức GRE sửa đổi.

GRE là giao thức đóng gói chung, cung cấp cơ chế đóng gói dữ liệu để định tuyến qua mạng IP. Đối với PPTP, phần tiêu đề của GRE được sửa đổi một số điểm như sau:

- Một trường xác nhận dài 32 bit được thêm vào
- Một bit xác nhận được sử dụng để chỉ định sự có mặt của trường xác nhận 32 bit
- Trường *Key* được thay thế bằng trường *độ dài Payload* 16 bit và trường *chỉ số cuộc gọi* 16 bit. Trường chỉ số cuộc gọi được thiết lập bởi máy trạm PPTP trong quá trình khởi tạo đường hầm PPTP

Đóng gói IP

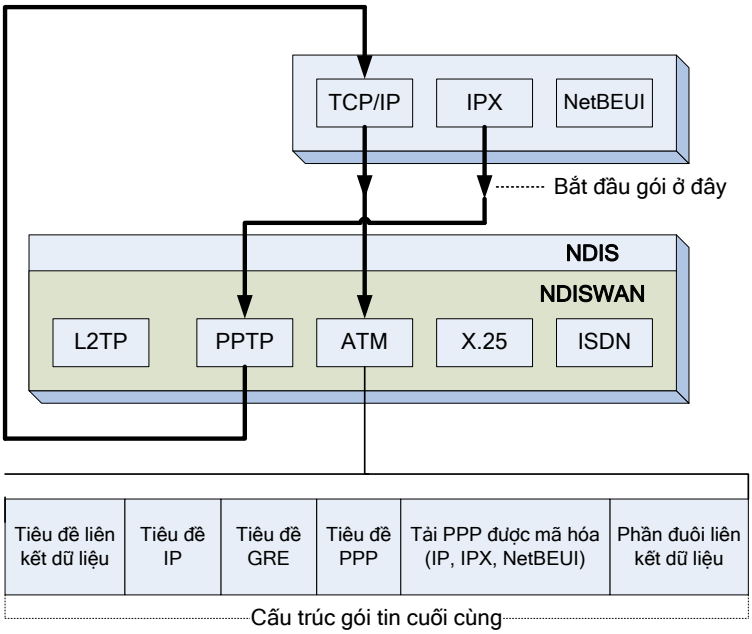
Phần tải PPP (đã được mật mã) và các tiêu đề GRE sau đó được đóng gói với một tiêu đề IP chứa các thông tin địa chỉ nguồn và đích thích hợp cho máy trạm và máy chủ PPTP.

Đóng gói lớp liên kết dữ liệu

Để có thể truyền qua mạng LAN hoặc WAN, gói IP cuối cùng sẽ được đóng gói với một tiêu đề và phần đuôi của lớp liên kết dữ liệu ở giao diện vật lý đầu ra. Ví dụ, nếu gói IP được gửi qua giao diện Ethernet, nó sẽ được gói với phần tiêu đề và đuôi Ethernet. Nếu gói IP được gửi qua đường truyền WAN điểm tới điểm (như đường điện thoại tương tự hoặc ISDN), nó sẽ được đóng gói với phần tiêu đề và đuôi của giao thức PPP.

Sơ đồ đóng gói

Hình 2-3 là ví dụ sơ đồ đóng gói PPTP từ một máy trạm qua kết nối truy nhập VPN từ xa sử dụng modem tương tự.



Hình 2 - 3 Sơ đồ đóng gói PPTP

Quá trình đóng gói được mô tả cụ thể như sau:

- Các gói IP, IPX hoặc khung NetBEUI được đưa tới giao diện ảo đại diện cho kết nối VPN bằng giao thức tương ứng sử dụng NDIS (Network Driver Interface Specification).
- NDIS đưa gói dữ liệu tới NDISWAN, nơi thực hiện mã hóa, nén dữ liệu và cung cấp tiêu đề PPP. Phần tiêu đề PPP này chỉ gồm trường mã số giao thức PPP (PPP Protocol ID Field), không có các trường Flags và FCS (Frame Check Sequence). Giả định trường địa chỉ và điều khiển đã được thỏa thuận ở giao thức điều khiển đường truyền LCP (Link Control Protocol) trong quá trình kết nối PPP.
- NDISWAN gửi dữ liệu tới giao thức PPTP, nơi đóng gói khung PPP với phần tiêu đề GRE. Trong tiêu đề GRE, trường chỉ số cuộc gọi được đặt giá trị thích hợp để xác định đường hầm.
- Giao thức PPTP sau đó sẽ gửi gói vừa hình thành tới TCP/IP.
- TCP/IP đóng gói dữ liệu đường hầm PPTP với phần tiêu đề IP, sau đó gửi kết quả tới giao diện đại diện cho kết nối quay số tới ISP cục bộ sử dụng NDIS.
- NDIS gửi gói tin tới NDISWAN, nơi cung cấp các phần tiêu đề và đuôi PPP.
- NDISWAN gửi khung PPP kết quả tới cổng WAN tương ứng đại diện cho phần cứng quay số (ví dụ, cổng không đồng bộ cho kết nối modem).

2.2.4 Xử lý dữ liệu tại đầu cuối đường hầm PPTP

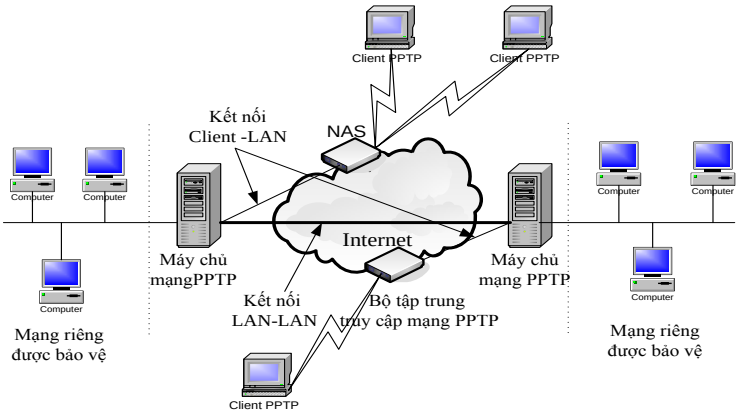
Khi nhận được dữ liệu đường hầm PPTP, máy trạm và máy chủ PPTP sẽ thực hiện các bước sau:

- Xử lý và loại bỏ phần tiêu đề và đuôi của lớp liên kết dữ liệu;
- Xử lý và loại bỏ tiêu đề IP;
- Xử lý và loại bỏ tiêu đề GRE và PPP;
- Giải mã và/hoặc giải nén phần tải PPP (nếu cần thiết);
- Xử lý phần tải tin để nhận hoặc chuyển tiếp.

2.2.5 Triển khai VPN dựa trên PPTP

Để triển khai VPN dựa trên giao thức PPTP yêu cầu hệ thống tối thiểu phải có các thành phần thiết bị như chỉ ra trên hình 2-4, cụ thể bao gồm:

- Một máy chủ truy nhập mạng dùng cho phương thức quay số truy nhập bảo mật vào VPN;
- Một máy chủ PPTP;
- Máy trạm PPTP với phần mềm client cần thiết.



Hình 2 - 4 Các thành phần của hệ thống cung cấp VPN dựa trên PPTP

Các máy chủ PPTP có thể đặt tại mạng của khách hàng và do nhân viên trong công ty quản lý.

Máy chủ PPTP

Máy chủ PPTP thực hiện hai chức năng chính: đóng vai trò là điểm kết nối của đường hầm PPTP và chuyển các gói đến từ đường hầm tới mạng LAN riêng. Máy chủ PPTP chuyển các gói đến máy đích bằng cách xử lý gói PPTP để có được địa chỉ mạng của máy tính đích. Máy chủ PPTP cũng có khả năng lọc gói. Bằng cách sử dụng cơ chế lọc gói PPTP máy chủ có thể ngăn cấm, chỉ cho phép truy nhập vào Internet, mạng riêng hay cả hai.

Thiết lập máy chủ PPTP tại site mạng có một hạn chế nếu như máy chủ PPTP nằm sau tường lửa. PPTP được thiết kế sao cho chỉ có một cổng TCP 1723 được sử dụng để chuyển dữ liệu đi. Sự khiếm khuyết của cấu hình cổng này có thể làm cho tường lửa dễ bị tấn công hơn. Nếu như tường lửa được cấu hình để lọc gói thì phải thiết lập nó cho phép GRE đi qua.

Phần mềm client PPTP

Nếu như các thiết bị của ISP đã hỗ trợ PPTP thì không cần phần cứng hay phần mềm bổ sung nào cho các máy trạm, chỉ cần một kết nối PPP chuẩn. Nếu như các thiết bị của ISP không hỗ trợ PPTP thì một phần mềm ứng dụng client vẫn có thể tạo kết nối bảo mật bằng cách đầu tiên quay số kết nối tới ISP bằng PPP, sau đó quay số một lần nữa thông qua cổng PPTP ảo được thiết lập ở máy trạm.

Phần mềm client PPTP đã có sẵn trong Windows 9x, NT và các hệ điều hành sau này. Khi chọn client PPTP cần phải so sánh các chức năng của nó với máy chủ PPTP đã có. Không phải tất cả các phần mềm client PPTP đều hỗ trợ MS-CHAP, nếu thiếu công cụ này thì không thể tận dụng được ưu điểm mã hoá trong RRAS.

Máy chủ truy cập mạng

Máy chủ truy nhập mạng NAS (Network Access Server) còn có tên gọi khác là máy chủ truy nhập từ xa RAS (Remote Access Server) hay bộ tập trung truy nhập (Access Concentrator). NAS cung cấp khả năng truy nhập đường dây dựa trên phần

mềm, có khả năng tính cước và có khả năng chịu đựng lỗi tại ISP POP. NAS của ISP được thiết kế cho phép một số lượng lớn người dùng có thể quay số truy nhập vào cùng một lúc.

Nếu một ISP cung cấp dịch vụ PPTP thì cần phải cài một NAS cho phép PPTP để hỗ trợ các client chạy trên các nền khác nhau như Unix, Windows, Macintosh, v.v. Trong trường hợp này, máy chủ ISP đóng vai trò như một client PPTP kết nối với máy chủ PPTP tại mạng riêng và máy chủ ISP trở thành một điểm cuối của đường hầm, điểm cuối còn lại là máy chủ tại đầu mạng riêng.

2.2.6 Ưu nhược điểm và ứng dụng của PPTP

Ưu điểm của PPTP là được thiết kế để hoạt động ở lớp 2 (liên kết dữ liệu) trong khi IPSec chạy ở lớp 3 của mô hình OSI. Bằng cách hỗ trợ việc truyền dữ liệu ở lớp 2, PPTP có thể truyền trong đường hầm bằng các giao thức khác IP trong khi IPSec chỉ có thể truyền các gói IP trong đường hầm.

Tuy nhiên, PPTP là một giải pháp tạm thời vì hầu hết các nhà cung cấp đều có kế hoạch thay thế PPTP bằng L2TP khi mà giao thức này đã được chuẩn hoá. PPTP thích hợp cho quay số truy nhập với số lượng người dùng giới hạn hơn là cho VPN kết nối LAN-LAN. Một vấn đề của PPTP là xử lý xác thực người dùng thông qua Windows NT hay thông qua RADIUS. Máy chủ PPTP cũng quá tải với một số lượng người dùng quay số truy nhập hay một lưu lượng lớn dữ liệu truyền qua, mà điều này là một yêu cầu của kết nối LAN-LAN.

Khi sử dụng VPN dựa trên PPTP mà có hỗ trợ thiết bị của ISP thì một số quyền quản lý phải chia sẻ cho ISP. Tính bảo mật của PPTP không mạnh bằng IPSec. Tuy nhiên, quản ý bảo mật trong PPTP lại đơn giản hơn.

2.3 Giao thức đường hầm lớp 2 – L2TP

2.3.1 Hoạt động của L2TP

Để tránh việc hai giao thức đường hầm không tương thích cùng tồn tại gây khó khăn cho người sử dụng, IETF đã kết hợp hai giao thức L2F và PPTP và phát triển thành L2TP. L2TP được xây dựng trên cơ sở tận dụng các ưu điểm của cả PPTP và L2F, đồng thời có thể sử dụng được trong tất cả các trường hợp ứng dụng của hai giao thức này. L2TP được mô tả trong khuyến nghị RFC 2661.

Một đường hầm L2TP có thể khởi tạo từ một PC ở xa quay về L2TP Network Server (LNS) hay từ L2TP Access Concentrator (LAC) về LNS. Mặc dù L2TP vẫn dùng PPP, nó định nghĩa cơ chế tạo đường hầm của riêng nó, tùy thuộc vào phương tiện truyền chứ không dùng GRE

L2TP đóng gói các khung PPP để truyền qua mạng IP, X.25, Frame Relay hoặc ATM. Tuy nhiên, hiện nay mới chỉ có L2TP trên mạng IP được định nghĩa. Khi truyền qua mạng IP, các khung L2TP được đóng gói như các bản tin UDP. L2TP có thể được sử dụng như một giao thức đường hầm thông qua Internet hoặc các mạng riêng Intranet. L2TP dùng các bản tin UDP qua mạng IP cho các dữ liệu đường hầm cũng như các dữ liệu duy trì đường hầm. Phần tải của khung PPP đã đóng gói có thể được mật mã và nén. Mật mã trong các kết nối L2TP thường được thực hiện bởi IPSec ESP

(chứ không phải MPPE như đối với PPTP). Cũng có thể tạo kết nối L2TP không sử dụng mật mã IPSec. Tuy nhiên, đây không phải là kết nối IP-VPN vì dữ liệu riêng được đóng gói bởi L2TP không được mật mã. Các kết nối L2TP không mật mã có thể sử dụng tạm thời để sửa các lỗi kết nối L2TP dùng IPSec.

L2TP giả định tồn tại mạng IP giữa máy trạm (VPN client dùng giao thức đường hầm L2TP và IPSec) và máy chủ L2TP. Máy trạm L2TP có thể được nối trực tiếp với mạng IP để truy nhập tới máy chủ L2TP hoặc gián tiếp thông qua việc quay số tới máy chủ truy nhập mạng NAS để thiết lập kết nối IP. Việc xác thực trong quá trình hình thành đường hầm L2TP phải sử dụng các cơ chế xác thực trong kết nối PPP như EAP, MS-CHAP, CHAP, PAP. Máy chủ L2TP là máy chủ IP-VPN sử dụng giao thức L2TP với một giao diện nối với Internet và một giao diện khác nối với mạng Intranet.

L2TP có thể dùng hai kiểu bản tin là điều khiển và dữ liệu. Các bản tin điều khiển chịu trách nhiệm thiết lập, duy trì và hủy các đường hầm. Các bản tin dữ liệu được sử dụng để đóng gói các khung PPP được chuyển trên đường hầm. Các bản tin điều khiển dùng cơ chế điều khiển tin cậy bên trong L2TP để đảm bảo việc phân phối, trong khi các bản tin dữ liệu không được gửi lại khi bị mất trên đường truyền.

2.3.2 Duy trì đường hầm bằng bản tin điều khiển L2TP

Không giống PPTP, việc duy trì đường hầm L2TP không được thực hiện thông qua một kết nối TCP riêng biệt. Các lưu lượng điều khiển và duy trì cuộc gọi được gửi đi như các bản tin UDP giữa máy trạm và máy chủ L2TP (đều sử dụng cổng UDP 1701).

Các bản tin điều khiển L2TP qua mạng IP được gửi như các gói UDP. Gói UDP lại được mật mã bởi IPSec ESP như trên hình 2-5

Hình 2 - 5 Bản tin điều khiển L2TP

Vì không sử dụng kết nối TCP, L2TP dùng thứ tự bản tin để đảm bảo việc truyền các bản tin L2TP. Trong bản tin điều khiển L2TP, trường Next-Received (tương tự như TCP Acknowledgment) và Next-Sent (tương tự như TCP Sequence Number) được sử dụng để duy trì thứ tự các bản tin điều khiển. Các gói không đúng thứ tự bị loại bỏ. Các trường Next-Sent và Next-Received cũng có thể được sử dụng để truyền dẫn tuần tự và điều khiển luồng cho các dữ liệu đường hầm.

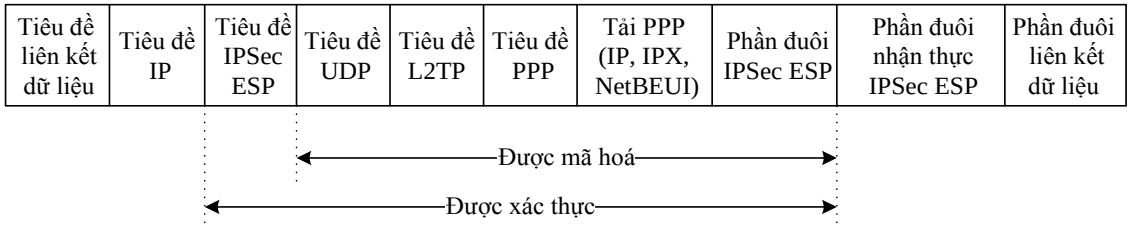
L2TP hỗ trợ nhiều cuộc gọi trên mỗi đường hầm. Trong bản tin điều khiển L2TP và phần tiêu đề L2TP của dữ liệu đường hầm có một mã số đường hầm (Tunnel ID) để xác định đường hầm, và một mã nhận dạng cuộc gọi (Call ID) để xác định cuộc gọi trong đường hầm đó.

2.3.3 Đóng gói dữ liệu đường hầm L2TP

Dữ liệu đường hầm L2TP được thực hiện thông qua nhiều mức đóng gói như sau:

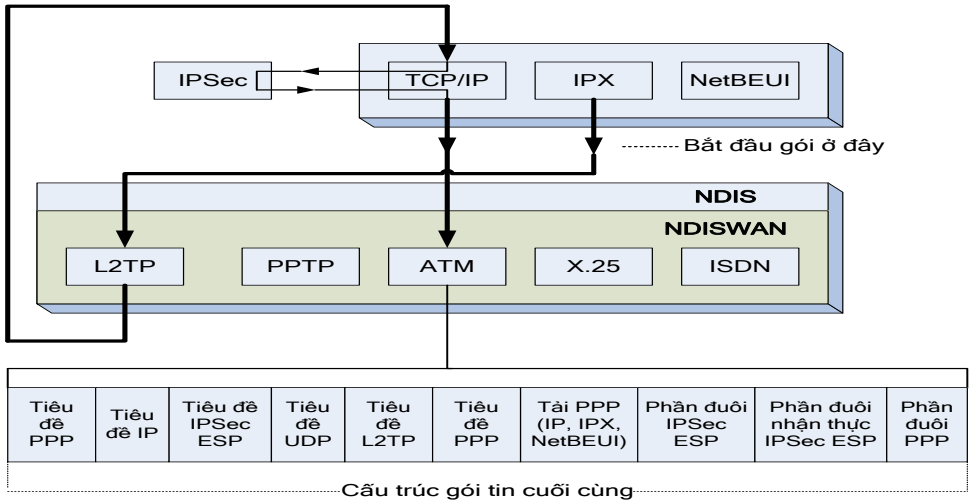
- *Đóng gói L2TP*. Phần tải PPP ban đầu được đóng gói với một tiêu đề PPP và một tiêu đề L2TP
- *Đóng gói UDP*. Gói L2TP sau đó được đóng gói với một tiêu đề UDP, các địa chỉ cổng nguồn và đích được đặt bằng 1701.
- *Đóng gói IPSec.* Tuỳ thuộc vào chính sách IPSec, gói UDP được mật mã và đóng gói với tiêu đề IPSec ESP, đuôi IPSec ESP, đuôi IPSec Authentication.
- *Đóng gói IP*. Gói IPSec được đóng gói với tiêu đề IP chứa địa chỉ IP nguồn và đích của máy trạm và máy chủ.
- *Đóng gói lớp liên kết dữ liệu.* Để truyền đi được trên đường truyền LAN hoặc WAN, gói IP cuối cùng sẽ được đóng gói với phần tiêu đề và đuôi tương ứng với kỹ thuật lớp liên kết dữ liệu của giao diện vật lý đầu ra. Ví dụ, khi gói IP được gửi vào giao diện Ethernet, nó sẽ được đóng gói với tiêu đề và đuôi Ethernet. Khi các gói IP được gửi trên đường truyền WAN điểm tới điểm (chẳng hạn đường dây điện thoại ISDN), chúng được đóng gói với tiêu đề và đuôi PPP.

Hình 2-6 chỉ ra cấu trúc cuối cùng của gói dữ liệu đường hầm L2TP trên nền IPSec.



Hình 2 - 6 Đóng gói dữ liệu đường hầm L2TP

Hình 2-7 là sơ đồ đóng gói L2TP từ một máy trạm VPN thông qua kết nối truy nhập từ xa sử dụng modem tương tự.



Hình 2 - 7 Sơ đồ đóng gói L2TP

Quá trình đóng gói được thực hiện thông qua các bước như sau:

- Gói tin IP, IPX hoặc NetBEUI được đưa tới giao diện ảo đại diện cho kết nối VPN sử dụng NDIS bằng giao thức thích hợp.
- NDIS đưa các gói tới NDISWAN, tại đây có thể nén và cung cấp tiêu đề PPP chỉ bao gồm trường chỉ số giao thức PPP. Các trường Flag hay FCS không được thêm vào.
- NDISWAN gửi khung PPP tới giao thức L2TP, nơi đóng gói khung PPP với một tiêu đề L2TP. Trong tiêu đề L2TP, chỉ số đường hầm và chỉ số cuộc gọi được thiết lập với các giá trị thích hợp để xác định đường hầm.
- Giao thức L2TP gửi gói thu được tới TCP/IP với thông tin để gửi gói L2TP như một bản tin UDP từ cổng UDP 1701 tới cổng UDP 1701 theo các địa chỉ IP của máy trạm và máy chủ.
- TCP/IP xây dựng gói IP với các tiêu đề IP và UDP thích hợp. IPSec sau đó sẽ phân tích gói IP và so sánh nó với chính sách IPSec hiện thời. Dựa trên những thiết lập trong chính sách, IPSec đóng gói và mật mã phần bản tin UDP của gói IP sử dụng các tiêu đề và đuôi ESP phù hợp. Tiêu đề IP ban đầu với trường Protocol được đặt là 50 và thêm vào phía trước của gói ESP. TCP/IP sau đó gửi gói thu được tới giao diện đại diện cho kết nối quay số tới ISP cục bộ sử dụng NDIS.
- NDIS gửi số tới NDISWAN.
- NDISWAN cung cấp tiêu đề và đuôi PPP, sau đó gửi khung PPP thu được tới cổng thích hợp đại diện cho phần cứng dial-up

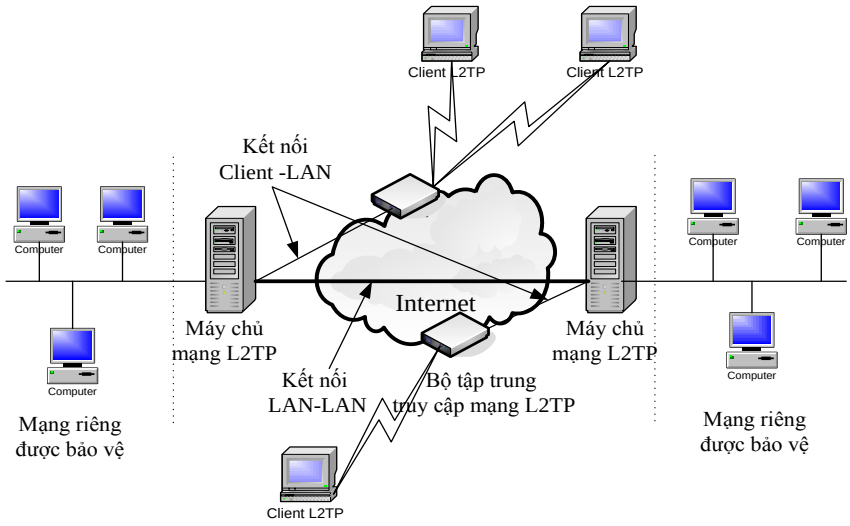
2.3.4 Xử lý dữ liệu tại đầu cuối đường hầm L2TP trên nền IPSec

Khi nhận được dữ liệu đường hầm L2TP trên nền IPSec, máy trạm và máy chủ L2TP sẽ thực hiện các bước sau:

- Xử lý và loại bỏ tiêu đề và đuôi của lớp liên kết dữ liệu.
- Xử lý và loại bỏ tiêu đề IP.
- Dùng phần đuôi IPSec ESP Auth để xác thực tải IP và tiêu đề IPSec ESP.
- Dùng tiêu đề IPSec ESP để giải mã phần gói đã mật mã.
- Xử lý tiêu đề UDP và gửi gói tới L2TP.
- L2TP dùng chỉ số đường hầm và chỉ số cuộc gọi trong tiêu đề L2TP để xác định đường hầm L2TP cụ thể.
- Dùng tiêu đề PPP để xác định tải PPP và chuyển tiếp nó tới đúng giao thức để xử lý.

2.3.5 Triển khai VPN dựa trên L2TP

Hệ thống cung cấp VPN dựa trên L2TP bao gồm các thành phần cơ bản sau: bộ tập trung truy nhập mạng, máy chủ L2TP và các máy trạm L2TP (hình 2-8).



Hình 2 - 8 Các thành phần hệ thống cung cấp VPN dựa trên L2TP

Máy chủ L2TP

Máy chủ L2TP có hai chức năng chính: đóng vai trò là điểm kết thúc của đường hầm L2TP và chuyển các gói đến từ đường hầm đến mạng LAN riêng hay ngược lại. Máy chủ chuyển các gói đến máy tính đích bằng cách xử lý gói L2TP để có được địa chỉ mạng của máy tính đích.

Không giống như máy chủ PPTP, máy chủ L2TP không có khả năng lọc các gói. Chức năng lọc gói trong L2TP được thực hiện bởi tường lửa.Tuy nhiên trong thực tế, người ta thường tích hợp máy chủ mạng và tường lửa. Việc tích hợp này mang lại một số ưu điểm hơn so với PPTP, đó là:

- L2TP không đòi hỏi chỉ có một cổng duy nhất gán cho tường lửa như trong PPTP. Chương trình quản lý có thể tuỳ chọn cổng để gán cho tường lửa, điều này gây khó khăn cho kẻ tấn công khi cố gắng tấn công vào một cổng trong khi cổng đó có thể đã thay đổi.
- Luồng dữ liệu và thông tin điều khiển được truyền trên cùng một UDP nên việc thiết lập tường lửa sẽ đơn giản hơn. Do một số tường lửa không hỗ trợ GRE nên chúng tương thích với L2TP hơn là với PPTP.

Phần mềm Client L2TP

Nếu như các thiết bị của ISP đã hỗ trợ L2TP thì không cần phần cứng hay phần mềm bổ sung nào cho các máy trạm, chỉ cần kết nối chuẩn PPP là đủ. Tuy nhiên, với các thiết lập như vậy thì không sử dụng được mã hoá của IPSec. Do vậy ta nên sử dụng các phần mềm client tương thích L2TP cho kết nối L2TP VPN.

Một số đặc điểm của phần mềm client L2TP là:

- Tương thích với các thành phần khác của IPSec như máy chủ mã hoá, giao thức chuyển khoá, giải thuật mã hoá, …
- Đưa ra một chỉ báo rõ ràng khi IPSec đang hoạt động;
- Hàm băm (hashing) xử lý được các địa chỉ IP động;

- Có cơ chế bảo mật khoá (mã hoá khoá với mật khẩu);
- Có cơ chế chuyển đổi mã hoá một cách tự động và định kỳ;
- Chặn hoàn toàn các lưu lượng không IPSec.

Bộ tập trung truy cập mạng

ISP cung cấp dịch vụ L2TP cần phải cài một NAS cho phép L2TP để hỗ trợ các máy trạm L2TP chạy trên nền các hệ điều hành khác nhau như Unix, Windows, Macintosh,…

Các ISP cũng có thể cung cấp các dịch vụ L2TP mà không cần phải thêm các thiết bị hỗ trợ L2TP vào máy chủ truy nhập của họ, điều này đòi hỏi tất cả người dùng phải có phần mềm client L2TP tại máy của họ. Khi đó người dùng có thể sử dụng dịch vụ của nhiều ISP trong trường hợp mô hình mạng của họ rộng lớn về mặt địa lý.

2.3.6 Ưu nhược điểm và ứng dụng của L2TP

L2TP là một thế hệ giao thức quay số truy nhập VPN phát triển sau. Nó phối hợp những đặc tính tốt nhất của PPTP và L2F. Hầu hết các nhà cung cấp sản phẩm PPTP đều đưa ra các sản phẩm tương thích với L2TP.

Mặc dù L2TP chủ yếu chạy trên mạng IP, nhưng khả năng chạy trên các mạng công nghệ khác như Frame Relay hay ATM đã làm cho nó thêm phổ biến. L2TP cho phép một lượng lớn khách hàng từ xa được kết nối vào VPN cũng như là các kết nối LAN-LAN có dung lượng lớn. L2TP có cơ chế điều khiển luồng để làm giảm tắc nghẽn trên đường hầm L2TP.

Việc lựa chọn một nhà cung cấp dịch vụ L2TP có thể thay đổi tuỳ theo yêu cầu thiết kế mạng. Nếu thiết kế một VPN đòi hỏi mã hoá đầu cuối tới đầu cuối thì cần cài các client tương thích L2TP tại các trạm từ xa và thoả thuận với ISP là sẽ xử lý mã hoá từ máy đầu xa đến tận máy chủ của VPN. Nếu xây dựng một mạng với múc độ bảo mật thấp hơn, khả năng chịu đựng lỗi cao hơn và chỉ muốn bảo mật dữ liệu khi nó đi trong đường hầm trên Inernet thì thoả thuận với ISP để họ hỗ trợ LAC và mã hoá dữ liệu chỉ từ đoạn LAC đến LNS của mạng riêng.

L2TP cho phép thiết lập nhiều đường hầm với cùng LAC và LNS. Mỗi đường hầm có thể gán cho một người dùng xác định hoặc một nhóm người dùng và gán cho các môi trường khác nhau tuỳ theo thuộc tính chất lượng dịch vụ QoS của người sử dụng.

2.4 Giao thức IPSec

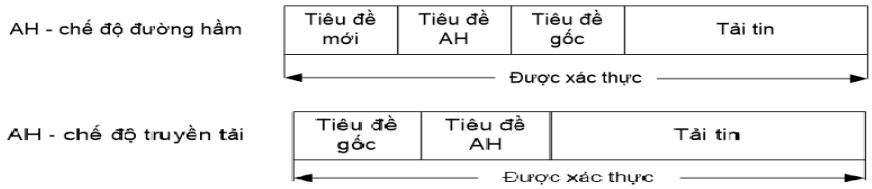
2.4.1 Hoạt động của IPSec

[5] IPSec đảm bảo tính tin cậy, tính toàn vẹn và tính xác thực truyền dữ liệu qua mạng công cộng. IPSec định nghĩa hai loại tiêu đề cho gói IP điều khiển quá trình xác thực và mã hóa: một là xác thực tiêu đề *Authentication Header (AH*), hai là đóng gói bảo mật tải *Encapsulating Security Payload (ESP).* Xác thực tiêu đề AH đảm bảo tính toàn vẹn cho những tiêu đề gói và dữ liệu. Trong khi đó đóng gói bảo mật tải ESP thực hiện mã hóa và đảm bảo tính toàn vẹn cho gói dữ liệu nhưng không bảo vệ tiêu đề cho gói IP như AH. IPSec sử dụng giao thức IKE (Internet Key Exchange) để thỏa thuận

liên kết bảo mật SA giữa hai thực thể và trao đổi các thông tin khóa. IKE cần được sử dụng phần lớn các ứng dụng thực tế để đem lại thông tin liên lạc an toàn trên diện rộng

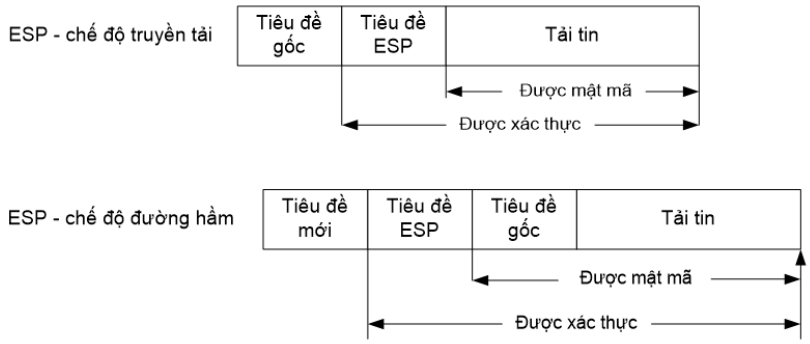
- **Xác thực tiêu đề AH**: AH là một trong những giao thức bảo mật IPSec đảm bảo tính toàn vẹn cho tiêu đề gói và dữ liệu cũng như việc chứng thực người sử dụng. Nó đảm bảo chống phát lại và chống xâm nhập trái phép như một tùy chọn. Trong những phiên bản đầu của IPSec đóng gói bảo mật tải ESP chỉ thực hiện mã hóa mà không có chứng thực nên AH và ESP được dùng kết hợp còn ở những phiên bản sau ESP đã có thêm khả năng chứng thực. Tuy nhiên AH vẫn được dùng do đảm bảo việc chứng thực cho toàn bộ tiêu đề và dữ liệu cũng như việc đơn giản hơn đối với truyền tải dữ liệu trên mạng IP chỉ yêu cầu chứng thực

  AH có hai chế độ: Transport và Tunnel (xem hình 2-9). Chế độ AH Tunnel tạo ra tiêu đề IP cho mỗi gói còn chế độ Transport AH không tạo ra tiêu đề IP mới. Hai chế độ AH luôn đảm bảo tính toàn vẹn (Integrity), chứng thực (Authentication) cho toàn bộ gói.



Hình 2 - 9 Xử lý gói tin AH ở hai chế độ: truyền tải và đường hầm

- **Xử lý đảm bảo tính toàn vẹn**: IPSec dùng thuật toán mã chứng thực thông báo băm HMAC (Hash Message Authentication Code) thường là HMAC-MD5 hay HMAC-SHA-1. Nơi phát giá trị băm được đưa vào gói và gửi cho nơi nhận. Nơi nhận sẽ tái tạo giá trị băm bằng khóa chia sẻ và kiểm tra sự trùng khớp giá trị băm qua đó đảm bảo tính toàn vẹn của gói dữ liệu. Tuy nhiên IPSec không bảo vệ tính toàn vẹn cho tất cả các trường trong tiêu đề IP. Một số trường trong tiêu đề IP như TTL (Time to Live) và trường kiểm tra tiêu đề IP có thể thay đổi trong quá trình truyền. Nếu thực hiện tính giá trị băm cho tất cả các trường của tiêu đề IP thì những trường đã nêu ở trên sẽ bị thay đổi khi chuyển tiếp và tại nơi nhận giá trị băm sẽ khác. Để giải quyết vấn đề này giá trị băm sẽ không tính đến những trường của tiêu đề IP có thể thay đổi hợp pháp trong quá trình truyền.
- **ESP cũng có hai chế độ**: Transport và Tunnel (xem hình 2-10). Chế độ Tunnel ESP tạo tiêu đề IP mới cho mỗi gói. Chế độ này có thể mã hóa và đảm bảo tính toàn vẹn của dữ liệu hay chỉ thực hiện mã hóa toàn bộ gói IP gốc. Việc mã hóa toàn bộ gói IP (gồm cả tiêu đề IP và tải IP) giúp che được địa chỉ IP gốc. Chế độ Transport ESP dùng lại tiêu đề của gói IP gốc chỉ mã hóa và đảm bảo tính toàn vẹn cho tải của gói IP gốc. Cả hai chế độ chứng thực để đảm bảo tính toàn vẹn nhưng được lưu ở trường ESP Auth



Hình 2 - 10 Xử lý gói tin ESP ở hai chế độ: truyền tải và đường hầm

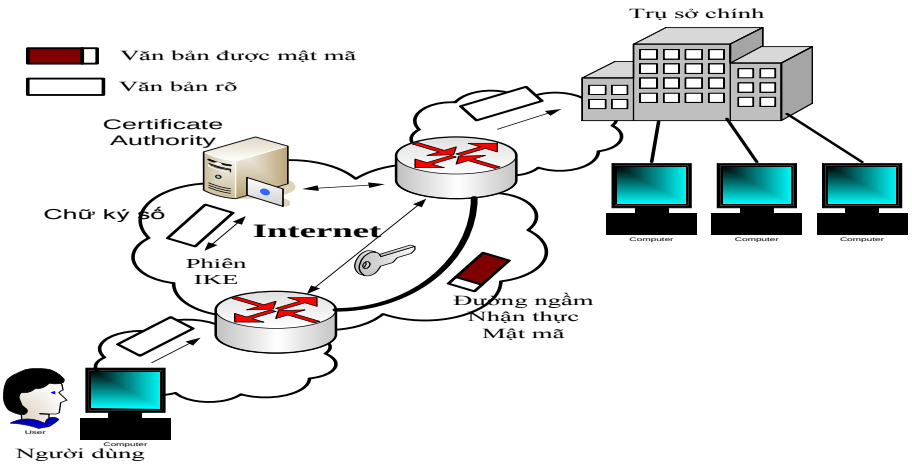
- **Xử lý mã hóa**: ESP dùng hệ mật mã đối xứng để mã hóa gói dữ liệu, nghĩa là thu và phát đều dùng một loại khóa để mã hóa và giải mã dữ liệu. ESP thường dụng loại mã khối AES-CBC (AES-Cipher Block Chaining), AES-CTR (AES Counter Mode) và 3DES
- **Liên kết an ninh**: IPSec cung cấp nhiều lựa chọn để thực hiện các giải pháp mật mã và xác thực ở lớp mạng. Phần này sẽ định nghĩa các thủ tục quản lý an ninh cho cả IPv4 và IPv6 để thực thi AH, ESP hoặc cả hai, phụ thuộc vào lựa chọn của người sử dụng. Khi thiết lập kết nối IPSec, hai bên phải xác định chính xác các thuật toán nào sẽ được sử dụng, loại dịch vụ nào cần đảm bảo an ninh. Sau đó bắt đầu xử lý thương lượng để chọn một tập các tham số và các giải thuật áp dụng cho mã hóa bảo mật hay xác thực. Như trên đã giới thiệu, dịch vụ bảo mật quan hệ giữa hai hay nhiều thực thể để thỏa thuận truyền thông an toàn được gọi là liên kết an ninh SA.
- **Trao đổi khóa mã IKE (Internet Key Exchange)**: Trong truyền thông sử dụng giao thức IPSec phải có sự trao đổi khóa giữa hai điểm kết nối, do đó đòi hỏi phải có cơ chế quản lý khóa. Có hai phương pháp chuyển giao khóa đó là chuyển khóa bằng tay và chuyển khóa băng giao thức IKE. Một hệ thống IPSec phụ thuộc phải hỗ trợ phương thức chuyển khóa bằng tay. Phương thức chìa khóa trao tay chẳng hạ khóa thương mại ghi trên giấy. Phương thức này chỉ phù hợp với số lượng nhỏ các Site, đối với các mạng lớn phải thực hiện phương pháp quản lý khóa tự động. Trong IPSec người ta dùng giao thức quản lý chuyển khóa IKE (Internet Key Exchange) IKE có các khả năng sau:
    - Cung cấp các phương tiện cho hai bên sử dụng các giao thức, giải thuật và khóa
    - Đảm bảo ngay từ lúc bắt đầu chuyển khóa
    - Quản lý các khóa sau khi chúng được chấp nhận trong tiến trình thỏa thuận
    - Đảm bảo các khóa được chuyển một cách bí mật

2.4.2 Thực hiện VPN trên nền IPSec

Để minh họa toàn bộ quá trình thực hiện kết nối VPN trên nền IPSec, ta xem xét một ví dụ như trên hình 2-11.

Trước khi thiết lập kết nối IPSec, cần phải chắc chắn rằng các thiết bị đang sử dụng dọc theo đường dẫn của VPN đảm bảo có hỗ trợ IPSec (bao gồm các giao thức, thuật toán), và không có kết nối IPSec nào trước đó hoặc nếu có thì các tham số trong SA đang tồn tại phải không xung đột với các tham số chuẩn bị thiết lập. Có thể thực hiện lệnh "ping" để chắc chắn rằng kết nối đã sẵn sàng.

Trong ví dụ này, người sử dụng muốn truyền thông an toàn với mạng ở trụ sở chính. Khi gói dữ liệu tới bộ định tuyến người dùng (đóng vai trò là một cổng an ninh), bộ định tuyến này sẽ kiểm tra chính sách an ninh và nhận ra gói dữ liệu cần truyền là một ứng dụng của VPN và cần được bảo vệ. Chính sách an ninh cấu hình trước cũng cho biết bộ định tuyến tại mạng trụ sở chính sẽ là đầu phía bên kia của đường hầm IPSec-VPN.



Hình 2 - 11 Ví dụ thực hiện kết nối VPN trên nền IPSec

Bộ định tuyến người dùng kiểm tra xem đã có liên kết an ninh nào được thiết lập cho phiên truyền thông này hay chưa. Nếu chưa có thì bắt đầu quá trình thương lượng IKE. Certificate Authority có chức năng giúp trụ sở chính xác thực người sử dụng xem có được phép thực hiện phiên truyền thông này hay không. Biện pháp xác thực ở đây là sử dụng chữ ký số được cung cấp bởi một đối tác có quyền chứng thực mà hai bên đều tin cậy. Ngay sau khi hai bộ định tuyến đã thỏa thuận được một IKE SA thì IPSec SA tức thời được tạo ra. Trong trường hợp thỏa thuận IKE SA không đạt được thì hai bên có thể tiến hành thương lượng lại hoặc ngừng phiên kết nối thông tin.

Việc tạo ra IPSec SA chính là kết quả của quá trình thỏa thuận giữa các bên về các chính sách an ninh, thuật toán mật mã (chẳng hạn là DES), thuật toán xác thực (chẳng hạn MD5), và một khóa chia sẻ được sử dụng. Dữ liệu về SA được lưu trong cơ sở dữ liệu của mỗi bên.

Tới đây, bộ định tuyến người sử dụng sẽ đóng gói dữ liệu theo các yêu cầu đã thỏa thuận trong IPSec SA (thuật toán mật mã, xác thực, giao thức đóng gói là AH hay ESP, …), sau đó thêm các thông tin thích hợp để đưa gói tin được mã hóa này về dạng gói IP và chuyển tới bộ định tuyến nối với mạng trung tâm. Khi nhận được gói tin từ bộ định tuyến người dùng gửi đến, bộ định tuyến mạng trung tâm tìm kiếm IPSec SA, xử lý gói theo yêu cầu, đưa về dạng gói tin ban đầu và chuyển tới mạng trung tâm.

2.4.3 Một số vấn đề còn tồn tại trong IPSec

Mặc dù IPSec đã sẵn sàng đưa ra các đặc tính cần thiết để đảm bảo thiết lập kết nối VPN an toàn thông qua mạng Internet, tuy nhiên vẫn còn tồn tại một số nhược điểm như sau:

- Tất cả các gói được xử lý theo IPSec sẽ bị tăng kích thước do phải thêm vào các tiêu đề khác nhau, và điều này làm cho thông lượng hiệu dụng của mạng giảm xuống. Vấn đề này có thể được khắc phục bằng cách nén dữ liệu trước khi mã hóa, song các kĩ thuật như vậy vẫn còn đang nghiên cứu và chưa được chuẩn hóa.
- IPSec được thiết kế chỉ để hỗ trợ bảo mật cho lưu lượng IP, không hỗ trợ các dạng lưu lượng khác.
- Việc tính toán nhiều giải thuật phức tạp trong IPSec vẫn còn là một vấn đề khó đối với các trạm làm việc và máy PC năng lực yếu.
- Việc phân phối các phần cứng và phần mềm mật mã vẫn còn bị hạn chế đối với chính phủ của một số quốc gia ví dụ Nga

2.5 Kết luận chương

Chương này trình bày ba công nghệ VPN có thể nói phổ biến nhất đến thời điểm hiện tại. Mỗi giao thức đều có những ưu và nhược điểm riêng, do vậy điều quan trọng là phải làm quen với các đặc điểm của từng loại rồi kết hợp với nhu cầu thực tế của người dùng để ra quyết định lựa chọn

Bảo mật luôn được coi là một trong những khía cạnh quan trọng nhất trong các công nghệ trên nền IP đặc biệt là đối với công nghệ VPN. Trong số những giao thức trình bày thì IPSec được phát triển để giải quyết vấn đề đảm bảo an ninh cho thông tin truyền trên mạng Internet và được coi là giao thức tối ưu nhất cho thực hiện IP-VPN. Nó là một tập hợp các tiêu chuẩn mở, cung cấp các dịch vụ bảo mật dữ liệu và điều khiển truy nhập. Tuy nhiên IPSec cũng còn nhiều điểm hạn chế không tránh khỏi do vậy hiện nay người ta đang phát triển thêm một vài loại hình VPN tốt hơn IPSec ở một khía cạnh nào đó như SSL VPN, MPLS VPN… mà chúng ta sẽ tìm hiểu ở các chương tiếp theo.

CHƯƠNG 3. MẠNG RIÊNG ẢO TRÊN NỀN MPLS

MPLS-VPN được coi là sự kết hợp ưu điểm của cả hai mô hình mạng riêng ảo *chồng lấn* và *ngang hàng*. Việc thiết lập mạng riêng ảo trên nền MPLS cho phép đảm bảo định tuyến tối ưu giữa các site khách hàng, phân biệt địa chỉ khách hàng thông qua nhận dạng tuyến và hỗ trợ xây dựng các mô hình VPN phức tạp trên cơ sở đích định tuyến.

Chương này trình bày những vấn đề cơ bản nhất về công nghệ MPLS, tiếp đó sẽ đi sâu tìm hiểu ứng dụng mạng riêng ảo trên nền MPLS, nguyên lý hoạt động cũng như khả năng mà MPLS-VPN mạng lại so với một loại hình mạng riêng ảo cũng rất phổ biến hiện này là IPSec qua đó làm nổi bật những ưu điểm của giải pháp MPLS-VPN

3.1 Công nghệ MPLS

3.1.1 Giới thiệu

Multi protocol label switching (MPLS) là một công nghệ được phát triển bởi IETF (Internet Engineering Task Force) để giải quyết các vấn đề của mạng IP truyền thống. Tên gọi của nó bắt nguồn từ việc nó sử dụng kỹ thuật hoán đổi nhãn để chuyển tiếp gói tin. "Đa giao thức" ở đây có nghĩa là nó có thể hỗ trợ nhiều giao thức lớp mạng không chỉ riêng IP. Ngoài IP, các nhà cung cấp dịch vụ còn có thể cấu hình và chạy MPLS trên các công nghệ lớp 2 khác như ATM, Frame Relay…

3.1.2 Các lợi ích của MPLS

[12]

3.1.2.1 Lợi ích không có thật

Một trong những lý do đầu tiên đưa ra của giao thức trao đổi nhãn 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 header 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 kích thước 4 byte 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.

Một số người nghĩ rằng việc tra cứu giá trị nhãn đơn giản trong một bảng nhanh hơn việc tra cứu địa chỉ IP truyền thống, tuy nhiên quá trình chuyển mạch IP bằng phần cứng làm cho luận điểm này không còn đúng nữa. Gần đây, các đường kết nối trên những bộ định tuyến có thể có băng thông lên tới 100Gbps. Một bộ định tuyến có một vài đường liên kết 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 định tuyến.

Mặt phẳng điều khiển là một tập các giao thức để thiết lập một mặt phẳng dữ liệu hay còn gọi là mặt phẳng chuyển tiếp. Các thành phần chính của mặt phẳng điều khiển là các giao thức định tuyến, bảng định tuyến và một số chức năng điều khiển khác hoặc giao thức báo hiệu được sử dụng để cung cấp cho 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 tin IP được chuyển mạch nhanh như các gói được gán 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 là điều không còn đúng nữa

3.1.2.2 Sử dụng một hạ tầng mạng hợp nhất

Với MPLS, ý tưởng là gán nhãn cho gói đi vào mạng dựa trên địa chỉ đích của nó hoặc một số 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 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) thông thường được chuyển qua IP mà còn cả các loại dữ liệu đa phương tiện như thoại/hình.

Bằng việc sử dụng MPLS với IP, ta có thể mở rộng khả năng truyền nhiều loại dữ liệu. Việc gán nhãn vào gói cho phép ta mang nhiều giao thức khác hơn là chỉ có IP qua mạng trục IP có tính năng MPLS, tương tự với những khả năng thực hiện được với mạng Frame Relay hoặc ATM lớp 2. MPLS có thể truyền IPv4, IPV6, Ethernet, HDLC, PPP và những kỹ thuật lớp 2 khác.

Chức năng mà bất kỳ khung lớp 2 nào 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 gán nhãn bằng việc tìm kiếm nhãn trên đầu của gói. 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 chấp dịch vụ cung cấp dịch vụ lớp 2 cho khách hàng như bất kỳ một nhà mạng không chạy MPLS 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.

3.1.2.3 Sự tích hợp tốt hơn giữa IP và ATM

Trong thập kỷ trước, IP đã chiến thắng trong cuộc chiến cạnh tranh với các giao thức lớp 3 khác như AppleTalk, Internetwork Packet Exchange (IPX) và DECnet. IP

khá đơn giản và có mặt khắp nơi. Một giao thức lớp 3 phổ biến lúc đó là ATM. ATM có rất nhiều thành công nhưng thành công chỉ giới hạn trong việc sử dụng nó như một giao thức WAN trong mạng lõi của nhà cung cấp dịch vụ. Có rất nhiều nhà cung cấp dịch vụ cũng triển khai thêm mạng trục IP. Sự kết hợp giữaa IP và ATM không phải ít quan trọng. Để kết hợp tốt hơn IP và ATM cộng đồng mạng có rất ít giải pháp.

Một phương pháp để kết hợp IP và ATM được đặc tả trong RFC 1483, nó chỉ ra cách đóng gói nhiều giao thức định tuyến và bắc cầu qua lớp thích nghi ATM 5 (ATM adaptation Layer AAL 5). Trong phương pháp này, tất cả các mạch ATM phải thiết lập bằng tay, tất cả các ánh xạ giữa địa chỉ IP trạm kế tiếp theo và điểm cuối ATM cũng phải thiết lập bằng tay trên tất cả các router có gắn ATM.

Một phương pháp khác là triển khai LAN Emulation (LANE). Ethernet trở thành một công nghệ lớp 2 phổ biến ở biên của mạng nhưng nó không thể đáp ứng được sự tin cậy và khả năng mở rộng trong mạng của những nhà cung cấp dịch vụ lớn. LANE về cơ bản làm cho mạng của ta trông giống như một mạng mô phỏng Ethernet. Điều đó có nghĩa là rất nhiều đoạn mạng Ethernet được bắc cầu thông với nhau như kiểu mạng ATM WAN ở giữa giống như một Ethernet switch.

Tất cả những phương pháp đó đều rất cồng kềnh để triển khai và sửa lỗi. Một phương pháp kết hợp tốt hơn giữa IP và ATM chính là một trong những lý do chính dẫn đến sự ra đời của MPLS. Điều kiện tiên quyết cho MPLS trên ATM switch là ATM switch phải trở lên thông minh hơn. ATM switch phải chạy giao thức định tuyến IP và triển khai giao thức phân phối nhãn.

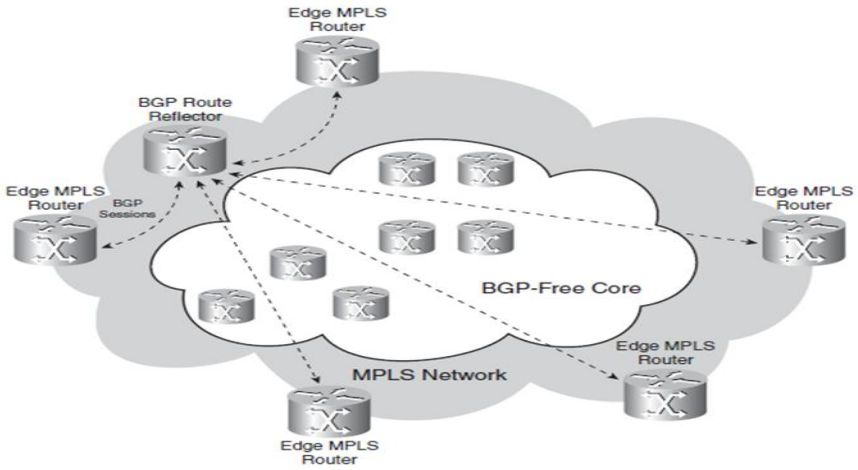
3.1.2.4 BGP - Free Core

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 xuất hiện trong bảng định tuyến của mỗi bộ định tuyến. BGP mang nhiều tiền tố ngoài như tiền tố của các khách hàng hay tiền tố ngoài Internet. Điều đó 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 chứ không phải là tìm kiếm địa chỉ IP. Nhãn này là thông tin được gán vào mỗi gói để chỉ cho các bộ định tuyến trung gian biết bộ định tuyến biên lối ra nào 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 nhà cung cấp dịch vụ không cần thiết chạy BGP.

Bộ định tuyến tại biên của mạng MPLS vẫn cần xem xét địa chỉ IP đích của gói và do đó vẫn cần phải chạy BGP. Mỗi tiền tố BGP trên những bộ định tuyến MPLS lối vào có một địa chỉ IP bước nhảy tiếp theo (next-hop) kết hợp với nó. Địa chỉ IP bước

nhảy tiếp theo BGP này chính là một địa chỉ IP của bộ định tuyến MPLS lối ra. Nhãn kết hợp với gói IP là nhãn mà kết hợp với địa chỉ IP bước nhảy tiếp theo này. Do tất cả các bộ định tuyến lõi chuyển tiếp gói dựa trên nhãn MPLS được gán mà có liên quan tới địa chỉ IP bước nhảy tiếp theo BGP nên mỗi địa chỉ IP bước nhảy của bộ định tuyến MPLS lối ra này phải được biết bởi tất cả các router lõi. Những giao thức định tuyến nội mạng như OSPF, RIP có thể thực hiện nhiệm vụ này (xem hình 3-1)



Hình 3 - 1 Mạng lõi BGP Free Core

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

Hiện nay tất cả các bộ định tuyến trong mạng lõi đang thực hiện chuyển tiếp những gói tin được gán nhãn, không phải tìm kiếm địa chỉ IP, do đó chúng phần nào bỏ bớt được các gánh nặng chạy BGP. Bởi vì bảng định tuyến Internet đầy đủ có thể có hơn 600.000 mạng, việc chạy BGP trên tất cả các bộ định tuyến là một điều rất đáng quan tâm. Bộ định tuyến mà không chứa bảng định tuyến trên toàn Internet sẽ cần rất ít bộ nhớ. Do vậy, ta có thể chạy các router lõi mà không gặp phải sự phức tạp của việc chạy BGP trên chúng.

3.1.3 Một số ứng dụng của MPLS

3.1.3.1 Điều khiển lưu lượng (TE – Traffic Engineering)

Ứng dụng điều khiển lưu lượng, trong một số trường hợp còn gọi là định tuyến với việc dành trước tài nguyên. Việc điều khiển lưu lượng ban đầu được thực hiện theo cấu hình tĩnh. Điều này có nghĩa là người quản trị phải cấu hình tất cả các bước để một luồng lưu lượng nào đó có thể truyền qua mạng. Bổ sung sau đó cho việc điều khiển lưu lượng là cấu hình động khi sử dụng giao thức định tuyến trạng thái liên kết. Người quản trị không phải cấu hình để điều khiển lưu lượng theo từng bước. Giao thức định tuyến theo trạng thái liên kết truyền nhiều thông tin hơn, để đường hầm tạo ra theo nhiều cách thức khác nhau. Do đó giảm được số lượng công việc cho người vận hành, và điều này đã làm cho điều khiển lưu lượng trong MPLS trở nên phổ biến hơn

3.1.3.2 Mạng riêng ảo

Trước khi xuất hiện MPLS-VPN, chuyển mạch nhãn vẫn chưa được phổ biến rộng rãi. Khi phiên bản phần mềm điều khiển bộ định tuyến hỗ trợ cho MPLS-VPN đầu tiên được phát hành, nó thành công ngay lập tức bởi vì nhiều nhà khai thác đang muốn nhanh chóng cung cấp dịch vụ mạng riêng ảo trên nền MPLS cho khách hàng của họ. Ngày nay, MPLS-VPN là ứng dụng phổ biến nhất trong tất cả các ứng dụng của MPLS

3.1.3.3 Ứng dụng AToM (Any Transport over MPLS)

Giải pháp AToM đầu tiên được đưa ra trong phiên bản Cisco 12.0(10)ST vào năm 2000, hỗ trợ truyền ATM AAl-5 qua mạng đường trục MPLS. Sau đó nhiều thành phần khác đã được thêm vào AToM. Ví dụ, tại lớp 2 các thành phần có thể truyền qua mạng AToM là Frame Relay, ATM, PPP, HDLC, Ethernet và 802.1Q. Đặc biệt, việc truyền Ethernet qua mạng MPLS đường trục ngày nay đã thu được nhiều thành công. Tuy nhiên AToM bị hạn chế khi nó truyền khung Ethernet qua mạng đường trục MPLS trong kiểu truyền điểm-điểm

3.1.3.4 Dịch vụ LAN riêng ảo VPLS (Virtual Private LAN Service)

Dịch vụ LAN riêng ảo VPLS cho phép truyền các khung Ethernet theo kiểu điểm-đa điểm. Thực chất, VPLS là một dịch vụ lớp 2 mô phỏng LAN qua mạng MPLS. Phiên bản Cisco IOS đầu tiên bổ sung được đưa ra vào đầu năm 2004 trên nền bộ định tuyến 7600 là 12.2(17d)SXB

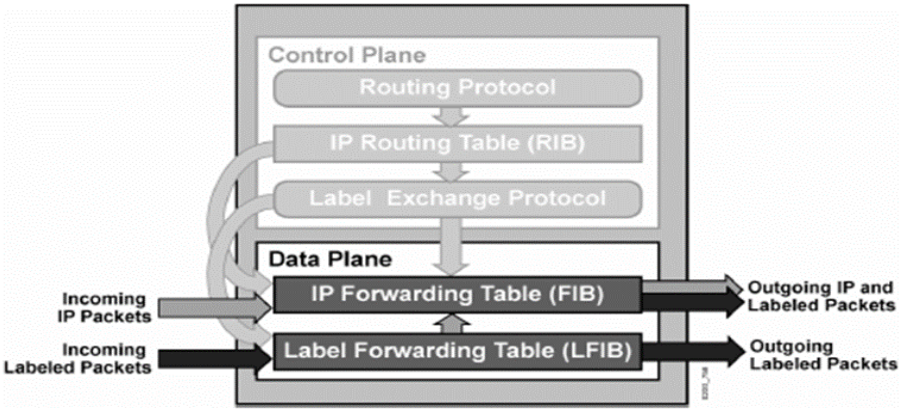
Như vậy có thể thấy MPLS đã kết hợp được những ưu điểm của cả Frame Relay, ATM và công nghệ trên nền IP. Giải pháp truyền gói mới này đã mở ra những lĩnh vực ứng dụng mang lại nhiều thành công lớn như là MPLS-VPN, MPLS-TE, AToM và VPLS

3.1.4 Kiến trúc của MPLS

MPLS gồm hai thành phần chính: Mặt phẳng điều khiển (Control plane) và mặt phẳng chuyển tiếp (Data plane). [10]

3.1.4.1 Mặt phẳng chuyển tiếp (Data plane)

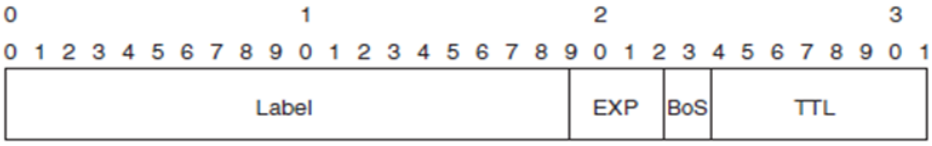
Mặt phẳng dữ liệu là thành phần chuyển tiếp gói tin qua thiết bị định tuyến hay chuyển mạch. Việc chuyển mạch hay chuyển tiếp gói tin được thực hiện bởi các mạch tích hợp chuyên dụng. Sử dụng các mạch tích hợp này trong mặt phẳng chuyển tiếp của bộ định tuyến cho phép các gói IP dán nhãn được chuyển mạch qua với tốc độ rất cao. Có thể coi mặt phẳng dữ liệu là nơi mà hoạt động chuyển tiếp gói tin thực sự xảy ra. Hoạt động chuyển tiếp này chỉ có thể thực hiện sau khi mặt phẳng điều khiển đã thiết lập các thông tin cần thiết (xem hình 3-2)



Hình 3 - 2 Mặt phẳng chuyển tiếp

Mặt phẳng chuyển tiếp có trách có trách nhiệm chuyển tiếp gói dựa trên giá trị chứa trong nhãn. Để làm việc này, mặt phẳng chuyển tiếp sử dụng một cơ sở thông tin chuyển tiếp nhãn LFIB để chuyển tiếp các gói. Mỗi nút MPLS có hai bảng liên quan đến việc chuyển tiếp là: cơ sở thông tin nhãn (LIB – Label Information Base) và cơ sở thông tin chuyển tiếp nhãn LFIB (Label Forwarding Information Base). 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 nút láng giềng của nó. LFIB sử dụng một tập con các nhãn chứa trong LIB để thực hiện chuyển tiếp gói.

- **Nhãn MPLS**



Hình 3 - 3 Cấu trúc nhãn MPLS

20 bít đầu tiên là giá trị nhãn. Giá trị này nằm trong dải từ 0 đến 2^20-1 hoặc 1048575. Tuy nhiên 16 giá trị đầu tiên không được sử dụng như bình thường do chúng có một ý nghĩa đặc biệt khác. Các bít từ 20 đến 22 là 3 bít thực nghiệm (EXP –experimental bit). Những bít này chỉ được sử dụng cho chất lượng dịch vụ (QOS).

Bit 23 là bit cuối của ngăn xếp (Bottom of Stack - BOS). Nó mang giá trị 0 trừ khi nó là nhãn cuối trong ngăn xếp, trong trường hợp đó nó mang giá trị 1. Ngăn xếp nhãn là tập hợp của những nhãn được đặt phía trên của gói. Ngăn xếp nhãn có thể chỉ gồm một 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 từ bít thứ 24 đến 31 là 8 bít sử dụng làm bit thời gian sống (TTL – Time to Live). TTL này có chức năng giống TTL trong IP header. Nó được giảm đi 1 sau mỗi bước nhảy và chức năng của nó là tránh cho một gói bị

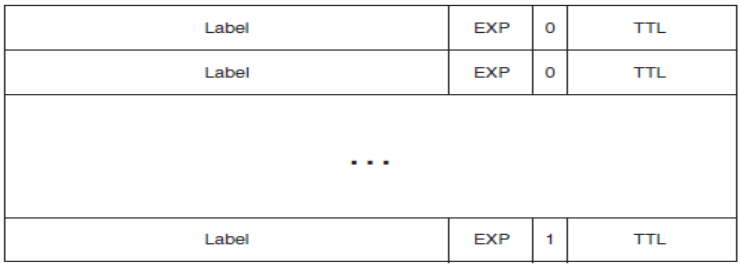
mắc kẹt trong vòng lặp. Nếu vòng lặp xảy ra và không có TTL thì vòng lặp đó sẽ xảy ra mãi mãi, nếu TTL của một nhãn về 0 thì gói sẽ bị loại bỏ (hình 3-3).

Các loại nhãn đặc biệt:

- 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. Việc sử dụng nhãn implicit-null ở cuối của LSP gọi là penultimate hop poping (PHP) điều này làm cho router gần router lối ra chỉ gửi một nhãn tới router lối ra sau khi nó gỡ bỏ nhãn trên cùng. Điều này giúp cho router lối ra không phải thực hiện việc truy vấn hai lần, một lần là LFIB để gỡ bỏ nhãn và lần thứ hai là FIB để chuyển tiếp gói tin.
- 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 *Router Alert*: Nhãn này có giá trị 1. Nhãn này có thể xuất hiện bất kì đâu trong ngăn xếp trừ ở đáy. Khi nhãn này là nhãn đỉnh, nó thông báo cho LSR cần phải truy vấn sâu hơn. Do đó, gói tin không được chuyển bằng phần cứng mà nó được xem xét bởi phần mềm. Khi gói tin được chuyển, nhãn 1 được gỡ bỏ. Sau đó, một truy vấn đến nhãn tiếp theo trong ngăn xếp được thực hiện trong LFIB để quyết định xem packet cần được chuyển đi đâu. Tiếp đó, một hành động trên nhãn (gỡ bỏ, hoán đổi, thêm vào) được thực hiện, nhãn 1 lại được thêm vào đầu của ngăn xếp và gói tin được chuyển.
- Nhãn *OAM Alert*: Nhãn này có giá trị 14 là nhãn Hoạt động và Bảo trì (Operation and Maintenance). OAM cơ bản được sử dụng để phát hiện lỗi và đánh giá hiệu năng. Nhãn này phân biệt gói tin OAM với các gói dữ liệu khác.

- ***Ngăn xếp nhãn***

Router có khả năng MPLS 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 các nhãn trong một ngăn xếp. Nhãn đầu tiên trong ngăn xếp được gọi là nhãn đỉnh và nhãn cuối cùng gọi là nhãn đáy. Ở giữa ta có thể có nhiều nhãn (xem hình 3-4)



Hình 3 - 4 Ngăn xếp nhãn MPLS

Trong ngăn xếp ở hình trên ta có thể thấy tất cả bit BoS bằng 0 đối với tất cả các nhãn trừ với nhãn đáy nó có giá trị 1.

Một vài ứng dụng thực tế của MPLS cần nhiều hơn 1 nhãn trong ngăn xếp 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.

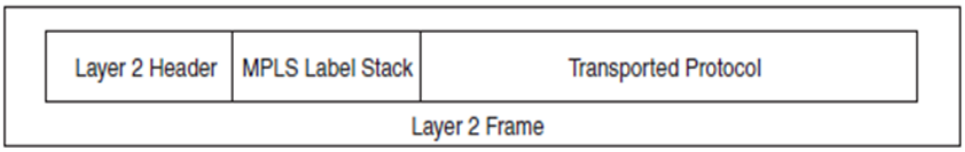
- ***Không gian nhãn***

Nhãn dùng trong một LSR để ánh xạ FEC - Nhãn được phân loại như sau:

- ✓ *Per platform*: Giá trị nhãn là duy nhất trong toàn LSR. Nhãn được cấp phát từ một dải chung. Không thể có hai nhãn trên những interface khác nhau có chung một giá trị.
- ✓ *Per interface:* Phạm vi nhãn được kết hợp với interface. Có rất nhiều dải nhãn được định nghĩa cho interface và nhãn được cung cấp trên những interface đó được cấp phát từ những dải riêng biệt. Giá trị nhãn trên những interface khác nhau có thể giống nhau.

- ***Mã hóa MPLS***

Ngăn xếp đặt trước gói lớp 3 – tức là trước header của giao thức được vận chuyển nhưng sau header của giao thức lớp 2. Ngăn xếp MPLS thường được gọi là *tiêu đề chèn* (*shim header*) bởi vị trí của nó (xem hình 3-5)



Hình 3 - 5 Cách đóng gói của gói tin gán nhãn

Sự đóng gói lớp 2 có thể là hầu hết cách đóng gói được hỗ trợ như: PPP, HDLC, Ethernet… Giả thiết rằng giao thức truyền tải là IPv4 và phương thức đóng gói lớp 2 là PPP, vị trí nhãn hiện tại 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 phải có những giá trị mới trong trường giao thức của lớp liên kết dữ liệu (data link layer), những giá trị này chỉ ra được phần tiếp theo của header lớp 2 sẽ là gói được gán nhãn MPLS. Trường giao thức (protocol) là một giá trị chỉ ra loại tải mà khung lớp 2 truyền đi. Bảng 3-1 chỉ ra tên và giá trị đối với trường nhận

dạng giao thức (Protocol Identifier - PI) này trong header lớp 2 đối với các loại đóng gói lớp 2 khác nhau:

Layer 2 Encapsulation Type	Layer 2 Protocol Identifier 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 3 - 1 Một số giá trị PI

Giao thức được vận chuyển về lý thuyết có thể là bất kì: IPv4 hoặc IPv6. Trong trường hợp AToM, ta sẽ thấy giao thức được vận chuyển có thể là bất kì giao thức phổ biến lớp 2 nào như Frame Relay, PPP, HDLC, ATM và Ethernet.

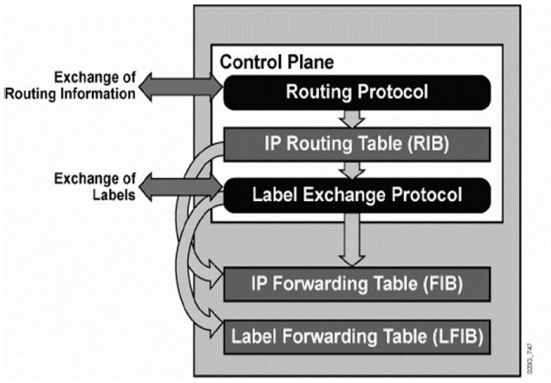
- ***LFIB (Label Forwarding Information Base)***

LFIB là một bảng dùng để chuyển tiếp gói tin đã được gán nhãn. Nó được tạo thành bởi các nhãn đến và đi cho các LSP. Nhãn đến là nhãn được gán nội bộ trên một LSR cụ thể. Nhãn ra là nhãn được gán từ xa được bởi một LSR từ tất cả các nhãn từ xa có thể. Tất cả các nhãn từ xa đó được tìm thấy ở LIB. LFIB chọn một trong số tất cả các nhãn ra có thể từ tất cả các nhãn được gán từ xa trong LIB và thêm vào trong LFIB. Nhãn được gán từ xa được chọn phụ thuộc vào tuyến đường tốt nhất tìm thấy trong bảng định tuyến.

Trong ví dụ IPv4 qua MPLS, nhãn được gán cho một tiền tố IPv4. Tuy nhiên, LFIB có thể được thu thập với nhãn mà LDP không gán. Trong trường hợp kỹ thuật lưu lượng (MPLS traffic engineering), các nhãn có thể được phân phối bởi RSVP. Trong trường hợp MPLS VPN, nhãn VPN được phân phối bởi BGP. Trong bất kì trường hợp nào, LFIB luôn được dùng để chuyển tiếp gói tin đến.

3.1.4.2 Mặt phẳng điều khiển (Control plane)

Mặt phẳng điều khiển là tập hợp các giao thức, chịu trách nhiệm trao đổi thông tin định tuyến và thông tin nhãn giữa các thiết bị láng giềng với nhau. Mặt phẳng điều khiển hỗ trợ cho việc thiết lập mặt phẳng dữ liệu hay chuyển tiếp. Hình 3-6 mô tả cấu trúc mặt phẳng điều khiển.



Hình 3 - 6 Mặt phẳng điều khiển

Mặt phẳng điều khiển xây dựng lên một bảng định tuyến (*Routing Information Base – RIB*) dựa trên các giao thức định tuyến. Có rất nhiều giao thức định tuyến như Open Shortest Path First (OSPF), Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), Intermediate System - to - Intermediate System (IS-IS), Routing Information Protocol (RIP) và Border Gateway Protocol (BGP) có thể được sử dụng trong mặt phẳng điều khiển cho việc quản lý định tuyến lớp 3.

Mặt phẳng điều khiển sử dụng giao thức trao đổi nhãn để tạo và duy trì nhãn bên trong, và trao đổi những nhãn này với những thiết bị láng riềng khác. Giao thức trao đổi nhãn gán nhãn cho những mạng học qua giao thức định tuyến. Giao thức trao đổi nhãn bao gồm MPLS Label Distribution Protocol (LDP), cũ hơn là Cisco Tag Distribution Protocol (TDP), và BGP (sử dụng bởi MPLS VPN), Resource Reservation Protocol (RSVP) được dùng bởi MPLS Traffic Engineering (TE) để thực hiện việc trao đổi.

Mặt phẳng điều khiển cũng xây dựng lên hai bảng, FIB từ thông tin của RIB và LFIB dựa trên giao thức trao đổi nhãn và RIB. Bảng LFIB chứa giá trị nhãn và cổng ra tương ứng cho mỗi tiền tố mạng.

3.1.5 Các phần tử chính của MPLS

3.1.5.1 LSR (Label Switch Router)

Thành phần cơ bản của mạng MPLS là router chuyển mạch nhãn LSR. Thiết bị này thực hiện chức năng chuyển tiếp gói tin trong phạm vi mạng MPLS dựa trên các tuyến đã thiết lập bằng thủ tục phân phối nhãn. Có ba loại LSR tồn tại trong mạng MPLS:

- *Ingress LSR* - LSR lối vào nhận gói chưa có nhãn, chèn nhãn vào trước gói và truyền đi trên đường liên kết dữ liệu.
- *Egress LSR* – LSR lối ra nhận các gói được gán nhãn, tách nhãn và truyền chúng trên đường kết nối dữ liệu. LSR lối ra và LSR lối vào đồng thời là các LSR biên.

- *Intermediate LSR* – LSR trung gian 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 3-2 mô tả các hoạt động đối với nhãn:

Hoạt động	Mô tả
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 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 khác.
Swap	Thay nhãn trên cùng trong ngăn xếp với giá trị khác
Untag	Gỡ bỏ nhãn trên cùng và chuyển tiếp gói IP tới trạm IP kế tiếp

Bảng 3 - 2 Một số hoạt động với nhãn

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. Một LSR phải có khả năng trao đổi nhãn. Nó có ý nghĩa rất đơn giản là khi nó nhận được gói đã gán nhãn, nhãn trên cùng của ngăn xếp được trao đổi với nhãn mới và gói tin được chuyển mạch trên đường kết nối dữ liệu.

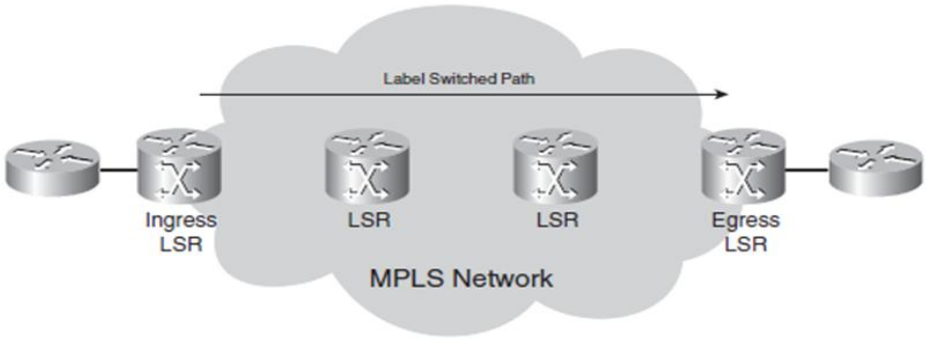
LSR gắn nhãn lên trên gói đầu tiên được gọi là *LSR imposing (gắn)* bởi vì nó là LSR đầu tiên đặt nhãn lên trên gói. Đây là một việc bắt buộc đối với một LSR lối vào. Một LSR tách tất cả các nhãn từ gói có gán nhãn trước khi chuyển mạch gói là một *LSR disposing (tách)* hay một LSR lối ra.

Trong MPLS VPN, các LSR lối vào và lối ra được biết đến như một router biên (PE). LSR trung gian được biết đến như một router lõi (P). Router PE và P trở lên phổ biến đến nỗi nó thường xuyên sử dụng khi mạng MPLS không chạy MPLS VPN.

Các LSR hoạt động ở ranh giới giữa mạng MPLS và mạng truy cập gọi là các LER (Label edge router).

3.1.5.2 LSP (Label Switched Path)

Đường chuyển mạch nhãn là một tập hợp các LSR 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 và là một LSR lối vào, ngược lại LSR cuối cùng của LSP là một LSR lối ra. Tất cả các LSR ở giữa LSR lối vào và lối ra chính là các LSR trung gian (xem hình 3-7). Trong hình 3-7 dưới đây mũi tên ở trên cùng chỉ hướng LSP bởi vì đường chuyển mạch nhãn là đường chỉ theo một chiều. Luồng các gói có nhãn theo một hướng khác – ví dụ từ phải sang trái – giữa các LSR biên sẽ là một LSP khác.



Hình 3 - 7 Một LSP qua mạng MPLS

3.1.5.3 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 đường và được xử lý theo cùng một cách chuyển tiếp. Tất cả các gói thuộc một FEC sẽ có nhãn giống nhau. Tuy nhiên không phải tất cả các gói có nhãn giống nhau 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 thuộc vào một FEC khác. Bộ định tuyến quyết định gói nào thuộc một FEC nào chính là LSR biên vào. Sau đây là một vài ví dụ về FEC:

Những gói với địa chỉ IP đích lớp 3 khớp với một tiền tố nào đó.

- Các gói tin có cùng một địa chỉ đích
- Gói multicast thuộc một nhóm nào đó.
- Gói với cùng phương thức chuyển tiếp, dựa trên thứ tự ưu tiên hoặc trường IP DiffServ Code Point (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 thuộc một tập tiền tố BGP, tất cả với cùng BGP bước tiếp theo.

3.1.6 Một số giao thức sử dụng trong MPLS

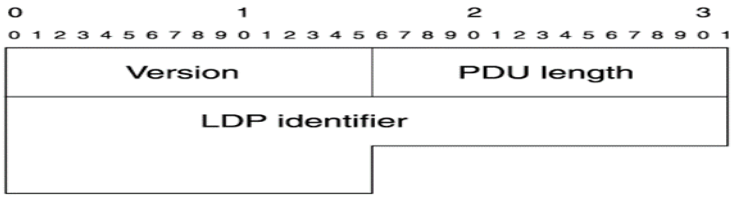
3.1.6.1 Giao thức phân phối nhãn

Để đưa gói tin qua một LSP trong một mạng MPLS, tất cả các LSR phải chạy giao thức phân phối nhãn và trao đổi thông tin nhãn với nhau. Khi tất cả các LSR đều có những nhãn cho một FEC nào đó, gói tin có thể được chuyển trên một LSP bằng cách chuyển mạch nhãn trên mỗi LSR. Các hoạt động trên nhãn (tráo đổi, chèn, gỡ bỏ) đều được LSR hiểu được khi nhìn vào LFIB. LIB được thu thập bằng những sự ràng buộc nhãn nhận bởi LDP, RSVP, MP-BGP hoặc ràng buộc tĩnh. RSVP phân phối nhãn cho MPLS Traffic Engineering và MP-BGP phân phối nhãn cho tuyến BGP, chúng ta chỉ còn lại LDP để phân phối nhãn cho các tuyến đường nội. Do đó, tất cả các LSR kết nối trực tiếp với nhau phải thiết lập mối quan hệ ngang hàng hay phiên LDP với nhau. Các

LDP ngang hàng trao đổi gói tin ánh xạ nhãn qua phiên LDP này. Sự ánh xạ nhãn là việc một nhãn được gán cho một FEC. LDP có bốn chức năng chính là:

- ***Sự phát hiện các LSR lân cận***
- ***Sự thiết lập và bảo trì phiên làm việc***
- ***Sự quảng bá ánh xạ nhãn***
- ***Duy trì nhãn bằng thông báo***

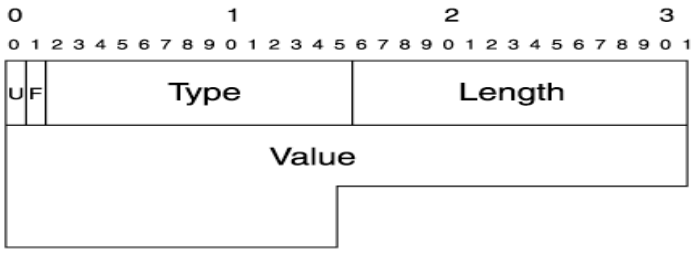
Trước khi đi sâu vào các chức năng chính của LDP, chúng ta hãy tìm hiểu định dạng cơ bản của gói tin LDP. Mỗi gói tin LDP được gọi là đơn vị dữ liệu giao thức (PDU), bắt đầu bằng tiêu đề gói tin (header) như hình 3-8 dưới đây tiếp sau đó là các bản tin LDP cụ thể nào đó:



Hình 3 - 8 Định dạng cơ bản của header LDP PDU

- *Phiên bản:* Số phiên bản của giao thức, hiện tại là phiên bản 1.
- *Độ dài PDU*: Tổng độ dài PDU tính theo octet, không tính trường phiên bản và trường độ dài.
- *Nhận dạng LDP:* Nhận dạng không gian nhãn của LSR gửi bản tin này. Bốn byte đầu chứa địa chỉ IP gán cho LSR: nhận dạng router. Hai octet sau nhận dạng không gian nhãn bên trong LSR. Nếu không gian nhãn là *per platform* thì trường này nhận giá trị 0 ngược lại *per interface* thì trường này nhận giá trị khác 0.

Định dạng các bản tin LDP theo sau header của gói tin LDP được đóng gói dưới dạng T-L-V như hình 3-9 sau:



Hình 3 - 9 Định dạng cơ bản của các bản tin LDP

- *U bit*: Nếu có giá trị 1 có nghĩa là các router nhận được sẽ bỏ qua nó nếu router đó hiểu được bản tin này.

- *Forward (F) bit:* Chỉ được sử dụng khi bit U có giá trị 1. Do những bit này luôn là 0 trong bản tin định nghĩa bởi RFC 3036 nên chúng ta không đi sâu vào phần này.
- *Trường Type:* Chỉ ra loại dữ liệu được mang trong vị trí Value của TLV.
- *Trường Length:* Chỉ ra độ dài dữ liệu mang trong vị trí Value của TLV.
- *Trường Value:* Phụ thuộc vào loại bản tin mà có các giá trị khác nhau. Một số loại bản tin có thể kể ra như: *Notification, Hello, Initialization, KeepAlive, Address, Address Withdraw, Label Mapping, Label Request, Lable Abort Request, Withdraw, Lable Release*. Chi tiết từng loại bản tin ở khuôn khổ đồ án không nhắc tới.

Sau đây chúng ta đi tìm hiểu sâu hơn về các chức năng của LDP:

- ***Sự phát hiện các LSR lân cận***: LSR chạy LDP gửi bản tin *LDP Hello* trên tất cả các interface mà LDP được kích hoạt. Bản tin *LDP Hello* là một bản tin UDP được gửi cho tất cả các router trên cùng mạng con này hay nói một cách khác tới địa chỉ multicast 224.0.0.2. Cổng UDP được sử dụng cho LDP là 646. LSR nhận được bản tin *LDP Hello* trên cổng nào sẽ nhận ra sự có mặt của router LDP này trên cổng đó.
- ***Sự thiết lập và bảo trì phiên làm việc:*** Nếu hai LSR phát hiện thấy nhau bằng LDP Hello, chúng sẽ cố gắng để thiết lập phiên LDP giữa chúng. Một LSR cố gắng mở một kết nối TCP port 646 tới LSR kia. Nếu kết nối TCP được thiết lập, cả hai LSR sẽ trao đổi bản tin *LDP Initialization* để thống nhất về các thông số của phiên làm việc. Những thông số này như sau:
  - Giá trị thời gian
  - Cách thức phân phối nhãn
  - Phạm vi VPI/VCI cho Label Controlled ATM (LC-ATM)
  - Phạm vi Data-link connection identifier (DLCI) cho LC-Frame Relay

  Nếu cả hai router thống nhất xong các tham số phiên, chúng sẽ giữ kết nối TCP với nhau. Và sau khi phiên LDP được thiết lập, chúng sẽ được duy trì bằng các gói tin *keepalive* định kì. Mỗi LDP ngang hàng nhận được gói tin *keepalive*, thời gian để chờ trước khi gỡ bỏ LSR đó ra các danh sách đã phát hiện ở bước trước (hold time) được thiết lập lại.

- ***Sự quảng bá ánh xạ nhãn***: Sự quảng bá ánh xạ nhãn là mục đích chính của LDP. Chúng ta có rất nhiều chế độ làm việc khác nhau của LSR khi phân phối nhãn:
  - *Chế độ phân phối theo yêu cầu (Downstream on Demand- DoD):* ở chế độ này, mỗi LSR yêu cầu LSR phía sau của nó thông báo về sự ánh xạ cho FEC nào đó. Mỗi LSR chỉ nhận một sự ánh xạ cho một FEC từ LSR phía sau.

- *Chế độ phân phối nhãn không yêu cầu trước (Unsolicited Downstream-UD):* Trong chế độ này, mỗi LSR phân phối ánh xạ nhãn cho những LSR láng giềng của nó mà không cần những LSR đó yêu cầu.
- *Chế độ duy trì nhãn tự do (Liberal Label Retention - LLR):* LSR giữ tất cả những ánh xạ nhận được từ các LSR khác trong LIB. Chỉ có ánh xạ của LSR xuôi dòng được dùng trong LFIB tất cả các ánh xạ từ các router khác đều không được đặt trong LFIB do đó, không phải tất cả đều được dùng để chuyển gói tin. Một lợi thế của phương pháp này là định tuyến luôn động, ở bất kì thời điểm nào nó cũng có thể thay đổi ví dụ như một đường liên kết bị hỏng hoặc router bị gỡ bỏ, do đó router kế tiếp cho một FEC có thể thay đổi. Ở thời điểm đó, nhãn cho router kế tiếp mới đã có trong LIB và LFIB có thể cập nhật nhanh chóng với nhãn ra mới.
- *Chế độ duy trì nhãn bảo thủ (Conservative Label Retention - CLR):* LSR không lưu trữ tất cả các ánh xạ từ xa trong LIB mà chỉ lưu trữ những ánh xạ từ xa nào có liên kết với một LSR kế tiếp cho một FEC nào đó. Điều này làm giảm bộ nhớ cần thiết để lưu trữ LIB.
- *Chế độ điều khiển độc lập (Independent LSP Control mode):* LSR có thể tạo các ánh xạ cục bộ cho một FEC độc lập với các LSR khác. Ở chế độ này mỗi LSR tạo ảnh xạ cục bộ cho một FEC nào đó ngay sau khi nó nhận ra FEC đó.
- *Chế độ điều khiển theo thứ tự (Ordered LSP Control mode):* Ở chế độ này LSR chỉ tạo ánh xạ cục bộ cho FEC mà nó nhận ra nó là LSR lối ra cho FEC hoặc nếu LSR đã nhận ánh xạ nhãn từ LSR kế tiếp cho FEC đó.

Dù là chế độ nào của LDP LSR đang hoạt động thì mục đích đều là ánh xạ nhãn. Mỗi LSR gán một nhãn cục bộ cho mỗi tiền tố IGP trong bảng định tuyến. Đây là sự ánh xạ nhãn cục bộ. Những ánh xạ cục bộ này được lưu trong LIB của router, sau đó lại được quảng bá cho tất cả các LDP ngang hàng thông qua phiên LDP và chúng sẽ trở thành ánh xạ từ xa trên những LDP ngang hàng đó.

- ***Sự thu hồi nhãn:*** Khi một LDP ngang hàng quảng bá ánh xạ nhãn, các LDP ngang hàng khác giữ nó cho đến khi phiên LDP đóng lại hoặc đến khi nhãn được thu hồi. Nhãn có thể được thu hồi nếu nhãn cục bộ thay đổi. Nhãn cục bộ có thể thay đổi, ví dụ interface với tiền tố cụ thể trên đó bị đứt kết nối nhưng LSR khác vẫn quảng bá tiền tố. Do đó, nhãn nội bộ cho tiền tố đó thay đổi từ implicit NULL tới một nhãn khác. Nếu điều đó xảy ra, nhãn implicit NULL sẽ ngay lập tức được thu hồi bằng cách gửi thông điệp *Label Withdraw* tới các LDP ngang hàng với nó. Nhãn mới được quảng bá trong một thông điệp *Label Mapping*.
- ***Duy trì nhãn bằng thông báo:*** Thông điệp *Notification* cần cho việc duy trì phiên LDP. Thông điệp này báo hiệu những sự kiện quan trọng tới LDP ngang hàng. Những thông điệp này có thể là lỗi không tránh được (*Error*

Notifications) hoặc thông tin tư vấn đơn giản (*Advisory Notification*). *Advisory Notification* được dùng để gửi thông tin về phiên LDP hoặc thông điệp nhận từ LDP ngang hàng. Những sự kiện có thể báo hiệu bằng gửi thông điệp *notification* có thể kể đến như:

- Protocol data unit (PDU) hoặc thông điệp không hợp lệ
- Type – Length – Value (TLV) không hợp lệ
- Hết thời gian keepalive của phiên
- Một bên đóng phiên
- Sự kiện thông điệp Initialization
- Sự kiện là kết quả từ thông điệp khác
- Lỗi bên trong
- Phát hiện thấy lặp
- Các sự kiện phức tạp khác

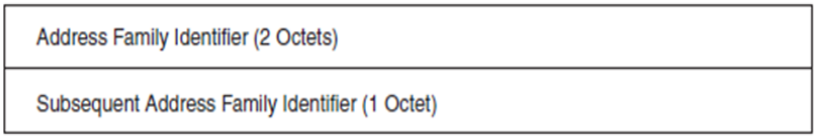
3.1.6.2 MP-BGP

BGP là một giao thức định tuyến phù hợp cho việc mang hàng trăm ngàn tuyến đường. Đồng thời BGP cũng là một giao thức cho phép thiết lập những chính sách mở rộng và mềm dẻo. Đó là lý do vì sao nó là một ứng cử viên tốt để mang tuyến đường MPLS VPN (vpnv4 route). BGP cần phải chuyển các tuyến đường vpnv4 (sẽ được đề cập phía sau) giữa các PE router với nhau.

- ***BGP mở rộng (MP-BGP)***

BGP được mô tả trong RFC 1771 chỉ có khả năng mang theo IPv4 tuy nhiên với việc RFC 2858 ra đời, BGP đã có khả năng mang theo nhiều thông tin định tuyến khác ngoài IPv4 ví dụ BGP có thể mang theo IPv6.

Sự mở rộng của BGP-4 định nghĩa hai thuộc tính BGP mới: *Multiprotocol Reachable NLRI* (Network Layer Reachability Information) và *Multiprotocol Unreachable NLRI*. Những thuộc tính này quảng bá và thu hồi tuyến đường. Tất cả chúng đều giữ hai trường: *Address Family Identifier (AFI)* và *Subsequent Address Family Identifier (SAFI)*. Khi kết hợp hai trường đó với nhau sẽ diễn tả chính xác tuyến đường nào mà BGP đang mang theo. Hình 3 – 10 mô tả bộ dữ liệu này.



Hình 3 - 10 Sự kết hợp giữa AFI và SAFI

Bảng 3- 3 Một vài số AFI và mô tả tương ứng

Number	Description
0	Reserved
1	IP (IP version 4)
2	IP6 (IP version 6)
11	IPX
12	AppleTalk

Bảng 3 - 3 Một vài số Address Family

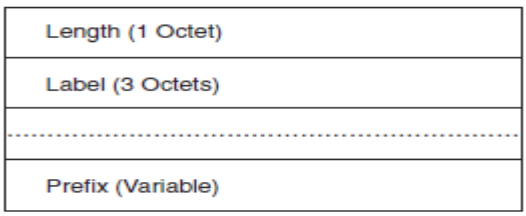
Bảng 3- 4 liệt kê một số các SAFI và mô tả tương ứng cho IP AFI

Number	Description
1	NLRI[1] for unicast forwarding
2	NLRI for multicast forwarding
3	NLRI for both unicast and multicast forwarding
4	NLRI for IPv4 and label forwarding
128	NLRI for labeled VPN forwarding

Bảng 3 - 4 Các số SAFI

- ***BGP mang theo nhãn***

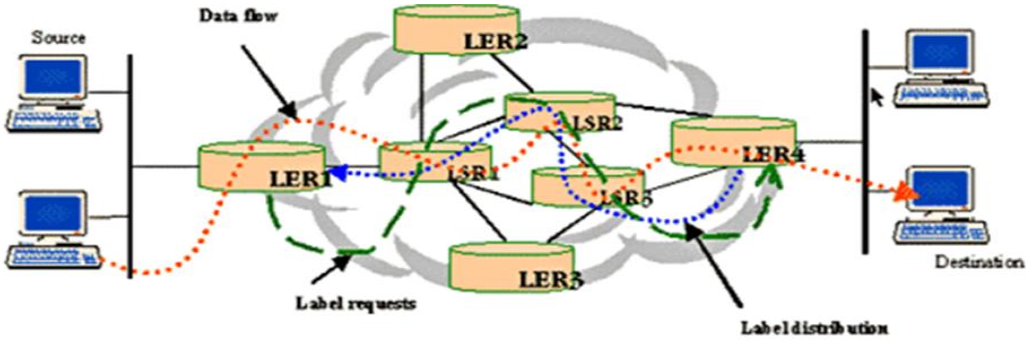
BGP quảng bá tiền tố vpnv4 trong mạng MPLS VPN. Điều này không đủ để chuyển lưu lượng VPN một cách chính xác. Để router PE đầu ra có thể chuyển lưu lượng VPN chính xác tới các router CE, nó phải chuyển gói tin dựa trên một nhãn. Router PE đầu ra có thể ánh xạ một nhãn tới một tiền tố vpnv4, nó gọi là nhãn VPN. Router PE đầu ra phải quảng bá nhãn cùng với tiền tố vpnv4 tới tất cả các router PE đầu vào có thể. Nhãn đơn giản được gắn vào tiền tố vpnv4 và được quảng bá bằng BGP sử dụng thuộc tính mở rộng đa giao thức. Nhãn được chứa trong trường NLRI. Ví dụ AFI bằng 1 và SAFI bằng 128 trong trường hợp MPLS VPN cho IPv4. Hình 3-11 cho thấy sự đóng gói của trường NLRI cho MPLS VPN.



Hình 3 - 11 Sự đóng gói nhãn

3.1.7 Hoạt động của MPLS

Hình 3-12 sau minh họa sự hoạt động của mạng MPLS:



Hình 3 - 12 Hoạt động của MPLS

Để gói tin truyền qua mạng MPLS, mạng sẽ thực hiện các bước sau:

- *Tạo và phân phối nhãn*
- *Tạo bảng ở mỗi router*
- *Tạo đường chuyển mạch nhãn*
- *Chèn nhãn / tra cứu bảng*
- *Truyền gói tin*

Nguồn gửi các dữ liệu của nó tới đích. Trong miền MPLS, không phải tất cả các lưu lượng từ một nguồn cần thiết truyền qua cùng một tuyến đường. Dựa trên các đặc tính lưu lượng, các LSP khác nhau có thể được tạo ra cho các gói tin với các yêu cầu khác nhau từ phía nguồn.

- *Tạo và phân phối nhãn:* Trước khi dữ liệu truyền, router quyết định tạo ra liên kết nhãn tới các FEC cụ thể và tạo bảng. Trong LDP các router phía dưới bắt đầu gán nhãn vào FEC và phân phối nhãn. Các đặc tính liên quan đến lưu lượng và dung lượng MPLS được điều chỉnh thông qua giao thức LDP. Giao thức báo hiệu nên dùng giao thức vận chuyển có thứ tự và đảm bảo tin cậy. LDP sử dụng TCP.
- *Tạo bảng ở mỗi router*: Khi chấp nhận các liên kết nhãn, mỗi LSR tạo ra bảng cơ sở dữ liệu nhãn (LIB). Nội dung bảng này xác định mối liên hệ giữa nhãn và FEC, các thông tin nhãn nó tự sinh ra và nhận được từ các router khác cho một FEC. Các LIB được cập nhật khi có sự thay đổi và điều chỉnh nhãn. Sau khi tạo LIB, router tiếp tục kết hợp với thông tin RIB hình thành bảng cơ sở chuyển tiếp thông tin nhãn (LFIB). Bảng này thể hiện rõ mối quan hệ giữa nhãn vào và nhãn ra cộng với địa chỉ router tiếp theo cần chuyển tiếp tới tương ứng.
- *Tạo đường chuyển mạch nhãn:* Các LSP được tạo ra theo chiều ngược với chiều tạo các mục trong các LIB như chỉ ra bằng nét đứt màu xanh đậm.
- *Chèn nhãn / tra cứu bảng*: Router đầu tiên LER1 trong hình trên sử dụng bảng LIB để tìm đường tiếp theo và yêu cầu nhãn cho FEC cụ thể. Các bộ định tuyến

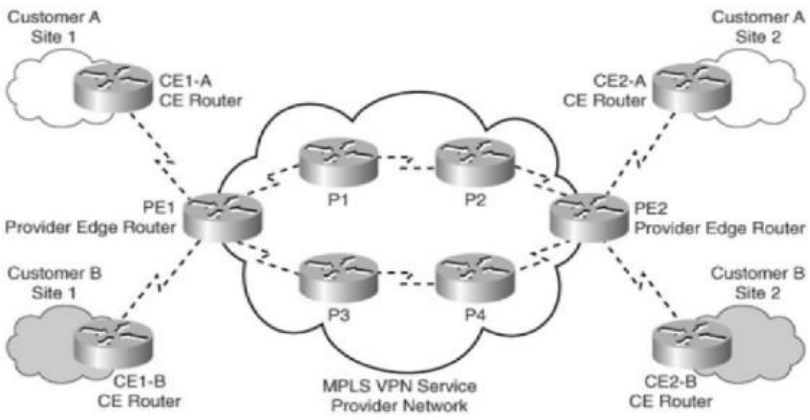
tiếp theo chỉ sử dụng nhãn để tìm đường tiếp theo. Khi gói tin đến LSR lối ra LER4 như hình trên nhãn được loại bỏ và gói tin được truyền tới đích.

- *Chuyển tiếp gói tin:* Hình 3-13 trên cũng mô tả đường đi của gói tin khi nó được truyền từ nguồn tới đích. Các gói tin có thể không có nhãn tại LER1 khi nó là router yêu cầu đầu tiên về nhãn này. Trong mạng IP, nó sẽ tìm địa chỉ trùng hợp dài nhất để tìm bước tiếp theo. LSR1 là bước tiếp theo của LER1. LER1 sẽ khởi tạo yêu cầu nhãn tới LSR1. Yêu cầu này được phát trên toàn mạng như chỉ ra bởi đường nét đứt xanh lá cây. Mỗi router trung gian LSR2 và LSR3 sẽ nhận gói tin gán nhãn từ các router luồng xuống của nó bắt đầu từ router LER2 ngược trở lên LER1. LDP sẽ xác định đường dẫn ảo đảm bảo QoS như chỉ ra bởi đường nét đứt xanh đậm trên hình. LER1 sẽ tạo nhãn và truyền gói tin tới LSR1. Các LSR tiếp theo ví dụ LSR2 và LSR3 sẽ kiểm tra nhãn trong gói tin nhận được, sửa nó với nhãn ra tương ứng và truyền gói tin. Khi gói tin đến LER4, nó sẽ gỡ hết nhãn vì gói tin đi ra khỏi miền MPLS và chuyển tới đích. Đường đi thực sự của gói tin được thể hiện bởi đường nét đứt màu đỏ.

3.2 Công nghệ VPN dựa trên MPLS

3.2.1 Các thành phần cơ bản của MPLS-VPN

Một cách khái quát, mô hình hệ thống cung cấp dịch vụ MPLS-VPN được thể hiện như trên hình 3-13 dưới đây: [8]



Hình 3 - 13 Các thành phần cơ bản của MPLS VPN

Như trên hình 3-13 có thể thấy các thành phần cơ bản của MPLS VPN bao gồm:

- Mạng lõi IP/MPLS được quản trị bằng nhà cung cấp dịch vụ
- Bộ định tuyến lõi (P) của nhà cung cấp dịch vụ
- Bộ định tuyến biên của nhà mạng (PE) cung cấp thông tin định tuyến của khách hàng và thực hiện đáp ứng dịch vụ cho khách hàng từ phía nhà cung cấp
- Mạng khách hàng được coi là mạng truy cập tới vùng mạng lõi

- Bộ định tuyến khách hàng (CE) đóng vai trò cầu nối giữa mạng khách hàng và mạng nhà cung cấp. Nó có thể được quản trị bởi khách hàng hoặc nhà cung cấp dịch vụ

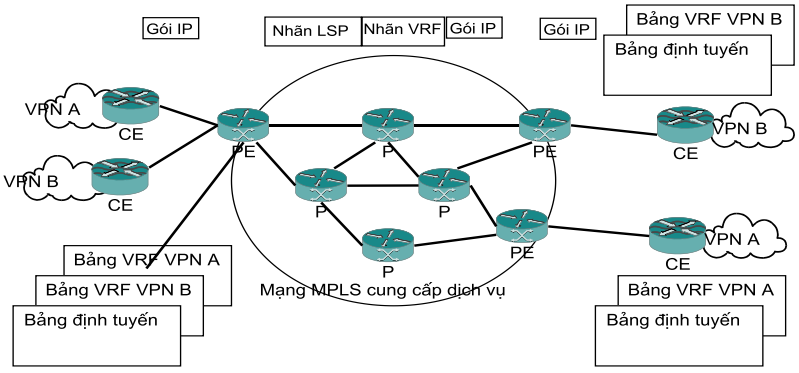
3.2.2 Các mô hình MPLS – VPN

Hiện nay có hai mô hình triển khai mạng riêng ảo trên nền MPLS phổ biến là mạng riêng ảo lớp 3 (Layer 3 VPN) và mạng riêng ảo lớp 2 (Layer 2 VPN). Sau đây sẽ giới thiệu những đặc điểm chính của hai mô hình này.[7]

3.2.2.1 Mô hình mạng riêng ảo lớp 3

Kiến trúc mạng riêng ảo L3VPN được chia thành hai lớp, tương ứng với các lớp 3 và 2 của mô hình OSI. L3VPN dựa trên RFC 2547, mở rộng một số đặc tính cơ bản của giao thức cổng biên BGP (Border Gateway Protocol) và tập trung vào hướng đa giao thức của BGP nhằm phân bổ các thông tin định tuyến qua mạng lõi của nhà cung cấp dịch vụ cũng như là chuyển tiếp các lưu lượng VPN qua mạng lõi.

Trong kiến trúc L3VPN, các bộ định tuyến khách hàng và của nhà cung cấp được coi là các phần tử ngang hàng. Bộ định tuyến biên khách hàng CE cung cấp thông tin định tuyến tới bộ định tuyến biên nhà cung cấp PE. PE lưu các thông tin định tuyến trong bảng định tuyến và chuyển tiếp ảo VRF. Mỗi khoản mục của VRF tương ứng với một mạng khách hàng và hoàn toàn biệt lập với các mạng khách hàng khác. Người sử dụng VPN chỉ được phép truy nhập tới các site hoặc máy chủ trong cùng một mạng riêng này. Bộ định tuyến PE còn hỗ trợ các bảng định tuyến thông thường nhằm chuyển tiếp lưu lượng của khách hàng qua mạng công cộng. Một cấu hình mạng L3VPN dựa trên MPLS được chỉ ra trên hình 3-14



Hình 3 - 14 Mô hình MPLS L3 VPN

Các gói tin IP qua miền MPLS được gắn hai loại nhãn, bao gồm nhãn MPLS chỉ thị đường dẫn chuyển mạch nhãn LSP và nhãn chỉ thị định tuyến/chuyển tiếp ảo VRF. Ngăn xếp nhãn được thiết lập để chứa các nhãn trên. Các bộ định tuyến P của nhà cung cấp xử lý nhãn LSP để chuyển tiếp các gói tin qua miền MPLS. Nhãn VRF chỉ được xử lý tại thiết bị định tuyến biên PE nối với bộ định tuyến khách hàng.

Mô hình L3VPN có ưu điểm là không gian địa chỉ khách hàng được quản lý bởi nhà khai thác, và do vậy nó cho phép đơn giản hóa việc triển khai kết nối với nhà cung cấp. Ngoài ra, L3VPN còn cung cấp khả năng định tuyến động để phân phối các thông

tin định tuyến tới các bộ định tuyến VPN. Tuy nhiên, L3VPN chỉ hỗ trợ các lưu lượng IP hoặc lưu lượng đóng gói vào gói tin IP. Đồng thời, việc tồn tại hai bảng định tuyến tại các thiết bị biên mạng cũng là một vấn đề phức tạp trong điều hành và ảnh hưởng tới khả năng mở rộng các hệ thống thiết bị.

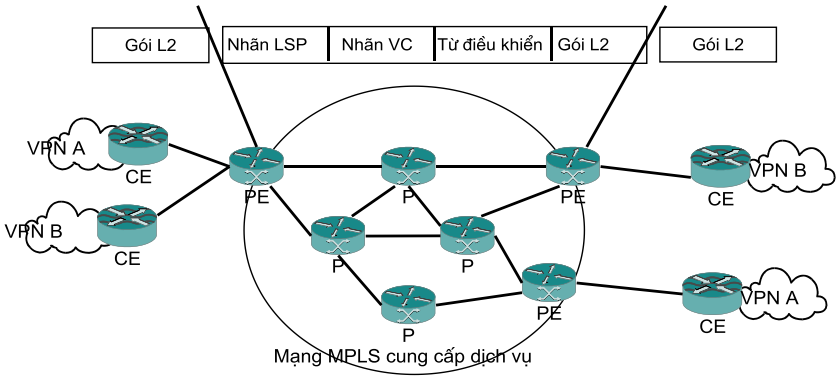
3.2.2.2 Mô hình mạng riêng ảo lớp 2

Mô hình mạng riêng ảo lớp 2 được phát triển sau và các tiêu chuẩn vẫn đang trong giai đoạn hoàn thiện. Cách tiếp cận L2VPN hướng tới việc thiết lập các đường hầm qua mạng MPLS để xử lý các kiểu lưu lượng khác nhau như Ethernet, FR, ATM và PPP/HDLC.

Có hai dạng L2VPN cơ bản là:

- ***Điểm tới điểm:*** tương tự như trong công nghệ ATM và FR, nhằm thiết lập các đường dẫn chuyển mạch ảo qua mạng;
- ***Điểm tới đa điểm:*** hỗ trợ các cấu hình mắt lưới và phân cấp.

Trong những năm gần đây, dịch vụ LAN ảo dựa trên mô hình Layer 2 VPN đa điểm sử dụng công nghệ truy nhập Ethernet đã được triển khai rộng rãi. Giải pháp này cho phép liên kết các mạng Ethernet qua hạ tầng MPLS trên cơ sở nhận dạng lớp 2, vì vậy mà giảm được độ phức tạp của các bảng định tuyến lớp 3. Trong mô hình Layer 2 VPN các bộ định tuyến CE và PE không nhất thiết phải được coi là ngang hàng (hình 3-15). Thay vào đó, chỉ cần tồn tại kết nối lớp 2 giữa các bộ định tuyến này. Bộ định tuyến PE chuyển mạch các luồng lưu lượng vào trong các đường hầm đã được cấu hình trước tới các bộ định tuyến PE khác.



Hình 3 - 15 Mô hình MPLS L2 VPN

Layer 2 VPN xác định khả năng tìm kiếm qua mặt phẳng dữ liệu bằng địa chỉ học được từ các bộ định tuyến lân cận. Layer 2 VPN sử dụng ngăn xếp nhãn tương tự như trong Layer 3 VPN. Nhãn MPLS bên ngoài được sử dụng để xác định đường dẫn cho lưu lượng qua miền MPLS, còn nhãn kênh ảo VC nhận dạng các mạng LAN ảo, VPN hoặc kết nối tại các điểm cuối. Một trường nhãn tuỳ chọn sử dụng để điều khiển đóng các kết nối lớp 2 được đặt trong cùng ngăn xếp sát với trường dữ liệu.

Later 2 VPN có ưu điểm quan trọng nhất là cho phép các giao thức lớp cao được truyền trong suốt đối với MPLS. Nó có thể hoạt động trên hầu hết các công nghệ lớp 2 gồm ATM, FR, Ethernet và mở ra khả năng tích hợp các mạng phi kết nối IP với các

mạng hướng kết nối. Ngoài ra, trong giải pháp này người sử dụng đầu cuối không cần phải cấu hình định tuyến cho các bộ định tuyến khách hàng CE.

Tuy nhiên, L2VPN không dễ dàng mở rộng như L3VPN. Một cấu hình đầy đủ cho các LSP phải được sử dụng để kết nối các VPN trong mạng. Hơn nữa, L2VPN không thể tự động định tuyến giữa các site. Vì vậy, tuỳ thuộc vào cấu hình mạng MPLS và nhu cầu cụ thể mà có thể sử dụng một trong hai mô hình nói trên.

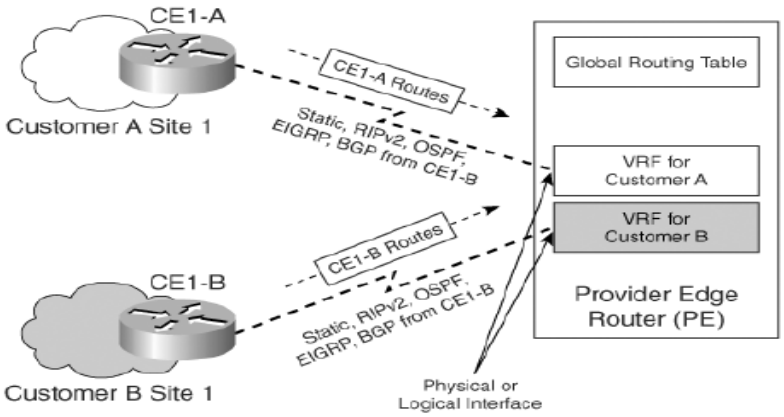
3.2.3 Kiến trúc tổng quan của MPLS-VPN

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 Target (đích của tuyến), sự ánh xạ tuyến qua MP-BGP và chuyển tiếp gói tin được gắn nhãn.

3.2.3.1 VRF- Virtual Routing and Forwarding Table

Khách hàng được phân biệt trên router PE bằng các bảng định tuyến và chuyển tiếp ảo (Virtual forwarding and routing table) 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 nhà cung cấp. Chức năng của VRF giống như một bảng 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 nói một cách khác là sử dụng VRF. Giao tiếp (interface) 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 không những 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 context), VRF còn chứa các định danh VPN (VPN identifier) như thông tin thành viên VPN (RD và RT). Hình 3-16 cho thấy chức năng của VRF trên một router PE thực hiện tách tuyến khách hàng.



Hình 3 - 16 Chức năng của VRF

Các giao thức định tuyến khác nhau chạy như những tiến trình định tuyến riêng biệt (OSPF, EIGRP…) trên router. Tuy nhiên một số giao thức như RIP và BGP, router chỉ hỗ trợ một instance của giao thức định tuyến. Do đó, thực thi định tuyến VRF bằng 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 cảnh 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.

3.2.3.2 Route Distinguisher - RD

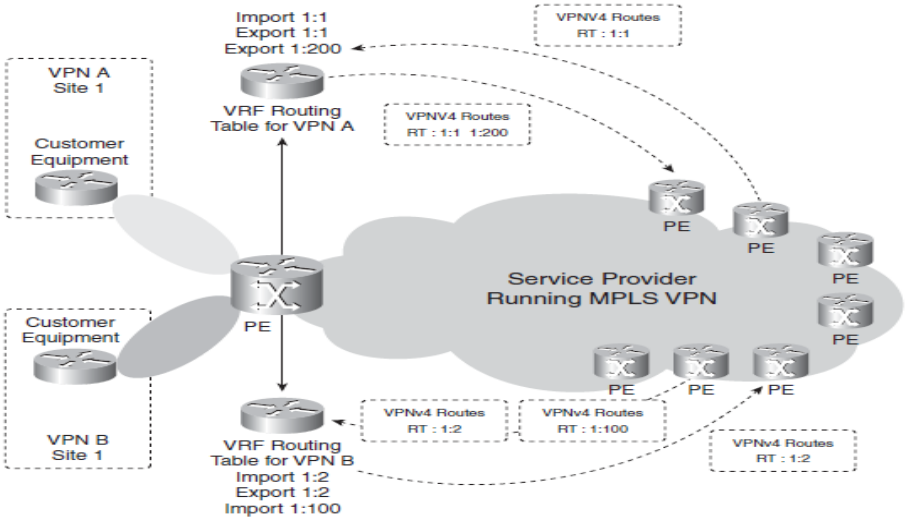
Các tiền tố VPN chuyển qua mạng MPLS VPN bằng MP-BGP. Tuy nhiên khi BGP mang những tiền tố IPv4 qua mạng nhà cung cấp, chúng phải là duy nhất. Nếu các khách hàng sử dụng địa chỉ chồng lấn nhau, quá trình định tuyến sẽ sai lệch. Để giải quyết vấn đề này, khái niệm RD được tạo ra để làm cho các tiền tố IPv4 trở nên duy nhất. Ý tưởng cơ bản là mỗi tiền tố từ khách hàng nhận được một định danh duy nhất (RD) để phân biệt các tiền tố giống nhau từ các khách hàng. Một tiền tố được tạo thành từ sự kết hợp của tiền tố IPv4 và RD gọi là tiền tố vpnv4. MP-BGP cần phải chuyển những tiền tố này giữa các router PE. Một RD là một trường 64-bit được sử dụng để làm cho các tiền tố VRF là duy nhất khi MP-BGP vận chuyển nó. RD không thể chỉ ra tiền tố đó thuộc VRF nào. Chức năng của RD không phải là định danh một VPN bởi vì có một số trường hợp VPN phức tạp cần nhiều hơn một RD. Mỗi tiến trình VRF trên PE router cần một RD gán cho nó. Giá trị 64 bit này có thể viết ở 2 dạng: ASN:nn hoặc IP-address:nn với nn biểu diễn là một số. Định dạng dùng phổ biến là ASN:nn với ASN là số mà IANA cấp cho nhà cung cấp dịch vụ và nn là số mà nhà cung cấp dịch vụ gán duy nhất cho VRF. RD chỉ dùng để làm cho tuyến đường VPN trở nên duy nhất. Sự kết hợp giữa RD và tiền tố IPv4 tạo thành tiền tố vpnv4 có chiều dài 96 bit. Mặt nạ vẫn có độ dài 32 bit như đối với địa chỉ IPv4. Nếu ta nhận một tiền tố IPv4 10.1.1.0/24 và một 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 đường IPv4. Khi một site VPN kết nối với hai PE router, tuyến đường từ VPN site đó có thể nhận hai giá trị RD khác nhau, tùy thuộc vào router PE nhận tuyến đường. Mỗi tuyến đường IPv4 có thể nhận hai giá trị RD khác nhau, do đó có thể có hai vpnv4 khác nhau. Điều này cho phép BGP xem xét chúng như là những tuyến đường khác nhau và áp dụng các chính sách khác nhau.

3.2.3.3 Route Target - RT

Nếu chỉ có RD được sử dụng cho 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 vì RD không giống nhau. Khái niệm nhiều site của công ty A có khả năng kết nối với nhiều site của công ty B 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 gọi là RT – route target. RT là một thuộc tính mở rộng của BGP chỉ ra tuyến nào có thể import từ MP BGP vào VRF. Export RT có nghĩa là một tuyến vpnv4 quảng bá ra nhận một thuộc tính mở rộng – đó chính là RT – khi tuyến được phân phối lại từ bảng định tuyến VRF vào trong MP-BGP. Import RT có nghĩa là tuyến vpnv4 nhận được từ MP-BGP được kiểm tra khớp thuộc tính mở rộng – đó là RT – với một cái đang tồn tại trong cấu hình thiết bị. Nếu kết quả là trùng nhau, tiền tố này được đặt trong bảng định tuyến VRF như một tuyến IPv4. Nếu kết quả không khớp tiền tố này sẽ được đẩy ra.

Hình 3-17 chỉ ra RT điều khiển những tuyến đường nào sẽ được nhập vào VRF nào từ các router PE đằng xa và các tuyến đường vpnv4 sẽ được xuất ra với các RT nào tới các router PE đằng xa. Có thể có nhiều hơn một RT gắn với tuyến đường vpnv4. Để có thể nhập được vào VRF chỉ cần một RT từ tuyến đường vpnv4 cần phải trùng khớp trong cấu hình RT nhập bằng lệnh ip vrf trước đó trên router PE.

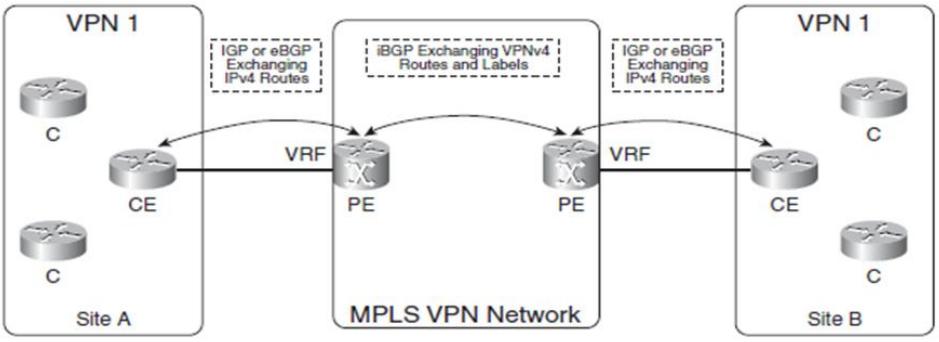


Hình 3 - 17 Route Target

3.2.4 Định tuyến VPNv4 trong mạng MPLS-VPN

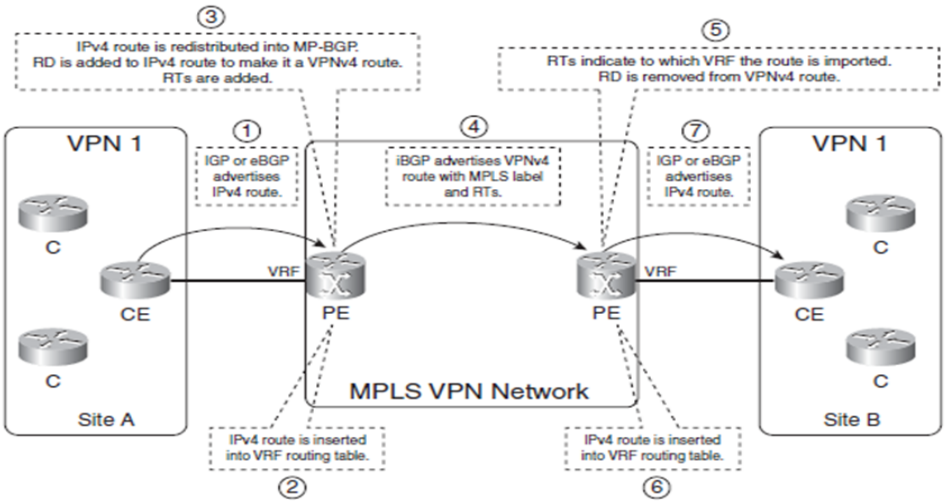
VRF phân biệt các tuyến đường của khách hàng trên các router PE nhưng làm thế nào để tiền tố vận chuyển qua mạng của nhà cung cấp dịch vụ. Bởi vì nhiều khả năng có một số lượng lớn các tuyến – có thể hàng trăm nghìn - được vận chuyển qua, BGP là một ứng cử viên tốt bởi vì nó là giao thức định tuyến đã được chứng minh và đảm bảo có thể mang rất nhiều tuyến. Thực tế BGP là giao thức định tuyến cơ bản để mang bảng định tuyến Internet hoàn chỉnh. Do 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 cũng có thể được vận chuyển một cách an toàn qua mạng MPLS VPN.

Hình 3-18 mô tả cái nhìn tổng quan về sự vận chuyển tuyến đường trong một mạng MPLS VPN.



Hình 3 - 18 Sự quảng bá tuyến đường trong mạng MPLS VPN

PE router nhận tuyến đường IPv4 từ các router CE thông qua giao thức định tuyến nội (IGP) hoặc ngoại BGP. Những tuyến IPv4 từ site VPN được đặt vào bảng định tuyến VRF. VRF nào được sử dụng phụ thuộc vào VRF nào được cấu hình trên interface của router PE nối với CE router. Những tuyến đường này được gắn với RD mà được chỉ định cho VRF đó. Vì vậy chúng trở thành tuyến đường vpnv4 và sau đó được đưa vào MP-BGP. BGP có trách nhiệm phân phối những tuyến đường vpnv4 tới tất cả các router PE trong mạng MPLS. Trên router PE, các tuyến đường vpnv4 được gỡ bỏ RD ra và đặt vào trong các bảng định tuyến VRF như tuyến đường IPv4. Liệu tuyến đường vpnv4 sau khi gỡ bỏ RD có được đưa vào VRF hay không lại tùy thuộc vào RT có cho phép nhập vào VRF đó hay không. Những tuyến IPv4 đó cuối cùng được quảng bá cho router CE thông qua một IGP hoặc eBGP chạy giữa PE và CE router. Hình 3-19 mô tả lần lượt các bước trong việc truyền tuyến đường từ CE tới CE qua mạng MPLS VPN.



Hình 3 - 19 Sự quảng bá tuyến đường trong mạng MPLS VPN theo từng bước

Do nhà cung cấp dịch vụ có mạng MPLS VPN chạy BGP trong một vùng tự trị nên iBGP đang được chạy giữa các router PE.

Sự lan truyền từ eBGP - chạy giữa PE và CE router - tới MP-iBGP trong mạng MPLS VPN và ngược lại là tự động và không phải cấu hình gì thêm. Tuy nhiên việc phân phối lại (redistribute) từ MP-iBGP vào IGP đang chạy giữa PE và CE router là không tự động. Ta phải cấu hình phân phối lại lẫn nhau giữa MP – iBGP và IGP.

3.2.5 Chuyển tiếp gói tin trong mạng MPLS-VPN

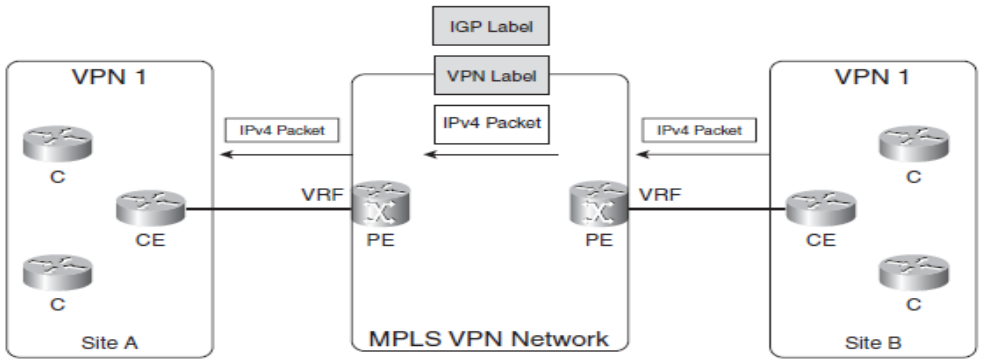
Như đã đề cập, những gói tin không thể được chuyển tiếp như những gói IP đơn thuần giữa các site. Router P không thể chuyển tiếp chúng bởi vì nó không có thông tin VRF từ mỗi site. MPLS có thể giải quyết vấn đề này bằng việc gán nhãn vào gói. Router P sau đó phải có thông tin chuyển tiếp đúng cho nhãn để chuyển tiếp gói. Cách chung nhất là cấu hình giao thức phân phối nhãn (LDP) giữa các bộ định tuyến P và PE để tất cả các lưu lượng IP có thể chuyển mạch nhãn giữa chúng. Ta 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 router PE đầu vào tới router PE đầu ra. Bộ định tuyến P không bao giờ phải thực hiện việc tìm kiếm địa chỉ IP đích. Đây là cách để các gói tin được chuyển mạch giữa các bộ định tuyến PE lối vào và ra. Những nhãn này gọi là nhãn IGP bởi vì nó là nhãn được gán cho các tiền tố IPv4 trong bảng định tuyến toàn cục của router P, PE và IGP của nhà cung cấp dịch vụ quảng bá nó.

Làm thế nào để router PE lối ra biết được gói nào thuộc VRF nào. Thông tin này không có trong header của IP và nó không thể được suy ra từ nhãn IGP bởi vì nó chỉ được sử dụng để chuyển tiếp nhãn qua mạng nhà cung cấp dịch vụ. Giải pháp là thêm một nhãn khác trong ngăn xếp nhãn. Nhãn này chỉ ra VRF mà gói tin thuộc về. Do đó, tất cả các gói tin của khách hàng được truyền đi với hai nhãn: Nhãn IGP là nhãn trên cùng và nhãn VPN là nhãn dưới cùng. Nhãn VPN phải được đặt lên bởi router PE đầu

vào để chỉ ra cho router PE đầu ra biết được gói tin thuộc VRF nào. Bằng cách nào mà router PE đầu ra báo hiệu cho router PE đầu vào nhãn nào được dùng cho tiền tố VRF? Bởi vì MP-BGP đã được sử dụng để quảng bá tiền tố vpnv4, nó cũng dùng để báo hiệu nhãn VPN được gắn với tiền tố vpnv4.

Nói tóm lại, lưu lượng VRF-tới-VRF có hai nhãn trong mạng MPLS VPN. Nhãn trên cùng là nhãn IGP và được quảng bá bởi LDP hoặc RSVP cho TE giữa các router P và PE từng chặng một. Nhãn dưới cùng là nhãn VPN được quảng bá bởi MP-iBGP từ PE tới PE. Router P sử dụng nhãn IGP để chuyển tiếp gói tin tới đúng router PE đầu ra. Router PE biên ra sử dụng nhãn VPN để chuyển tiếp gói tin tới đúng router CE.

Hình 3-20 mô tả một gói tin được chuyển tiếp trong một mạng MPLS VPN. Gói tin đi vào router PE trên một interface VRF như một gói tin IPv4. Nó được chuyển tiếp qua mạng MPLS VPN với hai nhãn. Những router P chuyển gói tin bằng cách xem xét nhãn trên cùng. Nhãn trên cùng được hoán đổi ở mỗi router P. Nhãn được gỡ bỏ ở router PE biên ra và gói tin được chuyển tiếp như một gói tin IPv4 trên interface VRF hướng tới router CE. Router CE chính xác được tìm thấy bằng cách nhìn vào nhãn VPN.



Hình 3 - 20 Chuyển tiếp gói tin trong mạng MPLS VPN

3.2.6 Bảo mật trong MPLS-VPN

[7] Bảo mật là một trong những yếu tố rất quan trọng đối với tất cả các giải pháp mạng VPN. Về khía cạnh bảo mật thì giải pháp VPN dựa trên BGP/MPLS có thể đạt được mức độ tương đương với các giải pháp VPN xây dựng trên công nghệ ATM hoặc Frame Relay.

Bảo mật cho VPN phải đảm bảo được sự cách ly về thông tin định tuyến cũng như về không gian địa chỉ của mỗi VPN. Nghĩa là việc cấp địa chỉ của mỗi VPN là hoàn toàn độc lập nhau. Thông tin định tuyến từ VPN này không được phép sang VPN khác và ngược lại. Yêu cầu thứ hai là bảo mật phải đảm bảo được cấu trúc mạng lõi hoàn toàn trong suốt với khách hàng sử dụng dịch vụ. Thứ ba, bảo mật phải đảm bảo được việc tránh làm giả nhãn như việc làm giả địa chỉ IP và chống lại các cuộc tấn công từ chối dịch vụ (Denial of Service) cũng như tấn công truy nhập dịch vụ (Instrusion).

Để thấy rõ việc bảo mật trong MPLS-VPN được thực hiện như thế nào, trước hết cần hiểu rằng MPLS-VPN cho phép sử dụng cùng không gian địa chỉ giữa các VPN nhưng vẫn đảm bảo được tính duy nhất của địa chỉ các site khách hàng nhờ vào giá trị 64 bit của trường phân biệt tuyến. Do đó, khách hàng sử dụng dịch vụ MPLS-VPN không cần phải thay đổi địa chỉ hiện tại của mình.

Việc định tuyến trong mạng của nhà cung cấp dịch vụ VPN được thực hiện trên chuyển mạch nhãn chứ không phải dựa trên địa chỉ IP truyền thống. Hơn nữa, mỗi LSP tương ứng với một tuyến VPN-IP được bắt đầu và kết thúc tại các bộ định tuyến PE chứ không bắt đầu và kết thúc ở một điểm trung gian nào trong mạng của nhà cung cấp. Do đó mạng lõi bên trong hoàn toàn trong suốt đối với khách hàng. Mỗi bộ định tuyến PE duy trì một bảng VRF riêng cho từng VPN, và VRF này chỉ phổ biến các tuyến thuộc về VPN đó. Nhờ vậy đảm bảo được sự cách ly thông tin định tuyến giữa các VPN với nhau.

Đối với giải pháp MPLS-VPN, thật khó có thể tấn công trực tiếp vào VPN. Chỉ có thể tấn công vào mạng lõi MPLS, rồi từ đó tấn công vào VPN. Mạng lõi có thể tấn công theo hai cách là trực tiếp vào bộ định tuyến PE hoặc vào các cơ chế báo hiệu MPLS. Tuy nhiên, để tấn công vào mạng, trước hết cần phải biết địa chỉ IP của nó. Nhưng mạng lõi MPLS lại hoàn toàn trong suốt với bên ngoài, do đó kẻ tấn công không thể biết được địa chỉ IP của bất kì bộ định tuyến nào trong mạng lõi. Chúng có thể đoán địa chỉ và gửi gói tin đến những địa chỉ này. Song trong mạng MPLS mỗi gói tin đi vào đều được xem như là thuộc về không gian địa chỉ nào đó của khách hàng, do đó khó có thể tìm được các bộ định tuyến bên trong ngay cả khi đoán được địa chỉ.

Có thể việc trao đổi thông tin định tuyến giữa các bộ định tuyến PE và CE sẽ là điểm yếu trong mạng MPLS-VPN, nhưng trên bộ định tuyến PE có thể dùng ACL và các phương pháp xác thực của giao thức định tuyến dùng trên kết nối đó sẽ đảm bảo được vấn đề bảo mật. Việc làm giả nhãn cũng khó có thể xảy ra vì bộ định tuyến PE chỉ chấp nhận những gói tin từ bộ định tuyến CE gửi đến không có nhãn. Nếu gói tin là có nhãn thì nhãn đó phải do PE kiểm soát và quản lý.

Từ những vấn đề nêu trên, có thể thấy việc bảo mật trong MPLS-VPN được bảo đảm ở mức độ rất cao và hoàn toàn có thể so sánh ngang bằng với việc bảo mật trong các giải pháp dựa trên ATM hay Frame Relay.

3.3 So sánh các đặc điểm của VPN trên nền IPSec và MPLS

[3]

3.3.1 VPN trên nền IPSec

Để bảo vệ dữ liệu qua mạng công cộng, giao thức IPSec hỗ trợ tổ hợp các chức năng bảo mật mạng sau:

- Nhận dạng và mã hoá các gói tin trước khi truyền dẫn;
- Xác thực các gói nhằm đảm bảo tính toàn vẹn của dữ liệu;
- Xác thực dữ liệu nguyên thuỷ của các nguồn gửi tin;
- Xác nhận và loại bỏ các gói quá hạn, gửi lặp và từ chối các gói lặp.

Giao thức IPSec cung cấp khả năng bảo vệ các gói tin IP theo thiết kế mạng để chỉ ra các lưu lượng đặc biệt cần bảo vệ. IPSec định nghĩa cách thức bảo vệ lưu lượng và điều khiển thiết bị nhận lưu lượng. VPN trên nền IPSec thay thế hoặc bổ sung các mạng riêng dựa trên hạ tầng WAN truyền thống như đường dây thuê riêng, Frame Relay hoặc ATM. Ưu điểm nổi trội của IPSec là nó đáp ứng được các yêu cầu của mạng về mặt giá thành.

Khi một doanh nghiệp sử dụng IPSec-VPN, nhà cung cấp dịch vụ thường cấu hình IPSec trong cấu hình Hub-and-Spoke, nơi tất cả các nhánh Spoke duy trì kết nối điểm-điểm với đầu cuối. IPSec rất phù hợp với cấu hình VPN điểm tới điểm và truy nhập từ xa.

Một số đặc điểm khiến cho các doanh nghiệp lựa chọn giải pháp IPSec-VPN là:

- IPSec cung cấp hệ thống bảo mật rất tốt, hỗ trợ cho các doanh nghiệp cần bảo mật bằng mã hoá dữ liệu và nhận dạng thiết bị;
- Giá thành triển khai mạng thấp do IPSec-VPN có thể thực hiện trên bất kỳ mạng IP nào đã tồn tại;
- Khả năng triển khai các dịch vụ nhanh, kể cả việc bổ sung hoặc loại bỏ các site;
- Luồng lưu lượng rẽ nhánh theo Hub-and-Spoke.

Thông thường, người sử dụng VPN dùng phần mềm VPN lựa chọn đích thích hợp cho các thông tin cần gửi qua mạng. Một khi nhận dạng thành công và đường hầm IPSec được thiết lập, người sử dụng có thể truy nhập từ xa tới các ứng dụng một cách đơn giản mà không cần phải sửa đổi hàng loạt các tham số tại các site.

Với các kết nối điểm-điểm qua IPSec-VPN, người sử dụng không cần phải có phần mềm client trên máy tính của họ. Người sử dụng tại các nhánh khởi tạo ứng dụng nếu nó tồn tại ở trong site, hoặc trong một phiên với trung tâm. Sau khi phiên thoả thuận và nhận dạng thành công, một đường hầm đảm bảo giữa các nhánh và trung tâm được thiết lập không phụ thuộc vào hoạt động của người dùng.

3.3.2 VPN trên nền MPLS

MPLS cung cấp môi trường định tuyến thông minh và hiệu năng chuyển mạch cao như đã trình bày ở trên. Ưu điểm nổi trội nhất của MPLS-VPN là khả năng mở rộng nhiều VPN trên cùng một mạng lõi. Thêm vào đó là các đặc tính đảm bảo QoS, sửa lỗi nhanh, bảo vệ đường dẫn và cung cấp nền tảng để phát triển các dịch vụ giá trị gia tăng. Một số lí do để các doanh nghiệp lựa chọn MPLS-VPN là:

- Các công ty cần thoả thuận mức độ chất lượng dịch vụ SLA;
- Bảo mật được hỗ trợ bởi việc tách các luồng lưu lượng tương tự như Frame Relay và ATM;
- Các mẫu lưu lượng phù hợp với cả cấu hình từng phần và đầy đủ;
- Các doanh nghiệp muốn hội tụ nhiều dịch vụ đa phương tiện trên cùng một mạng;
- Các doanh nghiệp muốn phát triển những kết nối Multicast.

Khía cạnh an toàn mạng của MPLS dựa trên việc phân tách luồng lưu lượng giữa các VPN trên cùng mạng lõi thông qua trường phân biệt tuyến. Các tuyến được phân biệt đảm bảo tính riêng tư của MPLS-VPN tương tự như trong mạng diện rộng Frame Relay hay ATM. Các nhà cung cấp có thể dễ dàng thiết kế và tối ưu hóa mạng do khách hàng không cần biết kiến trúc mạng lõi, còn các bộ định tuyến lõi thì không cần biết thông tin về mạng biên của khách hàng.

MPLS-VPN có độ mềm dẻo và linh hoạt cao, nó không yêu cầu cấu hình kết nối đầy đủ hoặc ngang hàng đối với các kết cuối như các mô hình khác đòi hỏi. Mặt khác, MPLS-VPN cũng hỗ trợ tốt các thoả thuận mức dịch vụ SLA. Đây là điều mà khách hàng VPN quan tâm nhiều nhất, nó cho phép đáp ứng các yêu cầu về hiệu năng và tính đàn hồi của mạng. Ngoài ra, MPLS-VPN còn hỗ trợ các kỹ thuật lưu lượng nhằm đáp ứng yêu cầu QoS, hỗ trợ chính sách quản lý và phân bổ lưu lượng tối ưu cho mạng.

3.4 Kết luận chương

Trong những năm gần đây, công nghệ chuyển mạch nhãn đa giao thức MPLS đã được triển khai trên rất nhiều quốc gia. Một trong những ứng dụng điển hình của MPLS là dịch vụ mạng riêng ảo MPLS-VPN. Dịch vụ này đã góp phần rất lớn vào sự phát triển nhanh chóng của MPLS và mở ra nhiều khả năng ứng dụng mới

Trong chương này đã trình bày các khái niệm cơ bản của MPLS-VPN, các mô hình cũng như những kỹ thuật then chốt của MPLS-VPN. Ngoài ra cũng đã đưa ra một số phân tích và so sánh các đặc điểm nổi bật của hai giải pháp VPN phổ biến nhất hiện này là VPN dựa trên IPSec và VPN dựa trên MPLS.

Có thể thấy rõ ràng về mặt bảo mật, MPLS VPN đã thực hiện rất tốt công việc của mình bằng việc phân biệt các tuyến giữa các khách hàng, đảm bảo tính riêng tư giữa các khách hàng, các khách hàng cũng không biết về mạng của nhà cung cấp…Ngoài ra chất lượng dịch vụ cũng là một vấn đề quan tâm hàng đầu của cả nhà cung cấp và khách hàng. MPLS-VPN có đủ các cơ chế QoS mềm dẻo để đáp ứng các nhu cầu của các khách hàng khác nhau đồng thời cũng có khả năng mở rộng để đảm bảo hỗ trợ được một số lượng lớn khách hàng VPN. Vấn đề MPLS QoS sẽ được nghiên cứu ở các chương tiếp theo.

CHƯƠNG 4. CÁC MÔ HÌNH ĐẢM BẢO CHẤT LƯỢNG DỊCH VỤ VÀ ÁP DỤNG CHO MẠNG RIÊNG ẢO TRÊN NỀN MPLS

4.1 Chất lượng dịch vụ - QoS và các độ đo

4.1.1 Giới thiệu chất lượng dịch vụ - QoS

Chất lượng dịch vụ (QoS) đã trở nên phổ biến trong những năm gần đây. Một vài mạng có băng thông hạn chế, vì vậy nghẽn mạng thường xuyên có thể xảy ra. QoS là một cách để ưu tiên những lưu lượng (traffic) quan trọng so với những lưu lượng ít quan trọng hơn và đảm bảo nó được truyền đi.

Vì sao chúng tao cần QoS?

Như trước đây, khi mà nhu cầu sử dụng mạng của con người chưa cao bởi vì sự mới mẻ, chưa phổ biến và các ứng dụng chưa nhiều thì lưu lượng trên mạng có thể đáp ứng cho hầu hết các ứng dụng lúc bây giờ, nhưng khi nó trở nên phổ biến số người dùng nhiều và các ứng dụng cũng tăng lên thì tài nguyên băng thông mạng trở nên thiếu hụt, điều này sẽ dẫn tới việc mất gói đáng kể khi truyền qua mạng. Để khắc phục điều này thì QoS ra đời với nhiệm vụ ưu tiên cho các ứng dụng thời gian thực bằng cách cấp phát thêm băng thông và đặt chúng ở mức ưu tiên cao hơn các ứng dụng khác. Nếu một mạng không áp dụng QoS thì sẽ xảy ra các trường hợp như sau:

- ***Thoại (Voice):***
  - Tín hiệu thoại không rõ ràng
  - Vỡ và vọng tín hiệu trong đàm thoại
  - Độ trễ tăng làm cho người nghe bên kia không biết khi nào cuộc gọi kết thúc.
  - Cuộc gọi bị ngắt giữa chừng.
- ***Hình (Video):***
  - Hình ảnh bị nhòe, giật không ổn định
  - Tiếng không khớp với video
  - Tốc độ video phát chậm hơn bình thường
- ***Dữ liệu (Data):***
  - Dữ liệu đến nhưng không dùng được
  - Dữ liệu đến chậm do độ trễ lớn
  - Số lần tín hiệu trả lời lại cho bên gửi không ổn định hoặc thất bại

4.1.2 Các tham số chất lượng dịch vụ

[2]

- *Băng thông (Bandwidth)*

Mô tả tốc độ truyền qua mạng của một phương tiện, giao thức hay kết nối, là thước đo đánh giá khả năng truyền tải lưu lượng dữ liệu qua mạng

- *Độ trễ (Delay)*

Trễ là thời gian truyền trung bình của dịch vụ từ điểm vào đến điểm ra khỏi mạng. Có thể kể đến các loại trễ như: trễ nối tiếp, trễ truyền lan, trễ chuyển mạch…

- *Biến động trễ (Jitter)*

Jitter là sự khác nhau về thời gian đến của các gói tin thuộc cùng một luồng lưu lượng

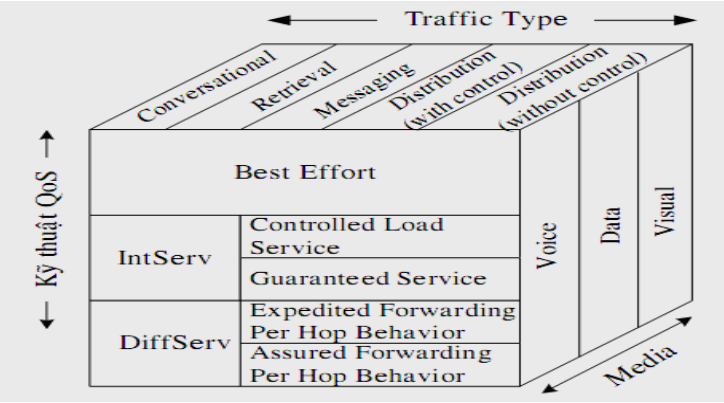
- *Tổn thất gói (Packet Loss)*

Hiện tượng tổn thất gói thường xảy ra khi có tắc nghẽ trên mạng. Gói tin bị loại bỏ khỏi điểm tắc nghẽn

4.2 Các mô hình đảm bảo QoS

Hiện nay trên thế giới ghi nhận 3 mô hình thực thi QoS trong mạng IP đó là: dịch vụ nỗ lực tối đa (Best-Effort), Dịch vụ tích hợp (Integrated Service - IntServ), dịch vụ phân biệt (Differentiated Service - DiffServ)

Một mô hình dịch vụ được gọi là một mức dịch vụ mô tả khả năng thiết lập từ đầu cuối đến đầu cuối của QoS. Hình 4-1 mô tả các kỹ thuật QoS trên mạng IP



Hình 4 - 1 Các kỹ thuật QoS trên mạng IP

4.2.1 Mô hình Best-Effort

Best-effort là một mô hình dịch vụ đơn và phổ biến trên mạng internet hay mạng IP nói chung, cho phép ứng dụng gửi dữ liệu bất cứ khi nào với bất cứ khối lượng nào nó có thể thực hiện và không đòi hỏi sự cho phép hoặc thông tin cơ sở mạng, nghĩa là mạng phân phối dữ liệu nếu có thể mà không cần sự đảm bảo về độ tin cậy, độ trễ hoặc khả năng thông mạng. QoS đặc tả dịch vụ Best-effort là xếp hàng đợi : first-in, first-out (FIFO).

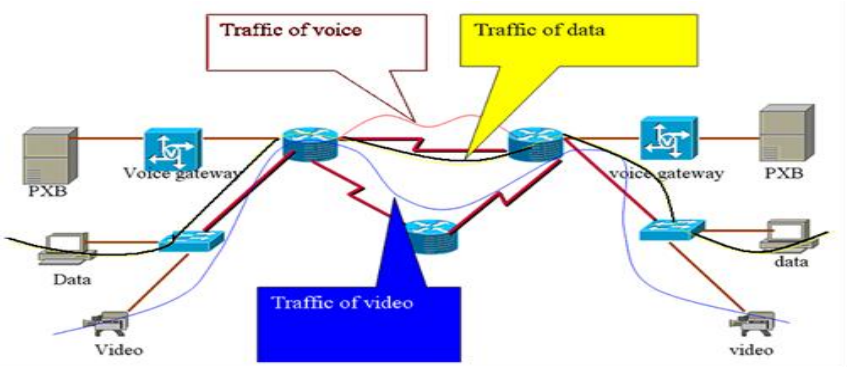
Dịch vụ Best- effort rất phù hợp cho những ứng dụng của mạng dải rộng như truyền file hoặc email. Cho đến thời điểm này đa phần các dịch vụ được cung cấp bởi mạng Internet vẫn sử dụng mô hình dịch vụ này.

4.2.2 Mô hình IntServ

Đứng trước nhu cầu ngày càng tăng trong việc cung cấp dịch vụ thời gian thực (thoại, video) và băng thông cao (đa phương tiện), dịch vụ tích hợp IntServ đã ra đời. Đây là sự phát triển của mạng IP nhằm đồng thời cung cấp dịch vụ truyền thống Best

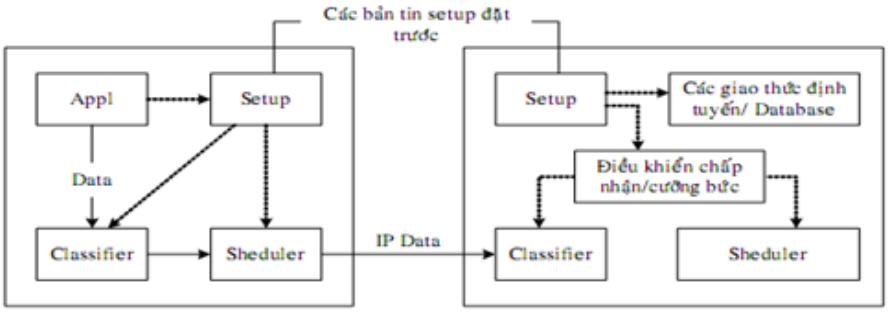
Effort và các dịch vụ thời gian thực. Sau đây là những động lực thúc đẩy sự ra đời của mô hình này:

- *Dịch vụ cố gắng tối đa không còn đủ đáp ứng nữa* : Ngày càng có nhiều ứng dụng khác nhau, các yêu cầu khác nhau về đặc tính lưu lượng được triển khai, đồng thời người sử dụng cũng yêu cầu chất lượng dịch vụ ngày càng cao hơn. Các ứng dụng đa phương tiện ngày càng xuất hiện nhiều.
- *Các ứng dụng đa phương tiện ngày càng xuất hiện nhiều* : Mạng IP phải có khả năng hỗ trợ không chỉ đơn dịch vụ mà còn hỗ trợ đa dịch vụ của nhiều loại lưu lượng khác nhau từ thoại, số liệu đến video. Tối ưu hóa hiệu suất sử dụng mạng và tài nguyên mạng.
- *Tối ưu hóa hiệu suất sử dụng mạng và tài nguyên mạng*: Đảm bảo hiệu quả sử dụng và đầu tư. Tài nguyên mạng sẽ được dự trữ cho lưu lượng có độ ưu tiên cao hơn, phần còn lại sẽ dành cho số liệu best effort.
- *Cung cấp dịch vụ tốt nhất*: Mô hình IntServ cho phép nhà cung cấp mạng đưa ra những dịch vụ tốt nhất, khác biệt với các đối thủ cạnh tranh khác.



Hình 4 - 2 Mô hình mạng IntServ

Mô hình IntServ được IETF giới thiệu vào giữa thập niên 90 với mục đích hỗ trợ chất lượng dịch vụ từ đầu cuối tới đầu cuối. Các ứng dụng nhận được băng thông đúng yêu cầu và truyền đi trong mạng với độ trễ cho phép.



Hình 4 - 3 Thành phần dịch vụ IntServ

Một số thành phần trong mô hình dịch vụ 4-3 như sau :

Giao thức thiết lập Setup : Cho phép các máy chủ và các router dự trữ động tài nguyên mạng để xử lý các yêu cầu của các luồng lưu lượng riêng. RSVP (Resource Reservation Protocol) là một trong những giao thức đó.

Đặc tính luồng: Xác định chất lượng dịch vụ QoS sẽ cung cấp cho các luồng xác định, luồng ở đây được định nghĩa như một luồng gói từ nguồn đến đích có cùng yêu cầu về QoS như băng thông tối thiểu mà mạng bắt buộc phải cung cấp để đảm bảo QoS cho các luồng yêu cầu.

Điều khiển lưu lượng: Trong các thiết bị mạng (máy chủ, router, chuyển mạch) có thành phần điều khiển và quản lý tài nguyên mạng cần thiết để hộ trợ QoS theo yêu cầu. Các thành phần điều khiển lưu lượng này có thể được khai báo bởi giao thức báo hiệu RSVP hay thủ công. Thành phần điều khiển lưu lượng bao gồm:

- *Điều khiển chấp nhận* : Xác định các thiết bị mạng có khả năng hỗ trợ QoS theo yêu cầu hay không.
- *Thiết bị phân lớp (Classifier)* : Nhận dạng và lựa chọn lớp dịch vụ trên nội dung của một số trường nhất định trong mào đầu gói.
- *Thiết bị lập lịch và phân phối (Scheduler)*: Cung cấp các mức chất lượng dịch vụ QoS ở kênh đầu ra của thiết bị.

Các mức QoS cung cấp bởi IntServ gồm :

- ***Dịch vụ đảm bảo GS (Guaranteed Service)***

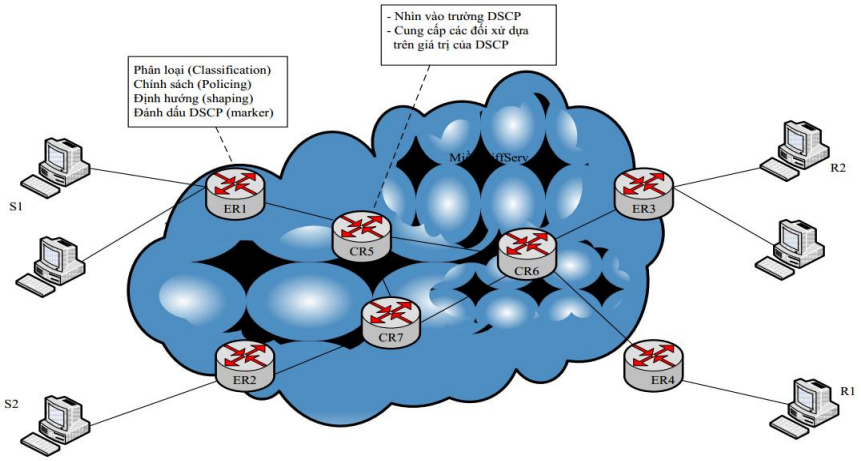
GS cung cấp các dịch vụ chất lượng cao như : Dành riêng băng thông, giới hạn độ trễ tối đa và không bị mất gói tin trong hàng đợi. Các ứng dụng có thể đến: Hội nghị truyền hình chất lượng cao, thanh toán tài chính thời gian thực,….

- ***Dịch vụ kiểm soát tải CL (Controlled Load)***

CL không đảm bảo về băng thông hay trễ, nhưng với các nỗ lực tối đa không giảm chất lượng một cách đáng kể khi tải mạng tăng lên. Dich vụ này phù hợp cho các ứng dụng không nhạy cảm lắm với độ trễ hay mất gói như truyền hình multicast audio/video chất lượng trung bình.

4.2.3 Mô hình DiffServ

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 (xem hình 4-4). DiffServ sử dụng việc đánh dấu gói và xếp hàng theo loại để hỗ trợ dịch vụ ưu tiên qua mạng IP.



Hình 4 - 4 Mô hình dịch vụ phân biệt DiffServ

Nguyên tắc cơ bản của DiffServ như sau:

- Phân loại và đánh dấu các gói riêng biệt tại biên của mạng vào các lớp dịch vụ. Việc phân loại có thể dựa trên nhiều cách thức như sửa dạng lưu lượng, loại bỏ gói tin, và cuối cùng là đánh dấu trường DS (DiffServ) trong mào đầu gói tin để chỉ thị lớp dịch vụ cho gói tin.
- Điều chỉnh lưu lượng này tại biên mạng. DS là mô hình có sự phân biệt dịch vụ trong mạng có nhiều ứng dụng khác nhau, bao gồm cả lưu lượng thời gian thực có thể được đáp ứng mức dịch vụ của chúng trong khi vẫn có khả năng mở rộng các hoạt động trong mạng IP lớn. Khả năng mở rộng có thể đạt được bằng:
    - Chia nhỏ lưu lượng ra thành nhiều lớp khác nhau.
    - Ánh xạ nhiều ứng dụng vào trong các lớp dịch vụ này trên biên mạng. Chức năng ánh xạ này được gọi là phân loại (classification) lưu lượng.
- Cung cấp các xử lý cố định cho mỗi lớp dịch vụ tại mỗi hop (được gọi là Per-hop behavior-PHB) tương ứng với các yêu cầu QoS của nó). PHB bao gồm hàng đợi, lập lịch, và các cơ chế loại bỏ gói tin.

4.2.4 So sánh mô hình IntServ và DiffServ

Trong một mạng sử dụng QoS, chúng ta có thể không cần dùng đến IntServ hay DiffServ mà mạng vẫn chạy bình thường, tuy nhiên nếu có ứng dụng DiffServ hay IntServ vào thì sẽ cho kết qua tốt hơn nhiều, và có thể đảm bảo chất lượng dịch vụ cao hơn. DiffServ ra đời để khắc phục các khuyết điểm của IntServ, giữa chúng có những sự khác nhau:

DiffServ	**IntServ**
Không dùng bất kì giao thức báo hiệu nào để dành trước băng thông mạng, do vậy tiết kiệm được băng thông mạng.	Dùng giao thức báo hiệu RSVP để dành trước băng thông mạng, do đó sẽ tốn tài nguyên mạng vô ích.

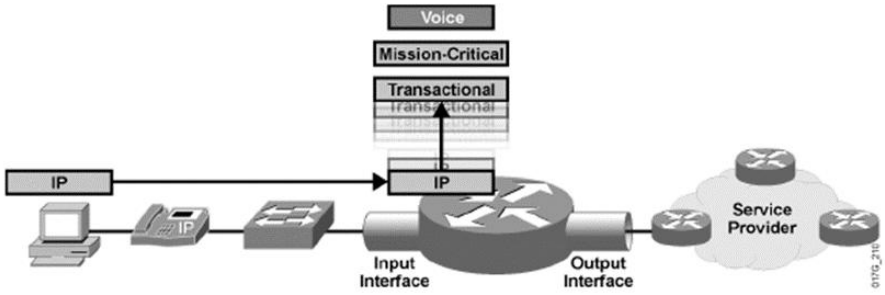
Có thể sử dụng cho mạng lớn và cả mạng nhỏ với số lưu lượng rất lớn	Chỉ có thể sử dụng cho mạng cỡ nhỏ với số lượng lưu lượng nhỏ
Ít tốn tài nguyên mạng	Tốn nhiều tài nguyên mạng
Xét ưu tiên gói trên từng chặn	Khởi tạo một kênh truyền trước khi truyền

4.3 Áp dụng mô hình DiffServ với gói tin IP

4.3.1 Cơ chế QoS áp dụng trên gói tin

[9] Cơ chế QoS được sử dụng để triển khai các chính sách QoS. Tại thời điểm gói tin IP đi vào mạng, nó được phân loại và thường được đánh dấu với các nhận dạng cho lớp. Từ đây gói tin được xử lý bằng rất nhiều cơ chế QoS tùy thuộc vào sự phân loại. Phụ thuộc vào cơ chế xử lý, gói tin có thể được chuyển tiếp nhanh, bị trễ, nén, phân mảnh hoặc thậm chí hủy bỏ. Chúng ta sẽ đi sâu vào từng cơ chế như sau:

4.3.1.1 Phân loại (Classifcation)

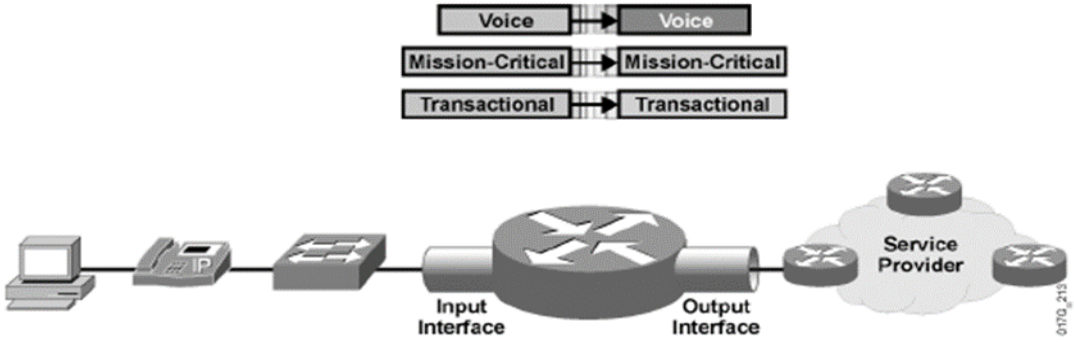


Hình 4 - 5 Classification

Phân loại là nhận dạng và tách lưu lượng (traffic) thành những lớp khác nhau. Trong mạng có khả năng QoS, tất cả các lưu lượng được phân loại ở những giao tiếp lối vào của tất cả các thiết bị có tính năng QoS. Phân loại gói tin có thể dựa vào nhiều yếu tố như:

- Điểm mã dịch vụ phân biệt (DSCP)
- IP precedence
- Địa chỉ đầu
- Địa chỉ đích

4.3.1.2 Đánh dấu (Marking)

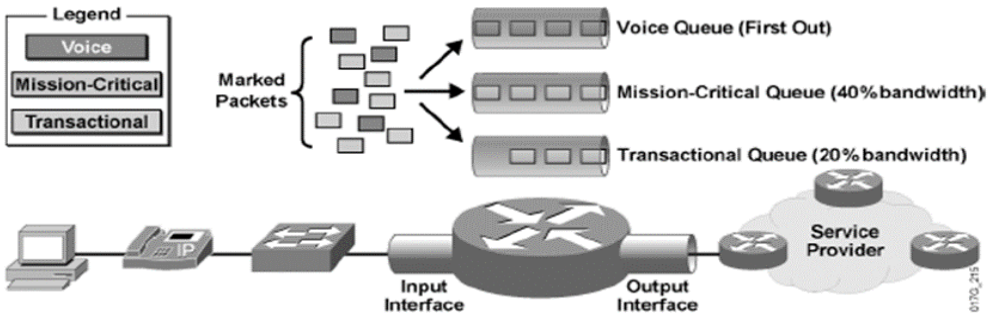


Hình 4 - 6 Marking

Đánh dấu (Marking) tức là đánh dấu các gói tin khi nó thuộc một lớp phân loại để các thiết bị khác còn lại trong mạng có thể nhanh chóng nhận ra lớp phân loại. Marking được thực hiện càng gần biên mạng càng tốt và thường được thực hiện bằng cách sử dụng MQC (Modular QoS CLI). MQC là một phương pháp thực hiện cấu hình trên các router.

Đánh dấu thường thiết đặt những bit trong trường DSCP hoặc IP Precedence (sẽ được đề cập sau) trong mỗi gói tin IP theo lớp mà gói tin thuộc về. Ngoài ra còn có các trường khác cũng có thể được thiết đặt như: QoS group, MPLS experimental bit, 802.1Q priority bit, Frame Relay DE bit, ATM CLP bit…

4.3.1.3 Quản lý nghẽn (Congestion Management)



Hình 4 - 7 Congestion Management

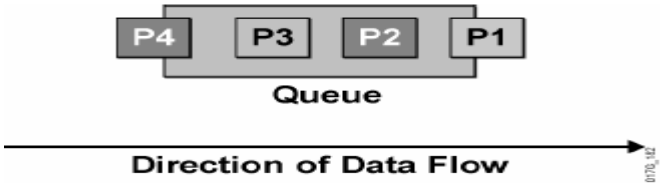
Cơ chế quản lý nghẽn (cơ chế hàng đợi) sử dụng đánh dấu trên mỗi gói tin để quyết định hàng đợi nào sẽ chứa gói tin. Những hàng đợi khác nhau được xử lý theo những cách khác nhau bằng thuật toán quản lý hàng đợi dựa trên lớp gói tin trong hàng đợi. Về cơ bản, hàng đợi với những gói tin có độ ưu tiên cao nhận được cách xử lý ưu tiên hơn.

Quản lý hàng đợi được triển khai trên tất cả các interface lối ra trong mạng có tính năng QoS bằng cách sử dụng cơ chế hàng đợi để quản lý luồng dữ liệu ra. Mỗi thuật

toán hàng đợi được thiết kế để giải quyết vấn đề về một lưu lượng mạng cụ thể và có những tác động đáng kể đến hiệu năng mạng.

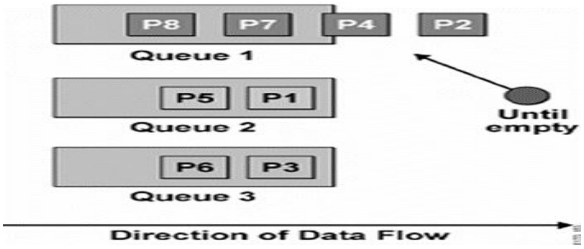
Trong Cisco IOS có một số cách quản lý hàng đợi quan trọng như sau:

- *FIFO (First In – Firtst Out)*: Không cần sự phân loại vì tất cả các gói tin đều thuộc một lớp giống nhau. Các gói tin bị hủy bỏ nếu hàng đợi ra bị đầy (còn gọi là tail drop). Hàng đợi phục vụ những gói tin theo thứ tự chúng đến. Đây là hàng đợi đơn giản và phổ biến nhất.



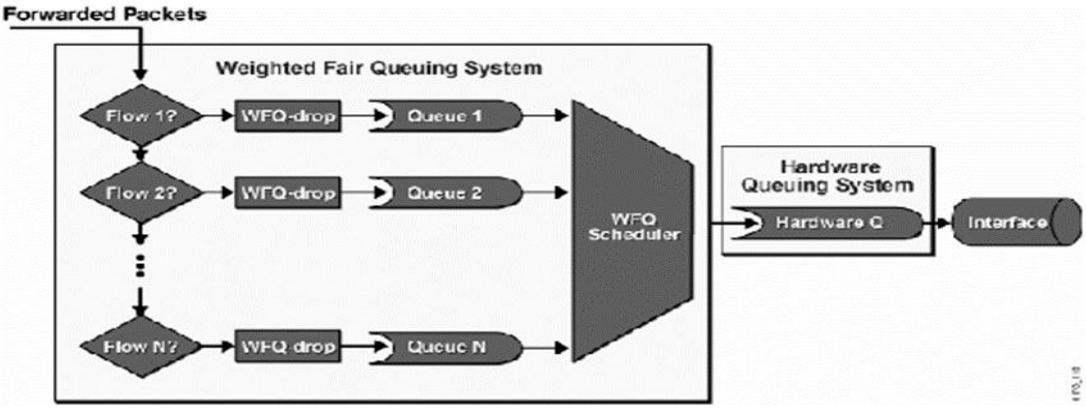
Hình 4 - 8 FIFO

- *Priority Queuing (PQ):* Cơ chế cũng khá đơn giản. Mỗi gói được gán một độ ưu tiên và được đặt trong những hàng đợi có sự phân cấp dựa vào độ ưu tiên. Đến khi nào hàng đợi cao nhất không còn gói tin nào thì những hàng đợi phía dưới mới được phục vụ. Gói tin sau đó được gửi đi từ hàng đợi cao nhất kế tiếp cho đến khi hàng đợi đó hết hoặc gói tin khác đến hàng đợi cao hơn nó. Gói tin sẽ được gửi đi từ hàng đợi thấp hơn chỉ khi nào tất cả các hàng đợi có độ ưu tiên cao hơn đều trống. Nếu có một gói tin đến hàng đợi cao hơn thì gói tin từ hàng đợi cao hơn sẽ gửi đi trước bất kì gói tin nào trong hàng đợi thấp hơn.



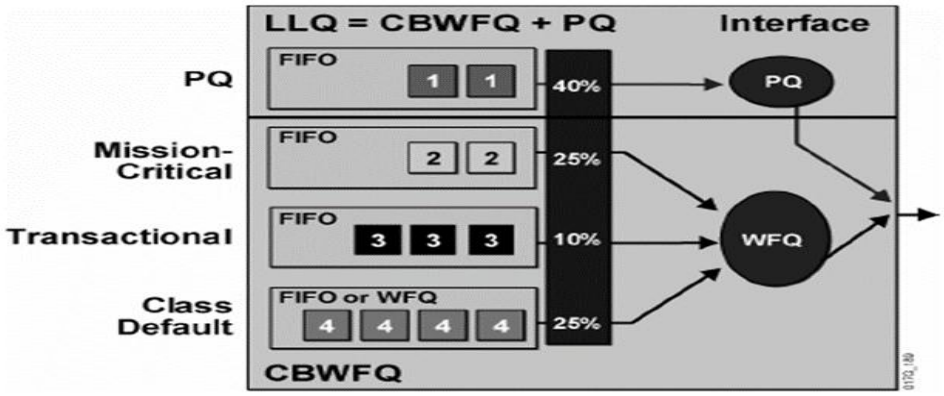
Hình 4 - 9 Priority Queue

- *Weighted Fair Queuing (WFQ):* Tự động phân loại dựa vào luồng dữ liệu (flow). Mỗi luồng dữ liệu sử dụng một hàng đợi khác. Hàng đợi với ít lưu lượng và IP precedence cao hơn được phục vụ nhiều hơn. Băng thông được phân chia một cách khá công bằng cho tất cả các luồng dữ liệu đang hoạt động.



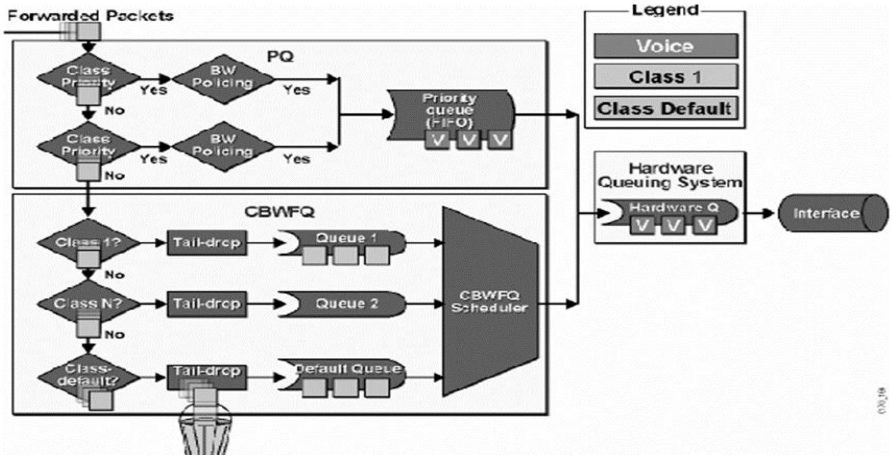
Hình 4 - 10 WFQ

- *Class-Based Weighted Fair Queuing (CBWFQ):* Mở rộng chức năng của WFQ để hỗ trợ cho những lớp lưu lượng người dùng tự định nghĩa. Với CBWFQ, ta định nghĩa những lớp lưu lượng dựa vào những tiêu chuẩn so khớp bao gồm giao thức, ACL, và những interface chiều vào. Gói tin thỏa mãn những tiêu chuẩn so khớp cho một lớp sẽ thuộc lớp đó. Một hàng đợi được dành sẵn cho mỗi lớp và lưu lượng thuộc về một lớp được chuyển tới hàng đợi lớp đó. Sau khi một lớp đã được định nghĩa theo các tiêu chuẩn so khớp, ta có thể ấn định các đặc điểm cho nó. Để đặc tả một lớp, ta có thể gán băng thông, trọng số, hoặc số lượng gói tối đa. Băng thông được gán cho lớp là băng thông tối thiểu khi xảy ra nghẽn. CBWFQ hỗ trợ nhiều lớp để phân loại dữ liệu thành các hàng đợi FIFO. Tail drop là hành vi loại bỏ mặc định của CBWFQ. Ta cũng có thể sử dụng WRED để tránh nghẽn cho từng lớp.



Hình 4 - 11 CBWFQ

- *Low-Latency Queuing (LLQ):* Là một tính năng mang *priority queuing (PQ)* vào CBWFQ. Priority Queuing cho phép các dữ liệu dễ bị ảnh hưởng bởi trễ như voice có thể được gửi đi trước (trước khi gói tin trong những hàng đợi khác được gửi), giúp cho những dữ liệu dễ bị ảnh hưởng bởi trễ được sự ưu tiên đối xử so với các lưu lượng khác. Bằng việc sử dụng một lớp trong CBWFQ để triển khai LLQ, nó cho phép chuyển hướng lưu lượng thuộc về lớp đó tới hàng đợi ưu tiên.



Hình 4 - 12 LLQ

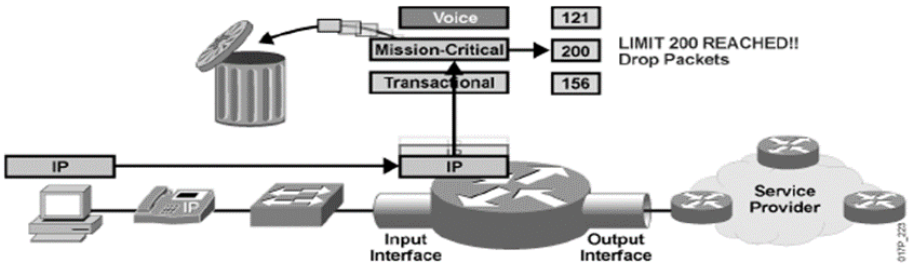
4.3.1.4 Tránh nghẽn (Congestion Avoidance)

Tránh nghẽn là giám sát lượng tải của mạng để dự báo và tránh nghẽn ở những điểm hay bị nghẽn. Tránh nghẽn được triển khai bằng cách hủy bỏ gói tin.

Tránh nghẽn thường được triển khai ở những giao diện (interface) lối ra nơi mà những liên kết tốc độ cao hoặc một tập hợp các liên kết đẩy vào một liên kết tốc độ thấp (ví dụ một mạng LAN đẩy vào một liên kết WAN).

Weighted random early detection (WRED) là một kỹ thuật tránh nghẽn chính. WRED làm giảm khả năng nghẽn xảy ra bằng cách hủy bỏ những gói tin có độ ưu tiên thấp hơn là hủy bỏ những gói tin có độ ưu tiên cao.

4.3.1.5 Chính sách (Policing)



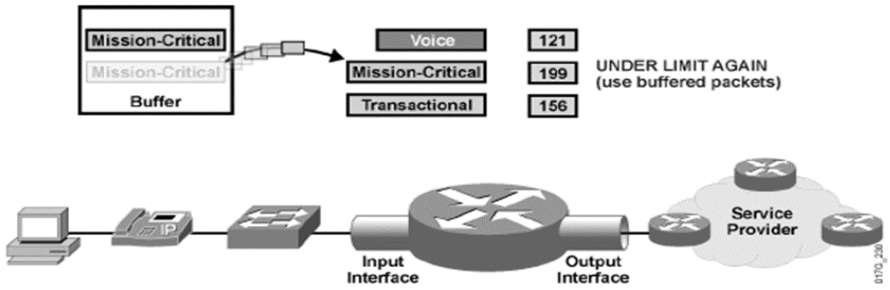
Hình 4 - 13 Policing

Chính sách (Policy) là khả năng kiểm soát những lưu lượng vượt quá hoặc tuân theo để đảm bảo những loại lưu lượng nhất định nhận được những loại băng thông nhất định.

Policing hủy bỏ hoặc đánh dấu những gói tin khi chạm tới những giới hạn định trước. Policing có thể thiết đặt để hủy bỏ những lớp lưu lượng có độ ưu tiên thấp trước. Ngoài ra nó cũng thường sử dụng để điều khiển những luồng lưu lượng đi vào thiết bị mạng từ những đường tốc độ cao bằng cách hủy bỏ những gói tin có độ ưu tiên thấp nhưng chiếm nhiều băng thông. Một ví dụ điển hình là việc sử dụng policing của

nhà cung cấp dịch vụ để ngăn chặn những luồng dữ liệu có tốc độ cao từ phía khách hàng vào mạng của nhà cung cấp dịch vụ sao cho nó nằm trong thỏa thuận dịch vụ.

4.3.1.6 Điều hòa (Shaping)



Hình 4 - 14 Shaping

Điều hòa (shaping) giúp làm mịn tốc độ không phù hợp trong mạng và giới hạn tốc độ truyền. Shaping được sử dụng trên các interface đầu ra và giới hạn các luồng dữ liệu từ các đường liên kết tốc độ cao đến các đường liên kết tốc độ thấp hơn để đảm bảo đường liên kết tốc độ thấp hơn không bị vượt quá lưu lượng. Shaping cũng có thể sử dụng để quản lý luồng lưu lượng ở một điểm trên mạng mà rất nhiều luồng lưu lượng được tập trung tại đó. Nhà cung cấp dịch vụ sử dụng shaping để quản lý luồng lưu lượng vào và ra của khách hàng để đảm bảo những luồng lưu lượng đó tuân theo cam kết giữa hai bên.

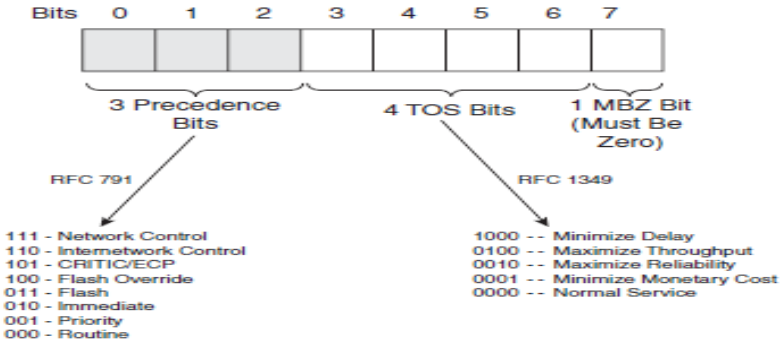
4.3.2 Áp dụng QoS với gói tin IP

[12] Hình 4-15 dưới đây mô tả các trường của header một gói tin IP:

Version	IHL	Type of Service (TOS)	Total Length
Identification		Flags	Fragment Offset
Time To Live	Protocol		Header Checksum
Source Address			
Destination Address			
Options			Padding

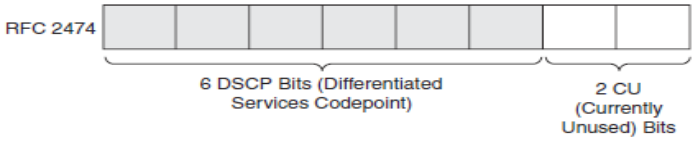
Hình 4 - 15 Các trường của header IP

Hình 4-16 chỉ ra cách phân chia trường ToS (Type of Service):



Hình 4 - 16 Byte ToS định nghĩa các bit Precedence

Việc sử dụng những bit precedence cho QoS ngày nay được sử dụng rộng rãi. Nhược điểm của nó là chỉ có 8 cấp dịch vụ.Vì vậy IETF quyết định sử dụng nhiều bit hơn cho QoS và 3 bit trong ToS được gán cho DiffServ ngoài 3 bit precedence phía trước. DiffServ sử dụng 6 bit, cung cấp một số lượng đủ lớn các cấp dịch vụ. Hình 4-17 chỉ ra những bit dùng cho DiffServ hay DSCP (Differentiated Services Codepoint).



Hình 4 - 17 Byte ToS định nghĩa các bit DSCP

Có hai loại lớp chuyển tiếp trong mô hình DiffServ được định nghĩa: *Chuyển tiếp nhanh (expedited forwarding - EF)* và chuyển tiếp đảm bảo *(assured forwarding-AF)*. EF là dịch vụ tỉ lệ mất, độ trễ thấp, đảm bảo băng thông, và kết nối điểm-điểm. AF định nghĩa rất nhiều dịch vụ đảm bảo chuyển tiếp. Có 4 lớp AF được định nghĩa, mỗi lớp lại có 3 mức ưu tiên hủy bỏ. Các lớp AF được kí hiệu *AFij* với *i* từ 1 đến 3 để chỉ lớp, *j* từ 1 đến 3 để chỉ độ ưu tiên hủy bỏ và bit cuối được dự trữ. Độ ưu tiên hủy bỏ càng cao thì gói tin càng dễ bị hủy bỏ khi có nghẽn xảy ra. Bảng 4-1 là các giá trị khuyến cáo cho 4 lớp AF:

Name	DSCP (binary)	DSCP (decimal)
AF11	001010	10
AF12	001100	12
AF13	001110	14
AF21	010010	18
AF22	010100	20
AF23	010110	22
AF31	011010	26
AF32	011100	28
AF33	011110	30
AF41	100010	34
AF42	100100	36
AF43	100110	38

Bảng 4 - 1 Các giá trị đề nghị cho bốn lớp AF

Bảng 4-2 chỉ ra 4 lớp AF, mỗi lớp lại có 3 mức ưu tiên hủy bỏ:

Drop Precedence	Class 1	Class 2	Class 3	Class 4
Low	001010	010010	011010	100010
Medium	001100	010100	011100	100100
High	001110	010110	011110	100110

Bảng 4 - 2 Bốn lớp AF và ba mức ưu tiên hủy bỏ

Nếu ta sử dụng EF, trường DiffServ khuyến cáo là 101100 (thập phân 46).

Ta cũng có thể sử dụng lớp Class Selector (CS) - nếu ta chỉ muốn dùng 3 bit đầu của trường DSCP cho QoS (cái này để tương thích ngược với trường precedence).

4.4 Áp dụng mô hình DiffServ cho MPLS-VPN

4.4.1 Tổng quan về QoS cho MPLS-VPN

Chất lượng dịch vụ là một thành phần quan trọng của các mạng gói đa dịch vụ. Mô hình Diffserv hiện nay là mô hình kiến trúc QoS phổ biến nhất trong chuyển mạch gói IP với ưu điểm nổi bật là linh hoạt và khả năng mở rộng cao.

Trên cơ sở mỗi VPN phải có rất nhiều mức dịch vụ (Class of Service - CoS). Các ứng dụng thời gian thực ví dụ VoIP phải có mức dịch vụ riêng ưu tiên hơn so với mức dịch vụ dành cho truyền tải file hoặc email. Hai mô hình chất lượng dịch vụ dùng cho mạng riêng ảo trên nên MPLS là : *Pipe model (mô hình ống)* và *Hose model (mô hình vòi)* [6]

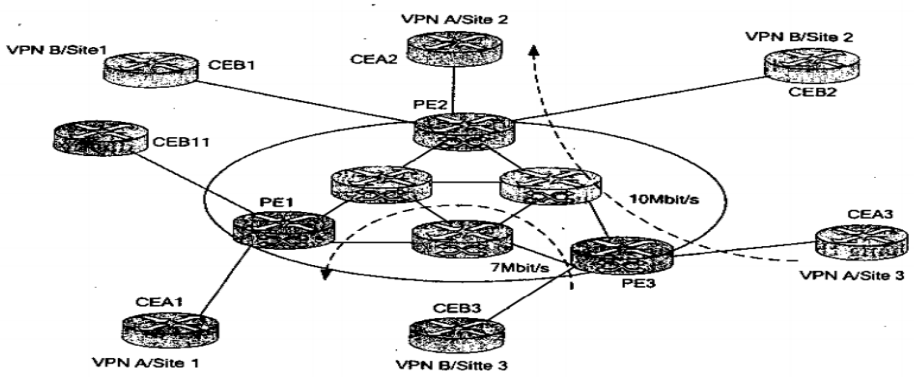
4.4.1.1 Pipe model

Trong mô hình ống, nhà cung cấp dịch vụ cung cấp cho khách hàng VPN mức chất lượng dịch vụ QoS nhất định giữa các CE trong cùng một VPN. Về hình thức, có thể hình dung mô hình này nư một đường ống kết nối hai bộ định tuyến với nhau và lưu lượng giữa hai bộ định tuyến trong ống nay được đảm bảo một mức QoS xác định. Ví dụ về một hình thức đảm bảo QoS có thể cung cấp trong mô hình ống là đảm bảo giá trị băng thông nhỏ nhất giữa hai Site.

Các bộ định tuyến biên phía nhà cung cấp PE tại hai đầu của ống sẽ thực hiện quá trình lọc và loại bỏ các lưu lượng dư nhằm đảm bảo băng thông cho luồng lưu lượng trong ống. Có thể cải tiến mô hình ống bằng việc chỉ cho phép một số loại lưu lượng (ứng với một số ứng dụng) từ một CE tới các CE khác sử dụng đường ống. Quy định lưu lượng nào có thể sử dụng đường ống được xác định tại bộ định tuyến PE phía đầu ống.

Chú ý là mô hình ống khá giống với mô hình QoS mà các khách hàng VPN có được với các giải pháp dựa trên Frame Relay/ATM. Điểm khác nhau cơ bản là với ATM/Frame Relay thì các kết nối là song công, trong khi mô hình ống cung cấp các kết nối đảm bảo theo một hướng. Đặc điểm một hướng này của mô hình ống cho phép thiết lập các kết nối cho những ứng dụng sử dụng luồng lưu lượng không đối xứng, trong đó lưu lượng từ một Site tới Site khác có thể khác với lưu lượng theo hướng ngược lại.

Hình 4-18 minh hoạt một ví dụ về mô hình ống chất lượng dịch vụ. Như chỉ ra trên hình vẽ, các nhà cung cấp dịch vụ cung cấp cho VPN A một đường ống đảm bảo băng thông 7Mbps cho lưu lượng từ Site 3 đến Site 1 (cụ thể hơn là từ CE A3 đến CE A1) và một đường ống khác đảm bảo băng thông 10Mbps cho lưu lượng từ Site 3 đến Site 2 (từ CE A3 đến CE A2). Như vậy, một bộ định tuyến CE có thể có nhiều hơn một ống xuất phát từ nó (ví dụ hai ống xuất phát từ Site 3). Tương tự, có thể có hơn một ống kết thúc tại một Site.



Hình 4 - 18 Mô hình ống chất lượng dịch vụ trong MPLS-VPN

Một ưu điểm của mô hình ống là nó giống với mô hình QoS đang được khách hàng sử dụng với FR hay ATM, do đó khách hàng có thể dễ dàng ứng dụng. Tuy nhiên mô hình ống cũng có một số nhược điểm. Ví dụ, nó đòi hỏi khách hàng VPN phải kiểm soát toàn bộ ma trận lưu lượng giữa các Site. Điều đó có nghĩa là, khách hàng phải biết tổng lương lượng đi từ một Site tới tất cả các Site khác. Thông thường thì thông tin nà không có sẵn, thậm chí là nếu có thì cũng bị lỗi thời.

Mô hình ống gần giống với mô hình tích hợp dịch vụ để cung cấp chất lượng dịch vụ đảm bảo. MPLS-VPN cung cấp khả năng đảm bảo băng thông cho các LSP và cho phép sử dụng mô hình ống này một cách đơn giản. Các LSP khởi tạo và kết thúc tại các PE sẽ đảm bảo băng thông qua mạng lõi, còn thỏa thuận dịch vụ giữa PE và CE sẽ đảm bảo QoS từ đầu cuối tới đầu cuối. Để đạt được hiệu quả tốt nhất đối với mô hình ống, khách hàng VPN cần biết rõ yêu cầu sử dụng lưu lượng trong kế hoạch mạng.

4.4.1.2 Hose Model

Trong mô hình vòi, nhà cung cấp dịch vụ VPN cung cấp cho khách hàng một sự đảm bảo QoS cho lưu lượng và một bộ định tuyến CE của khách hàng gửi đi và nhận về từ các bộ định tuyến CE khác trong cùng một VPN. Trong các trường hợp khác, khách hàng phải chỉ định cách phân phối lưu lượng tới các bộ định tuyến CE trong mạng. Như vậy, đối với khách hàng, mô hình vòi cung cấp chất lượng dịch vụ trong từng VPN và không yêu cầu phải phân tích lưu lượng hoặc lập kế hoạch lưu lượng cho tới từng CE, nhờ đó mà giảm bớt được gánh nặng cho khách hàng sử dụng dịch vụ VPN

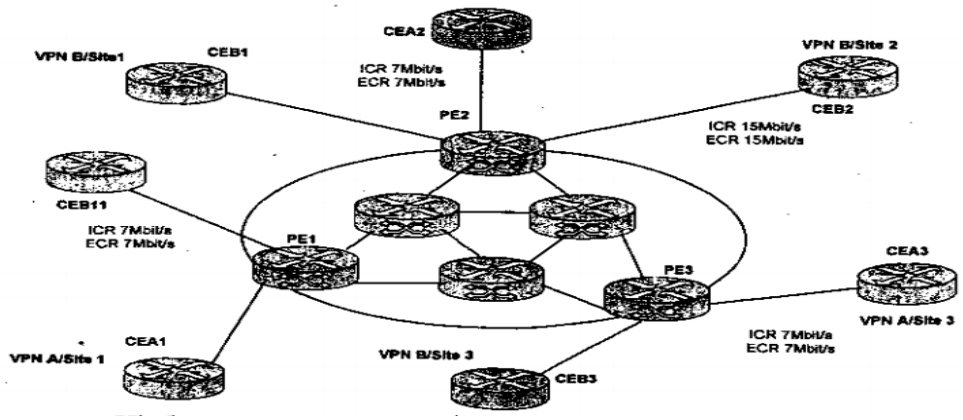
Mô hình vòi sử dụng hai tham số tốc độ là tốc độ cam kết đầu vào ICR (Ingress Commited Rate) và tốc độ cam kết đầu ra ECR (Egress Commited Rate). Trong đó ICR là tốc độ liên quan tới lưu lượng mà CE đầu vào có thể gửi tới những CE khác, còn ECR là tốc độ liên quan đến lưu lượng mà một CE có thể nhận từ các CE khác. Nói cách khác, ICR đại diện cho tổng lưu lượng từ một CE cụ thể, trong đó ECR đại diện cho tổng lưu lượng tới một CE cụ thể. Lưu ý đối với một CE không nhất thiết ICR phải bằng ECR.

Hình 4-19 minh họa ví dụ về mô hình vòi chất lượng dịch vụ. Ở đây nhà cung cấp dịch vụ cung cấp cho VPN B sự đảm bảo băng thông 15Mpbs cho lưu lượng từ

Site 2 tới các Site khác (ICR = 15Mpbs) mà không quan tâm đến lưu lượng này đi tới Site 1 hay Site 3. Tương tự, nhà cung cấp dịch vụ cung cấp cho VPN A sự đảm bảo băng thông 7Mpbs cho lưu lượng từ Site 3 gửi tới các Site khác trong cùng VPN (ICR = 7Mbps) mà không quan tâm tới việc lưu lượng tới Site 1 hay Site 2. Cung như thế, nhà cung cáp dịch vụ cung cấp cho VPN B sự đảm bảo băng thông 15Mpbs cho lưu lượng gửi tới Site 2 (ECR = 15Mbps) mà không quan tâm tới việc lưu lượng xuất phát từ Site 1 hay Site 3

Mô hình vòi hỗ trợ nhiều mức CoS ứng với các dịch vụ có nhiều tham số khác nhau. Ví dụ, một dịch vụ có thể yêu cầu tham số về mất gói tin ít hơn so với dịch vụ khác. Để hỗ trợ lớp dịch vụ ta phải đưa vào mô hình vòi, cho phép nhà cung cấp dịch vụ sử dụng cơ chế phân biệt dịch vụ cùng với MPLS. Vì vậy, mô hình vòi là hướng tiếp cận từ mô hình phân biệt dịch vụ Diffserv. Với các dịch vụ đòi hỏi phải có sự đảm bảo chắc chắn (như về băng thông) thì mô hình ống phù hợp hơn.

Nhà cung cấp dịch vụ có thể cung cấp cho khách hàng VPN mô hình ống, mô hình vòi hoặc tổ hợp cả hai mô hình trên nhằm đáp ứng các yêu cầu cụ thể về QoS. Các bộ định tuyến PE của nhà cung cấp dịch vụ xác định lưu lượng được nhận trong các lớp dịch vụ. Tùy thuộc vào giao diện đầu vào, địa chỉ nguồn, địa chỉ đích, chỉ số cổng và các cam kết chất lượng dịch vụ mà các gói sẽ được đánh dấu cho phù hợp với yêu cầu về chất lượng dịch vụ.

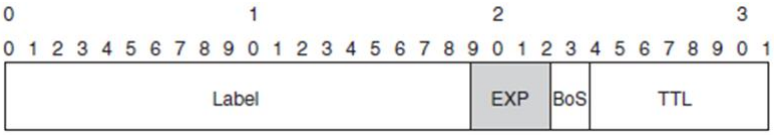


Hình 4 - 19 Mô hình vòi chất lượng dịch vụ trong MPLS-VPN

4.4.2 Áp dụng QoS với gói tin MPLS

Để đạt được chất lượng dịch vụ trong môi trường MPLS VPN ta chọn mô hình vòi hay mô hình DiffServ QoS bởi vì nó được đang được sử dụng rộng rãi trong công nghiệp do tính mềm dẻo như đã nói ở trên. Thực hiện DiffServ với gói tin MPLS cũng gần giống như với gói tin IP trong chương 3 tất nhiên có một vài điều khác biệt.

Nhớ lại cấu trúc của nhãn MPLS như sau:



Hình 4 - 20 Cấu trúc nhãn MPLS

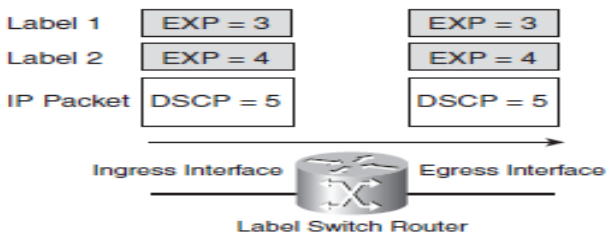
Chúng ta có thể thấy 3 bit thử nghiệm EXP được dùng trong QoS tương tự như 3 bit precedence trong gói tin IP. Và nếu ta sử dụng 3 bit đó, ta có thể gọi LSP là E-LSP ám chỉ rằng LSR sử dụng bit EXP để phân loại gói tin và quyết định sự ưu tiên hủy bỏ. Tuy nhiên khi sử dụng MPLS, ta có một tùy chọn khác để triển khai QoS cho các gói tin dán nhãn. Một LSP là một đường được báo hiệu qua mạng giữa hai router. Ta có thể sử dụng nhãn trên cùng của gói tin để mang QoS cho gói tin đó. Tuy nhiên sau đó, ta cần một nhãn trên một lớp cho mỗi dòng lưu lượng giữa hai đầu của LSP. Loại LSP đó được gọi là L-LSP, ngụ ý rằng nhãn mang một phần thông tin QoS.

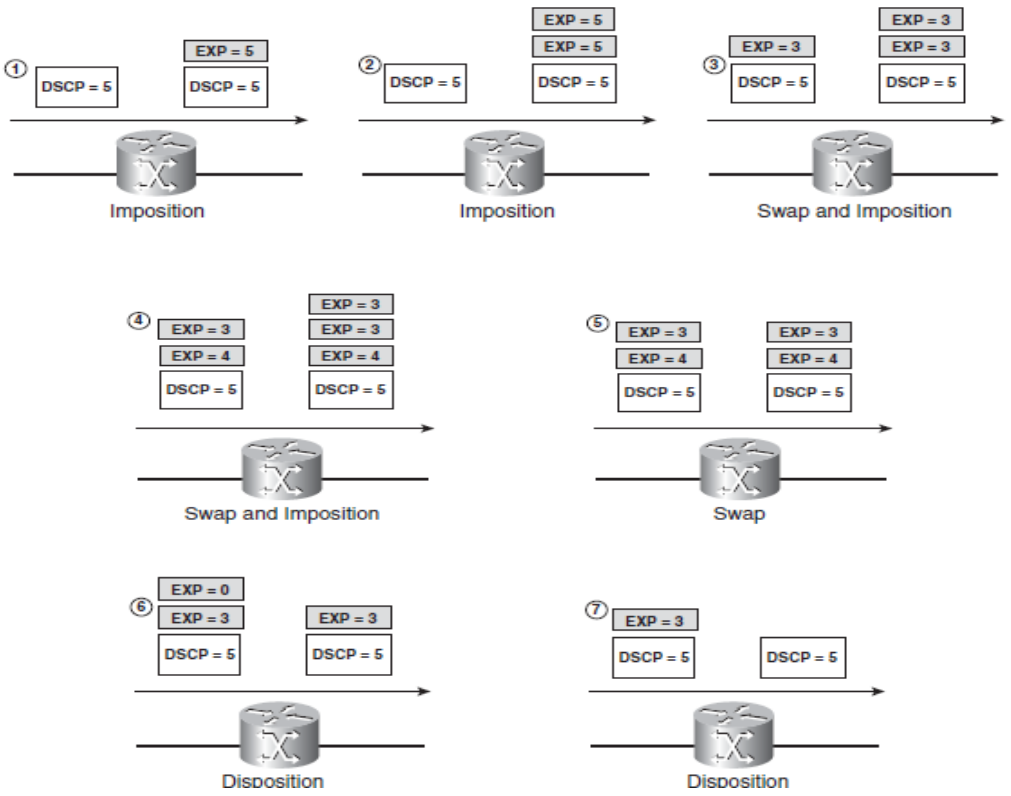
Khi LSR chuyển tiếp gói tin gán nhãn, nó chỉ cần nhìn vào nhãn trên cùng và quyết định nơi sẽ chuyển gói tin. Điều này cũng đúng với hành vi của QoS. LSR cũng chỉ cần nhìn vào những bit EXP của nhãn trên cùng để quyết định cách đối xử với gói tin này. Nhớ lại rằng QoS bao gồm đánh dấu lưu lượng, quản lý nghẽn, tránh nghẽn và điều hòa lưu lượng, ta sử dụng low-latency queuing (LLQ), class-based weighted fair queuing (CBWFQ), weighted random early detection (WRED), policing và shaping để triển khai nó cho gói tin IP. Ta hoàn toàn cũng có thể sử dụng các tính năng đó để triển khai QoS dựa trên bit EXP cho gói tin dán nhãn.

Các hành vi QoS mặc định trong MPLS:

1. *Mặc định trong Cisco IOS, các bit precedence hoặc ba bit đầu tiên của trường DSCP trong header IP được sao chép tới các bit EXP của tất cả các nhãn được chèn vào ở LSR lối vào.*
2. *Mặc định trong Cisco IOS, các bit EXP của nhãn đầu sao chép tới nhãn được hoán đổi và tất cả các nhãn được chèn lên nó.*
3. *Mặc định trong Cisco IOS, các bit EXP của nhãn đầu không được sao chép tới nhãn lộ ra sau khi gỡ bỏ nhãn đầu.*
4. *Mặc định trong Cisco IOS, các bit EXP của nhãn đầu không được sao chép tới các bit precedence hoặc các bit DSCP khi ngăn xếp nhãn được gỡ bỏ.*
5. *Khi ta thay đổi giá trị các bit EXP thông qua cấu hình, giá trị của các bit EXP trong các nhãn ngoại trừ nhãn đầu thì các nhãn được hoán đổi, các nhãn được chèn thêm vào và các bit precedence hoặc các bit DSCP trong header IP giữ nguyên không đổi.*

Ví dụ như hình 4-21 chỉ ra các hành vi chuyển tiếp mặc định như thêm, hoán đổi, gỡ bỏ nhãn:





Hình 4 - 21 Các hành vi mặc định của Cisco IOS đối với các bit EXP

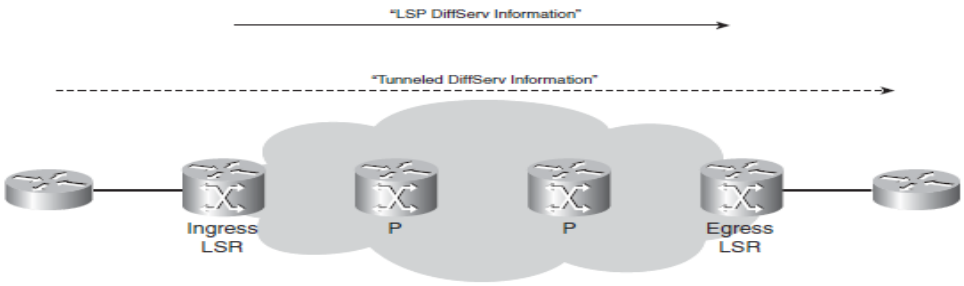
Hai bức tranh đầu mô tả cho ta về sự phản ánh ToS. Mặc định, IP precedence được sao chép tới nhãn được chèn vào. Đây chính là luật 1. Bức tranh thứ ba chỉ cho ta rằng bit EXP của nhãn trên cùng của gói tin đến được sao chép tới nhãn được hoán đổi và nhãn được đẩy thêm. Đó chính là luật 2. Hình 4, 5 là một ví dụ của luật 2 nhưng hiện tại nó chỉ ra cả các bit EXP của các nhãn phía dưới nhãn đầu không thay đổi (Luật 5). Hình số 6 chỉ ra một ví dụ về luật 3 và hình số 7 là một ví dụ về luật số 4.

4.4.3 Các mô hình đường hầm DiffServ trong MPLS

[14] MPLS QoS luật 4 nảy sinh một vấn đề thú vị: bất kể giá trị EXP được thay đổi bởi LSR lối vào hoặc bất kì LSR khác, giá trị không được sao chép tới gói tin IP lộ ra ở LSR lối ra của mạng MPLS. Do đó, điều này giúp nhà mạng có thể chuyển giá trị QoS của gói tin IP một cách trong suốt. IP precedence hoặc DSCP của gói tin IP được bảo toàn, giá trị ở LSR lối vào và lối ra bằng nhau. Lúc này ta có thể tạo đường hầm giá trị DiffServ của gói tin IP. Một ưu điểm rõ ràng là mạng MPLS có thể có các chính sách QoS khác nhau với các khách hàng kết nối tới. IETF đã định nghĩa ba mô hình để tạo đường hầm thông tin DiffServ. Tất cả ba mô hình đều có sự khác biệt và đều có những ưu điểm riêng. Sự khác biệt giữa chúng chỉ ở vị trí những LSR biên.

Thông tin Tunneled DiffServ là thông tin QoS của gói tin được gán nhãn hoặc precedence/DSCP của gói tin IP đến LSR lối vào. Thông tin LSP DiffServ là thông tin QoS của gói tin MPLS chuyển qua LSP từ LSR lối vào tới LSR lối ra. Thông tin Tunneled DiffServ là thông tin QoS cần chuyển qua mạng MPLS một cách trong suốt

trong khi thông tin LSP DiffServ là thông tin QoS tất cả các LSR trong mạng MPLS sử dụng để chuyển gói tin được dán nhãn



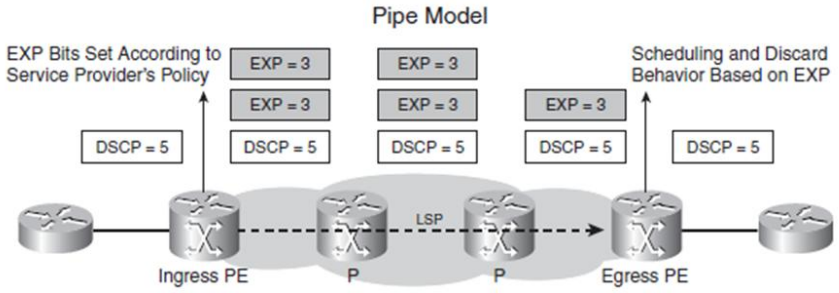
Hình 4 - 22 Hoạt động chung của các mô hình đường hầm DiffServ

4.4.3.1 Mô hình ống (Pipe Model)

Trong mô hình này những luật sau được áp dụng:

- Thông tin LSP DiffServ là không cần thiết (nhưng có thể) được kế thừa từ thông tin Tunneled DiffServ trên LSR lối vào.
- Trên các LSR trung gian (P router), thông tin LSP DiffServ của nhãn ra được kế thừa từ thông tin LSP DiffServ của nhãn vào.
- Trên các LSR lối ra, cách xử lý chuyển tiếp gói tin dựa vào thông tin LSP DiffServ và thông tin LSP DiffServ không được sao chép tới thông tin Tunneled DiffServ.

Xử lý chuyển tiếp (hành vi phân loại và hủy bỏ) của gói tin IP dựa trên những bit precedence hoặc DSCP của gói tin IP. Vì vậy nó có thể gọi là IP PHB (per-hop behavior). Tương tự xử lý chuyển tiếp của gói tin MPLS dựa trên những bit EXP. Cái này gọi là MPLS PHP (per-hop behavior).



Hình 4 - 23 Mô hình ống

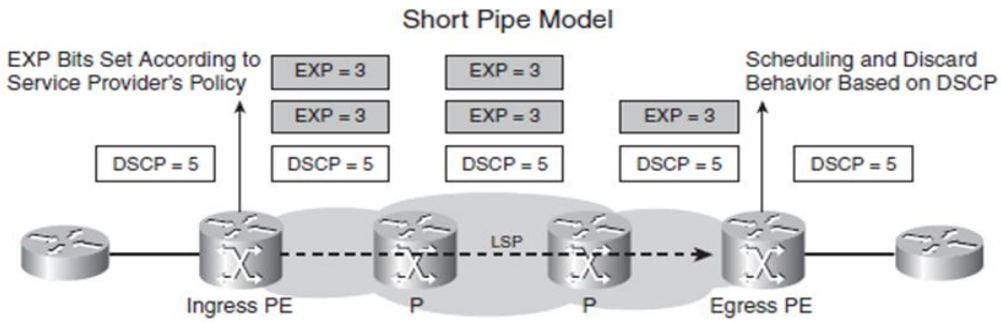
Ưu điểm của mô hình này là thông tin Tunneled DiffServ ban đầu được bảo toàn khi gói tin ra khỏi mạng MPLS. Điều đó nghĩa là thông tin IP DiffServ hoặc thông tin Tunneled MPLS DiffServ giữ nguyên không đổi. Khi khách hàng kết nối tới mạng MPLS, thông tin QoS của họ được chuyển bằng đường hầm một cách trong suốt qua mạng MPLS. Hơn nữa nếu khách hàng có riêng luật QoS của họ, nhà cung cấp dịch vụ MPLS cũng đưa ra luật riêng của họ trên những gói tin ở LSR lối vào mà không thay đổi thông tin QoS ban đầu của gói tin, và do đó có thể bỏ qua luật của

khách hàng. Điều này có khả năng mở rộng hơn việc phục vụ QoS của từng khách hàng. Bởi vì một nhãn chỉ có thể có 3 bit EXP, nhà cung cấp dịch vụ MPLS phải khớp mỗi mức QoS của mỗi khách hàng vào một trong 8 mức QoS trong mạng MPLS.

4.4.3.2 Mô hình ống ngắn (Short Pipe Model)

Mô hình ống ngắn tương tự mô hình ống với một điểm khác ở việc xử lý chuyển tiếp gói tin trên LSR lối ra. Ở mô hình này nó dựa vào thông tin của Tunneled DiffServ thay vì LSP DiffServ như ở mô hình ống, điều này cho phép gói tin được chuyển tiếp tùy theo thông tin QoS khác nhau của khách hàng. Do đó điểm thứ ba của mô hình ống ngắn sẽ được sửa thành:

- Trên LSR lối ra, xử lý chuyển tiếp gói tin dựa trên thông tin Tunneled DiffServ và thông tin LSP DiffServ không được sao chép tới thông tin Tunneled Diffserv.



Hình 4 - 24 Mô hình ống ngắn

Mô hình này cũng có ưu điểm tương tự như mô hình ống trên.

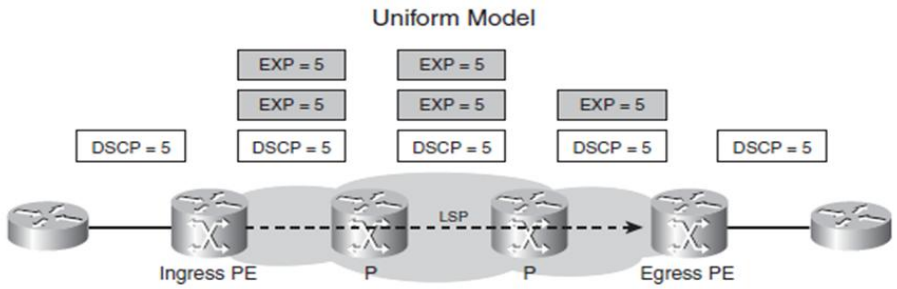
4.4.3.3 Mô hình thống nhất (Uniform Model)

Mô hình thống nhất hơi khác so với mô hình ống ngắn và mô hình ống. Trong mô hình thống nhất các luật sau được áp dụng:

- Thông tin LSP DiffServ phải được kế thừa từ thông tin Tunneled DiffServ trên LSR lối vào.
- Trên LSR trung gian (P router), thông tin LSP DiffServ của nhãn ra được kế thừa từ thông tin LSP DiffServ của nhãn tới.
- Trên LSR lối ra, thông tin LSP DiffServ phải được sao chép tới thông tin Tunneled DiffServ.

Chú ý sự thay đổi ở điểm đầu tiên: thông tin LSP DiffServ phải được kế thừa từ thông tin Tunneled DiffServ trên LSR lối vào. Trên LSR lối ra, thông tin Tunneled DiffServ phải kế thừa từ thông tin LSP DiffServ. Điều này có nghĩa là một gói tin thuộc cùng một lớp QoS tại bất kì thời điểm nào. Thông tin QoS luôn luôn ở nhãn trên cùng hoặc trong header của gói tin chưa được gắn nhãn. Mạng MPLS không gây ra tác động nào trên thông tin QoS mà nó chỉ chuyển gói tin qua mạng. Chúng ta có thể thay đổi những bit EXP trên những nhãn đầu tiên thông qua cấu hình tại một vị trí nào đó trên mạng. Thay đổi này là thay đổi trên thông tin LSP DiffServ, nó sẽ không được sao

chép tới thông tin Tunneled DiffServ trong mô hình ống và mô hình ống ngắn tuy nhiên nó sẽ được sao chép trong mô hình thống nhất ở LSR lối ra.



Hình 4 - 25 Mô hình thống nhất

Ưu điểm của mô hình này là chỉ có một thông tin DiffServ cho một gói tin. Đây là thông tin DiffServ đóng gói trên nhãn đỉnh. Việc nó khác với thông tin DiffServ phía dưới là không quan trọng vì thông tin DiffServ trên cùng sẽ được sao chép xuống ở LSR lối ra của LSP.

4.5 Thiết kế QoS cho MPLS-VPN

[13]

4.5.1.1 Một số nguyên tắc thiết kế

Bên cạnh vai trò cơ bản của QoS trong các mạng doanh nghiệp, vai trò của QoS trong mạng MPLS-VPN có thể được mở rộng bao gồm những khía cạnh sau:

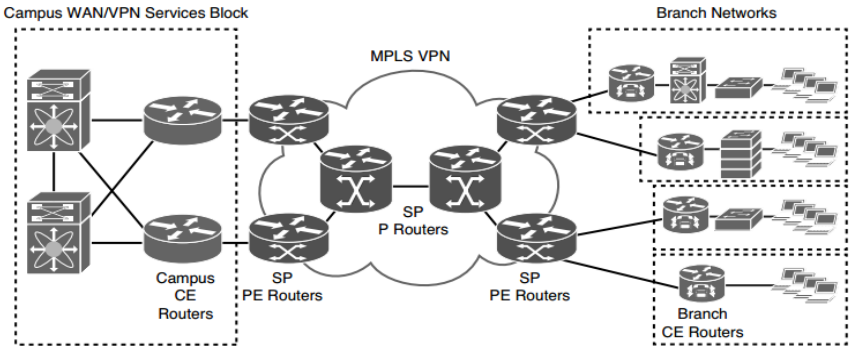
- Định hình lưu lượng với tốc độ hợp đồng
- Ánh xạ các lớp dịch vụ trong doanh nghiệp tới các lớp dịch vụ của ISP
- Loại bỏ gói tin trong các lớp dịch vụ cho phù hợp với tốc độ hợp đồng
- Phục hồi các đánh dấu trên gói tin

Do vậy, có khá nhiều nguyên tắc chiến lược trong việc thiết kế QoS áp dụng cho MPLS VPN bao gồm:

- ***Phân loại và đánh dấu ứng dụng càng gần nguồn càng tốt về hai khía cạnh kỹ thuật và quản trị***: Một số chính sách phân loại có thể yêu cầu sự hiểu biết ở lớp 7 và có thể sẽ không thể thực hiện được trên các switch. Vì vậy Router CE có thể là điểm khả thi về mặt kỹ thuật nhất để thực hiện việc phân loại chi tiết này.
- ***Loại bỏ các luồng dữ liệu không mong muốn càng gần nguồn càng tốt***: Các nhà cung cấp dịch vụ sẽ loại bỏ lưu lượng ở PE router đầu vào theo hợp đồng dịch vụ. Những luồng lưu lượng vượt quá tốc độ có thể bị đánh dấu lại, hủy bỏ hoặc tính chi phí thêm cho khách hàng
- ***Thực thi chính sách hàng đợi ở tất cả các nút có khả năng xảy ra tắc nghẽn***: Thực thi chính sách hàng đợi trên tất cả các Router CE và PE đồng thời trên cả các thiết bị lõi P router của nhà cung cấp dịch vụ (nếu cần thiết)
- ***(Tùy chọn) Bảo vệ mặt phẳng điều khiển và mặt phẳng chuyển tiếp bằng cách áp dụng chính sách bảo vệ với mặt phẳng điều khiển***: Để gia cố (harden) hạ tầng mạng để ngăn chặn và kiềm chế các tấn công mạng

Tuy nhiên trước khi những nguyên tắc chiến lược kể trên có thể được chuyển thành các cấu hình khuyến nghị cụ thể trên một nền tảng nhất định chúng ta sẽ đi qua một vài khía cạnh liên quan sẽ được tình bày lần lượt ở các phần tiếp theo

Đầu tiên chúng ta xem xét lại các thành phần chủ yếu của MPLS-VPN được thể hiện trong hình 4-26. Mô hình này sẽ được sử dụng trong thiết kế QoS ở mục này.



Hình 4 - 26 Kiến trúc của MPLS và vai trò của các router

Hình trên giúp chúng ta nhớ lại các thành phần chủ yếu của mạng MPLS-VPN đồng thời vai trò của các router trong mô hình bao gồm:

- CE Router
- PE Router
- Provider Router

Một điều cần ghi nhớ nữa là MPLS VPN cung cấp dịch vụ VPN Layer 3 ở dạng lưới đầy đủ và điều này làm tăng tính phức tạp của mô hình QoS áp dụng cho nó.

4.5.1.2 Mối quan hệ chặt chẽ với công nghệ truyền dẫn Ethernet

Khuyến nghị: Hiểu được mối quan hệ chặt chẽ của công nghệ truyền dẫn Ethernet với QoS

Sự phổ biến và tính mềm dẻo của công nghệ Ethernet làm cho nó trở thành lựa chọn hấp dẫn phục vụ cho lớp truyền dẫn VPN ở cả hai phía doanh nghiệp và khách hàng. Khách hàng sẽ không còn phải mua những mô đun mở rộng riêng để phục vụ kết nối WAN như ATM hay POS. Tương tự nhà cung cấp dịch vụ cũng đơn giản hơn trong yêu cầu thiết bị phần cứng. Thêm nữa, nhà cung cấp dịch vụ có thể cung cấp dịch vụ một cách mềm dẻo và có khả năng mở rộng bằng việc cung cấp cho khách hàng dịch vụ truy cập Ethernet với tốc độ thấp hơn mặc định (sub-line-rate Ethernet)

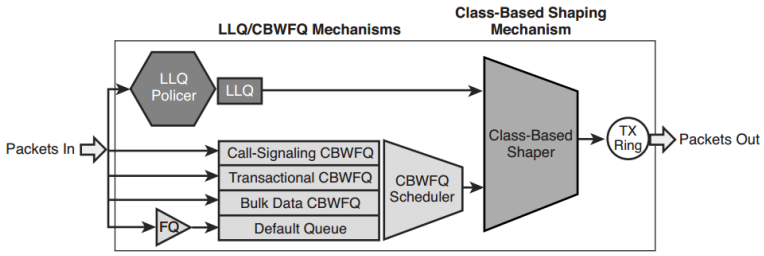
Sub-line-rate Ethernet, như cái tên của nó diễn tả hợp đồng dịch vụ cung cấp lưu lượng thấp hơn khả năng của đường truyền Gigabit Ethernet (GE). Nó có thể từ 1 – 999 Mbps. Thêm nữa, hợp đồng sẽ rất mềm dẻo, có thể được điều chỉnh dễ dàng theo yêu cầu khách hàng mà không cần phải nâng cấp phần cứng trái ngược với công nghệ chuyển mạch WAN truyền thống mang tính cố định cao. Ví dụ muốn nâng đường truyền WAN truyền thống từ T3/DS3 (45 Mbps) lên OC3 (155 Mbps) thì phải

mua mô đun kết nối khác nhưng với công nghệ Ethernet sub-line-rate thì không cần thiết.

Tuy nhiên từ góc nhìn QoS, công nghệ sub-line-rate cần phải có sự chú ý hơn. Chúng ta biết rằng, chính sách hàng đợi chỉ được sử dụng khi đường truyền vật lý bị tắc nghẽn. Điều đó có nghĩa là chính sách hàng đợi sẽ không bao giờ được sử dụng trong đường truyền với công nghệ truy cập sub-line-rate. Trong những trường hợp này, chính sách hàng đợi chỉ có thể đạt được ở tốc độ thấp hơn mặc định bằng việc sử dụng chính sách gồm hai phần hay còn gọi là chính sách chất lượng dịch vụ phân cấp hay chính sách QoS lồng nhau. Nó gồm hai phần sau:

- Thực hiện định hình (shape) lưu lượng phù hợp với tốc độ thỏa thuận
- Lưu lượng được đặt trong hàng đợi theo chính sách hàng đợi LLQ/CBWFQ mỗi khi đường truyền vượt quá dung lượng được thỏa thuận trên

Để hiểu rõ hơn, ta có thể xem thêm mô tả bằng hình 4-27 bên dưới:



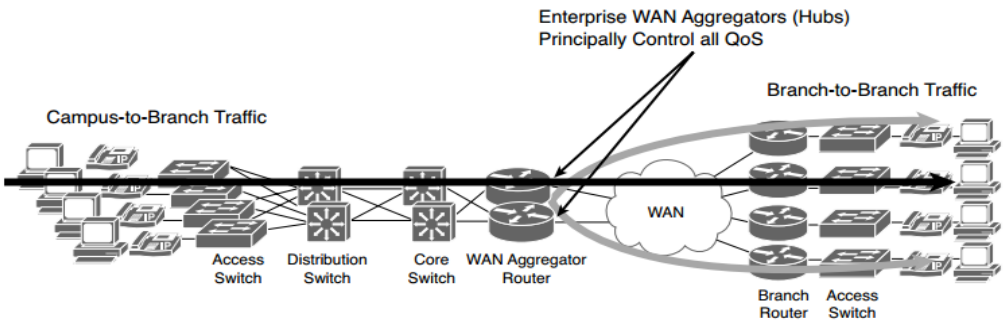
Hình 4 - 27 Chính sách QoS lồng nhau

4.5.1.3 Chuyển đổi mô hình QoS

Khuyến nghị: Thừa nhận rằng doanh nghiệp và nhà cung cấp dịch vụ phải phối hợp để cùng nhau thực hiện QoS qua MPLS VPN

Như đã đề cập, MPLS VPN cung cấp cấu hình lưới giữa trụ sở chính và các chi nhánh. Chính sự kết nối dạng lưới đầy đủ này kéo theo những thay đổi quan trọng trong thiết kế QoS so với mô hình WAN truyền thống thường triển khai theo mô hình point-to-point (điểm-điểm) hoặc hub-and-spoke.

Do sự ràng buộc về chi phí, khả năng mở rộng và khả năng quản lý nên các mô hình WAN truyền thống hiếm khi sử dụng mô hình lưới. Thay vào đó, hầu hết sự thiết kế WAN thường xoay quanh mô hình hub-and-spoke. Trong mô hình hub-and-spoke, QoS thường được quản lý ở hub router (ví dụ thiết bị tập trung WAN…) bởi doanh nghiệp. Thiết bị tập trung WAN điều khiển không chỉ dữ liệu từ trụ sở đến chi nhánh mà còn giữa các chi nhánh với nhau. Hình 4-28 dưới đây mô tả QoS chủ yếu được quản trị bởi khách hàng doanh nghiệp:

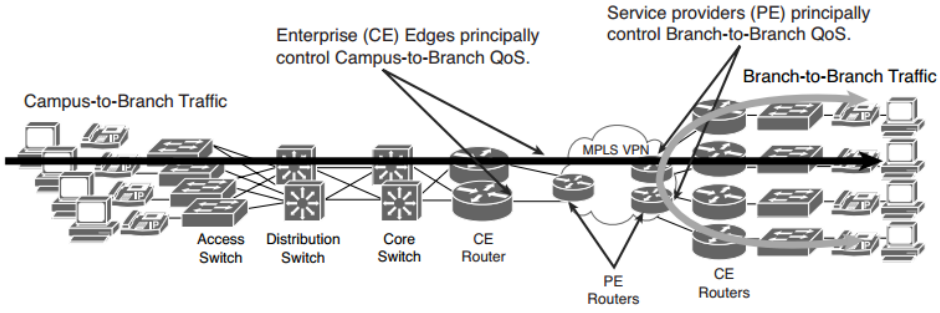


Hình 4 - 28 Quản trị QoS trong thiết kế WAN truyền thống dạng Hub-and-Spoke

Tuy nhiên, với MPLS-VPN vốn đã cung cấp kết nối dạng lưới đầy đủ, mô hình quản trị QoS cần phải có sự thay đổi. Dưới thiết kế dạng lưới, Router ở trụ sở chính (hub router) vẫn điều khiển QoS cho tất cả dữ liệu từ trụ sở đến các chi nhánh nhưng sẽ không còn điều khiển được lưu lượng giữa các chi nhánh với nhau. Mặc dù có thể nhận ra phương án cho kịch bản mới này là đảm bảo QoS được cung cấp trên tất cả các router của chi nhánh nhưng điều này là chưa đầy đủ vì nó chỉ giải quyết một phần của vấn đề.

Lấy một ví dụ, giả sử trường hợp cung cấp hội nghị truyền hình cho tất cả các chi nhánh. Như trong trường hợp WAN truyền thống, thực hiện chính sách hàng đợi để ưu tiên các gói tin hội nghị truyền hình trên bộ tập trung WAN là yêu cầu bắt buộc. Sau đó doanh nghiệp phải cung cấp chính sách tương tự trên các router chi nhánh. Theo cách này bất kỳ cuộc gọi nào từ bất kỳ vị trí nào tới bất kỳ vị trí nào trong doanh nghiệp được bảo vệ chống lại các lưu lượng ít ưu tiên hơn. Vấn đề phức tạp trong mô hình lưới đó là các lưu lượng cạnh tranh không phải luôn luôn đến từ cùng một site mà nó có thể đến từ bất kỳ một site nào. Hơn nữa doanh nghiệp cũng không thể điều khiển hoàn toàn QoS giữa các chi nhánh với nhau vì lưu lượng giữa các chi nhánh có thể không đi qua router trung tâm. Tiếp tục với ví dụ, nếu một cuộc gọi hội nghị truyền hình được thiết lập giữa hai chi nhánh và một người dùng từ một trong các chi nhánh trên cũng khởi tạo một phiên tải FTP đến chi nhánh chính, khả năng quá tải của đường liên kết giữa PE-to-CE khá lớn thậm chí sẽ gây gián đoạn cuộc gọi hội nghị truyền hình.

Cách duy nhất để đảm bảo chất lượng dịch vụ trong trường hợp này là nhà cung cấp dịch vụ thực hiện chính sách hàng đợi phù hợp với chính sách của doanh nghiệp trên tất cả các đường liên kết trên PE tới các chi nhánh (PE-to-CE). Điều này tạo nên sự chuyển đổi mô hình quản trị QoS cho mô hình lưới đầy đủ mà ta gọi là "Doanh nghiệp và nhà cung cấp dịch vụ phải kết hợp với nhau một cách chặt chẽ để thực hiện QoS qua mạng MPLS", như chỉ ra trên hình 4-29



Hình 4 - 29 Thực hiện QoS trong thiết kế dạng lưới đầy đủ của MPLS-VPN

Tóm lại, chính sách hàng đợi phải là điều bắt buộc trên router PE và CE đầu ra vì tính chất lưới đầy đủ của MPLS VPN. Ngoài ra, router PE cũng sẽ phải có chính sách chặn lưu lượng để đảm bảo thỏa thuận chất lượng dịch vụ

4.5.1.4 Các mô hình lớp dịch vụ của nhà cung cấp dịch vụ

Khuyến nghị:

- Hiểu một cách đầy đủ về các mô hình lớp dịch vụ của nhà cung cấp
- Nếu có nhiều lựa chọn, lựa chọn mô hình phù hợp nhất với chiến lược QoS của doanh nghiệp

Tùy thuộc vào nhà cung cấp dịch vụ định nghĩa các mô hình lớp dịch vụ, các khách hàng sẽ nhận được các mức dịch vụ tương ứng. Không có mô hình nào phù hợp với tất cả các khách hàng, nó tùy thuộc vào chiến lược cạnh tranh của từng nhà cung cấp dịch vụ. Tuy nhiên, hầu hết các nhà cung cấp dịch vụ thường cung cấp mô hình 4 hoặc 6 lớp dịch vụ (hình 4-30)

Service Provider Classes-of-Service		Service Provider Classes-of-Service	
EF CS5	SP-REALTIME-CLASS LLQ 30%	EF CS5	SP-REALTIME-CLASS (RTP) LLQ 10%
		AF41 CS4	SP-AF4-CLASS (RTP) CBWFQ 20% BW + DSCP-WRED
AF31 CS3	SP-AF3-CLASS CBWFQ 10% BW	AF31 CS3	SP-AF3-CLASS (UDP) CBWFQ 10% BW + DSCP-WRED
AF21 CS2	SP-AF2-CLASS CBWFQ 35% BW + DSCP-WRED	AF21 CS2	SP-AF2-CLASS (TCP) CBWFQ 25% BW + DSCP-WRED
		AF11 CS1	SP-AF1-CLASS (Control) CBWFQ 10% BW + DSCP-WRED
DF	SP-Default-Class CBWFQ 25% BW + WRED	DF	SP-DEFAULT-CLASS CBWFQ 25% BW + WRED

Hình 4 - 30 Mô hình 4 lớp và 6 lớp ISP

Việc cung cấp một lớp dịch vụ (CoS) cụ thể phụ thuộc vào sự đánh dấu dữ liệu (thường là trường DSCP). Tuy nhiên cách đánh dấu trong mỗi lớp thường khác nhau, tương tự cho các chính sách đánh dấu lại/loại bỏ của các nhà cung cấp cụ thể và băng thông phân bổ cho mỗi lớp

Khi có nhiều mô hình chất lượng dịch vụ được tùy chọn, khách hàng nên lựa chọn mô hình gần khớp với chiến lược QoS của doanh nghiệp nhất.

4.5.1.5 Các chế độ đường hầm DiffServ trong MPLS

Khuyến nghị:

- Hiểu rõ các chế độ đường hầm trong MPLS và cách nó tác động đến đánh dấu DSCP của khách hàng
- Mô hình ống ngắn (Short Pipe Mode) cung cấp cho khách hàng doanh nghiệp

Bởi vì nhãn MPLS chứa 3 bit EXP thường sử dụng cho đánh dấu QoS nên có thể giữ nguyên được cách đánh dấu (marking) của gói tin IP khi đi qua mạng MPLS VPN của nhà cung cấp dịch vụ

Ba mô hình đường hầm khác nhau được định nghĩa. Cả ba mô hình này đã được trình bày phía trên. Sau đây là các khuyến cáo cho từng mô hình:

- ***Mô hình thống nhất (Uniform Model)***

Mô hình này thường được sử dụng khi khách hàng và nhà cung cấp dịch vụ chia sẻ chung một miền DiffServ, như trong trường hợp doanh nghiệp tự triển khai mạng lõi MPLS VPN

Cần lưu ý rằng các gói tin của bạn có thể bị thay đổi trường DSCP khi nhà cung cấp dịch vụ hoạt động trong mô hình này

- ***Mô hình ống ngắn (Short Pipe Model)***

Mô hình này thường được sử dụng khi khách hàng và nhà cung cấp dịch vụ khác miền DiffServ.

Mô hình này hữu ích khi nhà cung cấp dịch vụ muốn thiết lập một chính sách DiffServ riêng và khách hàng yêu cầu các thông tin DiffServ của khách hàng phải được giữ nguyên khi đi qua mạng MPLS VPN của nhà cung cấp dịch vụ.

- ***Mô hình ống (Pipe Model)***

Mô hình này tương tự như mô hình ống ngắn

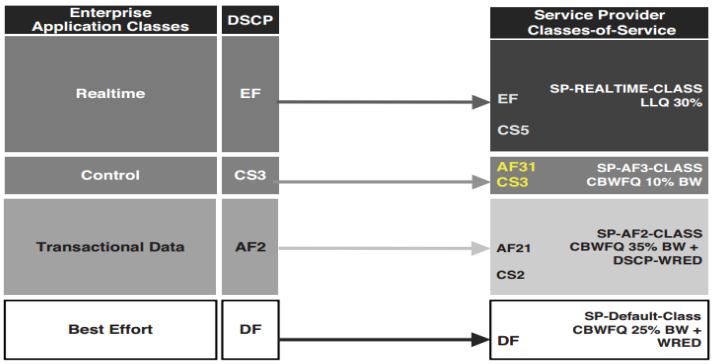
Tuy nhiên điểm khác giữa mô hình này và mô hình ống ngắn phía trên là các router PE đầu ra xử lý gói tin đến router khách hàng (CE Router) tùy thuộc vào sự đánh dấu của nhà cung cấp dịch vụ chứ không phụ thuộc vào trường DSCP của gói tin khách hàng như ở mô hình ống ngắn

4.5.1.6 Ánh xạ lưu lượng giữa khách hàng và nhà cung cấp dịch vụ

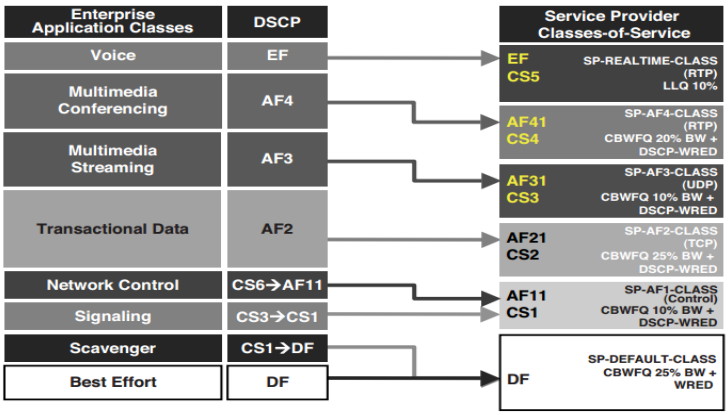
Nhiều khi số lượng các lớp dịch vụ của nhà cung cấp dịch vụ bằng hoặc lớn hơn số lượng lớp dịch vụ mà doanh nghiệp định nghĩa trong chiến lược của họ, tuy nhiên điều đó không phải luôn luôn đúng

Nếu số lượng lớp trong khách hàng lớn hơn số lượng các lớp dịch vụ của nhà cung cấp dịch vụ thì khách hàng phải ánh xạ cho phù hợp với mô hình nhà cung cấp dịch vụ một cách khôn khéo và hiệu quả bằng cách gộp hoặc loại bỏ một số lớp đồng thời thực hiện đánh dấu lại nếu cần thiết.

Hình 4-31 và hình 4-32 minh họa cách ánh xạ các lớp lưu lượng khách hàng và nhà cung cấp dịch vụ



Hình 4 - 31 Mô hình 4 - lớp dịch vụ của khách hàng ánh xạ với mô hình 4-lớp của nhà cung cấp dịch vụ



Hình 4 - 32 Mô hình 8 – lớp dịch vụ của khách hàng ánh xạ với mô hình 6-lớp của nhà cung cấp dịch vụ

- ***Ánh xạ lưu lượng Voice và Video***

Nhà cung cấp dịch vụ thường cung cấp một lớp dịch vụ thời gian thực ví dụ lớp "Real-Time Interactive", bạn sẽ phải chọn liệu có ánh xạ cả video vào lớp thời gian thực này hay không.

Lựa chọn ánh xạ cả lưu lượng voice và video vào lớp thời gian thực này sẽ đạt hiệu quả chất lượng dịch vụ cao nhất cho những ứng dụng này. Tuy nhiên giá thành của lớp này thường khá cao. Nếu lựa chọn cách này thì nên triển khai hai lớp LLQ (Low Latency Queuing) để bảo vệ lưu lượng voice khỏi lưu lượng video.

Một cách tốt hơn là chuyển lớp video sang lớp không phải thời gian thực (non-real-time class). Với cách này chất lượng video có giảm đôi chút tuy nhiên sẽ đạt hiệu quả về mặt giá thành tốt hơn.

- ***Ánh xạ lưu lượng điều khiển và báo hiệu***

Đầu tiên chú ý nên tránh kết hợp các lưu lượng điều khiển với lưu lượng dữ liệu thông thường trong cùng một lớp dịch vụ

Bất cứ khi nào có thể, các lưu lượng điều khiển và báo hiệu nên được gán cho một lớp dịch vụ riêng của nhà cung cấp dịch vụ để tránh các lưu lượng điều khiển và báo hiệu bị loại bỏ. Khi các lưu lượng điều khiển bị loại bỏ thì rất có thể làm cho hoặc mạng hoặc các lưu lượng voice/video hoặc cả hai bị ảnh hưởng.

Nếu không có một lớp dịch vụ dành riêng cho các lưu lượng loại này thì có thể xem xét ánh xạ nó vào lớp lưu lượng thời gian thực (real-time) vì những lưu lượng loại này thường nhỏ và cực kỳ quan trọng

- ***Tách biệt lưu lượng TCP và UDP***

Một điều đặc biệt lưu ý là không nên kết hợp hai lưu lượng TCP và UDP trong một lớp dịch vụ. Lưu lượng UDP có thể kể đến như các ứng dụng streaming video (broacast video hoặc multimedia streaming). Sở dĩ phải làm việc này bởi vì các hành vi trái ngược nhau của các loại lưu lượng này trong khoảng thời gian tắc nghẽn. Cụ thể hơn, các nguồn phát TCP sẽ chủ động giảm các luồng khi nhận ra có sự hủy bỏ gói tin. Mặc dù một số ứng dụng UDP có khả năng điều khiển lưu lượng và khả năng gửi lại gói tin bị mất, hầu hết các nguồn phát UDP hoàn toàn không quan tâm tới mất gói và do đó không bao giờ giảm tốc độ truyền vì có sự hủy bỏ gói tin

Khi các luồng TCP kết hợp với các luồng UDP trong một lớp lưu lượng và lớp này xuất hiện tắc nghẽn, luồng TCP sẽ giảm liên tục tốc độ truyền, khả năng từ bỏ băng thông cao để nhường cho các lưu lượng UDP không quan tâm tới việc mất gói. Hiệu ứng này gọi là TCP starvation/UDP dominance

Tất nhiên không phải lúc nào cũng có thể tách biệt hai loại lưu lượng này nhưng nó cũng có nhiều lợi ích khi nhận thức được các hành vi khi kết hợp hai loại lưu lượng trên

- ***Đánh dấu lại và khôi phục đánh dấu***

Một số nhà cung cấp dịch vụ sử dụng đánh dấu trong trường DSCP của khách hàng để quyết định lớp dịch vụ nào gói tin đó sẽ thuộc về. Do vậy, khách hàng phải đánh dấu lưu lượng một cách nhất quán với các điều kiện đánh dấu của nhà cung cấp dịch vụ

Nguyên tắc chung là đánh dấu càng gần nguồn càng tốt như đã trình bày phía trên. Tuy nhiên một số loại lưu lượng phải cần đánh dấu lại trước khi gửi đến nhà cung cấp dịch vụ để nhà cung cấp dịch vụ có thể gán nó vào đúng lớp dịch vụ khách hàng mong muốn. Nếu trường hợp đó xảy ra, khuyến cáo sẽ thực hiện ở CE router đầu ra bởi vì các dịch vụ của nhà cung cấp thường sẽ phát triển hoặc mở rộng theo thời gian và sự điều chỉnh cho những thay đổi đó sẽ dễ dàng quản lý nếu nó thực hiện trên router CE đầu ra

Trong một vài trường hợp, nhiều loại dữ liệu có thể yêu cầu phải đánh dấu lại cho cùng một giá trị DSCP để được gán chính xác bởi nhà cung cấp dịch vụ. Ngoài ra, nhà cung cấp dịch vụ hoạt động trong mô hình thống nhất có thể phải đánh dấu lại các lưu lượng vi phạm chính sách điều này làm ảnh hưởng đến chính sách nhất quán QoS của khách hàng

Trong bất kỳ trường hợp nào trên, khi ra khỏi MPLS VPN, những lớp lưu lượng này đều sẽ không thể phân biệt được với nhau chỉ bằng giá trị DSCP. Tuy nhiên những giá trị đánh dấu DSCP này có thể dễ dàng được khôi phục bằng việc sử dụng kỹ thuật deep packet inspection (tạm dịch phân tích sâu trong gói) áp dụng ở CE Router theo chiều vào

4.6 Kết luận chương

Chương này đã trình bày một số khái niệm liên quan tới QoS, cơ chế và cách thức áp dụng với các gói tin IP truyền thống. Từ đó tìm cách áp dụng các khái niệm, cơ chế đó cho mạng MPLS và đặc biệt là mạng MPLS VPN. Chương này cũng đã tìm hiểu và đưa ra các khái niệm, cách thức hoạt động của các mô hình đường hầm phổ biến trong MPLS VPN. Tiếp theo chương cũng đưa ra một số vấn đề cần lưu ý và cách thiết kế tốt nhất để có chất lượng dịch vụ QoS tối ưu cho mạng MPLS VPN như các trường hợp sử dụng các mô hình đường hầm thế nào, mô hình nào là tối ưu, các cách ánh xạ từ mô hình chất lượng dịch vụ sẵn có của khách hàng tới nhà cung cấp dịch vụ và những điều cần lưu ý. Chắc chắn với những vấn đề đã trình bày sẽ đem đến cho mỗi người những chỉ dẫn thiết kế QoS cho mạng MPLS VPN một cách khá rõ ràng, dễ hiểu để có thể dễ dàng áp dụng cho mạng của mình.

CHƯƠNG 5. MÔ PHỎNG QOS TRONG MPLS – VPN

5.1 Giới thiệu GNS3

GNS3 là một phần mềm giải lập mạng, cho phép mô phỏng lại các hệ thống mạng máy tính một cách rất gần với thực tế. Để cung cấp khả năng mô phỏng chính xác, GNS3 liên kết với Dynamips (giả lập IOS thật của Cisco), Qemu (mô phỏng và ảo hóa nguồn mở), Virtualbox (phần mềm ảo hóa máy trạm mạnh mẽ)…

GNS3 hỗ trợ đắc lực thực hành các mô hình thực tế cho các kỹ sư mạng, các quản trị viên hoặc những người muốn theo học các chứng chỉ Cisco như: CCNA, CCNP, CCIE…

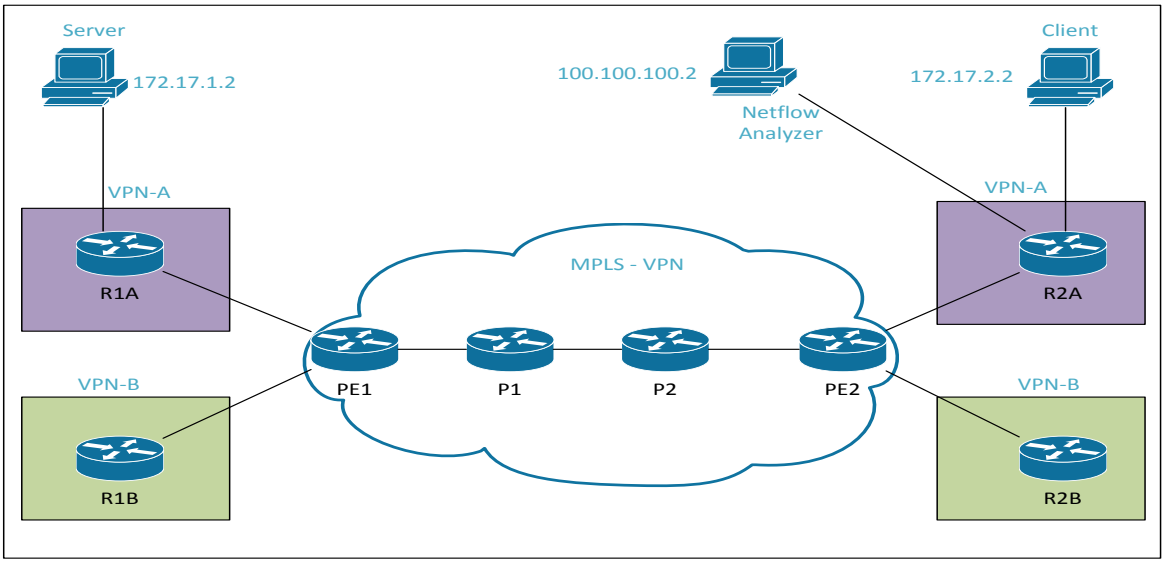
GNS3 là một phần mềm mã nguồn mở và có sẵn trên nhiều nền tảng khác nhau như: Windows, Linux, MacOS…

5.2 Đặt vấn đề

Để hiểu rõ hơn cơ chế hoạt động, hiệu quả của việc triển khai QoS trên MPLS-VPN, đầu tiên luận văn đã tiến hành xây dựng một mạng mô phỏng MPLS quy mô nhỏ, kết hợp sử dụng một số phần mềm sinh lưu lượng để tạo ra những tình huống cần sử dụng QoS tương tự trong thực tế. Sau đó sẽ áp dụng QoS để giải quyết các tình huống này một cách phù hợp, để thấy được hiệu quả của nó.

5.3 Mô hình và kịch bản mô phỏng

Mô hình đề xuất:



Hình 5 - 1 Mô hình đề xuất

QoS cho mạng MPLS VPN có thể được chia thành hai trường hợp nhỏ tùy thuộc vào việc thực hiện QoS trong mạng khách hàng hay thực hiện QoS trong mạng nhà cung cấp dịch vụ

5.3.1 Trường hợp 1: Thực hiện QoS trong mạng khách hàng

Trong mô hình 5-1 thì R1A, R2A, R1B, R2B là bộ định tuyến của các khách hàng A và B. Giả sử rằng khách hàng A đăng ký tốc độ truyền 18 Mbps với các yêu cầu băng thông như sau:

Loại lưu lượng	Tốc độ cam kết
Video	12 Mbps
FTP	2 Mbps
HTTP	2 Mbps
PC Anywhere	1 Mbps
Còn lại	1 Mbps

Máy tính ở dải địa chỉ 172.17.1.0/24 nằm ở site 1 khách hàng A (R1A) sẽ đóng vai trò Server còn máy tính ở dải 172.17.2.0/24 nằm ở site 2 khách hàng A (R2A) sẽ đóng vai trò Client. Tại phía Server ta sẽ dùng phần mềm VLC thực hiện stream video đồng thời tại đây tạo ra một luồng FTP lưu lượng lớn gây nghẽn đường truyền. Tiếp đó ta sẽ thực hiện QoS trên mạng MPLS-VPN, phân lớp lưu lượng sao cho các gói tin Video được ưu tiên, các gói tin còn lại sẽ nhận được đủ băng thông cho mỗi loại theo yêu cầu đồng thời kiểm tra chất lượng các luồng lưu lượng về trực quan và số liệu liên quan.

5.3.1.1 Cấu hình mô phỏng

Sau khi thiết lập mô hình MPLS-VPN, ta tiếp tục sử dụng phần mềm Iperf v3 để tạo 4 luồng lưu lượng: HTTP, PC Anywhere, Video, custom, kết hợp phần mềm FileZilla để tạo luồng FTP. Chúng ta sử dụng mô hình Uniform cho mạng MPLS-VPN, thực hiện phân lớp lưu lượng như sau:

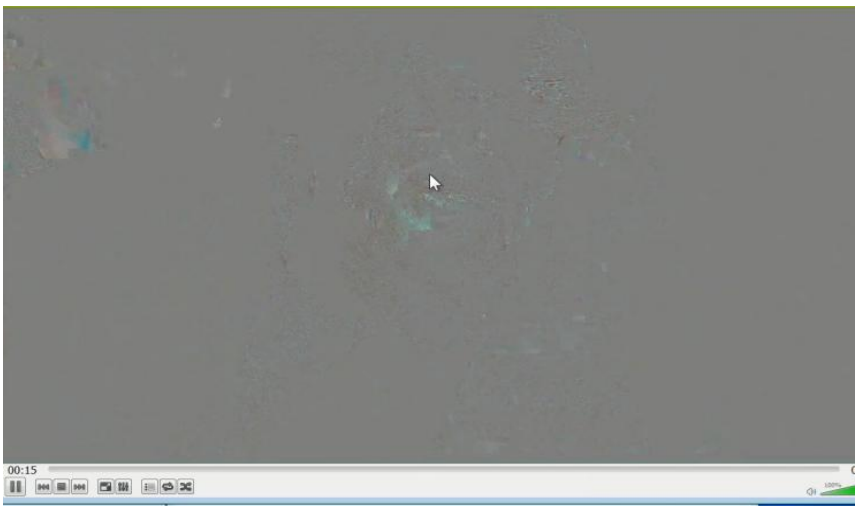
Lớp lưu lượng	Cổng	DSCP	Băng thông
video	8080	EF	12 Mbps
http	80	AF41	2 Mbps
pcanywhere	5631	CS3	1 Mbps
ftp	21	CS2	2 Mbps
custom	9090	CS1	1 Mbps

5.3.1.2 Kết quả mô phỏng

Để kiểm tra tính hiệu quả của QoS, luận văn sẽ đưa ra kết quả trước và sau khi thực hiện áp dụng chính sách QoS.

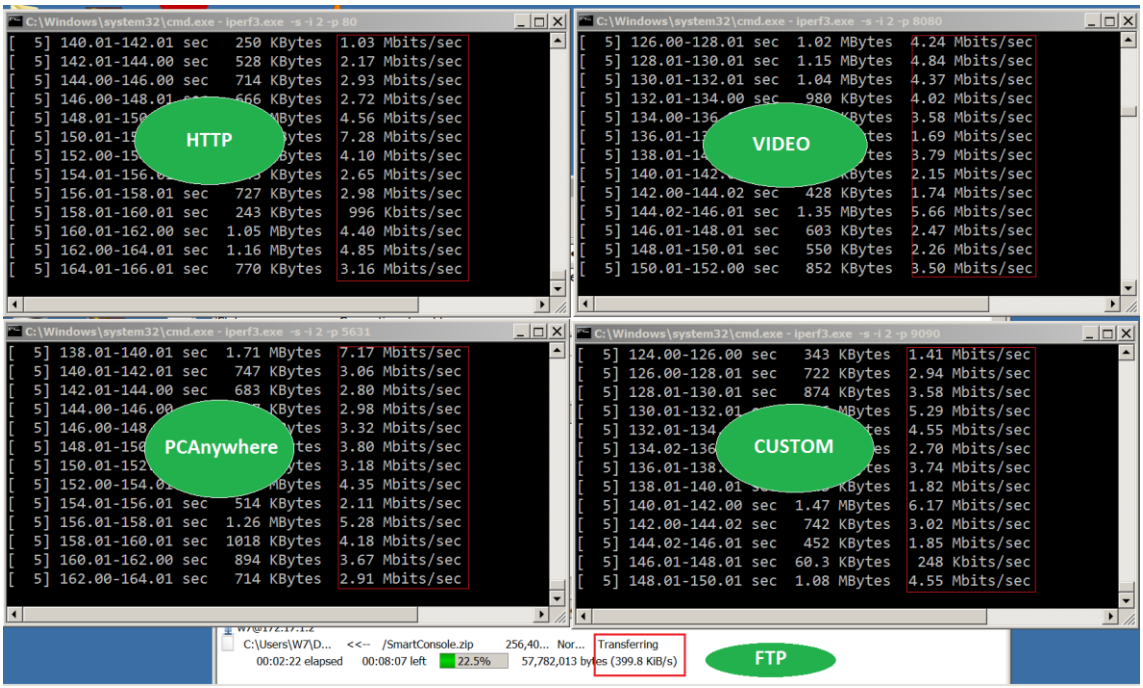
a) Trước khi thực hiện QoS

Khi chưa thực hiện cấu hình QoS, hình ảnh thu được ở phía client khi phát Video sẽ có hiện tượng bị nhiễu, giật như hình 5-2 dưới:

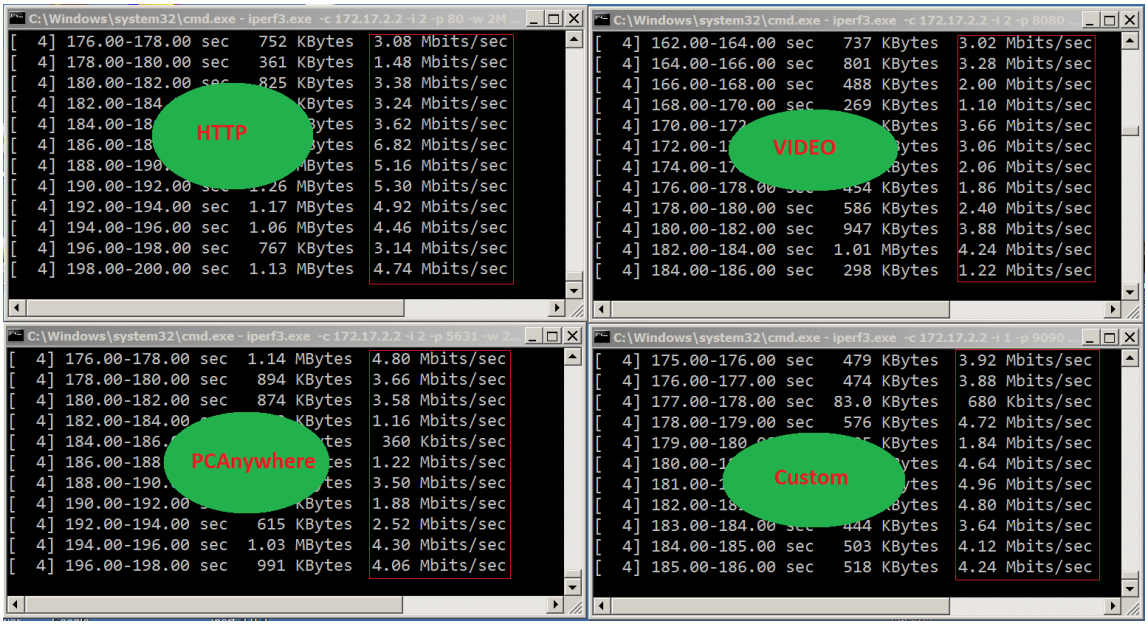


Hình 5 - 2 Tín hiệu video phía client khi chưa có QoS

Kiểm tra băng thông từng loại lưu lượng với phần mềm giải lập Iperf v3 chúng ta thấy như sau:



Hình 5 - 3 Màn hình bên máy Client



Hình 5 - 4 Màn hình phía server

Có thể nhận thấy ở cả hai phía Client và Server băng thông sẽ bị chia sẻ bởi các luồng gần như công bằng xấp xỉ 4 Mbps.

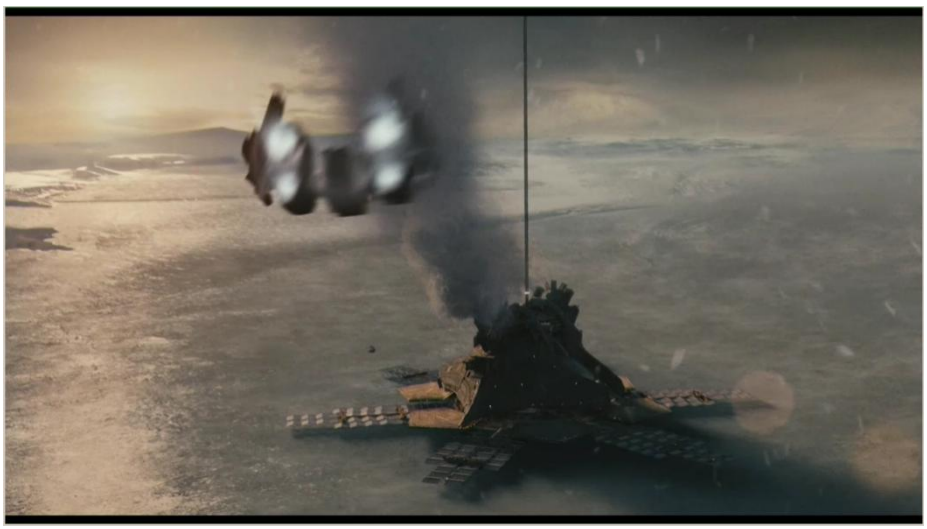
Sử dụng chương trình Netflow Analyzer để thu thập băng thông các luồng trên router R2A chúng ta cũng thấy rõ tỉ lệ băng thông cân bằng trong hình dưới đây:

Application	Protocol	Total Traffic	Total Packets	Traffic Percentage
pcANYWHE	TCP	451008.6 K	38426	20%
WebSM (90	TCP	445364.0 K	37940	20%
49189	TCP	444768.7 K	37505	20%
HTTP Altern	TCP	436925.0 K	37175	20%
World Wide	TCP	432122.8 K	36808	20%

Hình 5 - 5 Netflow khi chưa QoS

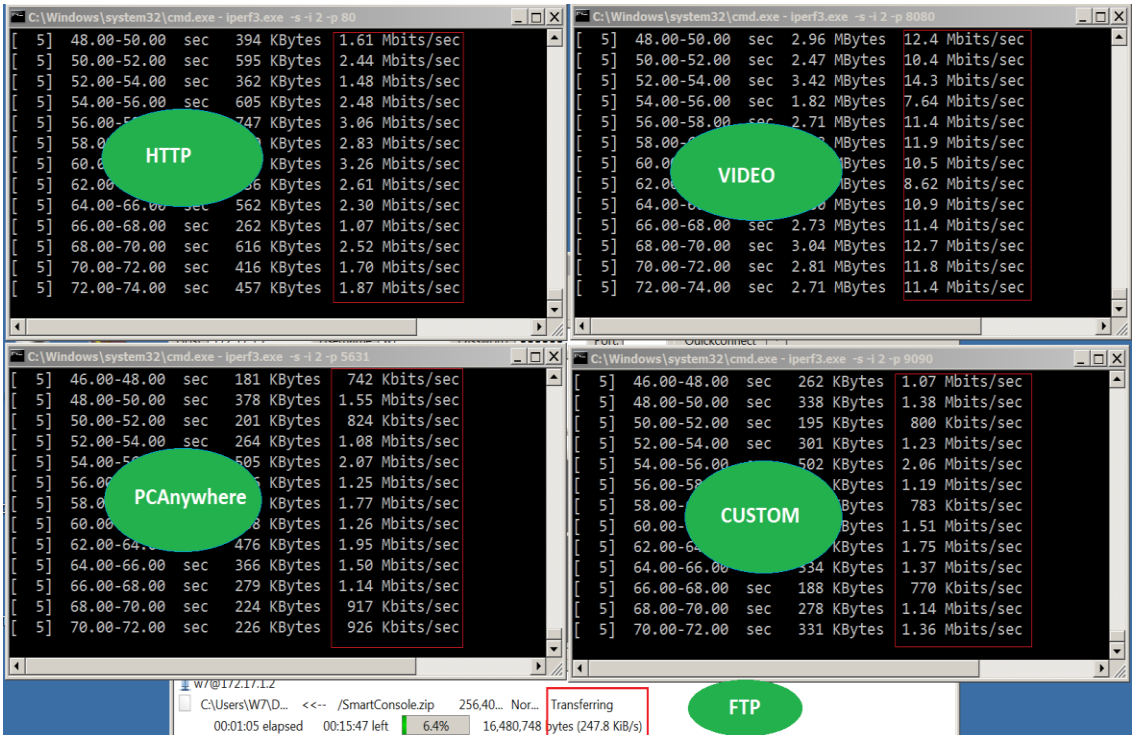
b) Sau khi thực hiện QoS

Sau khi thực hiện QoS, đường truyền sẽ được ưu tiên cho những loại lưu lượng chúng ta thiết lập, vì vậy tại Client chúng ta sẽ thấy chất lượng Video sắc nét gần như không còn hiện tượng giật hình nữa như hình 5-6:

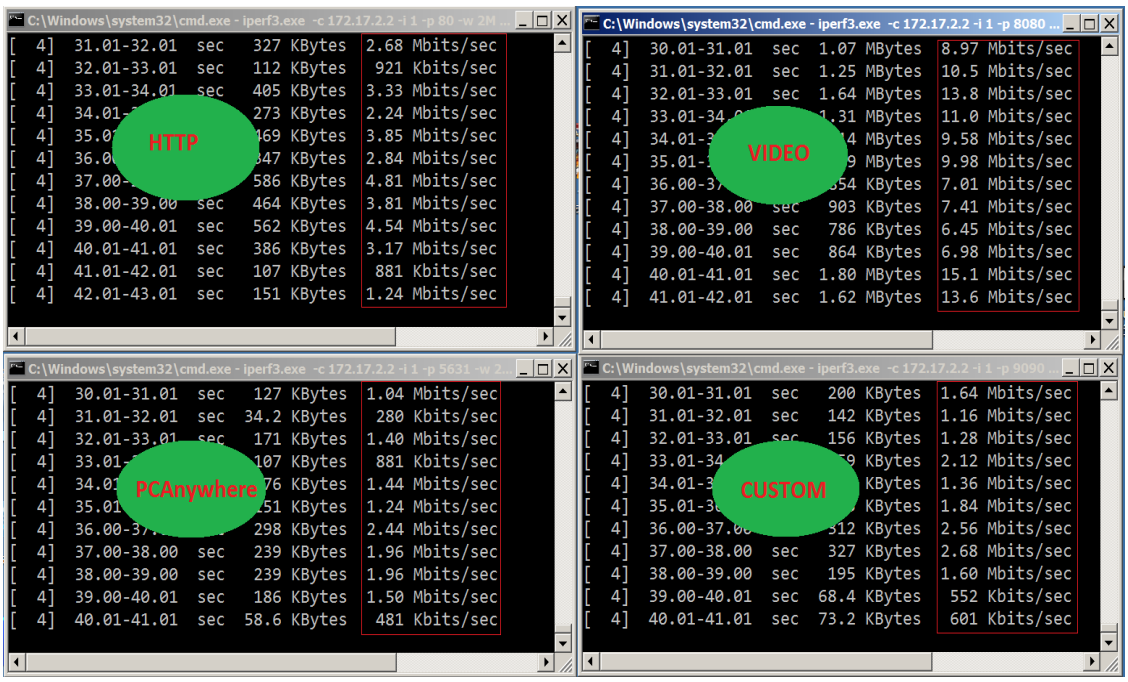


Hình 5 - 6 Tín hiệu thu được phía Client sau khi áp dụng QoS

Tiếp tục kiểm tra băng thông từng loại dữ liệu phát từ Server thu được bên phía Client (Hình 5-7 và 5-8) chúng ta thấy như sau: Băng thông của từng loại gói tin FTP, HTTP, PCAnywhere, Video và Ứng dụng port 9090 mà thiết bị cấp phát cho nó phù hợp với các giá trị QoS chúng ta thiết lập:



Hình 5 - 7 Màn hình bên phía Client



Hình 5 - 8 Màn hình bên phía Server

Sử dụng thêm chương trình Netflow Analyzer để xem biểu đồ băng thông chúng ta cũng thấy kết quả với tỉ lệ băng thông phù hợp như hình 5-9 dưới đây:

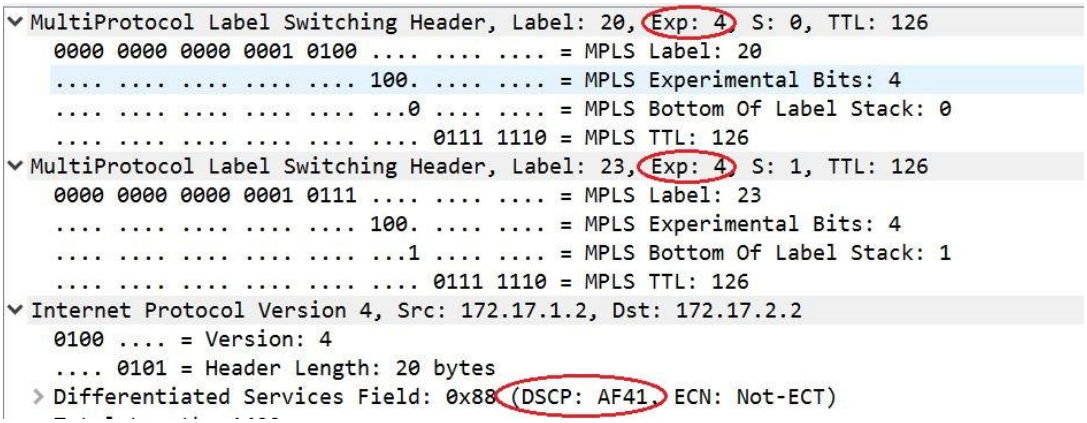
Application	Protocol	Total Traffic	Total Packets	Traffic Percentage
World Wide Web HTTP (80)	TCP	667122.8 K	56795	20%
pcANYWHEREdata (5631)	TCP	312208.4 K	26469	9%
HTTP Alternate (see port 80) (8	TCP	1480354.6	125477	44%
WebSM (9090)	TCP	314498.3 K	26661	9%
49187	TCP	606597.5 K	51102	18%

Hình 5 - 9 Netflow sau QoS

Tiếp tục dùng phần mềm Wireshark bắt các gói tin giữa client và server tiến hành phân tích:

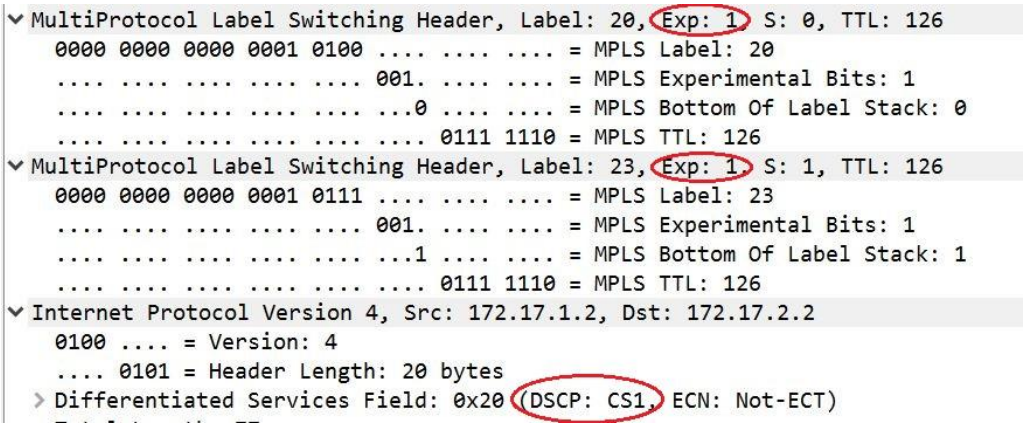
Với gói tin HTTP như hình 5-10 phía dưới:

Chúng ta thấy gói tin HTTP có hai nhãn do đây là MPLS-VPN. Nhãn dưới là nhãn VPN và nhãn trên là nhãn LDP. Gói tin HTTP được gán trường DSCP AF41 và EXP tương ứng là 4 phù hợp thiết kế.



Hình 5 - 10 Phân tích gói tin HTTP

Tiếp tục phân tích gói tin của ứng dụng nội bộ cổng 9090 chúng ta được như hình 5-11



Hình 5 - 11 Phân tích gói tin cổng 9090

Một lần nữa chúng ta thấy gói tin cổng 9090 được gán DSCP CS1 và trường EXP được gán là 1 đúng thiết kế đồng thời gói tin này cũng có hai nhãn VPN và LDP như với gói tin HTTP phía trên.

Tiếp tục phân tích các gói tin khác chúng ta thấy kết quả hoàn toàn phù hợp với lý thuyết.

Lưu ý với trường hợp này chúng ta không tác động cấu hình vào các thiết bị mạng lõi MPLS/VPN nên trường EXP của nhãn được gán theo giá trị DSCP của gói tin. Đây là hành vi mặc định.

5.3.2 Trường hợp 2: Thực hiện QoS trong mạng lõi MPLS VPN

Ở trường hợp này có thể coi khách hàng và nhà cung cấp dịch vụ thỏa thuận thuê một kênh truyền với băng thông giới hạn nhưng khách hàng muốn dữ liệu đi qua mạng lõi phải có sự ưu tiên với các gói tin có yêu cầu chất lượng dịch vụ cao như voice, video…Lúc này nhà cung cấp dịch vụ phải chạy QoS trong mạng của họ. Tùy thuộc vào yêu cầu cụ thể, khách hàng có thể tự thực hiện đánh dấu và nhà cung cấp dịch vụ sẽ tin tưởng dựa vào đó hoặc không tin tưởng đánh dấu lại để thực hiện QoS trong mạng của nhà cung cấp. Thường nhà cung cấp sẽ tạo ra các mẫu cấu hình và khách hàng sẽ phải đánh dấu theo yêu cầu của nhà cung cấp dịch vụ.

5.3.2.1 Cấu hình mô phỏng

Thực hiện cấu hình mô phỏng tương tự như trường hợp 1 tuy nhiên để phục vụ mục đích mô phỏng, chính sách trong mạng nhà cung cấp dịch vụ sẽ như sau: đảm bảo lưu lượng ftp có băng thông tối đa 1Mbps tuy nhiên khi lưu lượng vượt quá cũng sẽ không hủy bỏ ngay mà sẽ bị đánh dấu lại với EXP là 6 và lưu lượng vượt quá này sẽ bị hủy bỏ nếu tốc độ vượt 1 Mbps. Chính sách này thể hiện ở bảng sau:

Lớp lưu lượng	Cổng	DSCP	Băng thông
video	8080	EF (EXP 5)	12 Mbps
http	80	AF41 (EXP 4)	2 Mbps
pcanywhere	5631	CS3 (EXP 3)	1 Mbps
ftp	21	CS2 (EXP 2)	1 Mbps
ftp-exceed	21	EXP 6 (EXP 2 -> 6)	<= 1Mbps
custom	9090	CS1 (EXP 1)	1 Mbps

5.3.2.2 Kết quả mô phỏng

Thực hiện truyền tương tự như trường hợp 1 và xem băng thông ftp được gán lại bởi nhà cung cấp dịch vụ thế nào. Kiểm tra chính sách áp dụng trên router lối ra PE-2 ta được kết quả như sau:

```
show policy-map interface e0/1
 Ethernet0/1

  Service-policy output: CustA-out

    queue stats for all priority classes:
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 94793/141486531

    Class-map: video-out (match-all)
      94793 packets, 141486531 bytes
      30 second offered rate 10878000 bps, drop rate 0000 bps
      Match: qos-group 5
      Priority: 12000 kbps, burst bytes 300000, b/w exceed drops: 0


    Class-map: http-out (match-all)
      28908 packets, 42900793 bytes
      30 second offered rate 2937000 bps, drop rate 0000 bps
      Match: qos-group 4
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 28908/42900793
      bandwidth 2000 kbps

    Class-map: pcanywhere-out (match-all)
      15597 packets, 23164738 bytes
      30 second offered rate 1401000 bps, drop rate 0000 bps
      Match: qos-group 3
      Queueing
      queue limit 64 packets
```

```
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 15597/23164738
    bandwidth 1000 kbps

  Class-map: ftp-out (match-all)
    7788 packets, 11630133 bytes
    30 second offered rate 955000 bps, drop rate 0000 bps
    Match: qos-group 2
    Queueing
    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 7788/11630133
    bandwidth 1000 kbps
    police:
        cir 1000000 bps, bc 125000 bytes, be 125000 bytes
      conformed 7788 packets, 11630133 bytes; actions:
        transmit
      exceeded 0 packets, 0 bytes; actions:
        drop
      violated 0 packets, 0 bytes; actions:
        drop
      conformed 955000 bps, exceeded 0000 bps, violated 0000 bps

  Class-map: custom-out (match-all)
    14842 packets, 22103170 bytes
    30 second offered rate 1547000 bps, drop rate 0000 bps
    Match: qos-group 1
    Queueing
    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 14842/22103170
    bandwidth 1000 kbps

  Class-map: ftp-exceed-out (match-all)
    6398 packets, 9617214 bytes
    30 second offered rate 779000 bps, drop rate 0000 bps
    Match: qos-group 6
    police:
        cir 1000000 bps, bc 125000 bytes, be 125000 bytes
      conformed 6398 packets, 9617214 bytes; actions:
        transmit
      exceeded 0 packets, 0 bytes; actions:
        drop
      violated 0 packets, 0 bytes; actions:
        drop
      conformed 779000 bps, exceeded 0000 bps, violated 0000 bps
```

Đặc biệt lưu ý hai lớp lưu lượng: ftp-out và ftp-exceed-out, chúng ta thấy nếu truyền tương tự như trường hợp 1 thì lưu lượng FTP sẽ bị chia sẻ thành hai luồng khác nhau với băng thông mỗi loại gần 1Mbps phù hợp với mong muốn.

5.4 Kết luận chương

Kết quả thu được cho chúng ta một cái nhìn về khái niệm chất lượng dịch vụ trong thực tế, cũng như ảnh hưởng và tác dụng của nó. Nếu các luồng được truyền đồng thời thì sẽ bị ảnh hưởng lẫn nhau và làm giảm hiệu năng của tất cả các ứng dụng sử dụng

các luồng đó. Chỉ sau khi áp dụng QoS cho mạng và cụ thể là với mạng MPLS thì các luồng khác nhau tùy độ ưu tiên sẽ nhận được các mức độ ưu tiên cũng như băng thông khác nhau. Như vậy chỉ cần một lượng băng thông cố định thì khi áp dụng QoS sẽ làm cho hiệu năng của mạng tăng lên rất nhiều với giá thành không đổi.

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Ngày nay các ứng dụng Internet được sử dụng rộng rãi ở mọi lĩnh vực và ở khắp nơi trên thế giới. Điều đó kéo theo nhu cầu truyền thông tin một cách an toàn, hiệu quả. Một trong những ứng dụng quan trọng đó là mạng riêng ảo.

Luận văn ngoài việc giới thiệu các khái niệm chung về mạng riêng ảo, luận văn còn đi sâu phân tích các loại mạng riêng ảo hiện nay, những hạn chế cũng như thế mạnh của từng mô hình để mỗi người đọc rút ra được mô hình thích hợp nhất

Hiện nay có khá nhiều công nghệ mạng mới ra đời nhằm mục đích truyền thông tin một cách an toàn trên Internet và nổi bật nhất chính là MPLS VPN. Luận văn ngoài việc phân tích, nghiên cứu cấu trúc, cách thức hoạt động của mạng MPLS nói chung, còn đi sâu vào nghiên cứu cách thức truyền gói tin trong mạng MPLS VPN từ địa chỉ nguồn đến địa chỉ đích ở các khu vực khác nhau một cách an toàn.

Sau khi truyền được thông tin qua mạng VPN trên nền tảng MPLS một vấn đề đặt ra là phải đảm bảo chất lượng dịch vụ cho các dữ liệu truyền qua nó. Luận văn cũng đã trình bày một cách rõ ràng về các cơ chế QoS cho mạng IP và cách thức thực thi nó trên mạng MPLS VPN như thế nào. Đồng thời luận văn cũng đã phân tích, thử nghiệm tính năng QoS trên mạng MPLS VPN trong một mô hình mô phỏng với các thiết bị và dữ liệu rất gần với thực tế để người đọc có được cái nhìn trực quan cũng như kiểm nghiệm được tính đúng đắn của lý thuyết.

Hướng nghiên cứu tiếp theo của luận văn là sẽ áp dụng cách thực thi QoS trong môi trường thực tế như các doanh nghiệp lớn cũng như các nhà cung cấp dịch vụ với các thiết bị phức tạp, thuộc nhiều hãng cung cấp và có hiệu năng cao. Tiến tới sẽ tìm cách áp dụng QoS với mô hình có nhiều nhà cung cấp dịch vụ MPLS VPN khác nhau tạo điều kiện cho các khách hàng/doanh nghiệp có được chất lượng dịch vụ cao nhất và giá thành rẻ nhất.

Mặc dù đã cố gắng hết sức nhưng do thời gian có hạn nên luận văn chắc chắn sẽ không tránh khỏi những hạn chế và thiếu sót nhất định. Ngữ cảnh mô phỏng trong luận văn vẫn còn hạn chế, chưa đánh giá được rõ hơn các ứng dụng nghiệp vụ, đa phương tiện trong thực tế. Em mong sẽ nhận được các ý kiến của các thầy cô trong hội đồng để luận văn có thể hoàn thiện hơn.

TÀI LIỆU THAM KHẢO

Tiếng Việt

1. Nguyễn Đình Việt (2008), *Bài giảng Mạng và Truyền số liệu nâng cao*, Hà Nội.
2. Nguyễn Đình Việt (2008), *Bài giảng đánh giá hiệu năng mạng máy tính*, Hà Nội.
3. Nguyễn Tiến Ban (2011), *Công nghệ IP/MPLS và các mạng riêng ảo*, Nhà xuất bản Thông Tin và Truyền Thông
4. Nguyễn Văn Linh (2015), *Giáo trình mạng máy tính*, Đại học Thái Nguyên
5. Phạm Thế Quế (2006), *Giáo trình mạng máy tính*, Học viện công nghệ bưu chính viễn thông
6. Trần Công Hùng (2009), *Chuyển mạch nhãn đa giao thức MPLS*, Nhà xuất bản Thông Tin và Truyền Thông.
7. Trung Tâm Đào Tạo Bưu Chính Viễn Thông (2007), *Giáo trình bồi dưỡng kỹ sư điện tử viễn thông về công nghệ IP và NGN*, Học viện công nghệ bưu chính viễn thông

Tiếng Anh

8. Ivan Pepelnjak, Jim Guichard (2001), *MPLS and VPN Architecture*, Cisco press 201 West 103rd Street Indianapo
9. Cisco Systems Learning (2006), *Implementing Cisco Quality of Service*, Cisco Systems
10. Cisco Systems Learning (2006), *Implementing Cisco MPLS*, Cisco Systems
11. https://vi.wikipedia.org/
12. Luc De Ghein (2007), *MPLS Fundamentals*, Cisco Press 800 East 96th Street Indianapolis.
13. Tim Szigeti, Christina Hattingh, Robert Barton, Kenneth R. Briley, Jr (2014), *End-to-End QoS Network Design Second Edition*, Cisco Press
14. Vivek Alwayn (2001), *Advanced MPLS design and Implementation*, Cisco press
    201 west 103rd Street Indianapolis