BỘ GIÁO DỤC VÀ ĐÀO TẠO

**TRƯỜNG ĐẠI HỌC NHA TRANG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO CHUYÊN ĐỀ TỐT NGHIỆP**

**TÌM HIỂU VÀ TRIỂN KHAI MẠNG CAMPUS CHO TRƯỜNG HỌC**

**Giảng viên hướng dẫn : THS.Mai Cường Thọ**

**Sinh viên thực hiện : Đinh Hữu Hoàng**

**Lớp : 57CNTT-1**

**Mã số sinh viên : 57132344**

Khánh Hòa - 2019

TRƯỜNG ĐẠI HỌC NHA TRANG

**KHOA CÔNG NGHỆ THÔNG TIN**

**BỘ MÔN MẠNG VÀ TRUYỀN THÔNG**



**BÁO CÁO CHUYÊN ĐỀ TỐT NGHIỆP**

**TÌM HIỂU VÀ TRIỂN KHAI MẠNG CAMPUS CHO TRƯỜNG HỌC**

GVHD: THS.Mai Cường Thọ

SVTH: Đinh Hữu Hoàng

Lớp: 57CNTT-1

MSSV: 57132344

Khánh Hòa, Tháng 5 - 2019

MỤC LỤC

[MỤC LỤC](#_Toc7818610)

[DANH MỤC HÌNH ẢNH](#_Toc7818611)

[THUẬT NGỮ VIỆT TẮT](#_Toc7818612)

[LỜI CẢM ƠN](#_Toc7818613)

[MỞ ĐẦU](#_Toc7818614)

[CHƯƠNG I KIẾN TRÚC MẠNG CAMPUS 1](#_Toc7818615)

[1.1. Giới thiệu mạng Campus: 1](#_Toc7818616)

[1.2. Mạng Campus truyền thống: 2](#_Toc7818617)

[1.2.1. Vấn đề khả năng hoạt động của mạng và giải pháp: 2](#_Toc7818618)

[1.2.2. Luật 80/20: 4](#_Toc7818619)

[1.3. Các mô hình mạng Campus: 6](#_Toc7818620)

[1.3.1. Mô hình mạng chia sẻ: 6](#_Toc7818621)

[1.3.2. Mô hình phân đoạn LAN: 7](#_Toc7818622)

[1.3.3. Mô hình lưu lượng mạng: 8](#_Toc7818623)

[1.3.4. Mô hình mạng dự đoán trước: 10](#_Toc7818624)

[1.4. Mô hình mạng 3 lớp của Cisco: 11](#_Toc7818625)

[1.5. Lớp truy cập (Access): 11](#_Toc7818626)

[Lớp phân phối (Distribution): 12](#_Toc7818627)

[Lớp lõi (Core): 12](#_Toc7818628)

[1.6. Mô hình Modular trong thiết kế mạng Campus: 12](#_Toc7818629)

[1.6.1. Khối Switch: 13](#_Toc7818630)

[1.6.2. Khối Core: 16](#_Toc7818631)

[1.6.3. Các khối Building khác: 21](#_Toc7818632)

[CHƯƠNG II VLAN, TRUNK VÀ VTP (VLAN TRUNKING PROTOCOL) 24](#_Toc7818633)

[2.1. Mạng LAN ảo: 24](#_Toc7818634)

[2.1.1. Các kiểu thành viên của VLAN (VLAN Membership): 25](#_Toc7818635)

[2.1.2. Triển khai VLAN: 26](#_Toc7818636)

[2.1.2.1. Tạo mạng LAN ảo với một bộ chuyển mạch: 28](#_Toc7818637)

[2.1.2.2. Tạo mạng LAN ảo với nhiều bộ chuyển mạch: 28](#_Toc7818638)

[2.1.2.3. Cách xây dựng mạng LAN ảo: 29](#_Toc7818639)

[2.1.2.3. Ưu và nhược điểm của mạng LAN ảo: 30](#_Toc7818640)

[2.2. VLAN Trunk: 30](#_Toc7818641)

[2.2.1. Sự ra đời của thuật ngữ Trunking: 30](#_Toc7818642)

[2.2.2. Khái niệm Trunking: 31](#_Toc7818643)

[2.2.3. Hoạt động của Trunking: 31](#_Toc7818644)

[2.2.4. Các chuẩn trunking trong một hệ thống mạng: 32](#_Toc7818645)

[2.2.5. Chuẩn IEEE và kỹ thuật trunking DOT1Q: 32](#_Toc7818646)

[2.2.6. Native VLAN trong kỹ thuật Trunking: 34](#_Toc7818647)

[2.2.7. Chuẩn Cisco và kỹ thuật trunking ISL: 34](#_Toc7818648)

[2.3. VLAN Trunking Protocol – Giao thức mạch nối VLAN – VTP: 36](#_Toc7818649)

[2.3.1. Nguồn gốc VTP: 36](#_Toc7818650)

[2.3.2. Khái niệm VTP: 36](#_Toc7818651)

[2.3.3. Các chế độ VTP: 37](#_Toc7818652)

[2.3.4. Lợi ích của VTP: 41](#_Toc7818653)

[CHƯƠNG III SPANNING TREE PROTOCOL – STP 42](#_Toc7818654)

[3.1. Spanning Tree là gì và tại sao phải sử dụng nó: 42](#_Toc7818655)

[3.2. Hai khái niệm cơ bản của STP: 46](#_Toc7818656)

[3.3. Các bước ra quyết định của STP: 48](#_Toc7818657)

[3.4. Sự hội tụ của STP ban đầu (Initial STP Convergence): 49](#_Toc7818658)

[3.5. Các trạng thái của STP: 56](#_Toc7818659)

[3.6. Bộ định thời gian STP: 59](#_Toc7818660)

[3.7. Hai loại BPDU: 61](#_Toc7818661)

[3.8. Quá trình thay đổi cấu trúc mạng: 63](#_Toc7818662)

[CHƯƠNG IV CHUYỂN MẠCH NHÃN ĐA GIAO THỨC – MPLS. 67](#_Toc7818663)

[4.1. Tổng quan: 67](#_Toc7818664)

[4.1.1. Định tuyến và chuyển mạch gói truyền thống: 67](#_Toc7818665)

[4.1.2. MPLS là gì? 68](#_Toc7818666)

[4.1.3. Chức năng của MPLS: 69](#_Toc7818667)

[4.1.4. Lợi ích của MPLS: 69](#_Toc7818668)

[4.2. Các khái niệm cơ bản: 69](#_Toc7818669)

[4.2.1. LERs và LSRs. 69](#_Toc7818670)

[4.2.2. Lớp chuyển tiếp tương đương – FEC: 70](#_Toc7818671)

[4.2.3. Nhãn: 71](#_Toc7818672)

[4.2.4. Kỹ thuật điều khiển lưu lượng: 76](#_Toc7818673)

[4.3. Các bảng tra FIB và LFIB: 76](#_Toc7818674)

[4.4. Control plane (mặt phẳng điều khiển): 77](#_Toc7818675)

[4.5. Data plane (mặt phẳng dữ liệu): 78](#_Toc7818676)

[4.6. Giao thức phân phối nhãn – LDP: 79](#_Toc7818677)

[4.7. Các chế độ hoạt động của MPLS: 83](#_Toc7818678)

[4.7.1. Chế độ khung (frame-mode): 83](#_Toc7818679)

[4.7.2. Chế độ hoạt động tế bào MPLS: 85](#_Toc7818680)

[4.8. Các ứng dụng cảu MPLS: 87](#_Toc7818681)

[CHƯƠNG V THIẾT KẾ MẠNG CHO TRƯỜNG HỌC. 88](#_Toc7818682)

[5.1. Tóm tắt mục tiêu hệ thống: 88](#_Toc7818683)

[5.2. Hệ thống triển khai: 88](#_Toc7818684)

[5.2.1. Sơ đồ mạng tổng thể triển khai cho trường học: 88](#_Toc7818685)

[5.2.2. Triển khai hệ thống mạng nội bộ: 89](#_Toc7818686)

[5.3. Vấn đề an ninh hệ thống: 91](#_Toc7818687)

[5.3.1. Tường lửa: 91](#_Toc7818688)

[5.3.2. Ngăn ngừa xâm nhập: 91](#_Toc7818689)

[5.3.3. Phòng chống virut: 91](#_Toc7818690)

[KẾT LUẬN 92](#_Toc7818691)

[DANH MỤC TÀI LIỆU THAM KHẢO 93](#_Toc7818692)

DANH MỤC HÌNH ẢNH

[Hình 1.1: Một ví dụ về internetwork. 1](#_Toc7817899)

[Hình 1.2: Mạng 80/20 truyền thống. 4](#_Toc7817900)

[Hình 1.3 Biểu diễn mạng 20/80 mới. 5](#_Toc7817901)

[Hình 1.4 Tạo VLAN trong mạng. 6](#_Toc7817902)

[Hình 1.5 Biểu diễn phân đoạn mạng bằng bộ định tuyến. 8](#_Toc7817903)

[Hình 1.6: Mô hình mạng 3 lớp của Cisco. 11](#_Toc7817904)

[Hình 1.7: Biểu diễn một Modular thiết kế Campus. 13](#_Toc7817905)

[Hình 1.8: Biểu diễn khối Switch, ở lớp 3 có hai switch dự phòng dùng cho việc cân bằng tải. 16](#_Toc7817906)

[Hình 1.9: Biểu diễn khối Collapsed. 17](#_Toc7817907)

[Hình 1.10: Minh họa khối Dual Core. 19](#_Toc7817908)

[Hình 1.11: Biểu diễn mạng nhỏ với hai khối Switch chứa hai switch chuyển mạch lớp 3 (xử lý định tuyến bên trong switch của lớp Distribution). 20](#_Toc7817909)

[Hình 2.1: Vlan theo chức năng các phòng ban. 24](#_Toc7817910)

[Hình 2.2: Biểu diễn Dynamic VLAN với bảng địa chỉ MAC. 26](#_Toc7817911)

[Hình 2.3: Cấu hình bộ chuyển mạch tạo thành các miền quảng bá cho VLAN. 28](#_Toc7817912)

[Hình 2.4: Đường trunk kết nối giữa các switch. 31](#_Toc7817913)

[Hình 2.5: Kỹ thuật trunking 802.1Q. 32](#_Toc7817914)

[Hình 2.6: Cách thức xử lý Frame. 34](#_Toc7817915)

[Hình 2.7: Kỹ thuật trunking ISL. 34](#_Toc7817916)

[Hình 2.8: VTP domain. 37](#_Toc7817917)

[Hình 2.9: VTP modes. 38](#_Toc7817918)

[Hình 2.10: VTP Prunning. 39](#_Toc7817919)

[Hình 3.1: Bridging loop trong mạng. 42](#_Toc7817920)

[Hình 3.2: Không có STP, broadcast tạo feedback loop. 43](#_Toc7817921)

[Hình 3.3: Mô tả định dạng của một DIXv2 Ethernet frame. 44](#_Toc7817922)

[Hình 3.4: frame unicast cũng có thể gây ra Bridging Loop và sai lệch bảng bridge. 46](#_Toc7817923)

[Hình 3.5: Hai trường của BID. 46](#_Toc7817924)

[Hình 3.6: Mô hình mạng sử dụng STP. 49](#_Toc7817925)

[Hình 3.7: Chọn Bridge Root. 50](#_Toc7817926)

[Hình 3.8: Các thành phần cơ bản của BPDU. 51](#_Toc7817927)

[Hình 3.9: Chọn Root Port. 53](#_Toc7817928)

[Hình 3.10: Chọn Designated Port. 54](#_Toc7817929)

[Hình 3.11: Trạng thái các cổng và hoạt động chuyển trạng thái. 58](#_Toc7817930)

[Hình 3.12: Sơ đồ mạng với các cổng được định danh. 58](#_Toc7817931)

[Hình 3.13: Lỗi xảy ra trên liên kết giữa Root bridge và Root port của Cat-C. 60](#_Toc7817932)

[Hình 3.14: TCN BPDU được dùng để cập nhật bảng bridge nhanh hơn. 63](#_Toc7817933)

[Hình 3.15: Trình tự các bước trong quá trình thay đổi cấu trúc mạng. 64](#_Toc7817934)

[Hình 3.16: Trường cờ trong BPDU cấu hình. 66](#_Toc7817935)

[Hình 4.1: Vị trí LSR và LER trong mạng MPLS. 70](#_Toc7817936)

[Hình 4.2: Định dạng chung của nhãn. 71](#_Toc7817937)

[Hình 4.3: Chồng nhãn. 72](#_Toc7817938)

[Hình 4.4: Cách đóng gói tin. 73](#_Toc7817939)

[Hình 4.5: Nhãn lớp 2. 73](#_Toc7817940)

[Hình 4.6: Bảng tra FIB và LFIB. 77](#_Toc7817941)

[Hình 4.7: Giao thức LDP với các giao thức khác. 80](#_Toc7817942)

[Hình 4.8: Thủ tục phát hiện LSR lân cận. 81](#_Toc7817943)

[Hình 4.9: Vị trí nhãn trong khung lớp 2. 84](#_Toc7817944)

[Hình 4.10: Định dạng của ATM – cell. 86](#_Toc7817945)

[Hình 4.11: Đường hầm trong MPLS. 86](#_Toc7817946)

THUẬT NGỮ VIỆT TẮT

|  |  |  |
| --- | --- | --- |
| **Viết tắt** | **Tiếng Anh** | **Tiếng Việt** |
| ATM | Asynchronous Transfer Mode | Chế độ chuyển mạch không đồng bộ |
| CE | Customer Edge | Phía khách hàng |
| CoS | Class of Service | Lớp dịch vụ |
| DoS | Data over SDH | Dữ liệu trên SDH |
| DSLAM | Digital subscriber line | Đường thuê bao số |
| E-LAN | Ethernet LAN Service | Dịch vụ LAN ethernet |
| ELS | Ethernet Line Service | Dịch vụ đường kết nối Ethernet |
| EoS | Ethernet over SDH | Ethernet trên SDH |
| ERS | Ethernet Relay Service | Dịch vụ chuyển tiếp Ethernet |
| GE | Gigabit Ethernet | Gigabit Ethernet |
| GFR | Generic Framing Procedure | Thủ tục đóng khung tổng quát |
| GMPLS | Generalized Multiprotocol Label Switching | Chuyển mạch nhãn đa giao thức tổng quát |
| IETF | Internet Engineering Task Force | Tổ chức đặc nhiệm kỹ thuật Internet |
| IP | Internet Protocol | Giao thức internet |
| ISP | Internet Service Provider | Nhà cung cấp dịch vụ internet |
| ITU-T | International Telecommunications Union (Telecommunications Standardisation Sector) | Hiệp hội viễn thông quốc tế |
| LAN | Local area network | Mạng nội bộ |
| LSP | Label-Switched Path | Đường chuyền mạch nhãn |
| MAC | Medium Access Control | Điều khiển truy nhập môi trường |
| MAN | Metro Area Network | Mạng vùng đô thị |
| MPLS | Multiprotocol Label Switching | Chuyển mạch nhãn đa giao thức |
| NGN | Next Generation network | Mạng thế hệ sau |
| OTN | Optical Transport Network | Mạng truyền tải quang |
| OAM | Object access method | Phương pháp truy cập đối tượng |
| PDH | Plesiochronous Digital Hierarchy | Phân cấp số cận đồng hồ |
| PPP | Point to Point Protocol | Giao thức điểm tới điểm |
| PSTN | Public Switched Telephone Network | Mạng điện thoại công cộng |
| QoS | Quality of Service | Chất lượng dịch vụ |
| RSVP | Resource Reservation Protocol | Giao thức dành trước tài nguyên |
| RPR | Resilient Packet Ring | Vòng ring gói phục hồi nhanh |
| SDH | Synchronous Digital Hierarchy | Hệ thống phân cấp số đồng bộ |
| SLA | Service Level Agreement | Thỏa thuận mức dịch vụ |
| SONET | Synchronous Optical Network | Mạng quang đồng bộ |
| STM-n | Synchronous Transport Module level N | Mô đun truyền tải đồng bộ mức n |
| TCP | Transmission Control Protocol | Giao thức điều khiển truyền tải |
| TDM | Time division multiplexing | Ghép kênh theo thời gian |
| UNI | User-to-Network Interface | Giao diện kết nối người dùng – mạng |
| VCC | Virtual Channel Connection | Kênh kết nối ảo |
| VPN | Virtual Private Network | Mạng riêng ảo |
| VLAN | Virtual LAN | LAN ảo |
| WAN | Wide area network | Mạng diện rộng |
| WDM | Wavelength Division Multiplex | Ghép kênh theo bước sóng |

LỜI CẢM ƠN

Em xin gửi lời cảm ơn chân thành và sự tri ân sâu sắc đối với các thầy cô của trường Đại học Nha Trang, đặc biệt là các thầy cô khoa Công nghệ thông tin của trường đã tạo điều kiện cho em có thời gian thực tập ở doanh nghiệp IT Solutions Consulting, giúp em tiếp cận được với hệ thống mạng thực tế và có nhiều tư liệu để làm báo cáo chuyên đề tốt nghiệp. Và em cũng xin chân thành cám ơn thầy Mai Cường Thọ đã nhiệt tình hướng dẫn hướng dẫn em hoàn thành bài báo cáo tốt nghiệp. Trong quá trình thực tập, cũng như là trong quá trình làm bài báo cáo tốt nghiệp, khó tránh khỏi sai sót, rất mong các thầy, cô bỏ qua. Đồng thời do trình độ lý luận cũng như kinh nghiệm thực tiễn còn hạn chế nên bài báo cáo không thể tránh khỏi những thiếu sót, em rất mong nhận được ý kiến đóng góp thầy, cô để em học thêm được nhiều kinh nghiệm tích lũy cho bản thân.

Em xin chân thành cảm ơn!

MỞ ĐẦU

Ngày nay với một lượng lớn về thông tin, nhu cầu xử lý thông tin ngày càng cao. Mạng máy tính hiện nay trở nên quá quen thuộc đối với chúng ta, trong mọi lĩnh vực như khoa học, quân sự, quốc phòng, thương mại, dịch vụ, giáo dục... Hiện nay ở nhiều nơi mạng đã trở thành một nhu cầu không thể thiếu được. Người ta thấy được việc kết nối các máy tính thành mạng cho chúng ta những khả năng mới to lớn như:

* Sử dụng chung tài nguyên: Những tài nguyên của mạng (như thiết bị, chương trình, dữ liệu) khi được trở thành các tài nguyên chung thì mọi thành viên của mạng đều có thể tiếp cận được mà không quan tâm tới những tài nguyên đó ở đâu.
* Tăng độ tin cậy của hệ thống: Người ta có thể dễ dàng bảo trì máy móc và lưu trữ (backup) các dữ liệu chung và khi có trục trặc trong hệ thống thì chúng có thể được khôi phục nhanh chóng. Trong trường hợp có trục trặc trên một trạm làm việc thì người ta cũng có thể sử dụng những trạm khác thay thế.
* Nâng cao chất lượng và hiệu quả khai thác thông tin: Khi thông tin có thể được sử dụng chung thì nó mang lại cho người sử dụng khả năng tổ chức lại các công việc với những thay đổi về chất như:
* Ðáp ứng những nhu cầu của hệ thống ứng dụng kinh doanh hiện đại.
* Cung cấp sự thống nhất giữa các dữ liệu.
* Tăng cường năng lực xử lý nhờ kết hợp các bộ phận phân tán.
* Tăng cường truy nhập tới các dịch vụ mạng khác nhau đang được cung cấp trên thế giới.

Với nhu cầu đòi hỏi ngày càng cao của xã hội nên vấn đề kỹ thuật trong mạng là mối quan tâm hàng đầu của các nhà tin học. Ví dụ như làm thế nào để truy xuất thông tin một cách nhanh chóng và tối ưu nhất, trong khi việc xử lý thông tin trên mạng quá nhiều đôi khi có thể làm tắc nghẽn trên mạng và gây ra mất thông tin một cách đáng tiếc.

Hiện nay việc làm thế nào để thiết kế một hệ thống mạng tốt, an toàn với lợi ích kinh tế cao đang rất được quan tâm. Một vấn đề đặt ra có rất nhiều giải pháp về công nghệ, một giải pháp có rất nhiều yếu tố cấu thành, trong mỗi yếu tố có nhiều cách lựa chọn. Như vậy để đưa ra một giải pháp hoàn chỉnh, phù hợp thì phải trải qua một quá trình chọn lọc dựa trên những ưu điểm của từng yếu tố, từng chi tiết rất nhỏ.

Ðể giải quyết những vấn đề trên, chuyên đề này trình bày cách thiết kế mạng Campus theo công nghệ của Cico và sau đó áp dụng lý thuyết vào thực tiễn thiết kế mạng campus cho trường học. Cấu trúc của chuyên đề tổ chức như sau:

Chương 1: KIẾN TRÚC MẠNG CAMPUS.

Chương 2: VLAN, TRUNK, VÀ VTP.

Chương 3: SPANNING TREE PROTOCOL - STP.

Chương 4: CHUYỂN MẠCH NHÃN ĐA GIAO THỨC – MPLS.

Chương 5: THIẾT KẾ MẠNG CHO TRƯỜNG HỌC.

CHƯƠNG I   
KIẾN TRÚC MẠNG CAMPUS

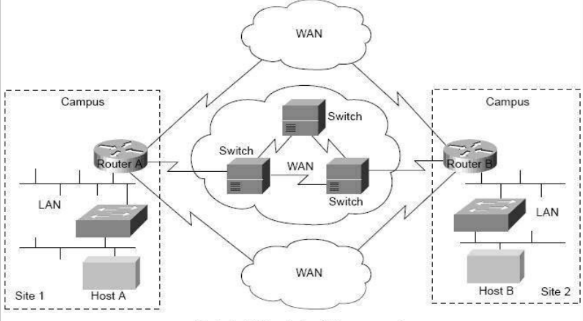
* 1. Giới thiệu mạng Campus:

Internet đã thay đổi cuộc sống chúng ta, với sự gia tăng số lượng của các dịch vụ giao dịch trực tuyến, giáo dục, và giải trí,… điều này thúc đẩy chúng ta tìm ra nhiều phương pháp để truyền thông với nhau.

Liên mạng (internetworing) là sự truyền thông giữa một hay nhiều mạng, gồm có nhiều máy tính kết nối lại với nhau. Liên mạng máy tính ngày càng lớn mạnh để hỗ trợ cho các nhu cầu truyền thông khác nhau của hệ thống đầu cuối. Một liên mạng đòi hỏi nhiều giao thức và tính năng để cho phép sự mở rộng. Các liên mạng lớn gồm có 3 thành phần như sau:

* Mạng Campus: gồm có các user kết nối cục bộ trong một hay một nhóm các tòa nhà.
* Mạng WAN: kết nối các mạng Campus lại với nhau.
* Kết nối từ xa: liên kết các nhánh và các user đơn lẻ tới mạng Campus hay Internet.

Hình 1.1: Một ví dụ về internetwork.



Thiết kế một liên mạng là một công việc thử thách năng lực đối với người thiết kế. Để thiết kế một liên mạng có độ tin cậy và có tính mở rộng, thì người thiết kế phải hiểu rõ về ba thành phần quan trọng của một liên mạng với những đòi hỏi thiết kế khác nhau.

* 1. Mạng Campus truyền thống:

Trong các năm 1990, mạng Campus truyền thống bắt đầu là một mạng LAN và lớn dần. Tuy nhiên, các LAN không thể lớn dần mãi mãi, mà đến một độ lớn nào đó, chúng ta cần phải cần phân đoạn mạng (chia mạng thành các khu vực hay miền cho dễ quản lý) để duy trì khả năng hoạt động của mạng sao cho: thời gian đáp ứng (trả lời) cần được đảm bảo với các chức năng của mạng. Thêm nữa, phần lớn các ứng dụng phải được lưu trữ và chuyển tiếp có một điều cần thiết nữa là chất lượng các dịch vụ tùy.

* + 1. Vấn đề khả năng hoạt động của mạng và giải pháp:

Tính sẵn sàng và khả năng hoạt động là hai vấn đề chính đối với mạng Campus truyền thống. Tính sẵn sàng bị ảnh hưởng bởi số lượng user cố gắng truy cập mạng ở cùng một thời điểm, cộng với độ tin cậy của chính mạng đó. Khả năng hoạt động trong mạng Campus truyền thống báo gồm các vấn đề như: đụng độ, băng thông, broadcast, multicast.

Đụng độ (Collision)

Đụng độ là: hiện tượng các tín hiệu phát từ hai máy gây nhiễu lẫn nhau. Hai tín hiệu gây nhiễu lẫn nhau còn gọi là xung đột.

Miền đụng độ(Collision Domain): đây là một vùng có khả năng bị đụng độ do hai hay nhiều máy tính cùng gởi tín hiệu lên môi trường truyền thông.

Miền quảng bá (Broadcast Domain): đây là một vùng mà gói tin phát tán hay quảng bá (gói tin broadcast) có thể đi qua được. Trong miền quảng bá có thể bao gồm nhiều miền đụng độ.

Một mạng Campus truyền thống có miền đụng độ lớn, vì vậy tất cả các dịch vụ có thể thấy và đụng độ với nhau. Nếu một host thực hiện broadcast, thì tất cả các thiết bị khác đều nghe, thậm chí chính nó cũng cố gắng truyền. Và nếu một thiết bị gặp sự cố do việc truyền liên tục, thì nó có thể làm down toàn bộ mạng.

Cuối 1980, công nghệ bridge (cầu) được dùng để giảm miền đụng độ. Tuy miền đụng độ nhỏ hơn nhưng mạng vẫn có miền broadcast lớn và các vấn đề về miền broadcast vẫn còn tồn tại. Bridge cũng giải quyết được vấn đề giới hạn về khoảng cách, bởi vì nó có chức năng repeater nên mở rộng được các đoạn mạng vật lý.

Băng thông (Bandwidth)

Băng thông của một đoạn mạng được đo bằng số lượng dữ liệu được truyền tại bất kỳ thời điểm nào. Băng thông tương tự như ống nước, mà lượng nước chảy trong ống phụ thuộc vào hai yếu tố sau:

* Độ rộng.
* Khoảng cách.

Độ rộng là dòng nước và băng thông là kích thước ống. Nếu ta có một ống chỉ có đường kính 1/4 inch, thì ta không lấy được nhiều nước qua nó.

Vấn đề thứ hai là khoảng cách. Ống càng dài, thì càng nhiều nước bị giọt, ta có thể đặt repeater ở giữa ống, nhưng ta cần phải hiểu là tất cả các đường đều có sự tiêu hao tín hiệu.

Giải quyết vấn đề băng thông để duy trì giới hạn khoảng cách và thiết kế mạng với các đoạn mạng thích hợp chứa switch (bộ chuyển mạch) và router (bộ định tuyến). Sự tắc nghẽn xảy ra trên các đoạn mạng khi có quá nhiều thiết bị cố gắng sử dụng cùng một băng thông. Sự phân đoạn mạng hợp lý cũng không loại bỏ được vấn đề về băng thông, không bao giờ có đủ băng thông cho tất cả user, đó là sự thật mà ta phải chấp nhận, nhưng ta vẫn có thể làm cho nó tốt hơn.

Broadcast và multicast

Các giao thức gây ra vấn đề broadcast như IP, ARP, NetBIOS, IPX, SAP, và IP. Tính năng này cũng có trong hệ điều hành của bộ định tuyến Cisco, tuy nhiên nếu việc thiết kế và thực thi đúng cách có thể làm giảm bớt vấn đề broadcast này. Việc lọc gói, đưa vào hàng đợi và chọn giao thức định tuyến hợp lý là một ví dụ cho thấy làm thế nào bộ định tuyến cisco có thể làm giảm bớt vấn đề broadcast.

Multicast cũng gây nên vấn đề nếu cấu hình không đúng cách. Multicast là broadcast nhưng được định trước đối với một nhóm các user. Với nhóm multicast lớn hoặc ứng dụng băng thông chuyên dụng như ứng dụng IPTV của Cisco, thì lưu lượng multicast có thể dùng hầu hết băng thông và tài nguyên.

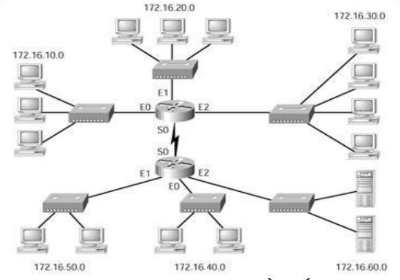
Để giải quyết vấn đề băng thông, ta sẽ phân đoạn mạng sử dụng bridge, router và switch. Tuy giảm được miền broadcast nhưng không loại bỏ được hiện tượng nghẽn cổ chai ở bộ định tuyến. Việc bộ định tuyến xử lý mỗi gói được truyền đi trên mạng sẽ gây nên nghẽn cổ chai nếu luồng lưu lượng đi lớn.

VLAN cũng là một giải pháp, nhưng VLAN chỉ là miền broadcast với đường biên ảo. Một VLAN là một nhóm các thiết bị trên các phân đoạn mạng khác nhau, đó là một miền broadcast bởi người quản trị mạng. Lợi ích của VLAN là vị trí vật lý không còn là nhân tố xác định cổng (port) mà ta sẽ thêm vào một thiết bị trong mạng. Ta có thể thêm một thiết bị vào bất kỳ cổng nào của bộ chuyển mạch và người quản trị mạng sẽ gán cổng cho VLAN. Lưu ý là chỉ có bộ định tuyến hoặc bộ chuyển mạch lớp 3 mới có thể truyền thông giữa các VLAN khác nhau.

* + 1. Luật 80/20:

Luật 80/20 có nghĩa là 80% lưu lượng của user là trên đoạn mạng cục bộ (các phân đoạn mạng), còn lại 20% hoặc ít hơn là qua bộ định tuyến hoặc bridge đến các đoạn mạng khác. Nếu nhiều hơn 20% lưu lượng qua thiết bị phân đoạn mạng, thì phát sinh vấn đề về khả năng hoạt động của mạng. Hình 1.2 sau biểu diễn một mạng 80/20 truyền thống.

Hình 1.2: Mạng 80/20 truyền thống.

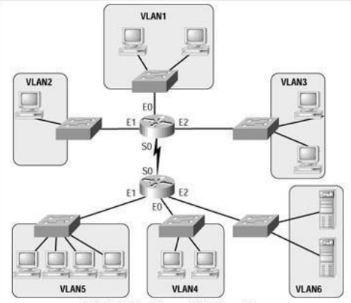


Bởi vì người quản trị mạng chịu trách nhiệm thiết kế và thực hiện, nên họ cải tiến khả năng hoạt động của mạng trong mạng 80/20 bằng cách chắc chắn rằng tất cả các tài nguyên mạng cho user được chứa bên trong đoạn mạng cục bộ. Tài nguyên bao gồm máy chủ, máy in, thư mục dùng chung, phần mềm, và các ứng dụng.

Luật mới 20/80

Ngày nay, thay vì phân tán các máy chủ, chúng được tập trung lại tạo thành “trang trại” máy chủ (server farm) để kiểm soát dịch vụ mạng có tính bảo mật, giảm chi phí và dễ quản trị, nên luật 80/20 đã trở nên lỗi thời và không còn làm việc trong môi trường này nữa. Trong môi trường như vậy, tất cả lưu lượng phải qua backbone (đường trục) của Campus, nghĩa là ta có luật mới 20/80, trong đó 20% là lưu lượng trên đoạn mạng cục bộ và 80% là lưu lượng qua đoạn mạng để lấy các dịch vụ mạng.

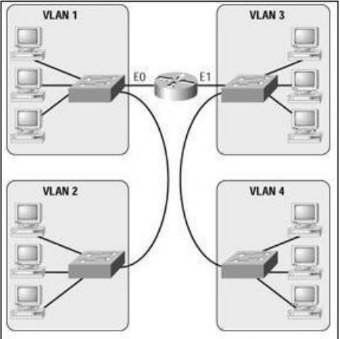
Hình 1.3 Biểu diễn mạng 20/80 mới.



VLAN (Virtual LAN)

Với luật 20/80 có nhiều user hơn cần truyền qua miền broadcast, và điều này gây thêm gánh nặng cho việc định tuyến hoặc chuyển mạch lớp 3. Bằng cách sử dụng VLAN, bên trong mô hình mạng Campus, ta có thể điều khiển được lưu lượng và user truy cập dễ dàng hơn trong mạng Campus truyền thống. VLAN làm giảm miền broadcast bằng cách sử dụng bộ định tuyến hoặc bộ chuyển mạch để thực hiện các chức năng lớp 3.

Hình 1.4 Tạo VLAN trong mạng.



* 1. Các mô hình mạng Campus:

Một mạng Campus gồm có nhiều LAN trong một hoặc nhiều tòa nhà, tất cả các kết nối nằm trong cùng một khu vực địa lý. Thông thường các mạng Campus gồm có Ethernet, Wireless LAN, Fast Ethernet, Fast EtherChannel, Gigabit Ethernet và FDDI.

Sau đây là các mô hình mạng được dùng để phân loại và thiết kế mạng Campus:

* Mô hình mạng chia sẻ (Shared Network Model).
* Mô hình phân đoạn LAN (LAN Segmentation Model).
* Mô hình lưu lượng mạng (Network Traffic Model).
* Mô hình mạng dự đoán trước (Predictable Network Model).
  + 1. Mô hình mạng chia sẻ:

Đầu các năm 1990, mạng Campus được xây dựng theo kiểu truyền thống chỉ có một LAN đơn giản cho tất cả các user kết nối đến và sử dụng. Tất cả các thiết bị trên LAN bắt buộc phải chia sẻ băng thông sẵn có. Môi trường truyền như Ethernet và TokenRing đều có giới hạn về khoảng cách cũng như giới hạn số thiết bị được kết nối vào LAN.

Khả năng hoạt động và tính sẵn sàng của mạng sẽ giảm nếu số thiết bị kết nối tăng dần. Ví dụ như tất cả các thiết bị của Ethernet LAN đều chia sẻ băng thông bán song công 10Mbps. Ethernet cũng sử dụng CSMA/CD để quyết định khi nào một thiết bị có thể truyền dữ liệu trên đoạn LAN chia sẻ này. Trong cùng thời điểm nếu có nhiều hơn một thiết bị có nhu cầu truyền thì sẽ xảy ra đụng độ, và tất cả các thiết bị phải “lắng nghe” và chờ để truyền lại, người ta gọi nó là miền đụng độ. Trong khi TokenRing LAN thì không xảy ra đụng độ vì các trạm chỉ đƣợc phép truyền khi nhận được thẻ bài.

Có một cách làm giảm tắt nghẽn mạng là phân đoạn mạng, hoặc chia một LAN thành nhiều miền đụng độ riêng biệt bằng cách sử dụng bridge chuyển tiếp frame dữ liệu ở lớp 2. Bridge cho phép giảm số thiết bị trên một đoạn, do đó sẽ giảm được xác suất đụng độ trên các đoạn đồng thời tăng giới hạn khoảng cách vật lý vì nó hoạt động như là một repeater.

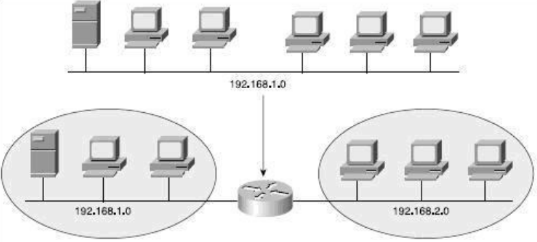
Tuy nhiên, các frame chứa địa chỉ broadcast (FF:FF:FF:FF:FF:FF) đều đến tất các các đoạn. Các frame broadcast thƣờng được dùng để kết hợp các yêu cầu về thông tin hoặc dịch vụ, bao gồm các thông báo về dịch vụ mạng. IP sử dụng broadcast cho giao thức ARP gửi yêu cầu để hỏi địa chỉ MAC tương ứng với địa chỉ IP. Các frame broadcast còn được dùng để gửi các yêu cầu DHCP, IPX, GNS (Get Nearest Server), SAP (Service Advertising Protocol), RIP, tên NetBIOS.

Một miền broadcast là một nhóm các đoạn mạng mà broadcast được tràn qua. Lưu lượng multicast là lưu lượng được định trước cho một nhóm các user được thiết lập cụ thể, mà không quan tâm đến vị trí của nó trong mạng Campus. Các frame multicast cũng qua tất cả các đoạn mạng bởi vì nó là một hình thức của broadcast. Mặc dù trạm đầu cuối phải chọn một nhóm multicast để cho phép nhận dữ liệu multicast, nhưng bridge phải cho lưu lượng tràn qua tất cả các đoạn mạng vì nó không biết được trạm nào là thành viên của nhóm multicast. Các frame multicast chia sẻ băng thông trên một đoạn mạng, nhưng không bắt buộc sử dụng tài nguyên CPU trên mỗi thiết bị kết nối. Chỉ có các CPU đăng ký là thành viên của nhóm multicast mới thực sự xử lý các frame này.

* + 1. Mô hình phân đoạn LAN:

Phân đoạn mạng sẽ giảm lưu lượng và số trạm trên một đoạn để khắc phục vấn đề đụng độ và broadcast. Việc giảm số lượng trạm sẽ giảm được miền đụng độ vì có ít máy hơn cùng có nhu cầu truyền. Đối với việc ngăn chặn broadcast, giải pháp là cung cấp một hàng rào tại biên của đoạn LAN để broadcast không qua được hoặc chuyển tiếp trên đó. Người thiết kế có thể dùng bộ định tuyến hoặc bộ chuyển mạch. Ta có thể dùng bộ định tuyến để kết nối các mạng con nhỏ và định tuyến các gói lớp 3. Bộ định tuyến không cho phép lưu lượng broadcast đi qua, do đó broadcast không thể chuyển tiếp qua các mạng con khác.

Hình 1.5 Biểu diễn phân đoạn mạng bằng bộ định tuyến.



Ngoài ra ta còn phân đoạn LAN bằng bộ chuyển mạch. Bộ chuyển mạch cung cấp khả năng thực thi cao hơn với băng thông chuyên dụng trên mỗi cổng (không chia sẽ băng thông). Người ta gọi bộ chuyển mạch là multi- bridge. Mỗi cổng của bộ chuyển mạch là một miền đụng độ riêng lẻ và không truyền đụng độ qua cổng khác, tuy nhiên các frame broadcast và multicast vẫn tràn qua tất cả các cổng của bộ chuyển mạch. Để phân chia miền broadcast ta sẽ dùng VLAN bên trong mạng chuyển mạch. Một bộ chuyển mạch sẽ chia các cổng một cách logic thành các đoạn riêng biệt. VLAN là một nhóm các cổng vẫn chia sẽ môi trường truyền của đoạn LAN. Vấn đề về VLAN sẽ được tìm hiểu rõ ở phần sau.

* + 1. Mô hình lưu lượng mạng:

Để thiết kế và xây dựng thành công mạng Campus thì ta phải hiểu lưu lượng sinh ra bởi việc sử dụng các ứng dụng cộng với luồng lưu lượng đi và đến từ toàn thể user. Tất cả các thiết bị sẽ truyền dữ liệu qua mạng với các kiểu dữ liệu và tải khác nhau.

Các ứng dụng như: email, word, print, truyền file, và duyệt web, sẽ mang các kiểu dữ liệu đã biết trước từ nguồn đến đích. Tuy nhiên các ứng dụng mới hơn như video, TV, VoIP… có kiểu lưu lượng khó đoán trước được.

Theo truyền thống, các user sử dụng các ứng dụng giống nhau thường được đặt vào cùng nhóm, cùng với server mà nó thường truy cập đến, những nhóm này là mạng luận lý hoặc vậy lý, với ý tưởng là giới hạn phần lớn lưu lượng giữa client và server trong phân đoạn mạng cục bộ. Trong trường hợp các LAN chuyển mạch kết nối bởi các bộ định tuyến đã đề cập trước đó thì cả client và server đều được kết nối đến bộ chuyển mạch lớp 2. Kết nối này cung cấp khả năng hoạt động tốt khi cực tiểu tải lưu lượng trên bộ định tuyến backbone.

Khái niệm của kiểu lưu lượng này được biết như luật 80/20. Trong một mạng Campus được thiết kế đúng cách thì 80% lưu lương trên đoạn mạng nhất định là cục. Và ít hơn 20% là lưu lượng được chuyển ra ngoài mạng đường trục (backbone).

Nếu backbone bị nghẽn thì người quản trị mạng sẽ nhận ra rằng, luật 80/20 không còn phù hợp nữa. Tài nguyên nào có sẵn để cải tiến khả năng hoạt động của mạng? Do phí tổn và tính rắc rối mà việc nâng cấp hoàn thiện Campus backbone là lựa chọn không mong muốn. Thay vì sử dụng luật 80/20 để giảm lưu lượng qua backbone, người quản trị có thể thực hiện hướng giải quyết như sau:

* Gán lại tài nguyên sẵn có để mang các user và các server lại gần với nhau.
* Chuyển các ứng dụng và các file đến các server khác nhau ở bên trong một nhóm.
* Chuyển các user một cách logic (VLAN) hoặc vật lý ở gần nhóm của nó.
* Thêm nhiều server mà có thể mang tài nguyên lại gần các nhóm tương ứng.

Như vậy, việc tuân theo luật 80/20 trong các mạng Campus hiện nay đã trở nên khó khăn đối với người quản trị mạng. Trong mô hình mới của mạng Campus, lưu lượng trở thành luật 20/80 nghĩa là chỉ có 20% lưu lượng là cục bộ, trong khi có ít nhất 80% lưu lượng di chuyển trên mạng backbone. Kiểu lưu lượng này đặt ra trọng tải lớn hơn trong mạng backbone lớp 3.

Chuyển tiếp lớp 3 đòi hỏi phải xử lý tài nguyên nhiều hơn bởi vì các gói phải được kiểm tra trên lớp cao hơn, điều này có thể gây nên tình trạng nghẽn cổ chai trong mạng Campus, nếu không thiết kế cẩn thận.

Như vậy, một mạng Campus với nhiều VLAN trở thành khó khăn trong việc quản lý. Trước kia, các VLAN thường sử dụng một cách logic chứa các nhóm và lưu lượng phổ biến. Với luật 20/80, các thiết bị đầu cuối cần truyền thông với nhiều VLAN khác. Việc đo lường lưu lượng và thiết kế lại mạng Campus trở nên quá nặng nề để theo kịp mô hình luật 20/80.

* + 1. Mô hình mạng dự đoán trước:

Ý tưởng là ta nên thiết kế một mạng với khả năng có thể dự đoán để cung cấp sự bảo dưỡng thấp và tính lợi ích cao. Ví dụ một mạng Campus cần khôi phục lại từ các hỏng hóc và thay đổi kỹ thuật nhanh chóng trong một kiểu định trước. Mạng phải có tính mở rộng để hỗ trợ dễ dàng cho sự phát triển trong tƣơng lai và nâng cấp hoàn thiện. Với sự đa dạng rộng lớn của nhiều giao thức và lưu lượng multicast, thì mạng phải có khả năng hỗ trợ luật 20/80. Mặt khác, thiết kế mạng quanh các luồng lưu lượng thay vì một kiểu lưu lượng riêng biệt.

Luồng lưu lượng trong mạng Campus có thể phân thành ba loại, dựa vị trí các dịch vụ mạng liên quan đến người dùng đầu cuối. Bảng 1.1 cho biết danh sách các kiểu lưu lượng này, cùng với phạm vi của nó.

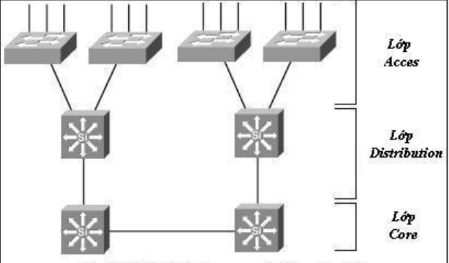
|  |  |  |
| --- | --- | --- |
| Kiểu dịch vụ | Vị trí dịch vụ | Phạm vi của luồng lưu lượng |
| Cục bộ | Trên cùng đoạn mạng/Vlan với user. | Chỉ có lớp Access (truy cập) |
| Từ xa | Trên đoạn mạng/Lan khác với user. | Từ lớp truy cập đến lớp Distribution (phân phối) |
| Enterprise | Giữa các user trong mạng Campus. | Từ lớp truy cập đển lớp Distribution và lớp Core (lõi) |
| Bảng 1.1: Các kiểu dịch vụ mạng. | | |

Lớp Truy cập, Phân phối và Core là ba lớp của mô hình thiết mạng ba lớp của Cisco mà ta sẽ tìm hiểu trong phần tiếp theo.

* 1. Mô hình mạng 3 lớp của Cisco:

Ta có thể thiết kế mạng Campus để mỗi lớp hỗ trợ các luồng lưu lượng hoặc dịch vụ như đã đề cập trong bảng 1.1. Cisco đưa ra mô hình thiết kế mạng cho phép người thiết kế tạo một mạng luận lý bằng cách định nghĩa và sử dụng các lớp của thiết bị mang lại tính hiệu quả, tính thông minh, tính mở rộng và quản lý dễ dàng.

Hình 1.6: Mô hình mạng 3 lớp của Cisco.



Mô hình này gồm có ba lớp: Truy cập, Phân phối, và Lõi. Mỗi lớp có các thuộc tính riêng để cung cấp cả chức năng vật lý lẫn luận lý ở mỗi điểm thích hợp trong mạng Campus. Việc hiểu rõ mỗi lớp và chức năng cũng như hạn chế của nó là điều quan trọng để ứng dụng các lớp đúng cách quá trính thiết kế.

* 1. Lớp truy cập (Access):

Lớp truy cập xuất hiện ở người dùng đầu cuối được kết nối vào mạng. Các thiết bị trong lớp này thường được gọi là các bộ chuyển mạch truy cập, và có các đặc điểm sau:

* Chi phí trên mỗi cổng của bộ chuyển mạch thấp.
* Mật độ cổng cao.
* Mở rộng các uplink đến các lớp cao hơn.
* Chức năng truy cập của người dùng như là thành viên VLAN, lọc lưu lượng và giao thức, và QoS.
* Tính co dãn thông qua nhiều uplink.

Lớp phân phối (Distribution):

Lớp phân phối cung cấp kết nối bên trong giữa lớp truy cập và lớp lõi của mạng Campus. Thiết bị lớp này được gọi là các bộ chuyển mạch phân phát, và có các đặc điểm như sau:

* Thông lượng lớp ba cao đối với việc xử lý gói.
* Chức năng bảo mật và kết nối dựa trên chính sách qua danh sách truy cập hoặc lọc gói.
* Tính năng QoS.
* Tính co dãn và các liên kết tốc độ cao đến lớp lõi và lớp truy cập.

Lớp lõi (Core):

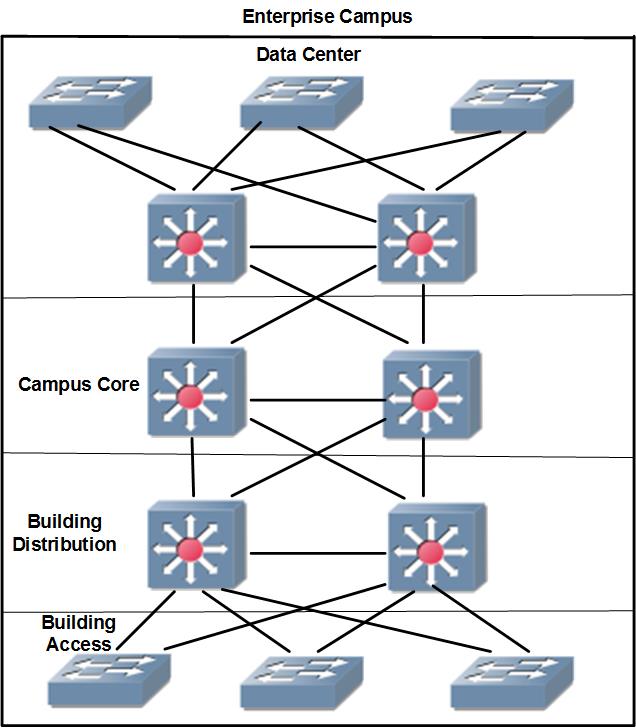
Lớp lõi của mạng Campus cung cấp các kết nối của tất cả các thiết bị lớp phân phối. Lớp lõi thường xuất hiện ở phần xương sống (backbone) của mạng, và phải có khả năng chuyển mạch lưu lượng một cách hiệu quả. Các thiết bị lớp lõi thường được gọi là các bộ chuyển mạch backbone, và có những thuộc tính sau:

* Thông lượng ở lớp 2 hoặc lớp 3 rất cao.
* Chi phí cao.
* Có khả năng dự phòng và tính co dãn cao.
* Chức năng QoS.
  1. Mô hình Modular trong thiết kế mạng Campus:

Như ta đã biết, một mạng được xây dựng và bảo trì tốt nhất bằng cách sử dụng mô hình mạng ba lớp của Cisco như đã được giới thiệu trong phần 1.4. Ta có thể thiết kế một mạng Campus trong kiểu logic, sử dụng phương pháp modular. Trong phương pháp này, mỗi lớp của mô hình mạng phân cấp là đơn vị chức năng cơ bản (module). Các module này được sắp xếp theo kích cỡ thích hợp và kết nối với nhau, và nó cho phép tính co dãn và mở rộng trong tương lai. Ta có thể chia mạng Campus thành các phần cơ bản sau:

* Khối chuyển mạch (switch): là một nhóm các switch thuộc lớp Access và lớp Distribution.
* Khối lõi (core): là backbone của mạng Campus. Các khối liên quan khác có thể tồn tại mặc dù nó không góp phần vào toàn bộ chức năng của mạng Campus, nhưng nó được thiết kế tách biệt và thêm vào thiết kế mạng. Các khối này gồm có:
* Khối Server Farm: gồm một nhóm các server cùng với các switch Access và Distribution.
* Khối quản lý (Management): gồm một nhóm tài nguyên quản lý mạng cùng với switch Access và Distribution.
* Khối Enterprise biên (Enterprise Edge): gồm một tập các dịch vụ liên quan đến việc truy cập mạng ở bên ngoài cùng với các switch Access và Distribution.
* Khối nhà cung cấp dịch vụ biên (Service Provider Edge): các dịch vụ mạng ở bên ngoài được sử dụng bởi mạng Enterprise, đó là các dịch vụ với các giao tiếp khối enterpride biên. Tập hợp các khối trên được gọi là mô hình mạng tổng hợp Enterprise. Chú ý một điều là mỗi building được giới hạn trong một khu vực và được kết nối đến khối Core.

Hình 1.7: Biểu diễn một Modular thiết kế Campus.



* + 1. Khối Switch:

Như ta đã biết mạng Campus được chia thành 3 lớp (lớp Access, Distribution, và Core), khối Switch chứa các thiết bị chuyển mạch từ lớp Access và lớp Distribution, sau đó tất cả các khối switch được kết nối vào trong khối Core để cung cấp kết nối end-to-end xuyên suốt mạng Campus.

Khối Switch chứa hỗn hợp các chức năng của lớp 2 và lớp 3 vì nó chứa các lớp Access và Distribution. Các chuyển mạch lớp 2 được đặt trong phòng dây cáp điện (lớp Access) để kết nối người dùng đầu cuối đến mạng Campus. Với tỉ lệ một người dùng đầu cuối trên một port của switch thì mỗi user nhận được băng thông riêng biệt.

Mỗi switch của lớp Access sẽ kết nối đến thiết bị trong lớp Distribution. Ở đây, chức năng lớp 2 là vận chuyển dữ liệu giữa tất cả các switch truy cập đến điểm kết nối trung tâm. Chức năng lớp 3 cũng được cung cấp trong cách thức định tuyến và các dịch vị mạng khác (bảo mật, QoS,…). Vì vậy, thiết bị của lớp Distribution là một chuyển mạch đa lớp.

Lớp Distribution cũng bảo vệ khối Switch khỏi các lỗi nào đó, ví dụ như việc broadcast sẽ không được truyền đến các khối Switch khác và khối Core. Vì vậy, giao thức Spanning Tree sẽ giới hạn mỗi khối Switch để định nghĩa và điều khiển tốt miền Spanning Tree.

Các switch lớp Acces có thể hỗ trợ VLAN bằng cách gán các port để đánh số VLAN rõ ràng. Vì vậy, các trạm kết nối đến các port được cấu hình cho cùng một VLAN có thể cùng thuộc một mạng con lớp 3. Tuy nhiên, điều đáng quan tâm là một VLAN có thể hỗ trợ nhiều mạng con.Vì switch cấu hình dựa vào port cho VLAN (không phải là địa chỉ mạng), nên bất cứ trạm nào nối vào một port đều thuộc miền địa chỉ mạng. Chức năng của VLAN cũng giống như môi trường truyền của truyền thống, và cho phép bất kỳ địa chỉ mạng kết nối đến.

Trong mô hình thiết kế mạng, ta không nên kéo dài các VLAN đến các switch Distribution ở xa. Lớp Distribution luôn là đường biên của các VLAN, mạng con và broadcast. Mặc dù các switch lớp 2 có thể kéo dài VLAN đến các switch khác ở xa, nhưng nó sẽ hoạt động không tốt. Lưu lượng VLAN không đi qua khối Core của mạng.

Kích thước của khối Switch

Ta nên xem xét một vài yếu tố quyết định kích thước thích hợp cho khối Switch. Phạm vi của các switch trong khối Switch có kích cỡ rất linh động. Ở lớp Access, sự lựa chọn switch thường dựa trên mật độ port hoặc số user được kết nối. Còn ở lớp Distribution phụ thuộc số switch của lớp Access. Các nhân tố phải được xem xét là:

* Kiểu lưu lượng.
* Tổng dung lượng chuyển mạch lớp 3 tại lớp Distribution.
* Số người được kết nối đến switch của lớp Access.
* Ranh giới địa lý của mạng con hoặc VLAN.
* Kích thước của miền Spanning Tree.

Việc thiết kế một khối Switch chỉ dựa vào số người dùng hoặc số trạm chứa trong khối thường không đúng lắm. Thông thường không quá 2000 user được đặt bên trong một khối Switch. Tuy nhiên việc ước lượng kích thước ban đầu cũng đem lại nhiều lợi ích vì vậy ta phải dựa vào các yếu tố sau:

* Loại lưu lượng và hoạt động của nó.
* Kích thước và số lượng của các nhóm làm việc (workgroup).

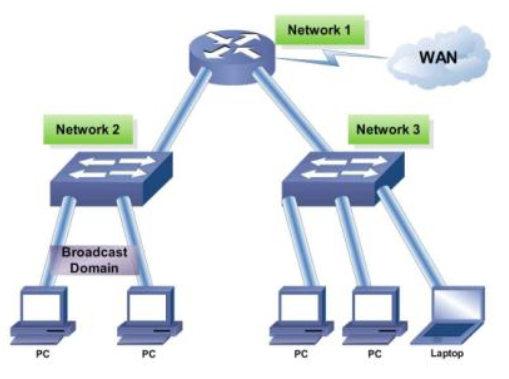
Dựa vào tính chất động của mạng, mà ta định kích thước khối Switch quá lớn sẽ không thể giữ được tải trên nó. Ngoài ra, số lượng người dùng và các ứng dụng trên mạng cũng tăng theo thời gian, do đó việc thay đổi kích thước khối Switch là cần thiết. Mặt khác, ta cũng dựa vào luồng lưu lượng thực tế và kiểu lưu lượng xuất hiện trong khối Switch để có thể ước lượng, mô hình hóa, hoặc đo lường các tham số này bằng các ứng dụng và các công cụ phân tích mạng. Thông thường, một khối switch quá lớn nếu xảy ra các sự kiện sau:

* Các router (chuyển mạch đa lớp) ở lớp Distribution bị nghẽn cổ chai. Sự tắt nghẽn này do lượng lưu lượng bên trong VLAN cần CPU xử lý nhiều hoặc số lần chuyển mạch được yêu cầu bởi chính sách và chức năng bảo mật (danh sách truy cập, hàng đợi…).
* Lưu lượng broadcast và multicast làm chậm chuyển mạch trong khối Switch do việc tạo bản sao và chuyển tiếp qua nhiều port. Điều này đòi hỏi các xử lý ban đầu trong chuyển mạch đa lớp, và nó sẽ trở nên quá tải nếu xuất hiện một lượng lưu lượng đáng kể.

Các switch ở lớp Acces có thể có nhiều hơn một kết nối dự phòng đến các thiết bị của lớp Distribution để cung cấp một môi trường vượt qua lỗi nếu liên kết đầu tiên bị hỏng. Thật vậy, vì lớp Dictribution sử dụng các thiết bị lớp 3, nên lưu lượng có thể được cân bằng tải trên cả kết nối dự phòng.

Thông thường ta có thể cung cấp hai switch trong khối Distribution để dự phòng, với mỗi switch lớp Acces kết nối đến hai switch này. Sau đó, mỗi switch lớp 3 có thể cân bằng tải trên kết nối dự phòng đến lớp Core bằng việc sử dung giao thức định tuyến.

Hình 1.8: Biểu diễn khối Switch, ở lớp 3 có hai switch dự phòng dùng cho việc cân bằng tải.



* + 1. Khối Core:

Một khối core được yêu cầu để kết nối 2 hoặc nhiều hơn các khối switch trong mạng Campus. Bởi vì lưu lượng từ tất cả các khối Switch, các khối Server Farm, và khối Enterprise biên phải đi qua khối Core, nên khối Core phải có khả năng và tính đàn hồi chấp nhận được. Core là khái niệm cơ bản trong mạng Campus, và nó mang nhiều lưu lượng hơn các khối khác.

Khối Core có thể sử dụng bất cứ công nghệ nào (Framrelay, cell, hoặc packet) để truyền dữ liệu trong mạng Campus. Nhiều mạng Campus sử dụng Gigabit hoặc 10 Gigabit Ethernet trong khối core. Ta cần phải xem lại chiều dài khối Ethernet Core.

Như chúng ta đã biết, cả hai lớp Distribution và Core đều cung cấp các chức năng lớp 3. Các mạng con IP đều kết nối đến tất cả các switch của Distribution và Core. Ta phải sử dụng ít nhất hai mạng con để cung cấp tính co dãn và cân bằng tải trong Core.Mặc dù ta có thể sử dụng VLAN nhưng VLAN ở lớp Distribution, nó được định tuyến bên trong Core.

Khối Core gồm có một switch đa lớp, để nhận hai liên kết dự phòng từ switch của lớp Distribution. Do tính quan trọng của khối Core trong mạng Campus nên ta phải thực thi hai hoặc nhiều switch giống nhau trong Core để dự phòng.

Các liên kết giữa các lớp cũng được thiết kế để mang ít nhất một lượng tải từ lớp Distribution. Các liên kết giữa các switch của khối Core trong cùng một mạng con phải có đủ kích cỡ để mang lưu lượng tổng hợp vào switch của Core. Ta coi như là tận dụng liên kết trung bình nhưng nó phải cho phép sự phát triển trong tương lai. Một Ethernet Core cho phép nâng cấp đơn giản và có tính leo thang, ví dụ như sự phát triển từ Etherne -> Fast Ethernet -> Fast EtherChannel ->Gigabit Ethernet -> Gigabit EtheeChannel…

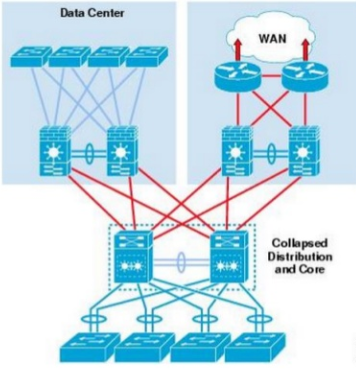
Hai khối core cơ bản được thiết kế là:

* Collapsed Core.
* Dual Core.

Collapsed Core.

Khối Collapsed Core là sự phân lớp của lớp Core, được che lấp trong lớp Distribution. Ở đây, các chức năng của cả Distribution và Core đều được cung cấp trong cùng các thiết bị switch. Điều này thường thấy trong mạng Campus nhỏ hơn mà không xác nhận sự tách rời của lớp Core.

Hình 1.9: Biểu diễn khối Collapsed.



Mặc dù chức năng của lớp Distribution và Core được thực hiện trong cùng một thiết bị, nhưng điều quan trọng là nó vẫn giữ các chức năng này một cách riêng biệt và được thiết kế đúng cách. Chú ý là khối Collapsed Core phụ thuộc khối building, nhưng nó được kết hợp vào trong lớp Distribution của khối Switch độc lập.

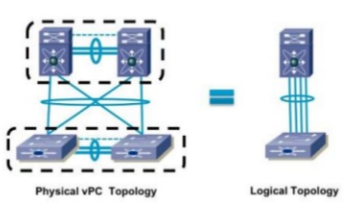
Trong khối Collapsed Core, mỗi switch lớp Access có một liên kết dự phòng đến mỗi switch của lớp Distributon và Core. Tất cả các mạng con lớp 3 có trong lớp Access đều được giới hạn tại các port lớp 3 của switch trong lớp Distribution, giống như khối Switch. Các switch của lớp Distribution và Core kết nối với nhau bằng một hoặc nhiều liên kết để dự phòng.

Kết nối giữa các switch của lớp Distribution và Core sử dụng các kết nối lớp 3. Các switch lớp 3 định tuyến lưu lượng ngay lập tức đến tới các switch khác. Trong hình 1.9 chú ý vị trí của VLAN A và B là thuộc các switch của lớp Access. Các VLAN bị giới hạn ở đó vì lớp Distribution sử dụng switch lớp 3 nên sẽ làm giảm miền broadcast, loại bỏ được khả năng lặp của cầu nối lớp 2 và cung cấp sự vượt lỗi nhanh nếu một kết nối bị lỗi.

Dual Core

Một Dual Core kết nối hai hay nhiều khối Switch để dự phòng, nhưng khối Core không thể có tính mở rộng khi có nhiều khối Switch được thêm vào. Chú ý rằng khối Core này xuất hiện như là một module độc lập và không được ghép vào trong bất kỳ khối hoặc lớp nào.

Hình 1.10: Minh họa khối Dual Core.

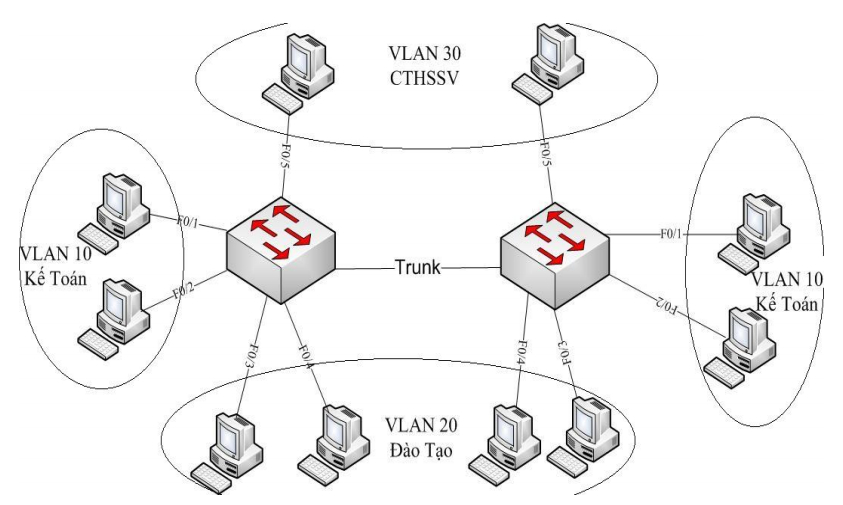


Trước đây, khối Dual Core thường được dùng xây dựng với switch lớp 2 để cung cấp thông lượng đơn giản nhất và hiệu quả nhất. Còn chuyển mạch lớp 3 được cung cấp trong lớp Distribution. Hiện nay, chuyển mạch đa lớp đã mang lại lợi nhuận và cung cấp hoạt động chuyển mạch cao. Việc xây dựng Dual Core với chuyển mạch đa lớp được đề nghị và có thể thực hiện được. Dual core sử dụng hai switch giống nhau để dự phòng. Các liên kết dự phòng kết nối lớp Distribution của khối Switch đến mỗi switch của Dual Core. Hai switch của khối Core kết nối bởi một liên kết. Trong Core lớp 2, các switch không được kết nối để tránh sự lặp vòng trong cầu nối. Một Core lớp 3 sử dụng cho định tuyến hơn là cầu nối, vì sự lặp vòng cầu nối không xảy ra. Trong Dual Core, mỗi switch của Distribution có hai con đường với chi phí bằng nhau, cho phép sử dụng đồng thời cùng một lúc băng thông sẵn có của cả hai con đường. Nếu một switch bị lỗi, thì giao thức định tuyến sẽ định tuyến lại lưu lượng sử dụng con đường khác qua switch dự phòng còn lại.

Kích thước của khối Core trong mạng Campus

Dual Core là khối các switch dự phòng được lắp ghép với nhau, được giới hạn và biệt lập bởi các thiết bị lớp 3. Các giao thức định tuyến xác định các con đường và duy trì hoạt động của khối Core. Đối với bất kỳ mạng nào, ta cũng phải chú ý đến việc thiết kế router và các giao thức định tuyến trong mạng. Bởi vì các giao thức định tuyến truyền bá cập nhật thông lượng mạng, nên hình trạng mạng phải chiu sự thay đổi. Kích thước mạng (số lượng router) sẽ ảnh hưởng đến hoạt động của giao thức định tuyến vì sự cập nhật được thay đổi.

Hình 1.11: Biểu diễn mạng nhỏ với hai khối Switch chứa hai switch chuyển mạch lớp 3 (xử lý định tuyến bên trong switch của lớp Distribution).



Còn đối với mạng Campus lớn, có thể có nhiều khối Switch kết nối đến khối Core. Nếu ta xem mỗi switch đa lớp là một router, thì ta nhớ lại rằng, mỗi bộ xử lý định tuyến sẽ giữ các thông tin truyền thông với các ngang cấp kết nối trực tiếp với nó. Thực tế, hầu hết các giao thức định tuyến đều giới hạn số router ngang cấp, mà kết nối trực tiếp trên liên kết point-to-point hoặc kết nối multicast. Trong một mạng với số lượng khối Switch lớn, thì số kết nối router khá lớn. Ta không nên đề cập quá nhiều switch của Distribution, bởi vì số lượng thực tế của các ngang cấp kết nối trực tiếp thì khá nhỏ, không quan tâm đến kích thước mạng Campus. Các VLAN của lớp Access sẽ giới hạn ở các switch của lớp Distribution. Chỉ các router ngang cấp ở biên là một cặp switch Distribution,cung cấp dự phòng cho mỗi mạng con VLAN của lớp Access. Ở biên của lớp Distribution và Core, mỗi switch của Distribution chỉ kết nối đến hai switch của khối Core trên giao tiếp của switch lớp 3. Vì vậy, chỉ thiết lập một cặp router ngang cấp.

Khi các switch đa lớp được sử dụng trong lớp Distribution và Core, thì các giao thức định tuyến sẽ chạy trên mỗi cặp liên kết dự phòng giữa các con đường với chi phí bằng nhau của cả hai lớp. Lưu lượng được định tuyến qua cả hai liên kết để chia sẽ tải và tận dụng băng thông của cả hai liên kết này.

Một điểm cuối cùng cảu việc thiết kế lớp Core là tính co dãn của các switch trong khối Core phải thỏa tải lưu lượng đi vào. Ở một mức độ nhỏ nhất, mỗi switch của khối core phải điều khiển được liên kết đi vào lớp Distribution với công suất 100%.

* + 1. Các khối Building khác:

Các tài nguyên khác trong mạng Campus được định danh và đặt vào mô hình khối building. Ví dụ như, một Server Farm gồm nhiều máy chủ chạy các chương trình ứng dụng được truy cập từ các người dùng từ tất cả Enterprise. Điều cần thiết là các máy chủ này phải có tính theo thang để mở rộng trong tương lai, có khả năng truy cập cao, và cũng đem lại lợi ích từ việc điều khiển lưu lượng và các chính sách bảo mật.

Để có được những điều cần thiết trên, ta có thể nhóm các tài nguyên vào các khối building giống như là mô hình khối switch. Các khối này cũng có switch của lớp Distribution và có các kết nối dự phòng nối trực tiếp vào lớp Core, nó cũng chứa các tài nguyên của Enterprise. Hầu hết các khối building đều có trong mạng Campus vừa và lớn, ta đã quen với khái niệm đặt chức năng Enterprise vào trong khối Switch của nó, cũng như xây dựng khối này.

Khối Server Farm

Bất kỳ một máy chủ hay ứng dụng nào được truy cập bởi hầu hết người dùng của Enterprise thường thuộc về một Server Farm. Toàn bộ Server Farm này được nhận dạng như là khối Switch của chính nó, và kết nối các switch của Distribution vào trong lớp Core với liên kết dự phòng tốc độ cao.

Các máy chủ riêng có các kết nối mạng đơn đến một trong các switch của Distribution. Nếu một máy chủ dự phòng được sử dụng, thì nó nên kết nối đến switch luân phiên của Distribution. Điều này được biết như là Dual-homing của các máy chủ.

Ví dụ: các máy chủ của Enterprise gồm có email, các dịch vụ intranet, các ứng dụng ERP (Enterprise Resource Planning), và hệ thống máy tính lớn. Chú ý là mỗi tài nguyên nội bộ đều được đặt ở bên trong một firewall hay vòng bảo mật.

Khối quản lý

Thông thường, các mạng Campus phải được kiểm tra qua việc sử dụng các công cụ quản trị mạng để đo lường hoạt động mạng và phát hiện lỗi. Ta có thể nhóm toàn bộ ứng dụng quản lý mạng vào trong một khối Switch quản lý mạng. Điều này trái ngược với khối Server Farm, bởi vì các công cụ quản trị mạng không phải là tài nguyên của Enterprise được truy cập bởi hầu hết các máy chủ. Hơn nữa, các công cụ này sẽ đi ra ngoài để truy cập vào các thiết bị mạng khác, các ứng dụng của máy chủ và hoạt động của người dùng trong tất cả các khu vực của mạng Campus. Khối Switch quản lý mạng thường có lớp Distribution kết nối vào các switch của khối Core. Vì các công cụ này được dùng để phát hiện lỗi xảy ra tại thiết bị và các kết nối, nên lợi ích của nó rất quan trọng. Các kết nối dự phòng và switch dự phòng đều được sử dụng.

Ví dụ: tài nguyên quản lý mạng trong khối switch bao gồm:

* Các ứng dụng kiểm tra mạng.
* Các server đăng nhập hệ thống (syslog).
* Các server xác thực, cấp quyền và cung cấp tài khoản (AAA).
* Các ứng dụng quản lý chính sách.
* Quản trị hệ thống và các dịch vụ điều khiển từ xa.
* Các ứng dụng quản lý, phát hiện xâm nhập.

Khối Enterprise biên

Hầu hết các mạng Campus phải kết nối đến các nhà cung cấp dịch vụ để truy câp đến tài nguyên bên ngoài, được gọi là các biên của Enterprise hoặc của Campus. Các tài nguyên này có sẵn trong toàn bộ mạng Campus và được truy cập chủ yếu như là khối Switch kết nối đến khối Core của mạng.

Các dịch vụ biên thường được chia thành:

* Truy cập internet: hỗ trợ lưu lượng ra ngoài internet, cũng như lưu lượng vào các dịch vụ công cộng, như email, và extranet web server. Các kết nối này được cung cấp bởi một hoặc nhiều nhà cung cấp dịch vụ Internet (ISP). Các thiết bị bảo mật mạng thường được đặt tại đây.
* Truy cập từ xa và VPN: hỗ trợ các truy cập quay số từ các người dùng bên ngoài qua mạng PSTN (Public Switched Telephone Network). Nếu lưu lượng thoại được hỗ trợ trên mạng Campus, thì gateway VoIP phải kết nối đến PSTN ở đây. Thêm nữa, các thiết bị VPN kết nối vào Internet hỗ trợ kết nối đường hầm bảo mật đến các vị trị từ xa.
* Thương mại điện tử: hỗ trợ web, ứng dụng và cơ sở dữ liệu cũng như firewall và các thiết bị bảo mật. Khối switch kết nối đến một hoặc nhiều ISP.
* Truy cập WAN: hỗ trợ tất cả các kết nối WAN truyền thống đến các vị trí từ xa như FrameRelay, ATM, Leased-Line, ISDN…

Khối nhà cung cấp dịch vụ biên

Mỗi nhà cung cấp dịch vụ kết nối đến một mạng Campus cũng phải có thiết kế mạng phân cấp của chính nó. Một mạng của nhà cung cấp dịch vụ đáp ứng cho một Enterprise ở biên nhà cung cấp, kết nối đến biên của khối Enterprise. Ở đây ta không quan tâm đến mạng của nhà cung cấp dịch vụ, mà chỉ cần biết là mạng Campus có một khối biên để kết nối đến biên của mạng nhà cung cấp.

CHƯƠNG II   
VLAN, TRUNK VÀ VTP (VLAN TRUNKING PROTOCOL)

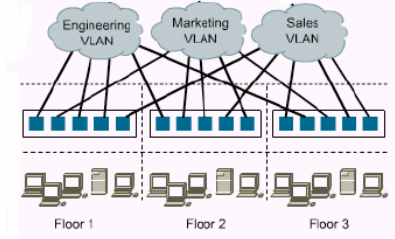
2.1. Mạng LAN ảo:

Mô hình mạng không có VLAN là một flat network vì nó chỉ hoạt động chuyển mạch ở lớp 2. Một flat network là một miền broadcast, mỗi gói broadcast từ một host nào đều đến được tất cả các host còn lại trong mạng. Mỗi port trong switch là một miền collision, vì vậy người ta sử dụng switch để chia nhỏ miền collision, tuy nhiên nó vẫn không ngăn được miền broadcast. Ngoài ra nó còn có các vấn đề như:

* Vấn đề về băng thông: trong một số trường hợp một mạng Campus ở lớp 2 có thể mở rộng thêm một số building nữa, hay số user tăng lên thì nhu cầu sử dụng băng thông cũng tăng, do đó băng thông cũng như khả năng thực thi của mạng sẽ giảm.
* Vấn đề về bảo mật: bởi vì user nào cũng có thể thấy các user khác trong cùng một flat network, do đó rất khó để bảo mật.
* Vấn đề về cân bằng tải: trong flat network ta không thể thực hiện truyền trên nhiều đường đi, vì lúc đó mạng rất dễ bị loop, tạo nên “broadcast storm” ảnh hưởng đến băng thông của đường truyền. Do đó không thể chia tải (còn gọi là cân bằng tải).

Để giải quyết các vấn đề trên, người ta đưa ra giải pháp VLAN. VLAN (Virtual Local Area Network) được định nghĩa là một nhóm logic các thiết bị mạng, và được thiết lập dựa trên các yếu tố như chức năng, bộ phận, ứng dụng… của công ty. Mỗi VLAN là một mạng con logic được tạo ra trên switch, còn gọi là segment hay miền broadcast.

Hình 2.1: Vlan theo chức năng các phòng ban.



Tuy nhiên trong phần này chúng ta nói tới khả năng khác của các bộ chuyển mạch

hiện đại, chúng có thể lọc các khung tin quảng bá và chỉ gửi chúng tới miền quảng

bá xác định. Sử dụng các bộ chuyển mạch để kết hợp các thiết bị thành các vùng

quảng bá logic sẽ tạo ra các mạng LAN ảo (VLAN).

2.1.1. Các kiểu thành viên của VLAN (VLAN Membership):

Khi VLAN được cung cấp ở switch lớp Access, thì các đầu cuối người dùng phải có một vài phương pháp để lấy các thành viên đến nó. Có 2 kiểu tồn tại trên Cisco Catalyst Switch đó là:

* Static VLAN.
* Dynamic VLAN.

Static VLAN

Static VLAN cung cấp kiểu thành viên dựa vào port, nghĩa là các port của switch được gán cho các VLAN riêng biệt. Các thiết bị người dùng đầu cuối trở thành thành viên trong VLAN dựa vào port vật lý của switch kết nối đến nó. Không có thiết lập quan hệ đối với thiết bị đầu cuối, mà nó tự động thừa nhận kết nối VLAN khi nó kết nối đến một port. Thông thường, thiết bị đầu cuối thậm chí không nhận thức được sự tồn tại của VLAN.

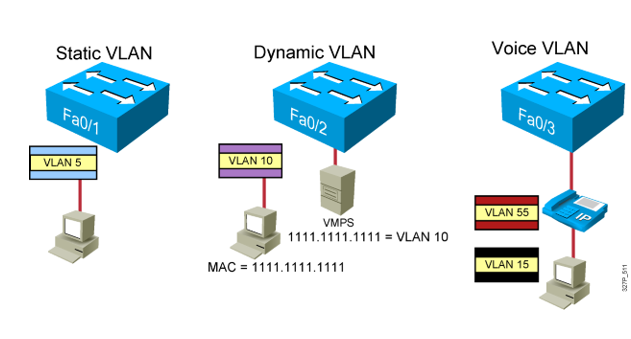
Người quản trị mạng sẽ cấu hình các port của switch gán cho các VLAN bằng tay, nên được gọi là trạng thái tĩnh. Mỗi port nhận một port VLAN ID với một số VLAN. Các port trên một switch có thể được gán và nhóm thành nhiều VLAN. Mặc dù hai thiết bị cùng kết nối đến một switch, nhưng nếu VLAN ID của nó khác nhau thì lưu lượng giữa chúng sẽ không qua nhau. Để thực hiện chức năng này, ta phải sử dụng thiết bị lớp 3 để định tuyến các gói hoặc thiết bị mở rộng lớp 2 để làm cầu nối các gói giữa hai VLAN.

Kiểu thành viên Static VLAN thường được quản lý trong phần cứng với mạch tích hợp ứng dụng đặc biệt ASIC (Application Specific Intergrated Circuit) trong switch. Kiểu này cung cấp khả năng hoạt động tốt vì tất cả việc ánh xạ các port được làm ở mức phần cứng vì vậy không cần có bảng truy tìm phức tạp.

Dynamic VLAN

Dynamic VLAN cung cấp thành viên dựa trên địa chỉ MAC của thiết bị người dùng đầu cuối. Khi một thiết bị kết nối đến một port của switch, switch phải truy vấn đến cơ sở dữ liệu để thiết lập thành viên VLAN. Người quản trị mạng phải gán địa chỉ MAC của user vào một VLAN trong cơ sở dữ liệu của VMPS (VLAN Membership Policy Server).

Hình 2.2: Biểu diễn Dynamic VLAN với bảng địa chỉ MAC.



Với Cisco Switch, dynamic LAN được tạo và quản lý bằng công cụ quản lý mạng như Cisco Work 2000. Dynamic VLAN cho phép tính mềm dẻo và tính di động cho người dùng đầu cuối.

2.1.2. Triển khai VLAN:

Để thực thi VLAN, ta phải xem xét số thành viên của VLAN, thông thường số VLAN sẽ phụ thuộc vào kiểu lưu lượng, kiểu ứng dụng, phân đoạn các nhóm làm viện phổ biến và các yêu cầu quản trị mạng.

Môt nhân tố quan trong cần xem xét là mối quan hệ giữa các VLAN và kế hoạch sử dụng địa chỉ IP. Cisco giới thiệu một sự tương thích 1-1 giữa VLAN và các mạng con, nghĩa là nếu một mạng con với một mask 24 bit được sử dụng cho một VLAN, như vậy có nhiều nhất 254 thiết bị trong VLAN và các VLAN không mở rộng miền lớp 2 đến Distribution Switch. Trong trường hợp khác, VLAN không đi đến Core của mạng, và khối Switch khác. Ý tưởng này giữ cho miền broadcast và lưu lượng không cần thiết ra khỏi khối Core.

Các VLAN được chia trong khối Switch bằng hai cách cơ bản sau:

* End-to-end VLAN.
* Local VLAN.

End-to-end VLAN

End-to-end VLAN còn được gọi là Campus-wide VLAN, nối toàn bộ switch của một mạng. Nó được xác định để hỗ trợ tính mềm dẻo và tính di động cực đại cho thiết bị đầu cuối. Các user được gán vào VLAN mà không quan tâm đến vị trí vật lý. Vì một user di chuyển quanh Campus, thì nó cũng thuộc VLAN đó, nghĩa là mỗi VLAN phải có hiệu lực (available)ở lớp Access trong mỗi khối Switch.

End-to-end VLAN nên nhóm các user theo nhu cầu phổ biến. Tất cả user trong một VLAN có cùng kiểu luồng lưu lượng theo luật 80/20. Luật này có nghĩa là 80% lưu lượng là của user trong nhóm cục bộ, trong khi 20% đến một tài nguyên từ xa trong mạng Campus. Mặc dù 20% của lưu lượng trong VLAN qua Core của mạng, nhưng end-to-end VLAN làm nó có thể thực hiện tất cả lưu lượng bên trong VLAN qua Core.

Vì tất cả VLAN phải có hiệu lực ở mỗi switch lớp Access, nên VLAN trunking phải được sử dụng để mạng tất cả các VLAN giữa switch lớp Access và lớp Distribution.

Chú ý: end-to-end VLAN không đựơc đề nghị trong mạng Enterprise, nếu không có một lý do hợp lý. Lưu lượng broadcast đựơc mạng trên một VLAN từ một đầu cuối của mạng đến một đầu cuối khác, nên bão broadcast (broadcast storm) hoặc lặp vòng cầu nối lớp 2 cũng có thể truyền bá qua phạm vi của tài nguyên. Khi đó, việc xử lý sự cố trở nên quá khó, và sự mạo hiểm sử dụng end-to-end VLAN làm ảnh hưởng đến lợi ích.

Local VLAN

Vì hầu hết mạng Enterprise hướng tới luật 20/80, nên end-to-end VLAN trở nên cồng kềnh và khó duy trì. Luật 20/80 có nghĩa là 20% lưu lượng cục bộ, còn 80% đến một tài nguyên từ xa qua lớp Core. Các người dùng đầu cuối đòi hỏi truy cập vào tài nguyên trung tâm bên ngoài VLAN của nó. Các uer phải qua Core của mạng thường xuyên hơn. Các VLAN được gán chứa các nhóm user dựa trên đường biên vật lý, liên quan đến lượng lưu lượng rời VLAN.

2.1.2.1. Tạo mạng LAN ảo với một bộ chuyển mạch:

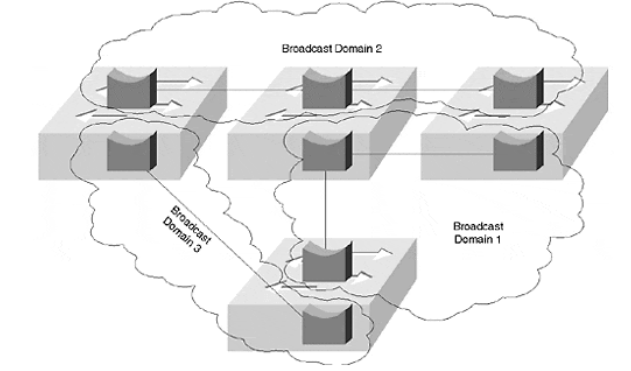
Mỗi mạng LAN ảo và các thành viên của nó được xác định bởi một nhóm các  
cổng trên bộ chuyển mạch. Mỗi cổng của bộ chuyển mạch thuộc về một mạng  
LAN ảo nào đó, do đó các thiết bị gắn với cổng này sẽ thuộc về mạng LAN ảo này.  
Các khung tin quảng bá chỉ được phát tới các cổng thuộc cùng một mạng LAN ảo.  
Một thiết bị có thể chuyển từ LAN ảo sang LAN ảo khác bằng cách kết nối tới  
cổng khác của bộ chuyển mạch. Một thiết bị khi thay đổi vị trí địa lý vẫn thuộc về  
LAN ảo cũ nếu nó vẫn duy trì kết nối tới một trong các cổng thuộc về LAN ảo này.

2.1.2.2. Tạo mạng LAN ảo với nhiều bộ chuyển mạch:

Trong thực tế, việc sử dụng nhiều bộ chuyển mạch để xây dựng các mạng LAN ảo

được thực hiện nhiều hơn.

Hình 2.3: Cấu hình bộ chuyển mạch tạo thành các miền quảng bá cho VLAN.



Để thực hiện mạng LAN ảo bằng nhiều bộ chuyển mạch, một số định danh đặc  
biệt – VLAN ID được gán cho các khung tin, số này xác định mạng LAN ảo mà  
khung tin cần chuyển tới.

Giả sử một máy trạm A gửi khung tin tới máy trạm B thuộc cùng LAN ảo với  
mình (nhưng không cùng thuộc một bộ chuyển mạch). Bộ chuyển mạch mà máy  
A nối trực tiếp tới sẽ gán thêm vào khung tin chỉ số VLAN ID và chuyển nó tới bộ  
chuyển mạch kế tiếp.

Mỗi bộ chuyển mạch sẽ sử dụng VLAN ID để định tuyến khung tin, nó sẽ đọc  
VLAN ID và chuyển tiếp khung tin cho bộ chuyển mạch thích hợp. Khi khung tin  
tới bộ chuyển mạch cuối cùng, bộ chuyển mạch này nhận ra đích tới nối trực tiếp  
tới một trong các cổng của mình. Nó sẽ loại bỏ phần đầu chứa chỉ số VLAN ID rồi  
gửi khung tới đúng cổng. Khung tin khi tới trạm đích sẽ được khôi phục nguyên  
dạng ban đầu.

2.1.2.3. Cách xây dựng mạng LAN ảo:

Để tạo ra mạng LAN ảo, cần phải xác định nhóm logic. Nhóm các máy tính (thiết

bị) trong mạng LAN ảo thường được tổ chức theo hai mô hình:

* Mô hình nhóm làm việc: Theo mô hình này, các thành viên trong mạng LAN ảo là các máy tính cùng thực hiện một chức năng, người sử dụng trong cùng một nhóm công việc. Các mạng LAN ảo thường được chia theo các phòng ban, ví dụ Phòng kế toán, phòng Bán hàng, Phòng nghiên cứu... Các tài nguyên khác chung của mạng sẽ thuộc về một hoặc nhiều mạng LAN ảo.
* Mô hình dịch vụ: Theo mô hình này, các mạng LAN ảo được phân chia theo loại hình dịch vụ cụ thể. Ví dụ, tất cả các máy tính cần truy nhập tới dịch vụ đặc thù nào đó sẽ là thành viện của cùng một mạng LAN ảo. Các máy tính có thể là thành viên của nhiều mạng LAN ảo khác nhau tuỳ thuộc vào các dịch vụ mà nó cần truy nhập tới.

2.1.2.3. Ưu và nhược điểm của mạng LAN ảo:

Ưu điểm:

* Có thể tạo ra mạng LAN ảo, tạo ra các nhóm làm việc không phụ thuộc vào vị trí của thiết bị, chẳng hạn, những người thuộc cùng nhóm nghiên cứu không cần ngồi cùng một phòng hay cùng một tầng trong toà nhà mà vẫn là các thành viên trong một mạng LAN ảo.
* Có thể dễ dàng di chuyển thiết bị từ mạng LAN ảo này sang mạng LAN ảo khác. Mạng LAN ảo cho phép kiểm soát kiểm soát các miền quảng bá và kiếm soát tính bảo mật.
* Ưu điểm khác là bằng việc sử dụng các bộ chuyển mạch thay cho các bộ định tuyến, hiệu năng làm việc đạt được cao hơn, giá thành rẻ hơn, khả năng quản trị tốt hơn.

Nhược điểm:

* Hiện nay, chuẩn chính thức cho VLAN ( Uỷ ban IEEE 802.1q đang soạn thảo) chưa được phê chuẩn mặc dù chuẩn này được hỗ trợ bởi nhiều nhà cung cấp. Do đó các thiết lập và cấu hình VLAN phụ thuộc vào nhà sản xuất thiết bị.

2.2. VLAN Trunk:

2.2.1. Sự ra đời của thuật ngữ Trunking:

Thuật ngữ Trunking bắt nguồn từ công nghệ Radio và công nghệ điện thoại. Trong công nghệ radio, một đường Trunk là một đường dây truyền thông mà trên đó truyền tải nhiều kênh tín hiệu radio.

Trong công nghiệp điện thoại, khái niệm thuật ngữ Trunking là kết hợp giữa đường truyền thông điện thoại hoặc các kênh điện thoại giữa hai điểm. Một trong các điểm có thể là một tổng đài.

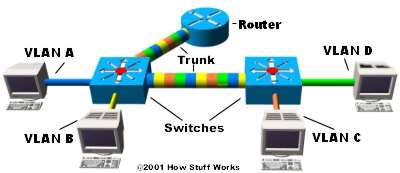
Ngày nay, nguyên lý trunking được chấp nhận sử dụng trong công nghệ mạng chuyển mạch. Một đường Trunk là kết nối vật lý và logic giữa 2 switch.

2.2.2. Khái niệm Trunking:

Trong khuôn khổ môi trường chuyển mạch VLAN, một đường Trunk là một kết nối point-to-point để hỗ trợ các VLAN trên các switch liên kết với nhau. Một đường được cấu hình Trunk sẽ gộp nhiều liên kết ảo trên một liên kết vật lý để chuyển tín hiệu từ các VLAN trên các switch với nhau dựa trên một đường cáp vật lý.

Các Host cùng một VLAN trên 2 hoặc nhiều Switch muốn đi đến nhau thì giữa các Switch này phải có một hoặc nhiều đường đấu nối với nhau. Giả sử hệ thống bạn có quá nhiều VLAN. Giữa các VLAN trên các Switch có quá nhiều đường đấu nối là không hợp lý. Nên cần có một giải pháp chỉ cần một đường kết nối mà vẫn đảm bảo tính thông suốt của các VLAN. Đường đấu nối này gọi là đường trunk. Lúc này Switch chỉ cần dành ra một đường kết nối để thông suốt các VLAN trên các Switch lại với nhau.

Hình 2.4: Đường trunk kết nối giữa các switch.



2.2.3. Hoạt động của Trunking:

Giao thức Trunking được phát triển để nâng cao hiệu quả quản lý việc lưu chuyển các Frame từ các VLAN khác nhau trên một đường truyền vật lý. Giao thức trunking thiết lập các thoả thuận cho việc sắp sếp các Frame vào các cổng được liên kết với nhau ở hai dầu đường trunk.

Hiện tại có 2 kỹ thuật Trunking là Frame Filtering và Frame Tagging. Trong khuôn khổ của luận văn này chỉ đề cập đến kỹ thuật Frame Tagging.

Giao thức Trunking sử dụng kỹ thuật Frame Tagging để phân biệt các Frame và để dễ dàng quản lý và phân phát các Frame nhanh hơn. Các tag được thêm vào trên đường gói tin đi ra vào đường trunk và được bỏ đi khi ra khỏi đường trunk. Các gói tin có gắn tag không phải là gói tin Broadcast.

Một đường vật lý duy nhất kết nối giữa hai switch thì có thể truyền tải cho mọi VLAN. Để lưu trữ, mỗi Frame được gắn tag để nhận dạng trước khi gửi đi, Frame của VLAN nào thì đi về VLAN đó.

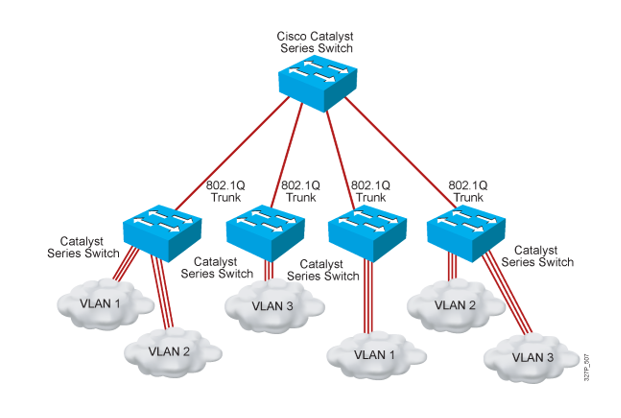
2.2.4. Các chuẩn trunking trong một hệ thống mạng:

Nhìn chung kỷ thuật trunking chèn thêm thông tin vào Ethernet frame. Khi nó đi trên đường trunk để biết frame này đến từ VLAN nào để đẩy frame đến VLAN nhận một cách đúng nhất.

2.2.5. Chuẩn IEEE và kỹ thuật trunking DOT1Q:

Kỹ thuật trunking DOT1Q thực hiện chèn thêm 4 byte vào sau trường Source MAC của Ethernet Frame trên đường trunk. Thông tin chèn này được gọi là DOT1Q Tag.

Hình 2.5: Kỹ thuật trunking 802.1Q.



Kỹ thuật trunking 802.1Q

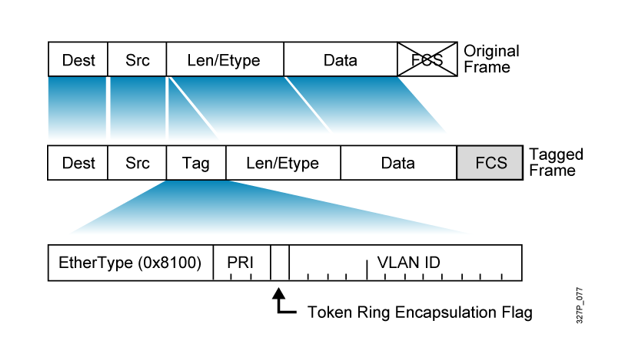
Các trường trong 802.1Q VLAN Tag bao gồm:

* Tag Protocol ID (16 bit) nôi dung trường này luôn được set 0x8100 dùng để định danh ra frame này đã đc tag 802.1q để phân biệt với frame untagged trên đường trunk.
* User Priority (3 bit) sử dụng cho kỹ thuật QoS.
* Canonical Format Indicator (1bit) cho biết địa chỉ MAC đang được sử dụng ở định dạng Token Ring hay Ethernet Frame.
* VLAN ID(12bit): cho biết Frame đang chạy trên đường trunk là của VLAN nào.

Cách thức xử lý Frame:

Khi switch nhận được Frame có tag thông tin 802.1Q, nó sẻ tiến hành đọc thông tin này, xem frame này đến từ VLAN nào. Sau đó nó sẻ xử lí gở bỏ Tag trả lại frame đúng VLAN mà frame thuộc về. Thực chất Tag DOT1Q chỉ được tag trên đường trunk để phân biệt các frame của các VLAN khác nhau. Các End users không nhận biết được rằng frame được Tag và chuyển trên đường trunk. Trunking hoàn toàn transparent với các thiết bị đầu cuối này.

Hình 2.6: Cách thức xử lý Frame.



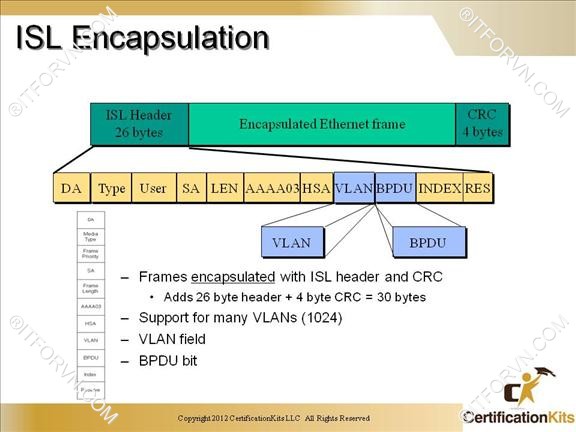
2.2.6. Native VLAN trong kỹ thuật Trunking:

Là một khái niệm trong kỹ thuật DOT1Q. Những frame nào thuộc về Native VLAN sẻ là nguyên trạng Ethernet Frame và không được gán Tag khi đi trên đường trunk. Điều đặt biệt về Native VLAN là các thiết bị đấu nối tiến hành trunking với nhau thì 2 thiết bị này phải cùng Native VLAN nếu Mismatch Native VLAN, khi xảy ra mismatch native VLAN CDP sẻ liên tục gửi các log báo Native VLAN mismatch. Trên thiết bị Switch Cisco VLAN 1 luôn được thiết lập mặc định là Native VLAN.

2.2.7. Chuẩn Cisco và kỹ thuật trunking ISL:

Kỹ thuật Trunking này của Cisco tiến hành chèn thêm Header 26 byte và trường CRC kiểm tra lỗi 4 byte vào Ethernet Frame.

Hình 2.7: Kỹ thuật trunking ISL.



Các trường trong môt ISL Tag bao gồm:

* DA(Destination Address): 40 bit sẻ set ở dạng "0x01-00-0C-00-00″ or “0x03-00-0c-00-00”. Để báo hiệu bên nhận rằng frame được tag ở dạng ISL.
* Type: 4bit chỉ ra type frame được và sử dụng là gì (0000:Ethernet, 0001: Token ring….).
* User: 4bit chỉ ra độ ưu tiên của frame khi đi qua switch(XX00: normal priority, XX01: priority 1, XX10: priority 2, XX11: highest priority).
* SA(Source Address): 48 bit địa chỉ nguồn của gói tin ISL. Tuy nhiên thiết bị nhận có thể bỏ qua địa chỉ này.
* LEN(Length): 16bit cho biết kích thước của gói tin thực tế.
* AAAA03 là một giá trị 24bit liên tục của 0xAAAA03.
* HSA(High Bits of Source Address):24 bit trường này chứa giá trị “0x00-00-0C.
* BPDU: được set để tất cả gói tin BPDU được tag ISL(hoạt động trên STP).
* INDEX: 16bit chỉ ra chỉ số port nguồn của gói tin tồn tại trên Switch.
* RES: dài 16bit sử dụng khi Token ring hoặc FDDI được đóng gói frame ISL, với frame Ethernet trường RES được set tất cả bit 0.

Chuẩn trunking này là chuẩn độc quyền của Cisco và chỉ chạy trên thiết bị Cisco. Hoạt động đóng Tag trên đường trunk và mở tag ISL cũng hoạt động giống như 802.1Q encapsulation.

2.3. VLAN Trunking Protocol – Giao thức mạch nối VLAN – VTP:

2.3.1. Nguồn gốc VTP:

VTP được thiết lập để giải quyết các vấn đề nằm bên trong hoạt động của môi trường mạng chuyển mạch VLAN.

Ví dụ: Một domain mà có các kết nối switch hỗ trợ bởi các VLAN. Để thiết lập và duy trì kết nối bên trong VLAN, mỗi VLAN phải được cấu hình trên cổng của switch.

Khi phát triển mạng và các switch được thêm vào mạng, mỗi switch mới phải được cấu hình với các thông tin của VLAN trước đó. Một kết nối đơn không đúng VLAN ẩn chứa 2 vấn đề:

* Các kết nối chồng chéo lên nhau do cấu hình VLAN không đúng.
* Các cấu hình không đúng giữa các môi trường truyền khác nhau như là: Ethernet và FDDI.

Với VTP, cấu hình VLAN được duy trì dễ dàng bằng Admin domain. Thêm nữa, VTP làm giảm phức tạp của việc quản lý VLAN.

2.3.2. Khái niệm VTP:

Vai trò của VTP là duy trì cấu hình VLAN thông qua admin domain của mạng. VTP là một giao thức lớp 2 sử dụng các Trunk Frame để quản lý việc thêm bớt, xoá và đổi tên các VLAN trên một domain. Thêm nữa, VTP cho phép tập trung các thay đổi tới tất cả các switch trong mạng.

Thông điệp VTP được đóng gói trong một chuẩn CISCO là giao thức ISL hoặc IEEE 802.1q và sau đó đi qua các liên kết Trunk tới thiết bị khác.

Giao thức đồng bộ thông tin VLAN giữa các thiết bị Switch của Cisco. Khi một hệ thống lớn thì việc tạo, xóa, sửa VLAN trong các Switch trở nên cực kì khó khăn. Thiếu tính chính xác và mất nhiều thời gian. Cisco đưa ra giao thức VTP tiến hành đồng bộ thông tin và cấu hình VLAN giữa các Switch trong cùng một miền Domain.

Các đặc điểm và cách thức hoạt động của VTP:

* VTP hoạt động trên các đường Trunking Layer 2 để trao đổi thông tin VLAN với nhau.
* 3 yếu tố quan trọng của VTP là : VTP domain, VTP password, VTP mode(Server, Client, Transparent).

2.3.3. Các chế độ VTP:

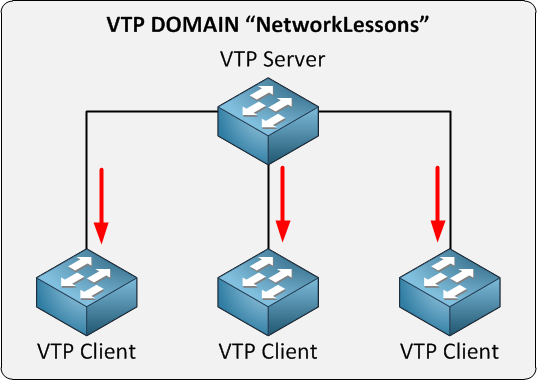
VTP Domain:

Một VTP domain được tạo ra từ một hay nhiều các thiết bị đa kết nối để chia sẻ trên cùng một tên VTP domain. Mỗi switch chỉ có thể có một VTP domain. Khi một thông điệp VTP truyền tới các switch trong mạng, thì tên domain phải chính xác để thông tin truyền qua.

VTP header có nhiều kiểu trên một thông điệp VTP, có 4 kiểu thường được tìm thấy trên tất cả các thông điệp VTP:

* Phiên bản giao thức VTP – 1 hoặc 2.
* Kiểu thông điệp VTP – 1 trong 4 kiểu.
* Độ dài tên của management domain.
* Tên mamagement domain.

Hình 2.8: VTP domain.



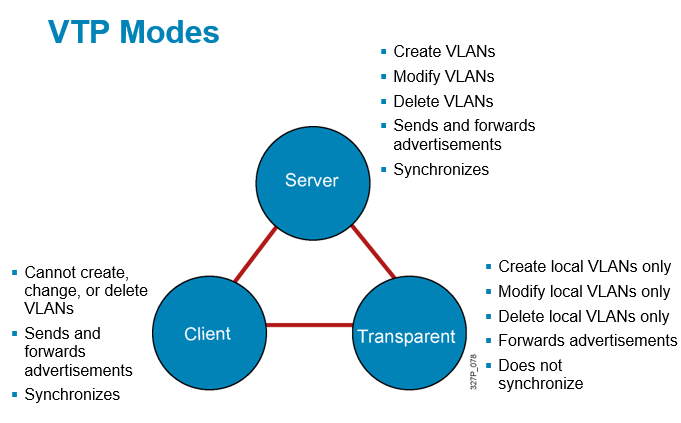
VTP mode:

Server: switch hoạt động ở mode này có toàn quyền quyết định tạo, xóa, sửa thông tin VLAN. Đồng bộ thông tin VLAN từ các Switch khác, Forward thông tin VLAN đến các Switch khác.

Client: switch hoạt động ở mode này không được thay đổi thông tin VLAN mà chỉ nhận thông tin VLAN từ Server. Đồng bộ thông tin VLAN từ switch khác và forward thông tin VLAN.

Transparent: switch hoạt động ở mode này không tiến hành tiếp nhận thông tin VLAN. Nó vẫn nhận được thông tin VLAN từ các Switch khác nhưng không tiến hành đồng bộ thông tin VLAN. Có thể tạo, xóa, sửa VLAN độc lập trên nó. Không gửi thông tin VLAN của bản thân cho các Switch khác nhưng nó có thể forward thông tin VLAN nhận được đến các Switch khác.

Hình 2.9: VTP modes.



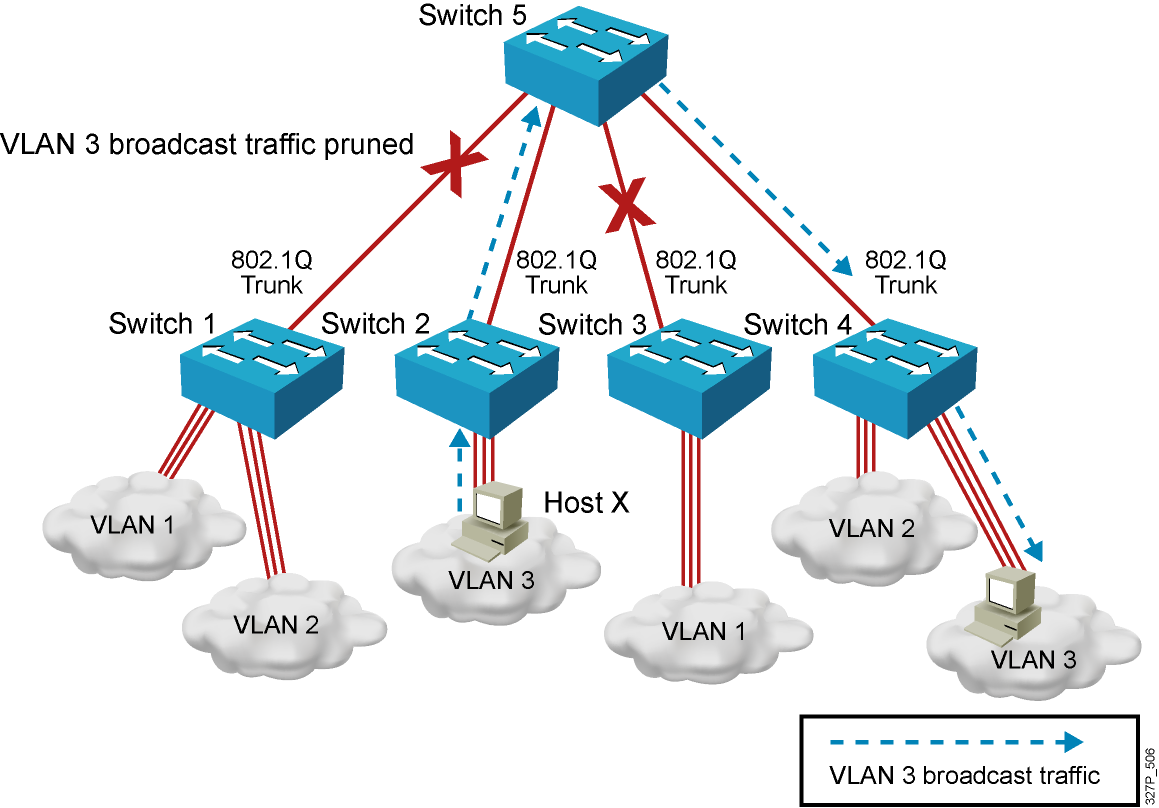
VTP Prunning:

Tính năng hữu ích trong hoạt động trao đổi thông tin giữa các Switch trong mạng chuyển mạch.

Giả sử Host thuộc VLAN 10 tiến hành gửi một Frame đến Host khác cũng thuộc VLAN 10 nhưng nằm trong một Switch khác. Vì mỗi VLAN là một broadcast domain nên frame này sẻ được chuyển đến tất các các host thuộc VLAN 10 của Switch 2. Mặc định trên đường trunk sẽ cho qua dữ liệu của tất cả VLAN nên SW4 cũng nhận được frame này. Khi mà nó không tồn tại VLAN 10 nên việc forward frame đến SW4 gây lãng phí tài nguyên và băng thông hệ thống.

Khi được bật tính năng VTP Prunning. SW4 sẻ gửi thông điệp báo cho SW1 rằng nó không cần dữ liệu của VLAN 10(vì không tồn tại VLAN10). Và khi SW1 khi nhận được frame broadcast này sẻ tiến hành chặn frame này không forward nó qua đường trunk đến các SW không tồn tại VLAN 10(SW4).

Hình 2.10: VTP Prunning.



VTP Server:

Nếu một switch được cấu hình ở chế độ server, thì switch đó có thể khởi tạo, thay đổi và xoá các VLAN. VTP server ghi thông tin cấu hình VLAN trong NVRAM. VTP server gửi các thông điệp VTP qua tất cả các cổng Trunk.

Các VTP server quảng bá cấu hình VLAN tới các switch trên cùng một VTP domain và đồng bộ cấu hình VLAN tới các switch khác dựa trên các quảng cáo nhận được qua đường Trunk.. Đây là chế độ mặc định trên switch.

VTP Client:

Một switch được cấu hình ở chế độ VTP Client không thể khởi tạo, sửa chữa hoặc xoá thông tin VLAN. Thêm nữa, Client không thể lưu thông tin VLAN. Chế độ này có ích cho các switch không đủ bộ nhớ để lưu trữ bảng thông tin VLAN lớn. VTP Client sử lý các thay đổi VLAN giống như server, nó cũng gửi các thông điệp qua các cổng Trunk.

VTP Transparent:

Các switch cấu hình ở chế độ Transparent không tham gia vào VTP. Một VTP Transparent switch không quản bá cấu hình VLAN của nó và không đồng bộ các cấu hình VLAN của nó dựa trên các quảng cáo nhận được. Chúng chuyển tiếp các quảng cáo VTP nhận được trên các cổng Trunk nhưng bỏ qua các thông tin bên trong thông điệp. Một Transparent switch không thay đổi database của nó, khi các switch nhận các thông tin cập nhật cũng gửi một bản cập nhật chỉ ra sự thay đổi trạng thái VLAN. Trừ khi chuyển tiếp một quảng cáo VTP, VTP bị vô hiệu hoá trên switch được cấu hình ở chế độ Transparent.

2.3.4. Lợi ích của VTP:

VTP có thể bị cấu hình không đúng, khi sự thay đổi được tạo ra. Các cấu hình không đúng có thể tổng hợp trong trường hợp thốg kê các vi phạm nguyên tắc bảo mật. Bởi vì các kết nối của VLAN bị chồng chéo khi các VLAn bị đặt trùng tên. Các cấu hình không đúng này có thể bị cắt kết nối khi chúng được ánh xạ từ một kiểu LAN tới một kiểu LAN khác. VTP cung cấp các lợi ích sau:

* Cấu hình đúng các VLAN qua mạng.
* Hệ thống ánh xạ cho phép 1 VLAn được trunk qua các môi trường truyền hỗn hợp. Giống như ánh xạ các VLAN Ethernet tới đường cáp trục tốc độ cao như ATM, LANE hoặc FDDI.
* Theo dõi chính xác và kiểm tra VLAN.
* Báo cáo động về việc thêm vào các VLAN.
* Dễ dàng cấu hình khi thêm mới VLAN.

Trước khi thiết lập các VLAN trên switch, ta phải setup một management domain trong phạm vi những thứ mà ta có thể kiểm tra các VLAN trong mạng. Các switch trong cùng một management domain chia sẻ thông tin VLAN với các VLAN khác và một switch có thể tham gia vào chỉ một VTP management domain. Các switch ở domain khác không chia sẻ thông tin VTP.

Các switch sử dụng giao thức VTP thì trên mỗi cổng trunk của nó có:

* Management domain.
* Số cấu hình.
* Biết được VLAN và các thông số cụ thể.

CHƯƠNG III  
SPANNING TREE PROTOCOL – STP

Một mạng mạnh mẽ được thiết kế không chỉ đem lại tính hiệu quả cho việc truyền các gói hoặc frame, mà còn phải xem xét làm thế nào để khôi phục hoạt động của mạng một cách nhanh chóng khi mạng xảy ra lỗi. Trong môi trường lớp 3, các giao thức định tuyến sử dụng con đường dự phòng đến mạng đích để khi con đường chính bị lỗi thì sẽ nhanh chóng tận dụng con đường thứ 2. Định tuyến lớp 3 cho phép nhiều con đường đến đích để duy trì tình trạng hoạt động của mạng và cũng cho phép cân bằng tải qua nhiều con đường.

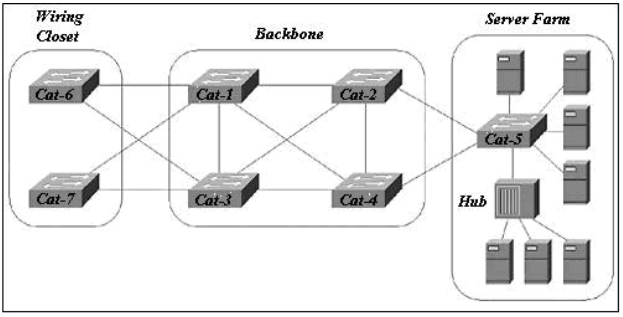
Trong môi trường lớp 2 (switching hoặc bridging), không sử dụng giao thức định tuyến và cũng không cho phép các con đường dự phòng, thay vì bridge cung cấp việc truyền dữ liệu giữa các mạng hoặc các cổng của switch. Giao thức Spanning Tree cung cấp liên kết dự phòng để mạng chuyển mạch lớp 2 có thể khôi phục từ lỗi mà không cần có sự can thiệp kịp thời. STP được định nghĩa trong chuẩn IEEE 802.1D.

3.1. Spanning Tree là gì và tại sao phải sử dụng nó:

Spanning Tree Protocol (STP) là một giao thức ngăn chặn sự lặp vòng, cho phép các bridge truyền thông với nhau để phát hiện vòng lặp vật lý trong mạng. Sau đó giao thức này sẽ định rõ một thuật toán mà bridge có thể tạo ra một cấu trúc mạng logic chứa vòng lặp (loop-free). Nói cách khác STP sẽ tạo một cấu trúc cây của free-loop gồm các lá và các nhánh nối toàn bộ mạng lớp 2.

Vòng lặp xảy ra trong mạng với nhiều nguyên nhân. Hầu hết các nguyên nhân thông thường là kết quả của việc cố gắng tính toán để cung cấp khả năng dự phòng, trong trường hợp này, một liên kết hoặc switch bị hỏng, các liên kết hoặc switch khác vẫn tiếp tục hoạt động, tuy nhiên các vòng lặp cũng có thể xảy ra do lỗi. *Hình 3.1* biểu diễn một mạng chuyển mạch với các vòng lặp cố ý được dùng để cung cấp khả năng dự phòng như thế nào.

Hình 3.1: Bridging loop trong mạng.

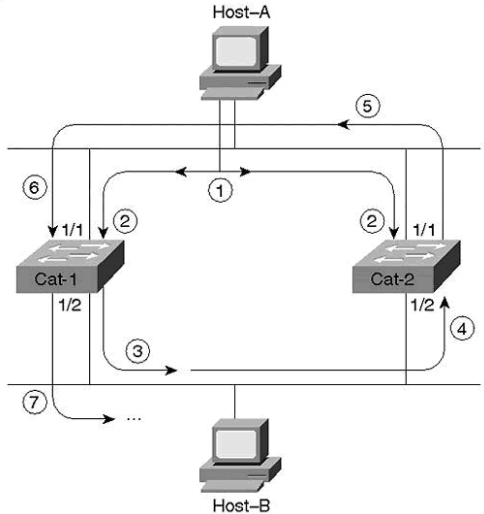


Hai nguyên nhân chính gây ra sự lặp vòng tai hại trong mạng chuyển mạch là do broadcast và sự sai lệch của bảng bridge.

Vòng lặp broadcast

Vòng lặp broadcast và vòng lặp lớp 2 là một sự kết hợp nguy hiểm. *Hình 3.2* biểu diễn broadcast tạo ra vòng lặp phản hồi (feedback loop).

Hình 3.2: Không có STP, broadcast tạo feedback loop.

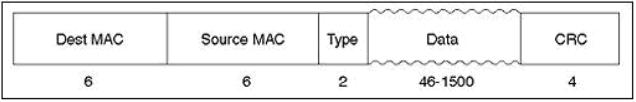


Giả sử rằng, không có switch nào chạy STP:

* Bước 1: host A gửi một frame bằng địa chỉ broadcast (FF-FF-FF-FF-FFFF).
* Bước 2: frame đến cả hai Cat-1 và Cat-2 qua cổng 1/1.
* Bước 3: Cat-1 sẽ đưa frame qua cổng 1/2.
* Bước 4: frame được truyền đến tất cả các nút trên đoạn mạng Ethernet kể cả cổng 1/2 của Cat-2.
* Bước 5: Cat-2 đưa frame này đến cổng 1/1 của nó.
* Bước 6: một lần nữa, frame xuất hiện cổng 1/1 của Cat-1.
* Bước 7: Cat-1 sẽ gửi frame này đến cổng 1/2 lần hai. Như vậy tạo thành một vòng lặp ở đây.

Chú ý: frame này cũng tràn qua đoạn mạng Ethernet và tạo thành một vòng lặp theo hướng ngược lại, vòng lặp feedback xảy ra ở cả hai hướng. Một kết luận quan trọng nữatrong hình 3.2 là vòng lặp bridge nguy hiểm hơn nhiều so với vòng lặp định tuyến.

Hình 3.3: Mô tả định dạng của một DIXv2 Ethernet frame.



DIXv2 Ethernet Frame chỉ chứa 2 địa chỉ MAC, một trường Type và một CRC. Trong IP header chứa trường time-to-live (TTL) được thiết lập tại host gốc và nó sẽ được giảm đi 1 mỗi khi qua một router. Gói sẽ bị loại bỏ nếu TTL = 0, điều này cho phép các router ngăn chặn các datagram bị “run-away”. Không giống như IP, Ethernet không có trường TTL, vì vậy sau khi một frame bắt đầu bị lặp trong mạng thì nó vẫn tiếp tục cho đến khi ai đó ngắt một trong các bridge hoặc ngắt một kiên kết.

Trong một mạng phức tạp hơn mạng được mô tả trong *hình 3.1, và 3.2* thì có thể gây ra vòng lặp feedback rất nhanh theo tỉ lệ số mũ. Vì cứ mỗi frame tràn qua nhiều cổng của switch, thì tổng số frame tăng nhanh rất nhiều.

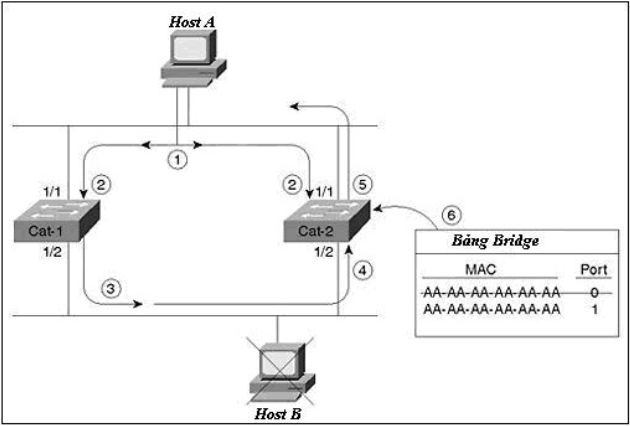
Ngoài ra cần phải chú ý đến cơn bão broadcast trên người dùng của host A và B trong *hình 3.2*. Broadcast được xử lý bởi CPU ở tất cả các thiết bị trên mạng. Trong trường hợp này, các PC đều cố xử lý bão broadcast. Nếu ta ngắt một trong số các kết nối, thì nó trở lại hoạt động bình thường. Tuy nhiên, ngay khi ta kết nối nó trở lại thì broadcast sẽ sử dụng 100% CPU. Nếu ta không xử lý điều này mà vẫn tiếp tục sử dụng mạng, thì sẽ tạo ra vòng lặp vật lý trong mạng.

Việc sai lệch bảng bridge

Nhiều nhà quản trị switch/bridge đã nhận thức vấn đề cơ bản của bão broadcast, tuy nhiên ta phải biết rằng thậm chí các unicast frame cũng có thể truyền mãi trong mạng mà chứa vòng lặp*. Hình 3.4* mô tả điều này.

* Bước 1: host A muốn gửi gói unicast đến host B, tuy nhiên host B đã rời khỏi mạng, và đúng với bảng bridge của switch không có địa chỉ của host B.
* Bước 2: giả sử rằng cả hai switch đều không chạy STP, thì frame đến cổng 1/1 trên cả hai switch.
* Bước 3: vì host B bị down, nên Cat-1 không có địa chỉ MAC (BB-BB-BBBB-BB BB) trong bảng bridge, và nó tràn frame qua các cổng.
* Bước 4: Cat-2 nhận được frame trên cổng 1/2 . Có 2 vấn đề xảy ra:
* Bước 5: Cat-2 tràn frame vì nó không học địa chỉ MAC BB-BB-BBBB-BB-BB, điều này tạo ra feedback loop và làm down mạng.
* Cat-2 chú ý rằng, nó chỉ nhận một frame trên cổng 1/2 với địa chỉ MAC là AA-AA-AA-AA-AA-AA. Nó thay đổi địa chỉ MAC của host A trong bảng bridge dẫn đến sai cổng.

Hình 3.4: frame unicast cũng có thể gây ra Bridging Loop và sai lệch bảng bridge.



Vì frame bị lặp theo hướng ngược lại, nên ta thấy địa chỉ MAC của host A bị lẫn giữa cổng 1/1 và 1/2. Điều này không chỉ làm mạng bị tràn với các gói unicast mà còn sửa sai bảng bridge. Như vậy không chỉ có broadcast mới làm hư hại mạng.

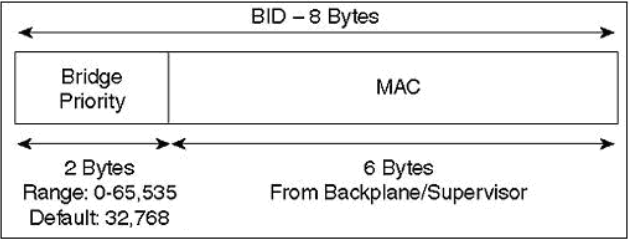
3.2. Hai khái niệm cơ bản của STP:

Việc tính toán Spanning Tree dựa trên hai khái niệm khi tạo ra vòng lặp logic trong cấu trúc mạng đó là: Bridge ID (BID) và chi phí đường đi.

Bridge ID (BID)

BID là một trường có 8 byte, nó gồm có 2 trường con được miêu tả như hình 3.5 sau:

Hình 3.5: Hai trường của BID.



Trong đó:

* Địa chỉ MAC: có 6 byte được gán cho switch. Catalyst 5000 và 6000 sử dụng một trong số các địa chỉ MAC từ vùng 1024 địa chỉ gán cho mỗi giám sát viên (supervisor) và bảng nối đa năng (backplane). Địa chỉ MAC trong BID sử dụng định dạng hexa.

Chú ý: một vài Catalyst lấy địa chỉ MAC từ module giám sát (như Catalyst 5000) và lấy địa chỉ khác từ backplane (như Catalyst 5500 và 6000)

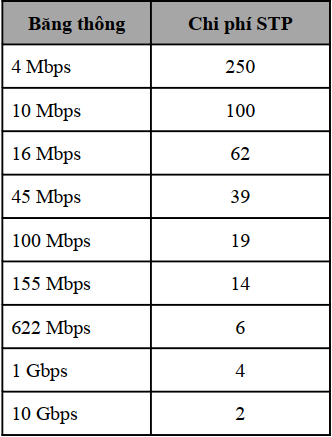
* Bridge Priority: là độ ưu tiên bridge có 2 byte tạo thành 216 giá trị từ 0 - 65.535. Độ ưu tiên bridge có giá trị mặc định là giá trị ở khoảng giữa (32.768).

Chú ý: ta chỉ tập trung vào phiên bản IEEE của giao thức Spanning Tree. Mặc dù về cơ bản là như nhau nhưng có một vài điểm khác biệt giữa IEEE STP và DEC STP như DEC STP sử dụng 8 bit Bridge priority.

Chi phí đường đi

Bridge sử dụng khái niệm chi phí để đánh giá các bridge khác. 802.1D định nghĩa chi phí là 1000 Mbps bằng cách chia băng thông của liên kết. Ví dụ như một liên kết 10BaseT có chi phí là 100 (1000/10), Fast Ethernet và FDDI sử dụng chi phí là 10 (1000/100). Tuy nhiên với việc gia tăng của Gigabit Ethernet và OC-48 ATM (2,4Gbps), thì chi phí được lưu trữ là một giá trị nguyên mà không phải là phân số. Ví dụ như kết quả OC-48 ATM trong 1000/2400 Mbps= 41667 bps, một giá trị chi phí không hợp lệ. Do đó các chi phí lớn hơn hoặc bằng 1 Gbps thì có chi phí là 1, tuy nhiên điều này ngăn cản STP lựa chọn chính xác “con đường tốt nhất” trong mạng Gigabit.

Để giải quyết tình trạng khó xử này, IEEE quyết định sửa đổi chi phí để sử dụng tính co dãn không tuyến tính. *Bảng 3.1* cho ta một danh sách giá trị chi phí mới.



Giá trị trong *bảng 3.1* được chọn cẩn thận để sơ đồ hoạt động cũ và mới có tốc độ liên kết nhanh như hiện nay. Một điểm chú ý là giá trị chi phí STP càng thấp càng tốt.

3.3. Các bước ra quyết định của STP:

Khi tạo ra cấu trúc mạng logic chứa vòng lặp (loop-free) thì Spanning Tree luôn dùng trình tự bốn bước sau:

* BID gốc (Root BID) thấp nhất.
* Chi phí đường đi đến Bridge gốc thấp nhất.
* BID của người gửi thấp nhất.
* ID của cổng (PortID) thấp nhất.

Bridge trao đổi thông tin Spanning Tree với nhau, sử dụng frame xác định là đơn vị dữ liệu giao thức bridge (Bridge Protocol Data Unit - BPDU). Một bridge sử dụng trình tự bốn bước này để lưu một bản sao của BPDU tốt nhất trên mỗi cổng. Khi đánh giá, nó xem tất cả BPDU nhận được trên cổng cũng như BPDU gửi đi trên cổng đó. Mỗi BPDU đến đều được kiểm tra theo trình tự bốn bước này, nếu tốt hơn BPDU hiện tại thì nó được lưu lại cổng đó và thay thế giá trị cũ.

Chú ý: các bridge sẽ gửi BPDU cấu hình cho đến khi nhận nhiều hơn một BPDU tốt.

Thêm vào đó, quá trình lưu lại BPDU tốt nhất cũng điều khiển việc gửi các BPDU. Khi một bridge lần đầu tiên hoạt động, thì tất cả các cổng của nó được gửi BPDU 2s một lần (đây là giá trị mặc định của bộ định thời). Tuy nhiên, nếu một cổng lắng nghe một BPDU từ một bridge khác tốt hơn BPDU mà nó gửi, thì cổng sẽ ngưng gửi BPDU. Nếu BPDU này từ một lân cận ngưng đến trong một khoảng thời gian (20 s là mặc định) thì cổng tiếp tục gửi BPDU lại lần nữa.

Chú ý: có 2 loại BPDU là BPDU cấu hình và BPDU thông báo thay đổi cấu trúc mạng (TCN).

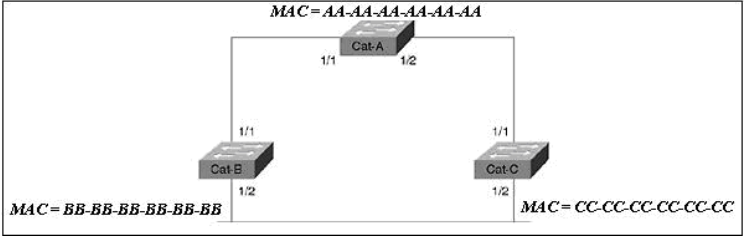
3.4. Sự hội tụ của STP ban đầu (Initial STP Convergence):

Khi một mạng khởi động lần đầu, tất cả các bridge thông báo thông tin BPDU một cách lộn xộn. Tuy nhiên, các bridge này sẽ lập tức áp dụng trình tự bốn bước (*ở phần 3.1.3*). Một bridge gốc được quyết định để hoạt động như là “trung tâm của vạn vật” đối với mạng. Tất cả các bridge còn lại tính toán việc thiết lập các cổng gốc và các cổng chỉ định để xây dựng cấu trúc mạng chứa loop-free. Kết quả là bridge gốc giống như một hub với các đường đi loop-free ra bên ngoài. Khi mạng có trạng thái ổn định, thì bridge gốc sẽ gửi các BPDU đến mỗi đoạn mạng.

Sau khi mạng hội tụ trên cấu trúc mạng loop-free, nếu có thêm sự thay đổi thì sẽ sử dụng quá trình thay đổi cấu trúc mạng.

*Hình 3.6* là mô hình của một mạng switch/bridge. Mạng này gồm có ba bridge kết nối thành một vòng lặp. Mỗi cầu nối được gán một địa chỉ MAC không có thật tương ứng với tên thiết bị (ví dụ như Cat-A sử dụng địa chỉ MAC là AA-AA-AA-AA-AA-AA).

Hình 3.6: Mô hình mạng sử dụng STP.



Bước 1: Quyết định một bridge gốc.

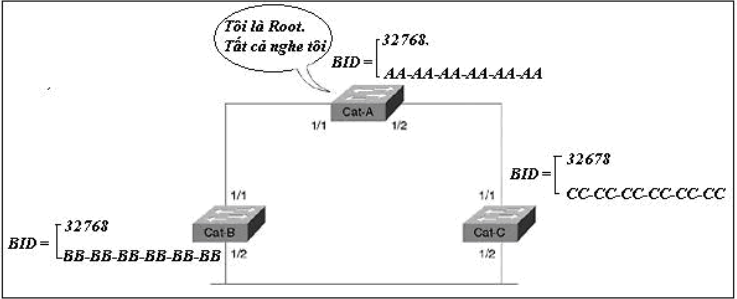
Đầu tiên các switch cần chọn một bridge gốc bằng cách tìm bridge có BID thấp nhất.

Chú ý: nhiều tài liệu sử dụng tính ưu tiên cao nhất khi nói đến kết quả của quá trình chọn bridge gốc. Tuy nhiên, bridge với tính ưu tiên cao nhất thực tế có giá trị thấp nhất. Để tránh nhầm lẫn, tài liệu này luôn đề cập đến giá trị thấp nhất.

Như đã nói đến ở phần trên BID là một định danh 8 byte được chia thành 2 trường con là Bridge Priority và địa chỉ MAC từ người giám sát (supervisor) hoặc backplane. Trở lại *hình 3.6*, ta thấy Cat-A có BID mặc định là 32.768 và địa chỉ MAC là AA AAAA-AA-AA-AA. Cat-B là (32.768, BB-BB-BB-BB-BB-BB) và Cat-C là (32.768, CCCC-CC-CC-CC-CC). Vì cả ba bridge đều sử dụng Bridge Priority là 32.678 nên địa chỉ MAC thấp nhất là AA-AA-AA-AA-AA-AA và Cat-A trở thành Bridge gốc. *Hình 3.7* mô tả quá trình này.

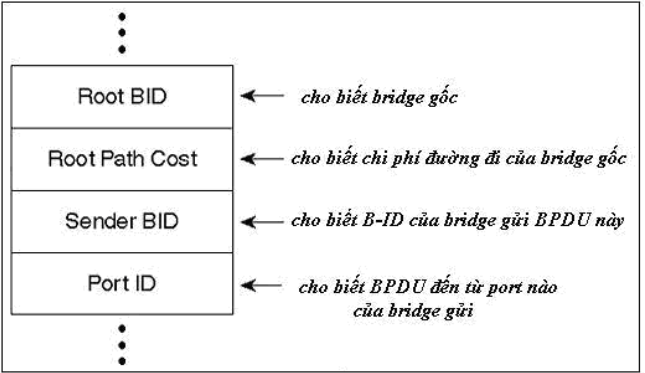
Chú ý: giá trị BID cũng là thấp nhất.

Hình 3.7: Chọn Bridge Root.



Như đã nói đến ở phần trên BID là một định danh 8 byte được chia thành 2 trường con là Bridge Priority và địa chỉ MAC từ người giám sát (supervisor) hoặc backplane. Trở lại *hình 3.6*, ta thấy Cat-A có BID mặc định là 32.768 và địa chỉ MAC là AA AAAA-AA-AA-AA. Cat-B là (32.768, BB-BB-BB-BB-BB-BB) và Cat-C là (32.768, CCCC-CC-CC-CC-CC). Vì cả ba bridge đều sử dụng Bridge Priority là 32.678 nên địa chỉ MAC thấp nhất là AA-AA-AA-AA-AA-AA và Cat-A trở thành Bridge gốc. *Hình 3.7* mô tả quá trình này.

Hình 3.8: Các thành phần cơ bản của BPDU.



Mục đích việc chọn bridge gốc chỉ liên quan đến trường Root BID và Sender BID. Khi một bridge phát ra một BPDU 2s một lần, ngay tức khắc nó sẽ xác định bridge gốc dựa vào trường Root BID. Bridge này luôn đặt BID của chính nó trong Sender BID.

Chú ý: Root BID là ID của bridge gốc hiện tại, trong khi Sender BID là ID của bridge cục bộ hoặc switch.

Khi bridge khởi động lần đầu tiên, nó luôn luôn đặt BID trong cả hai trường Root BID và Sender BID. Giả sử rằng, Cat-B khởi động đầu tiên và bắt đầu gửi các BPDU thông báo chính nó là Bridge gốc 2s một lần. Một vài phút sau Cat-C khởi động và thông báo chính nó là Bridge gốc. Khi BPDU của Cat-C đến Cat-B, Cat-B sẽ loại bỏ BPDU vì nó có B-ID thấp hơn được lưu trên các cổng của nó. Ngay lập tức Cat-B truyền BPDU, Cat-C biết được là giả định ban đầu của nó là sai. Tại thời điểm đó, Cat-C bắt đầu gửi BPDU với Root BID là B và Sender BID là C. Bây giờ mạng chấp nhận B là Bridge gốc.

Năm phút sau đó, Cat-A khởi động, nó giả sử rằng nó là bridge gốc và bắt đầu quảng bá điều này trong BPDU. Ngay lập tức các BPDU đến Cat-B và C, các switch này sẽ nhường bridge gốc lại cho Cat-A. Bây giờ tất cả 3 switch đều gửi các BPDU thông báo Cat-A là bridge gốc và chính nó là Sender BID.

Bước 2: Chọn cổng gốc.

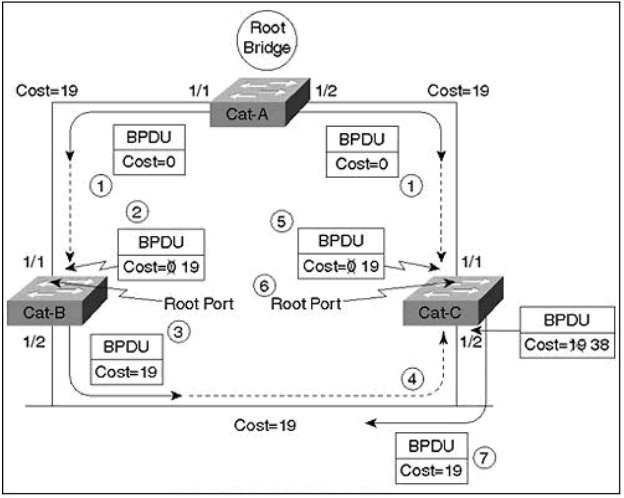
Sau khi xác định được bridge gốc, thì các switch sẽ chuyển qua chọn cổng gốc. Cổng gốc là một cổng trên bridge cục bộ. Mỗi brigde (trừ bridge gốc) phải lựa chọn một cổng gốc.

Chú ý: Mỗi bridge( trừ bridge gốc) sẽ lựa chọn cổng gốc.

Bridge sẽ sử dụng khái niệm chi phí để xét cổng gốc. Cụ thể là các bridge theo dõi chi phí đường đi gốc, chi phí tích lũy của tất cả các liên kết đến bridge gốc. *Hình 3.9* mô tả làm thế nào tính toán qua nhiều bridge và kết quả của việc quyết định cổng gốc.

* (1): khi Cat-A (bridge gốc) gửi các BPDU, thì nó chứa chi phí đường đi gốc là 0.
* (2): khi B nhận các BPDU này, nó thêm vào chi phí đường đi của cổng 1/1vào chi phí đường đi gốc chứa trong BPDU nhận. Giả sử rằng mạng đang chạy switch Catalyst 5000 có mã lớn hơn phiên bản 2.4 và ba liên kết trong *hình 3.9* đều là Fast Ethernet. Cat-B nhận chi phí đường đi gốc là 0 và thêm vào chi phí của cổng 1/1 là 19.
* (3): sau đó Cat-B sử dụng giá trị 19 và gửi BPDU với chi phí đường đi gốc là 10 ra cổng 1/2.
* (4): khi Cat-C nhận BPDU này từ B, thì nó tăng chi phí đường đi gốc thành 38 (19+19).
* (5): tuy nhiên Cat-C cũng nhận BPDU từ bridge gốc trên cổng 1/1. Cat-C sẽ thêm vào cổng 1/1 với chi phí là 0, và ngay lập tức nó tăng chi phí lên 19.
* (6): Cat-C thấy chi phí đường đi gốc là 19 trên cổng 1/1 và 38 trên cổng 1/2, nó quyết định cổng 1/1 là cổng gốc (chọn giá trị nhỏ nhất).
* (7): sau đó Cat-C bắt đầu quảng bá chi phí đường đi gốc với giá trị 19 đến các switch xuôi dòng.

Hình 3.9: Chọn Root Port.



Hình 3.9 biểu diễn Cat-B tính toán và chọn cổng 1/1 là cổng gốc với chi phí là 19, và chú ý là khi một cổng nhận BPDU thì chi phí sẽ giảm dần.

Chú ý:

Chi phí STP được tăng khi một cổng nhận BPDU, chứ không phải vì nó được gửi ra khỏi cổng. Ví dụ như, các BPDU đến trên cổng 1/1 của Cat-B với chi phí là 0 và tăng lên 19 bên trong Cat-B.

Sự khác nhau giữa chi phí đường đi và chi phí đường đi gốc.

Chi phí đường đi là giá trị được gán cho mỗi cổng, nó được thêm vào các BPDU được nhận trên cổng đó để tính toán chi phía đường đi gốc.

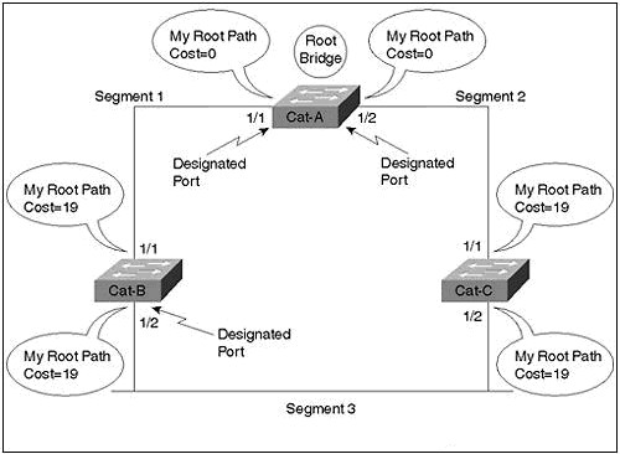
Chi phí đường đi gốc là chi phí tích lũy đến bridge gốc. Trong BPDU, đây là giá trị của trường chi phí. Đối với một bridge, giá trị này được tính bằng cách cộng các chi phí đường đi của các cổng nhận với giá trị chứa trong BPDU.

Bước 3: Quyết định cổng được chỉ định.

Mỗi đoạn mạng trên một bridge có một cổng được chỉ định, cổng này có chức năng nhận và gửi lưu lượng đến đoạn mạng kia và bridge gốc. Nếu chỉ có một cổng nắm giữ lưu lượng trên mỗi liên kết, thì tất cả vòng lặp bị phá bỏ. Bridge chứa cổng được chỉ định được gọi là designated bridge cho đoạn mạng đó.

Việc lựa chọn cổng được chỉ định dựa trên chi phí tích lũy của đường đi gốc đến bridge gốc.

Hình 3.10: Chọn Designated Port.



Để xác định cổng được chỉ định, ta hãy nhìn vào mỗi đoạn mạng. Đầu tiên là đoạn 1, liên kết giữa Cat-A và B có 2 cổng là Cat-A: cổng 1/1, và Cat-B: cổng 1/1. Cổng 1/1 của Cat-A có chi phí đường đi gốc là 0, và cổng 1/1 của B là 19 (giá trị 0 được nhận trong BPDU từ A cộng với chi phí đường đi được gán cho cổng 1/1 của B). Vì cổng 1/1 của A có chi phí đường đi thấp hơn nên nó trở thánh cổng được chỉ định đối với liên kết này.

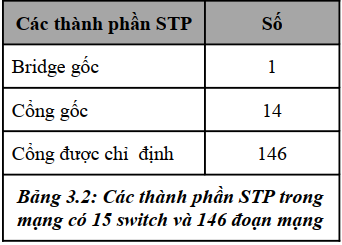
Đối với đoạn mạng 2 (kiên kết giữa Cat-A và C), tương tự cổng 1/2 của A trở thành cổng được chỉ định. Chú ý là mỗi cổng hoạt động trên bridge gốc đều trở thành cổng được chỉ định.

Bây giờ hãy xem đoạn 3 (liên kết giữa Cat-B và C), cả hai cổng 1/2 của B và 1/2 của C đều có chi phí đường đi gốc là 19. Đây là một sự hạn chế, và STP thường sử dụng trình tự bốn bước để quyết định:

* B-ID gốc thấp nhất.
* Chi phi đường đi đến bridge gốc thấp nhất.
* Sender BID thấp nhất.
* ID của cổng thấp nhất.

Trong ví dụ ở *hình 3.10*, tất cả các bridge đều tán thành Cat-A là Bridge gốc, cả B và C đều có chi phí là 19, nên ta sẽ lấy yếu tố BID để quyết định. BID của B là (32.768.BBBB-BB-BB-BB-BB) và của C là (32.768.CC-CC-CC-CC-CC-CC), do đó cổng 1/2 của B là Cổng được chỉ định cho đoạn 3.

Ví dụ trong một mạng chứa 15 switch và có 146 đoạn mạng (mỗi cổng là một đoạn mạng duy nhất), số thành phần STP hiện có là:



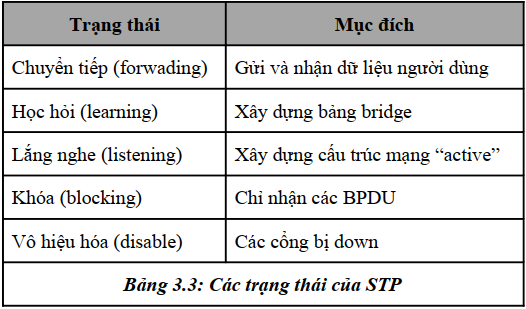
Tất cả các quyết định STP đều dựa trên một trình tự như đã đề cập:

* BID gốc thấp nhất.
* Chi phí đường đi đến bridge gốc thấp nhất.
* Sender BID thấp nhất.
* ID của cổng thấp nhất.

Khi một cổng nhận BPDU nó sẽ so sánh với các BPDU nhận được trên các cổng khác (cũng như BPDU được gửi trên cổng đó). Chỉ BPDU tốt nhất mới được lưu lại. Tốt nhất ở đây có nghĩa là giá trị thấp nhất (ví dụ như BID thấp nhất trở thành Bridge gốc, giá trị thấp nhất cũng được sử dụng để chọn cổng gốc và cổng được chỉ định). Một cổng sẽ ngưng truyền BPDU nếu nó nghe được một BPDU tốt hơn BPDU của nó.

3.5. Các trạng thái của STP:

Sau khi bridge phân chia được các cổng như cổng gốc, cổng được chỉ định và cổng không được chỉ định, thì việc tạo ra cấu trúc mạng chứa loop-free không phức tạp lắm, cổng gốc và cCổng được chỉ định chuyển tiếp lưu lượng, trong khi cổng không được chỉ định thì khóa lưu lượng. Việc chuyển tiếp và khóa chỉ là 2 trạng thái thông thường trong mạng, *bảng 3.3* mô tả 5 trạng thái của STP.



Trạng thái “disable” cho phép người quản trị mạng quản lý việc ngừng hoạt động của một cổng. Sau khi khởi tạo, các cổng bắt đầu trong trạng thái “blocking” để lắng nghe các BPDU.

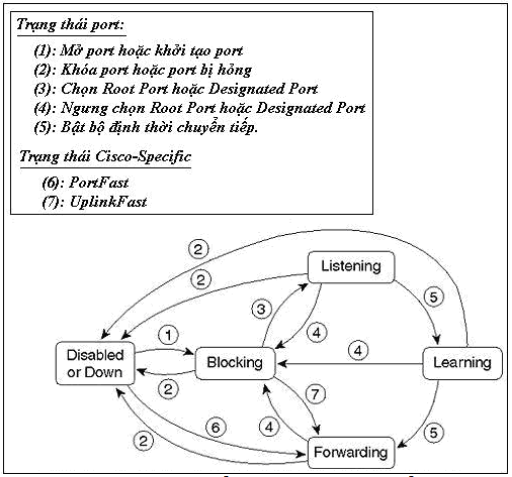
Do sự đa dạng của các sự kiện mà bridge truyền trong trạng thái “listening” (ví dụ như một bridge nghĩ nó là bridge gốc ngay sau khi khởi động). Ở trạng thái này, không có dữ liệu người dùng được truyền qua, tức là cổng đang gửi và nhận các BPDU để cố gắng tạo cấu trúc mạng hoạt động. Trong trạng thái “listening” sẽ sử dụng ba bước hội tụ đã nói ở trên, các cổng bị mất quyền cổng được chỉ định sẽ trở thành cổng không được chỉ định và trở lại trạng thái “blocking”.

Các cổng được chỉ định và cổng gốc sau 15s (giá trị mặc định của bộ định thời) sẽ chuyển qua trạng thái “learning”. Trong khoảng 15s khác, bridge vẫn không chuyển các frame của người dùng qua, mà xây dựng bảng bridge của nó. Khi bridge nhận frame, nó đưa địa chỉ MAC và cổng vào bảng bridge. Trạng thái “learning” sẽ giảm bớt số lượng tràn ngập khi việc chuyển tiếp dữ liệu bắt đầu.

Chú ý: Trong việc lưu trữ địa chỉ MAC và thông tin cổng, các Catalyst học các thông tin như VLAN nguồn.

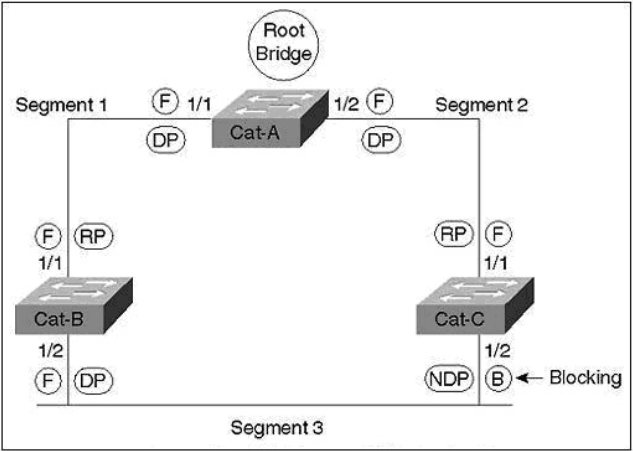
Nếu một cổng vẫn là cổng được chỉ định hay cổng gốc ở khoảng thời gian cuối của trạng thái “learning”, thì cổng chuyển qua trạng thái “forwading”. Ở trạng thái này, nó bắt đầu gửi và nhận các frame của người dùng. *Hình 3.11* mô tả trạng thái các cổng và việc chuyển trạng thái.

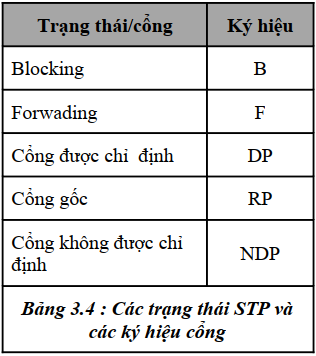
Hình 3.11: Trạng thái các cổng và hoạt động chuyển trạng thái.



*Hình 3.12* biểu diễn mạng với sự phân chia cổng và danh sách các trạng thái. Chú ý là tất cả các cổng đều chuyển tiếp trừ cổng 1/2 của Cat-C.

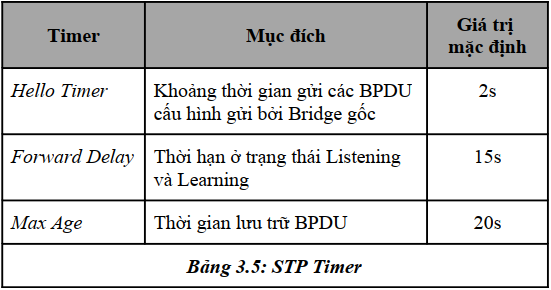
Hình 3.12: Sơ đồ mạng với các cổng được định danh.





3.6. Bộ định thời gian STP:

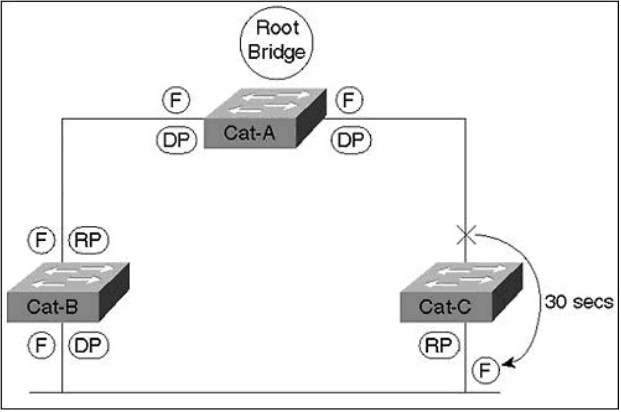
Một bridge trải qua 15s ở mỗi trạng thái “listening” và “learning”. STP được điều khiển bởi ba bộ đếm thời gian (timer) như trong *bảng 3.5.*



Ví dụ: giả sử rằng liên kết đoạn 3 trong hình 3.12 sử dụng một hub và cổng 1/2 của Cat-B truyền ra ngoài. Cat-C không thông báo lỗi liền vì nó vẫn đang nhận liên kết Ethernet từ hub. Cat-C chỉ thông báo là các BPDU ngừng đến. Sau 20s (Max Age), thì cổng 1/2 của Cat-C lấy thông tin BPDU cũ với cổng 1/2 của Cat-B là cổng được chỉ định cho đoạn mạng 3. Điều này làm cho cổng 1/2 của Cat-C truyền trong trạng thái “listening” để cố gắng trở thành cổng được chỉ định. Vì vậy cổng 1/2 của Cat-C cung cấp truy cập tốt nhất từ bridge gốc đến liên kết này, nên nó chuyển sang trạng thái “forwarding”. Như vậy, Cat-C mất 50s (20s Max Age + 15s Listenning + 15s Forwarding) để vượt qua sau khi cổng 1/2 trên Cat-B bị lỗi.

Trong trường hợp này, các bridge có thể phát hiện sự thay đổi cấu trúc mạng trên các liên kết kết nối trực tiếp và ngay lập tức chuyển sang trạng thái “listening” mà không cần chờ thời gian Max Age. Xem ví dụ trong hình 3.13.

Hình 3.13: Lỗi xảy ra trên liên kết giữa Root bridge và Root port của Cat-C.



Trong trường hợp này, cổng 1/1 của Cat-C bị lỗi, vì liên kết trên cổng gốc cũng bị lỗi nên ngay lập tức cổng 1/2 của Cat-C chuyển sang trạng thái “learning” để trở thành cổng gốc mới thay vì chờ 20s rồi mới lấy thông tin cũ. Điều này làm cho thời gian hội tụ STP giảm từ 50s xuống 30s (15s listening + 14s learning).

Chú ý: thời gian hội tụ STP từ 30s đến 50s.

Hai điểm quan trọng cần nhớ khi sử dụng bộ định thời gian STP là:

* Thứ nhất: không thay đổi giá trị thời gian mật định khi không có sự cân nhắc cẩn thận.
* Thứ hai: ta chỉ được sửa thời gian từ bridge gốc.

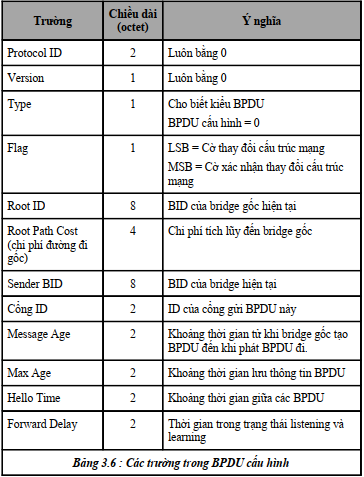
3.7. Hai loại BPDU:

Có hai loại BPDU là :

* BPDU cấu hình.
* BPDU thay đổi cấu trúc mạng – TCN BPDU (Topology Change Notification BPDU).

BPDU cấu hình được bắt đầu bởi bridge gốc và phát ra trên các con đường hoạt động từ bridge gốc, còn TCN BPDU hướng về bridge gốc để cảnh báo với bridge gốc là cấu trúc mạng mạng có sự thay đổi.

BPDU cấu hình : các trường trong BPDU cấu hình được tóm tắt trong bảng 3.6.



TCN BPDU (Topology Change Notification BPDU) :

TCN BPDU đơn giản hơn BPDU cấu hình và chỉ gồm có ba trường, giống như ba trường đầu tiên của BPDU cấu hình nhưng trường Type thì thay đổi với giá trị như sau.

* 0x00 (0000 0000): BPDU cấu hình.
* 0x80 (1000 0000): TCN BPDU.

Chú ý : TCN BPDU không mang bất cứ thông tin bổ sung nào.

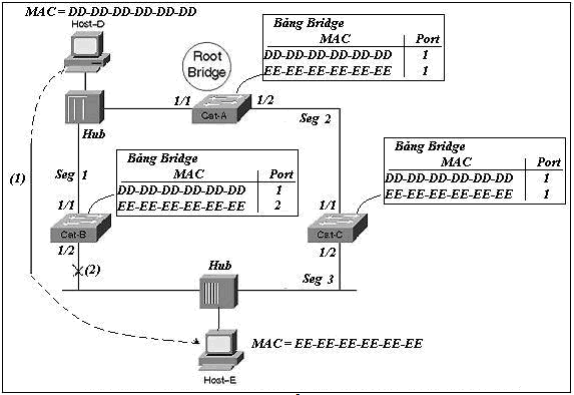
3.8. Quá trình thay đổi cấu trúc mạng:

Nếu TCP BPDU đơn giản thì làm thế nào nó thể hiện được vai trò quan trọng của nó? Ta hãy xem xét sự thay đổi cấu trúc mạng trong hình 3.14.

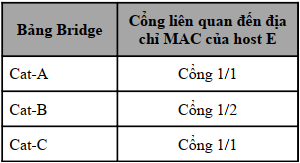
Host D đang liên lạc với host E qua hai bước:

* (1): lưu lượng từ host D qua Cat-B để liên lạc với host E.
* (2): giả sử bộ thu phát trên cổng 1/2 của Cat-B bị hỏng.

Hình 3.14: TCN BPDU được dùng để cập nhật bảng bridge nhanh hơn.



Như đã thảo luận, cổng 1/2 của Cat-C mất 50s để trở thành cổng được chỉ định. Tuy nhiên nếu không có TCN BPDU thì nó tiếp tục bị ngắt khoảng 250s. Trong khoảng thời gian lỗi, cả ba switch đều chứa địa chỉ MAC của host E trong bảng Bridge như bảng 3.7.



TCN BPDU là một phương pháp đơn giản để cải tiến thời gian hội tụ, và nó làm việc chặt chẽ với BPDU cấu hình như sau:

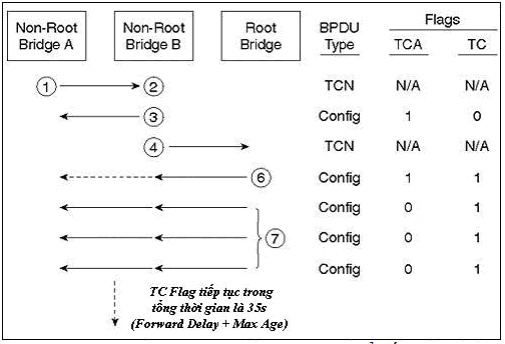
1. Một bridge bắt đầu một TCN BPDU khi:

* Nó chuyển một cổng sang trạng thái “forwarding” và nó có ít nhất một cổng được chỉ định.
* Nó chuyển một cổng từ trạng thái “forwarding” hoặc “learning” sang blocking.

Sự thay đổi cấu trúc mạng đòi hỏi phải gửi thông báo đến bridge gốc, giả sử rằng bridge hiện tại không phải là bridge gốc, thì nó bắt đầu quá trình thông báo bằng cách gửi TCN BPDU ra cổng gốc của nó. Nó tiếp tục gửi TCN BPDU cho đến khi thông điệp TCN được xác nhận.

1. Bridge upstream sẽ nhận TCN BPDU. Mặc dù, một vài bridge nghe được TCN BPDU (vì nó kết nối trực tiếp vào cổng gốc của đoạn mạng) nhưng chỉ có cổng được chỉ định chấp nhận và xử lý TCN BPDU.
2. Bridge upstream sẽ thiết lập cờ xác nhận thay đổi cấu trúc mạng TCA (Topology Change Acknowledgement) trong BPDU cấu hình kế tiếp được gửi ngược lại(ra cổng được chỉ định). Cờ này dùng để xác nhận với bridge khởi đầu để nó ngưng phát TCN BPDU.
3. Bridge upstream sẽ truyền TCN BPDU ra cổng gốc của nó.
4. Tiếp tục bước 2 đến bước 4 cho đến khi bridge gốc nhận TCN BPDU.
5. Sau đó bridge gốc sẽ thiết lập cờ xác nhận thay đổi cấu trúc mạng – TCA (để xác nhận với bridge trước đó), và cờ thay đổi cấu trúc mạng – TC (Topology Change) trong BPDU cấu hình mà nó sẽ gửi đi.
6. Bridge gốc tiếp tục thiết lập cờ thay đổi cấu trúc mạng – TC trong tất cả các BPDU cấu hình mà nó gửi ra ngoài với tổng thời gian là 35s (Forward Delay + Max Age). Cờ này sẽ thu ngắn giá trị 300s xuống 15s (tức độ trễ chuyển tiếp - Forward Delay).

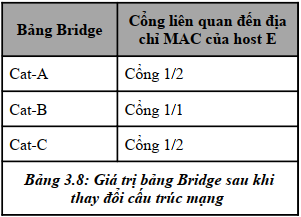
Hình 3.15: Trình tự các bước trong quá trình thay đổi cấu trúc mạng.



Dựa vào hình 3.15 ta có thể biết được quá trình thay đổi cấu trúc mạng cho hình 3.14 như sau: bước 1 Cat-B và C gửi TCN BPDU ra cổng 1/1. Vì bridge upstream cũng là bridge gốc nên bỏ qua bước 3 và 4. Sau đó bước 2 và 5 xảy ra đồng thời. Trong BPDU cấu hình kế tiếp mà bridge gốc gửi đi, cờ TCN ACK sẽ được thiết lập để xác nhận là đã nhận TCN của hai brigde downstream. Tiếp theo là bước 6 và 7, Cat-A cũng thiết lập cờ TA trong 35s (Forward Delay + Max Age) để cập nhật bảng bridge nhanh hơn. Như vậy cả ba switch đều nhận được cờ TA và khoảng thời gian cho bảng bridge là 15s.

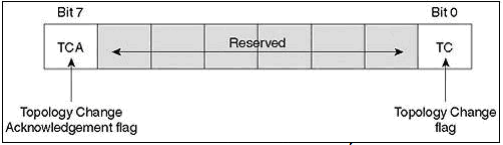
Chú ý là khoảng thời gian ngắn 15s này không bắt buộc cho toàn bộ bảng, nó chỉ làm quá trình này nhanh hơn thôi. Các thiết bị tiếp tục nói suốt 15s này mà không cho bảng bridge nghĩ. Tuy nhiên, nếu host D cố gắng gửi một frame đến host E trong 20s (giả sử host E không nói gì hết), thì frame sẽ được tràn đến tất cả các đoạn mạng vì địa chỉ EEEE-EE-EE-EE-EE không còn có trong bảng bridge nữa. Ngay khi frame đến host E và host E trả lời, thì switch học được giá trị bảng bridge mới tương ứng với cấu trúc mạng mới.

Bảng 3.8 biểu diễn toàn bộ bảng bridge cho địa chỉ MAC của E trên cả ba switch sau khi cấu trúc mạng mới hội tụ và lưu lượng lại tiếp tục.



Tại thời điểm này, kết nối giữa host D và E đã được thiết lập lại và lưu lượng lại tiếp tục. Chú ý là TCN BPDU giảm thời gian lỗi từ 300s (5ph) xuống 50s.

Hình 3.16: Trường cờ trong BPDU cấu hình.



Hình 3.16 mô tả trường cờ trong BPDU cấu hình, cả hai cờ TCA và TA đều được lưu trữ trong cùng một octet của BPDU cấu hình.

Như đã thảo luận, cờ TCN được thiết lập bởi bridge upstream để nói cho các bridge dowstream ngưng gửi TCN BPDU. Còn cờ TC được thiết lập bởi bridge gốc để giảm khoảng thời gian lỗi từ 300s xuống 15s (Forward Delay).

CHƯƠNG IV  
CHUYỂN MẠCH NHÃN ĐA GIAO THỨC – MPLS.

4.1. Tổng quan:

Trong một vài năm gần đây, Internet đã phát triển thành một mạng lưới rộng khắp và tạo ra một loạt các ứng dụng mới trong thương mại. Những ứng dụng này mang đến đòi hỏi phải tăng và bảo đảm được yêu cầu băng thông trong mạng đường trục. Thêm vào đó, ngoài các dịch vụ dữ liệu truyền thống được cung cấp qua Internet, dịch vụ thoại (voice) và các dịch vụ đa phương tiện đang được phát triển và triển khai. Internet đã làm nảy sinh vấn đề hình thành một mạng hội tụ cung cấp đầy đủ các dịch vụ. Tuy nhiên vấn đề đặt ra đối với mạng bởi các dịch vụ và ứng dụng mới là yêu cầu về băng thông và tốc độ lại đặt gánh nặng cho nguồn tài nguyên trên cơ sở hạ tầng Internet có sẵn.

Bên cạnh vấn đề quá tải nguồn tài nguyên mạng. Một thách thức khác liên quan tới việc truyền các byte và bit qua mạng đường trục để cung cấp các cấp độ dịch vụ khác nhau đối với người dùng. Sự phát triển nhanh chóng của số người dùng và lưu lượng đã làm tăng thêm sự phức tạp của vấn đề. Vấn đề cấp độ dịch vụ (CoS) và chất lượng dịch vụ (QoS) phải được quan tâm để có thể đáp ứng được những yêu cầu khác nhau của lượng lớn người dùng mạng.

Nhu cầu về một phương thức chuyển tiếp đơn giản mà các đặc tính quản lý lưu lượng và chất lượng với phương thức định tuyến, chuyển tiếp thông minh là một yêu cầu cấp thiết. Tất cả các yêu cầu đó có thể được đáp ứng bởi chuyển mạch nhãn đa giao thức, là một phương thức không bị hạn chế bởi các giao thức lớp 2 và lớp 3. Với các đặc tính đó MPLS đóng một vai trò quan trọng trong việc định tuyến, chuyển mạch và chuyển tiếp gói thông qua các mạng thế hệ sau để đáp ứng các yêu cầu của người dùng mạng.

4.1.1. Định tuyến và chuyển mạch gói truyền thống:

Bước phát triển khởi đầu của mạng Internet chỉ quan tâm tới những yêu cầu truyền dữ liệu qua mạng. Internet chỉ cung cấp các ứng dụng đơn giản như truyền file hay remote login. Để thực hiện những yêu cầu này, môt định tuyến nền dựa trên phần mền đơn giản, với giao diện mạng để hỗ trợ mạng đường trục dựa trên T1/E1- hay T3/E3 đã có là đủ. Với những yêu cầu đòi hỏi tốc độ cao và băng thông lớn, các thiết bị có khả năng chuyển mạch ở lớp 2 (Lớp liên kết dữ liệu) và lớp 3 (Lớp mạng) ở ngay mức phần cứng phải được phát triển. Thiết bị chuyển mạch lớp 2 quan tâm đến vấn đề nghẽn trong mạng con của môi trường mạng cục bộ. Thiết bị chuyển mạch lớp 3 giúp giảm bớt nghẽn trong định tuyến lớp 3 bằng cách chuyển việc tìm kiếm tuyến cho một chuyển mạch phần cứng tốc độ cao.

Các giải pháp trước đây chỉ quan tâm tới tốc độ truyền của các gói khi chúng truyền qua mạng chứ không quan tâm tới thông tin yêu cầu dịch vụ có trong gói. Hầu hết các giao thức định tuyến sử dụng ngày nay đều dựa trên thuật toán được thiết kế để tìm ra con đường ngắn nhất trong mạng với các gói truyền tải mà không quan tâm tới các yếu tố khác ( như trễ, rung pha, nghẽn), mà có thể làm giảm bớt đáng kể chức năng mạng.

4.1.2. MPLS là gì?

Mạng MPLS là sự kế thừa và kết hợp của routing thông minh trong mạng IP và chuyển mạch tốc độ cao trong mạng ATM, có cả routing ở layer 3 (IP) và switching ở layer 2 (VPI/VCI của ATM).

MPLS là cơ chế chuyển mạch nhãn do Cisco phát triển và được IETF chuẩn hóa, hỗ trợ khả năng chuyển mạch, định tuyến luồng thông tin một cách hiệu quả.

MPLS là một công nghệ kết hợp đặc điểm tốt nhất giữa định tuyến lớp ba và chuyển mạch lớp hai cho phép chuyển tải các gói rất nhanh trong mạng lõi (core) và định tuyến tốt ở mạng biên (edge) bằng cách dựa vào nhãn (label). MPLS là một phương pháp cải tiến việc chuyển tiếp gói trên mạng bằng các nhãn được gắn với mỗi gói IP, tế bào ATM, hoặc frame lớp hai. Phương pháp chuyển mạch nhãn giúp các Router và MPLS-enable ATM switch ra quyết định theo nội dung nhãn tốt hơn việc định tuyến phức tạp theo địa chỉ IP đích. MPLS kết nối tính thực thi và khả năng chuyển mạch lớp hai với định tuyến lớp ba, cho phép các ISP cung cấp nhiều dịch vụ khác nhau mà không cần phải bỏ đi cơ sở hạ tầng sẵn có. Cấu trúc MPLS có tính mềm dẻo trong bất kỳ sự phối hợp với công nghệ lớp hai nào. MPLS hỗ trợ mọi giao thức lớp hai, triển khai hiệu quả các dịch vụ IP trên một mạng chuyển mạch IP. MPLS hỗ trợ việc tạo ra các tuyến khác nhau giữa nguồn và đích trên một đường trục Internet. Bằng việc tích hợp MPLS vào kiến trúc mạng, các ISP có thể giảm chi phí, tăng lợi nhuận, cung cấp nhiều hiệu quả khác nhau và đạt được hiệu quả cạnh tranh cao.

4.1.3. Chức năng của MPLS:

* Định quá trình quản lý lưu lượng luồng của các mạng khác nhau, như luồng giữa các máy, phần cứng khác nhau hoặc thậm chí luồng giữa các ứng dụng khác nhau.
* Duy trì sự độc lập của giao thức lớp 2 và lớp 3.
* Cung cấp cách thức để ánh xạ các địa chỉ IP thành các nhãn đơn giản có độ dài không đổi được sử dụng bởi các công nghệ chuyển tiếp gói và chuyển mạch gói khác nhau.
* Giao diện dùng chung với các giao thức định tuyến RSVP hay OSPF.
* Hỗ trợ IP, ATM, Frame Relay.

4.1.4. Lợi ích của MPLS:

MPLS mang lại nhiều lợi ích như:

* Làm việc với hầu hết các công nghệ liên kết dữ liệu như IP, ATM….
* Tương thích với hầu hết các giao thức định tuyến và các công nghệ khác liên quan đến Internet.
* Hoạt động độc lập với các giao thức định tuyến (routing protocol).
* Tìm đường đi linh hoạt dựa vào nhãn (label) cho trước.
* Hỗ trợ việc cấu hình quản trị và bảo trì hệ thống (OAM).
* Có thể hoạt động trong một mạng phân cấp.
* Có tính tương thích cao.

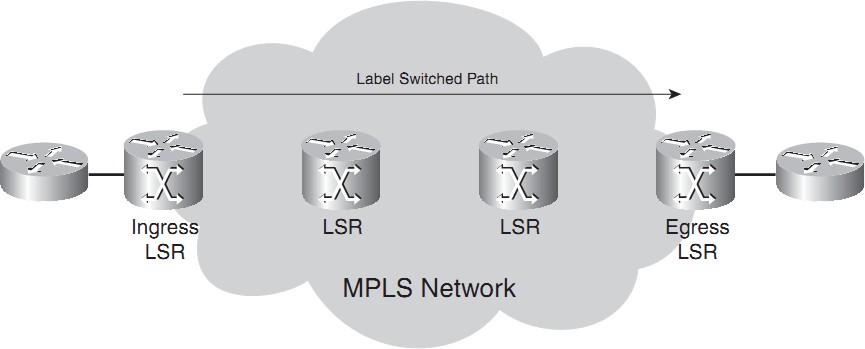
4.2. Các khái niệm cơ bản:

4.2.1. LERs và LSRs.

Thiết bị trong giao thức MPLS có thể được phân loại thành LERs và LSRs. Một LSR-Label Switch Router là một thiết bị định tuyến tốc độ cao trong lõi (core) của mạng MPLS tham gia vào quá trình thiết lập LSP-Label Switched Path sử dụng giao thức thích hợp và chuyển mạch tốc cao luồng dữ liệu dựa trên con đường đã được thiết lập.

Một LER-Label Edge Router là một thiết bị hoạt động ở biên của mạng truy cập và mạng MPLS. LER hỗ trợ nhiều cổng (port) nối tới các mạng không tương đồng (như ATM, Frame Relay, Ethenet) và chuyển những luồng lưu lượng này tới mạng MPLS sau khi thiết lập các LSP-Label Switch Path (tuyến chuyển mạch nhãn), sử dụng giao thức báo hiệu nhãn ở đầu vào và phân phối lưu lượng trở lại mạng truy cập ở đầu ra. LER đóng vai trò rất quan trọng trong việc gán và bỏ nhãn khi các luồng lưu lượng vào và tồn tại trong mạng MPLS.

Hình 4.1: Vị trí LSR và LER trong mạng MPLS.



Ingress-LSR (LSR lối vào): đảm nhận việc nhận gói tin chưa được gán nhãn, sau đó gán nhãn (có thể 1 hoặc nhiều nhãn) vào đầu gói tin và chuyển gói tin đến hộp kế tiếp.

Egress-LSR (LSR lối ra): đảm nhận việc nhận gói tin đã được gán nhãn, sau đó loại nhãn ra khỏi gói tin và chuyển đến đích kế tiếp.

LSP: Mỗi khi gói tin tiến vào mạng MPLS ở ingress-LSR và đi khỏi mạng ở egress-LSR. Cơ chế này sẽ tạo ra LSP, là tập hợp các LSR mà cá gói tin có gán nhãn phải qua để đến đích. LSP là đường đi 1 hướng (unidirectional), nghĩa là sẽ có 1 LSP khác dành riêng cho đường đi ngược lại.

4.2.2. Lớp chuyển tiếp tương đương – FEC:

FEC-Forwarding Equivalency Class là biểu diễn một nhóm các gói chia sẻ những yêu cầu như nhau về việc truyền tải. Tất cả các gói trong một nhóm được đối xử như nhau trên tuyến cho tới đích. Ngược lại so với chuyển tiếp của gói IP, trong MPLS việc gán một nhãn nhất định cho một FEC nhất định chỉ được thực hiện một lần, khi gói vào mạng. Các FEC dựa trên yêu cầu dịch vụ đối với một tập các gói cho sẵn. Mỗi LSR xây dựng một bảng để xác định một gói được chuyển tiếp như thế nào. Bảng này gọi là bảng cơ sở dữ liệu nhãn (LIB), gồm các ràng buộc FEC-tới-nhãn.

4.2.3. Nhãn:

Cấu trúc chung.

Thay thế cơ chế định tuyế lớp ba bằng cơ chế chuyển mạch lớp hai. MPLS hoạt động trong lõi của mạng IP. Các Router trong lõi phải enable MPLS trên từng gia tiếp. Nhãn được gán thêm vào gói IP khi đi vào mạng MPLS. Nhãn được tách ra khi gói ra khỏi mạng MPLS. Nhãn được chèn vào giữa header lớp ba và header lớp hai. Bộ định tuyến nhận được sẽ kiểm tra nội dung nhãn của gói để xác định chăng kế tiếp. Khi một gói được gán nhãn, cuộc hành trình của gói qua mạng đường trục sẽ dữa trên chuyển mạch nhãn.

Nhãn là giá trị có chiều dài cố định dùng để nhận diện một FEC nào đó. Sự kết hợp giữa FEC và nhãn được gọi là ánh xạ nhãn-FEC. MPLS được thiết kế để sử dụng ở bất kỳ môi trường và hình thức đóng gói lớp hai nào, hầu hết các hình thức đóng gói lớp 2 đều dựa tren frame, và MPLS chỉ đơn giản thêm vào nhãn 32 bit giữa header lớp 2 và lớp , gọi là shim header. Phương thức đóng gói này gọi là frame-mode MPLS.

ATM là một trường hợp đặc biệt sử dụng cell có chiều dài cố định. Do đó nhãn không thể được thêm vào trong mỗi cell. MPLS sử dụng các giá trị VPI/VCI trong ATM header để làm nhãn. Phương thức đóng gói này được gọi là Cell-mode MPLS. Nhãn của gói tin đi ra là nhãn ngõ ra, tương tự cho nhãn của gói tin đi vào là nhãn ngõ vào. Một gói tin có thể có cả nhãn ngõ vào và ngõ ra, và có thể có nhãn ngõ vào mà không có nhãn ngõ ra hoặc ngược lại. Định dạng thông thường của nhãn được cho như hình 2.

Hình 4.2: Định dạng chung của nhãn.

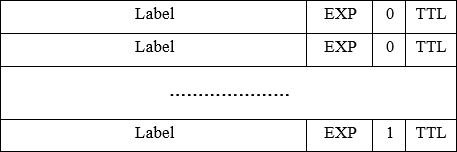


Label: Trường này gồm 20 bit, như vậy chúng ta sẽ có hơn 1 tỷ nhãn khác nhau sử dụng, đây chính là phần quan trọng nhất trong nhãn MPLS nó dùng để chuyển tiếp gói tin trong mạng.

Experimemtal (EXP): Trường này gồm 3 bit, nó dùng để mapping với trường ToS hoặc DSCP trong gói tin tới để thực hiện QoS.

BoS (Bottom of Stack): Chỉ có 1 bit, khi một gói tin đi qua một tunnel, nó sẽ có nhiều hơn 1 nhãn gắn vào, khi đó ta sẽ một stack nhãn, bit này dung để chỉ ra rằng nhãn này có nằm đáy Stack không, nếu ở đáy thì BoS=1, ngược lại BoS=0.

Hình 4.3: Chồng nhãn.



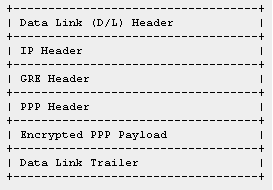
Time-to-live (TTL): Trường này như trường TTL trong IP header, khi chuyển tiếp gói tin nếu như router không tìm thấy destination mà vẫn cứ chạy trong mạng thì sẽ xảy ra loop làm nghẽ mạng (congestion). TTL dùng để khắc phục điều này, giá trị ban đầu của nó là 255, mỗi khi đi qua một router thì giá trị này sẽ giảm đi 1, nếu như giá trị này đã giảm về 0 mà gói tin vẫn chưa tới đích thì nó sẽ bị rớt (dropped). Khi gói tin đến router biên thì trường TTL trong IP header sẽ giảm đi một và copy qua trường TTL trong nhãn MPLS, giá trị này sẽ giảm dần khi đi qua mạng MPLS, khi ra khỏi mang MPLS thì trường nay lại được copy qua trường TTL trong IP header, nếu giá trị là 0 thì gói sẽ bị rớt (drop).

Các giá trị quy ước cho trường TTL:

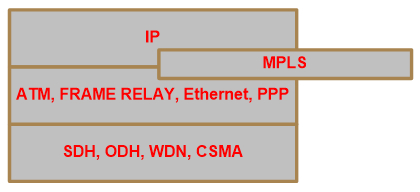
* 0: Chính nó (Host gửi tin đến chính nó).
* 1: Trong cùng một subnet.
* 32: Trong cùng một site (một mạng).
* 64: Trong cùng một vùng (có cùng AS).
* 128: Trong cùng một lục địa.
* 256: Không giới hạn.

Các cách đóng gói tin:

Hình 4.4: Cách đóng gói tin.



Hình 4.5: Nhãn lớp 2.



Như vậy, đối với mạng IP cách đóng gói tin sẽ là Ethernet hay PPP và nhãn là một shim được chèn vào như trình bày ở trên. Đối với mạng Frame-Relay nhãn sẽ là giá trị DLCI, vơi mạng ATM thì nhãn sẽ là VPI hoặc VCI.

Các loại nhãn đặc biệt.

* Untaged: gói MPLS đến được chuyển thành một gói IP và chuyển tiếp đến đích.
* Nhãn Implicit-nul hay POP: nhãn này được gán khi nhãn trên cùng (top label) của gói MPLS ddeend bị bóc ra và gói MPLS hay IP được chuyển tiếp tới trạm kế xuông dòng (downstream). Giá trị của nhãn là 3(trường 20 bits). Nhãn này được dùng trong mạng cho những trạm kế cuối.
* Nhãn Explicit-null: chỉ mang giá trị EXP, giá trị nhãn bằng 0, được gán để giữ giá trị EXP cho nhãn trên cùng (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 trong mô hình Pipe Mode.
* Nhãn Aggregate: với nhãn này, khi gói MPLS ddeend nó bị bóc tất cả nhãn trong chồng nhãn ra để trở thành một gói IP va thưc hiện tra cứu trong FIB để xác định giao tiếp ra cho nó.

Tạo nhãn.

Có một vài phương pháp để tạo nhãn:

* Phương pháp dựa trên giao thức (Topology-base method) sử dụng quá trình của các giao thức định tuyến như OSPF, BGP.
* Phương pháp dựa trên yêu cầu (Request-base method) sử dụng quá trình yêu cầu dựa trên điều khiển lưu lượng.
* Phương pháp dựa trên lưu lượng(Traffic-base method) sử dụng một gói để kích hoạt sự gán và phân phối nhãn.

Phương pháp dựa trên giao thức và dựa trên yêu cầu là ví dụ của ràng buộc nhãn control-driven, trong khi phương pháp dựa trên lưu lượng là ví dụ của ràng buộc data-driven.

Trước đây, trong quá trình “thai nghén” ra MPLS, Cisco đưa ra công nghệ tag-switching và hỗ trợ từ IOS 11.1CT. MPLS được hỗ trợ bởi các Router Cisco từ IOS 12.1(3)T.

Tag-switching chính là tiền thân của MPLS nên rất giống, chỉ có một số khác biệt như: Giao thức sử dụng phân phối nhãn của tag-switching là TDP-Tag Distribition Protocol – sử dụng tcp/udp port 711, còn MPLS là LDP-Label Distribution Protocol sử dụng tcp/udp port 646. Để cho phép chuyển mạch nhãn hoạt động thì IOS 11.1 ta dùng command tag-switching ip, IOS 12.1 ta dùng mpls ip.

MPLS là thế hệ sau của tag-switching, nó sử dụng giao thức LDP để phân phố nhãn, hoạt động như TDP chỉ khác là nó sử dụng LDP để phân phố nhãn, LDP phải đươc cấu hình trên tưng giao tiếp chạy MPLS, các láng giềng của chúng sẽ tự dộng nhạn ra các giao tiếp có chạy LDP kêt nối với chúng. Sử dụng UDP broadcast và Multicast để tìm ra các láng giềng của chúng.

Để kích hoạt LDP MPLS trên các Router ta dùng các lệnh sau:

Router (config)# configure terminal

Router (config)# ip cef

Router (config)# mpls ip

Router (config)# interface s0/0

Router (config-if)# mpls ip

MPLS là thế hệ sau của tag-switching, nó sử dụng giao thức LDP để phân phối nhãn, hoạt động như TDP chỉ khác là nó sử dụng LDP để phân phối nhãn, LDP phải được cấu hình trên từng interface chạy MPLS, các láng giềng của chúng sẽ tự động nhận ra các interface có chạy LDP kết nối với chúng. Sử dụng UDP broadcast và mulicast để tìm ra các láng giềng của chúng.

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

Không gian nhãn.

Nhãn được sử dụng bởi một LSR cho ràng buộc nhãn-FEC có thể được phân chia như sau:

* Per-platform: Giá trị nhãn là độc nhất quan toàn bộ LRS. Nhãn được cấp phát từ một quỹ chung. Không có hai nhãn trên hai giao diện khác nhau có cùng giá trị.
* Per-interface: Phạm vi của nhãn kết hợp với giao diện. Những quỹ nhãn được định nghĩa cho mỗi giao diện, và các nhãn được cung cấp ở những giao diện đó được cấp phát từ những quỹ tách biệt. Giá trị nhãn ở các giao diện khác nhau có thể giống nhau.

Kết hợp nhãn.

Luồng đầu vào của lưu lượng từ các giao diện khác nhau có thể được kết hợp lại với nhau và thực hiện chuyển mạch dựa trên một nhãn chung nếu nó được truyền qua mạng tới cùng đích cuối cùng. Nếu mạng truyền tải lớp dưới là mạng ATM, các LSR có thể thực hiện việc kết hợp VP và VC.

Cầm giữ nhãn.

MPLS định nghĩa cách đối xử với ràng buộc nhãn nhận được từ các LSR mà không có chặng tiếp với một FEC đã cho. Có hai mode được định nghĩa:

* Conservative: Trong mode này ràng buộc giữa nhãn và FEC nhận được từ các LSR mà không có chặng tiếp với một FEC đã cho sẽ bị bỏ. Mode này yêu cầu các LSR duy trì ít nhãn hơn. Đây là mode được khuyến cáo cho ATM-LSRs.
* Liberal: Trong mode này, ràng buộc giữa nhãn và FEC nhận được từ các LSR mà không có chặng tiếp với một FEC đã cho được giữ lại. Mode này đòi hỏi thích ứng nhanh hơn với sự thay đổi topo mạng và cho phép chuyển lưu lượng tới các LSP khác trong trường hợp thay đổi.

4.2.4. Kỹ thuật điều khiển lưu lượng:

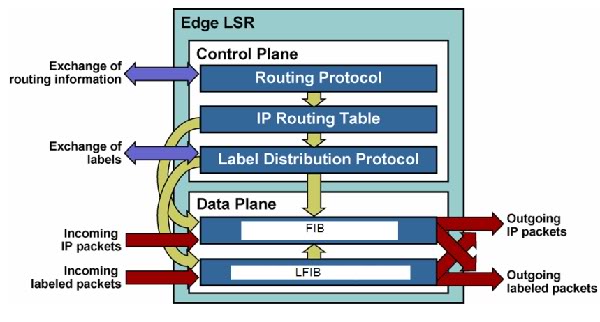
Kĩ thuật điều khiển lưu lượng là một quá trình nâng cao, tận dụng toàn bộ khả năng của mạng bằng cách cố gắng tạo một sự đồng đều hoặc phân bố thông lượng lưu lượng khác nhau qua mạng. Một kết quả quan trọng của quá trình này là tránh được tắc nghẽn ở bất kì tuyến nào. Một chú ý quan trọng là điều khiển lưu lượng không nhất thiết phải chọn con đường ngắn nhất giữa hai thiết bị. Có thể với hai luồng tải các gói dữ liệu, các gói có thể theo những con đường khác nhau thậm chí qua điểm gốc của chúng và điểm đích cuối cùng là như nhau. Theo cách này các phân đoạn mạng ít sử dụng hay ít biết tới có thể được sử dụng và có thể cung cấp các dịch vụ khác nhau.

4.3. Các bảng tra FIB và LFIB:

Bảng tra FIB-Forwarding Information Based - sẽ ánh xạ từ một gói tin IP không nhãn thành gói tin MPLS có nhãn ở ngõ vào của Ingress-LSR hoặc từ gói tin IP có nhãn thành gói tin IP không nhãn ở ngõ ra của Egress-LSR, bảng này được hình thành từ bảng Routing Table, từ giao thưc phân phối nhãn LDP và từ bảng tra LFIB.

Bảng tra LFIB-Label Forwarding Information Based là bảng chứa đựng thông tin các nhãn đến các mạng đích, một gói tin có nhãn khi đi vào một LSR nó sẽ sử dụng bảng tra LFIB để tìm ra hop kế tiếp , ngõ ra của gói tin này có thể là gói tin có nhãn cũng có thể là gói tin không nhãn.

Hình 4.6: Bảng tra FIB và LFIB.



Hai bảng tra FIB và LFIB có giá trị như bảng Routing Table trong mạng IP, nhưng trong mạng IP thì bảng Routing Table có số entry rất lớn khoảng vài ngàn, còn với FIB và LFIB số nhãn mà nó nắm giữ rất it khoản vài chục là tối đa.

4.4. Control plane (mặt phẳng điều khiển):

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

Các giao thức định tuyến Link-state như OSPF và IS-IS là các giao thức được chọn vì chúng cung cấp cho mỗi nút MPLS thông tin của toàn mạng. Trong các bộ định tuyến thông thường, bản định tuyến IP dùng để xây dựng bộ lưu trữ chuyển mạch nhanh (Fast switching cache) hoặc FIB .Tuy nhiên với MPLS, bản định tuyến IP cung cấp thông tin của mạng đích và subnet prefix. Các giao thức định tuyến link-state gửi thông tin định tuyến (flood) giữa một tập các router nối trực tiếp, thông tin liên kết nhãn chỉ được phân phối giữa các router nối trực tiếp với nhau bằng cách dùng giao thức phân phối (LDP hoặc TDP).

Các nhãn được trao đổi giữa các nút MPLS kế cận để xây dựng nên LFIB. MPLS dùng một mẫu chuyển tiếp dựa trên sự hoán đổi nhãn để kết nối với các node điều khiển khác nhau. Mỗi node điều khiển chịu trách nhiệm đánh dấu và phân phối một tập các nhãn cũng như lưu trữ các thông tin điều khiển có liên quan khác. Các giao thức cổng nội IGP – Interior Gateway Potocols-được dùng để xác nhận khả năng đến được, sự liên kết, và ánh xạ giữa FEC và địa chỉ trạm kế (next-hop address).

4.5. Data plane (mặt phẳng dữ liệu):

Mặt phẳng chuyển tiếp sử dụng một cơ sở thông tin chuyển tiếp nhãn (LFIB – Label Forwarding Information Base) để chuyển tiếp các gói. Mỗi nút MPLS có hai bảng liên quan đến việc chuyển tiếp là: cơ sở thông tin nhãn (FIB - Forwarding Information Base) và LFIB. FIB chứa tất cả các nhãn được nút MPLS cục bộ đánh dấu và ánh xạ của các nhãn này đến các nhãn được nhận từ láng giềng (MPLS neighbor) của nó. LFIB sử dụng một tập con các nhãn chứa trong FIB để thực hiện chuyển tiếp gói.

Các thành phần data plane và control plane của MPLS:

Cisco Express Forwarding (CEF) là nền tảng cho MPLS và hoạt động trên các router của Cisco. Do đó, CEF là điều kiện tiên quyết trong thực thi MPLS trên mọi thiết bị của Cisco ngoại trừ các ATM switch chỉ hỗ trợ chức năng của mặt phẳng chuyển tiếp dữ liệu.

CEF là một cơ chế chuyển mạch thuộc sở hữu của Cisco nhằm làm tăng tính đơn giản và khả năng chuyển tiếp gói IP. CEF tránh việc viết lại overhead của cache trong môi trường lõi IP bằng cách sử dụng một cơ sở thông tin chuyển tiếp (FIB – Forwarding Information Base) để quyết định chuyển mạch. Nó phản ánh toàn bộ nội dung của bảng định tuyến IP (IP routing table), ánh xạ 1-1 giữa FIB và bảng định tuyến. Khi router sử dụng CEF, nó duy trì tối thiểu 1 FIB, chứa một ánh xạ các mạng đích trong bảng định tuyến với các trạm kế tiếp (next-hop adjacencies) tương ứng. FIB ở trong mặt phẳng dữ liệu, nơi router thực hiện cơ chế chuyển tiếp và xử lý các gói tin.

Trên router còn duy trì hai cấu trúc khác là cơ sở thông tin nhãn (LIB – Label Information Base) và cơ sở thông tin chuyển tiếp nhãn (LFIB – Label Forwarding Information Base). Giao thức phân phối sử dụng giữa các láng giềng MPLS có nhiệm vụ tạo ra các chỉ mục (entry) trong hai bảng này. LIB thuộc mặt phẳng điều khiển và được giao thức phân phối nhãn sử dụng khi địa chỉ mạng đích trong bảng định tuyến được ánh xạ với nhãn nhận được từ router xuôi dòng. LFIB thuộc mặt phẳng dữ liệu và chứa nhãn cục bộ (local label) đến nhãn trạm kế ánh xạ với giao tiếp ngõ ra (outgoing interface), được dùng để chuyển tiếp các gói được gán nhãn. Như vậy, thông tin về các mạng đến được do các giao thức định tuyến cung cấp dùng để xây dựng bảng định tuyến (RIB - Routing Information Base). RIB cung cấp thông tin cho FIB. LIB được tạo nên dựa vào giao thức phân phối nhãn và từ LIB kết hợp với FIB tạo ra LFIB.

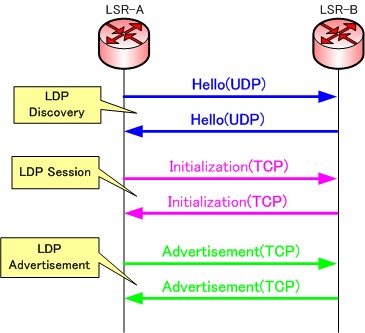
4.6. Giao thức phân phối nhãn – LDP:

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

Sự phân phối nhãn là hoạt động cơ bản của MPLS. MPLS giúp các nhãn nằm trên đỉnh của những giao thức khác. PIM được dùng để phân phối các nhãn trong trường hợp định tuyến multicast. Trong trường hợp unicast, MPLS dùng giao thức phân phối nhãn LDP-Label Switched Protocol và BGP- Border Gateway Protocol. Giao thức phân phối nhãn được sử dụng trong quá trình gán nhãn cho các gói thông tin yêu cầu. Giao thức LDP là giao thức điều khiển tách biệt được các LSR sử dụng để trao đổi và điều phối quá trình gán nhãn-FEC. Giao thức này là một tập hợp các thủ tục trao đổi các bản tin cho phép các LSR sử dụng giá trị nhãn thuộc FEC nhất định để truyền các gói thông tin. Vị trí của các giao thức LDP và các mối liên kết chức năng cơ bản của LDP với các bộ giao thức khác thể hiện ở hình 8 dưới đây. Giao thức phân phối nhãn LDP có các đặc trưng cơ bản sau:

* LDP cung cấp các kỹ thuật phát hiện LSR để cho phép LSR tìm kiếm và thiết lập truyền thông.
* LDP định nghĩa 4 loại bản tin .
* Discovery message: Thông báo và duy trì sự có mặt của một LSR trong mạng.
* Session message: Thiết lập, duy trì, kết thúc phiên giữa các LDP ngang hàng.
* Advertisement message: Tạo, thay đổi, và xoá ánh xạ nhãn cho các FEC.
* Notification message: Cung cấp thông tin tham khảo và thông tin báo hiệu lỗi.
* LDP chạy trên giao thức TCP để đảm bảo độ tin cậy của các bản tin (trừ bản tin phát hiện).
* LDP được thiết kết đêt dễ dàng mở rộng, sử dụng kiểu bản tin đặc biệt để thu thập các đối tượng mã hóa TVL (Type, Value, Length-kiểu, giá trị, độ dài).

Hình 4.7: Giao thức LDP với các giao thức khác.



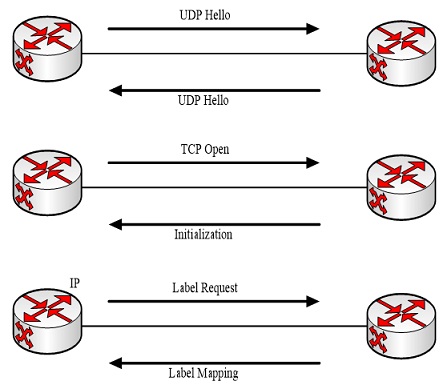
Một kết nối TCP được thiết lập giữa các LSR đồng cấp để đảm bảo các bản tin LDP được truyền một cách trung thực theo đúng thứ tự. Các bản tin LDP có thể xuất phát từ trong bất cứ một LSR nào để điều khiển đường chuyển mạch nhãn LSP độc lập hay từ egress-LSR (điều khiển LSP theo lệnh) và chuyển từ LSR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

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

* Một LSR định kỳ sẽ gửi đi bản tin HELLO tới các cổng UDP đã biết trong tất cả các bộ định tuyến trong mạng con của nhóm multicast.
* Tất cả các LSR tiếp nhận bản tin HELLO này trên cổng UDP. Như vậy, tai một thời điểm nào đó LSR sẽ biết được tất cả các LSR khác mà nó có thể kết nối trực tiếp.
* Khi LSR nhận biết được địa chỉ của LSR khác bằng cơ chế này thì nó sẽ thiết lập kết nối TCP trên LSR đó.

Khi đó phiên LDP được thiết lập giữa 2 LSR. Phiên LDP là phiên 2 chiều có nghĩa là mỗi LSR ở hai đầu kết nối đều có thể yêu cầu và gửi liên kết nhãn.

Hình 4.8: Thủ tục phát hiện LSR lân cận.



Trong trường hợp các LSR không kết nối trực tiếp trong một mạng con (subnet) người ta sử dụng môt cơ chế bổ sung như sau: LSR định kỳ gửi bản tin HELLO đến cổng UDP đã biết tại địa chỉ IP xác định được khai báo khi lập cấu hình. Đầu nhận bản tin này có thể trả lời lại bằng bản tin HELLO khác truyền theo chiều ngược lại đến LSR gửi và việc thiết lập các phiên LDP được thực hiện như trên. Thông thường, trường hợp này hay được áp dụng khi giữa 2 LSR có một đường LSP cho điều khiển lưu lượng và nó yêu cầu phải gửi các gói có nhãn qua đường LSP đó.

Như chúng ta đã biết , bản tin LDP được truyền trên giao thức TCP, nhưng việc quyết định sử dụng TCP để truyền các bản tin LDP là một vấn đề cần xem xét. Yêu cầu về độ tin cậy là rất cần thiết: nếu việc liên kết nhãn hay yêu cầu liên kêt nhãn được truyền một cách không tin cậy thì lưu lượng cũng không được chuyển mạch theo nhãn. Một vấn đề quan trọng nữa là thứ tự các bản tin phải bảo đảm đúng. Như vây, liệu việc sử dụng TCP để truyền LDP có bảo đảm hay không và có nên xây dựng luôn chức năng truyền tải này trong bản thân LDP hay không? Việc xây dựng các chức năng đảm bảo độ tin cậy trong LDP không nhất thiết phải thực hiện toàn bộ các chưc năng của TCP trong LDP mà chỉ cần dựng lại ở những chức năng cần thiết nhất ví dụ như chức năng điều khiển tránh tắt nghẽn đươc koi là không cần thiết trong LDP. Tuy nhiên, việc phát triển thêm các chức năng đảm bảo độ tin cậy trong LDP cũng có nhiều vấn đề xem xét ví dụ như các bộ định thời cho các bản tin ghi nhận và không ghi nhận, trong trường hợp sử dụng TCP chỉ cần 1 bô định thời của TCP cho toàn phiên LDP.

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

Các bản tin LDP

Như phần đầu đã trình bày có 4 kiểu bản tin cơ bản được sử dụng trong giao thức phân phối nhãn LDP, các bản tin thông dụng là:

* Bản tin khởi tạo(Initialization).
* Bản tin giữ đường (KeepAlive).
* Bản tin gán nhãn (Label Mapping).
* Bản tin giai phóng (Release).
* Bản tin Thu hồi nhãn (Label Withdraw).
* Bản tin yêu cầu (Request).
* Bản tin hủy bỏ (Request Abort).
* *Dạng bản tin Initialization*. Các bản tin thuộc loại này được gửi khi bắt đầu một phiên LDP giữa 2 LSR để trao đổi các tham số, các tùy chọn cho phiên. Các tham số này bao gồm: Chế đọ phân bổ nhãn, các giá trị bộ định thời, pham vi các nhãn sử dụng trong kện giửa 2 LSR đó. Cả 2 LSP đều có thể gửi các bản tin Initialization và LSR nhận sẽ trả lời bằng bản tin KeepAlive nếu các tham số được chấp nhận. Nếu có 1 tham số nào đó không được chấp nhận thì LSR thông báo lỗi và phiên kết thúc.
* *Dạng bản tin KeepAlive*. Các bản tin KeepAlive được gửi định kỳ khi không có bản tin nào được gửi để đảm bảo cho mỗi thành phần LDP biết rằng thành phần LDP khác đang hoạt động tốt. Trong trường hợp không xuất hiện bản tin KeepAlive hay một số bản tin khác của LDP trong khoảng thời gian nhất định thì LSR sẽ xác định đối phương hoặc kết nối bị hỏng và phiên LDP tạm dừng.
* *Dạng bản tin Label Mapping.* Các bản tin Label Mapping được sử dụng đẻ quảng bá liên kết giữa các FEC (prefix địa chỉ) và nhãn. Bản tin Label Withdraw thực hiện quá trình ngược lại: nó được sử dụng để xóa bỏ liên kết vừa thực hiện. Bản tin này được sử dụng khi có sự thay đổi trong bản định tuyến (thay đổi prefix địa chỉ) hay thay đổi trong cấu trúc LSR làm tạm dừng việc chuyển nhãn các gói trong FEC đó.
* *Dạng bản tin Label Release.* Bản tin này được sử dụng bởi các LSR khi nhận được chuyển đổi nhãn mà nó không cần thiết nữa. Điều đó thường xảy ra khi LSR giải phóng nhận thấy nút tiếp theo cho FEC đó không phải là LSR quảng bá liên kết nhãn/FEC đó.

4.7. Các chế độ hoạt động của MPLS:

Có hai chế độ hoạt động tồn tại với MPLS: chế độ khung (frame - mode) và chế độ tế bào (cell – mode).

4.7.1. Chế độ khung (frame-mode):

Chế độ này xuất hiện khi sử dụng MPLS trong môi trường các thiết bị định tuyến thuần điều khiển các gói tin IP điểm-điểm. Các gói tin gán nhãn được chuyển tiếp trên cơ sở khung lớp 2. Quá trình chuyển tiếp một gói tin IP qua mạng MPLS được thực hiện qua một số bước cơ bản sau đây:

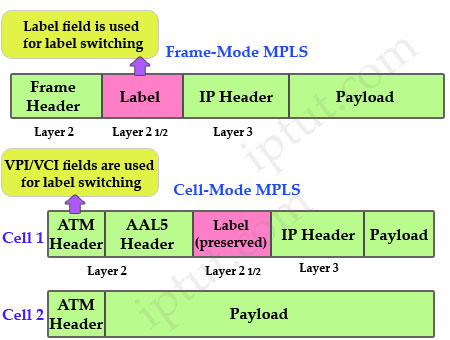
Ingress-LER nhận gói tin IP, phân loại gói vào nhóm chuyển tiếp tương đương FEC và gán nhãn cho gói với ngăn xếp nhãn tương ứng FEC đã xác định. Trong trường hợp định tuyến một địa chỉ đích, FEC sẽ tương ứng vói mạng con đích và việc phân loại gói sẽ đơn giản là việc so sánh bảng đinh tuyến lớp 3 truyền thống.

Các LSR tiếp theo sẽ nhận gói có nhãn và sử dụng bảng chuyển tiếp nhãn để thay đổi nhãn lối vào trong gói đến nhãn lối ra tương ứng cùng với vùng FEC (trong trường hợp này là mangh con IP).

Khi egress-LSR của vùng FEC này nhận được gói tin có nhãn, nó loại bỏ nhãn và thực hiện việc chuyển tiếp gói tin IP theo bảng đinh tuyến lớp 2 truyền thống.

Vì rất nhiều lý do nên nhãn MPLS phải được chèn trước số liệu được gán nhãn trong chế độ hoạt đông khung. Như vậy nhãn MPLS được chèn giữa tiêu đề lớp 2 và nội dụng thông tin lớp 3 của khung lớp 2 như thể hiện trong hình dưới đây:

Hình 4.9: Vị trí nhãn trong khung lớp 2.



Do nhãn MPLS được chèn vào vị trí như vậy nên bộ định tuyến gửi thông tin phải có phương tiện gì đó thông báo cho bộ đinh tuyến nhận biết rằng gói đang được gửi đi không phải là gói tin IP thuần mà là gói có nhãn (gói MPLS). Để đơn giản chức năng này, một số dạng giao thức mới định nghĩa trên lớp 2 như sau:

Trong môi trường LAN, các gói có nhãn truyển tải gói lớp 3 unicast hay multicast sử dụng giá trị 8847H và 8848H cho dạng Ethernet. Các giá trị này được sử dụng trực tiếp trên phương tiện Ethernet (bao gồm cả Fast Ethernet và Gigabit Ethernet).

Trên kênh điểm – điểm sử dụng tạo dạng PPP, sủ dụng giao thức điều khiển mạng mới gọi là MPLSCP (giao thức điểu khiển MPLS). Các gói MPLS được đánh dấu bởi giá trị 8281H trong trường giao thức PPP. Các gói tin MPLS truyền qua chuyển dịch khung DLCI giữa một cặp Router được đánh dấu bởi nhận dạng giao thức lớp mạng SNAP của chuyển dịch khung (NLPID), tiếp theo tiêu đề SNAP với giá trị 8847H cho dạng Ethernet.

Các gói MPLS truyền giữa một cặp Router qua kênh ảo ATM Forum được đóng gói với tiêu đề SNAP sử dụng giá trị cho dạng Ethernet như trong môi trường LAN.

Khi xuất hiện một LSR mới trong mạng MPLS hay bắt đầu khởi tạo mạng MPLS, các thành viên LSR trong mang MPLS phải có liên lạc với nhau trong quá trình khai báo thông tin qua bản tin HELLO. Sau khi bản tin này được gửi một phiên giao dịch giữa 2 LSR được thực hiện. Thủ tục trao đổi giao thức LDP. Ngay sau khi LIB (cơ sở dữ liệu nhãn) được tạo ra trong LSR, nhãn được gán cho mỗi FEC mà LSR nhạn biết được. Đối với trường hợp chúng ta đang xem xét (định tuyến dựa trên đích unicast) FEC tương đương với prefix trong bảng định tuyến IP. Như vây, nhãn đượcgán cho mỗi prefis trong bảng định tuyến IP và bảng chuyển đỏi chứa trong LIB. Bảng chuyển đổi định tuyến này được cập nhật liên tục khi xuất hiện những tuyến nội vùng mới, nhãn mới sẽ được gán cho tuyến mới.

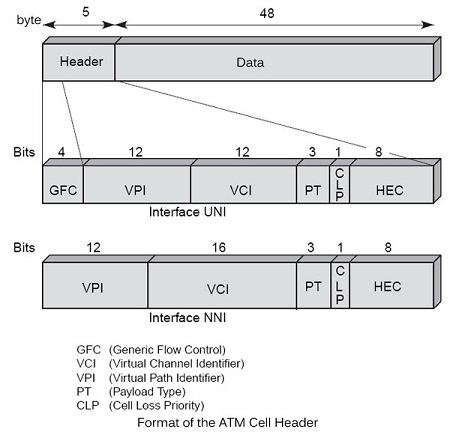
Do LSR gán nhãn cho mỗi tiền tố IP trong bảng định tuyến của chúng ngáy sau khi prefix xuất hiện trong bảng định tuyến và nhã là phương tiện được LSR khác sử dụng khi gửi gói tin có nhãn đến chính LSR đó nên phương pháp gán nhãn và phân phối nhãn này được gọi là gán nhãn điều khiển độc lập với quá trình phân phối ngược không yêu cầu.

Việc liên kết các nhãn được quãng bá ngay đến tất cả các bộ định tuyến thông qua giao thức phân bổ nhãn LDP.

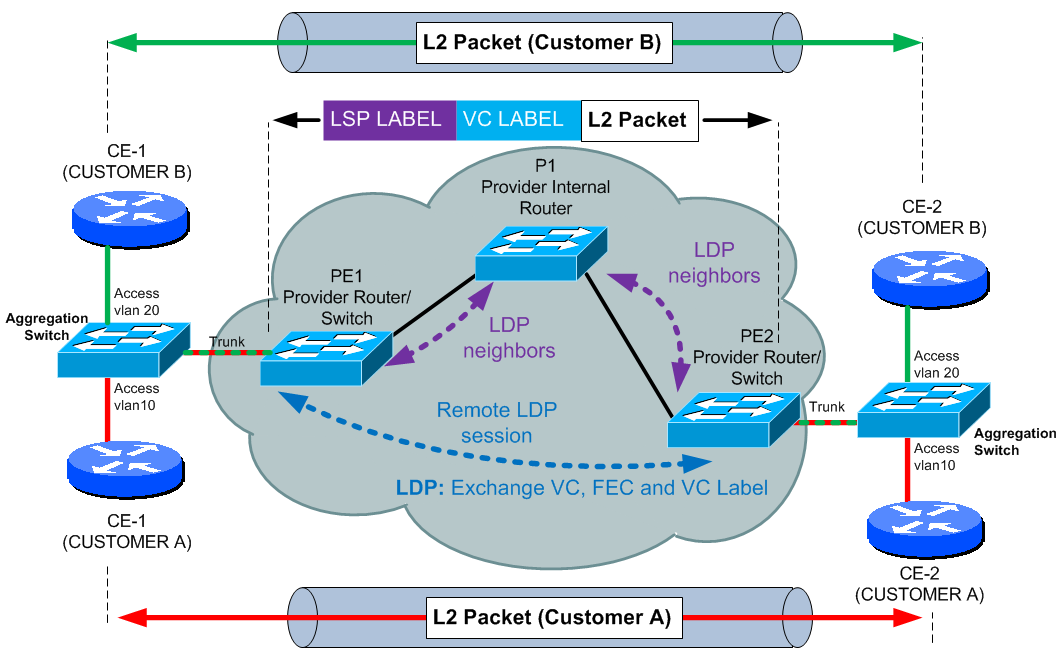
4.7.2. Chế độ hoạt động tế bào MPLS:

Thuật ngữ này dùng khi có một mạng gồm các ATM LSR dùng MPLS trong mặt phẳng điều khiển để trao đổi thông tin VPI/VCI thay vì dùng báo hiệu ATM. Trong kiểu tế bào, nhãn là trường VPI/VCI của tế bào. Sau khi trao đổi nhãn trong mặt phẳng điều khiển, ở mặt phẳng chuyển tiếp, router ngõ vào (ingress router) phân tách gói thành các tế bào ATM, dùng giá trị VCI/CPI tương ứng đã trao đổi trong mặt phẳng điều khiển và truyền tế bào đi. Các ATM LSR ở phía trong hoạt động như chuyển mạch ATM – chúng chuyển tiếp một tế bào dựa trên VPI/VCI vào và thông tin cổng ra tương ứng. Cuối cùng, router ngõ ra (egress router) sắp xếp lại các tế bào thành một gói.

Hình 4.10: Định dạng của ATM – cell.



Hình 4.11: Đường hầm trong MPLS.



Đặc tính duy nhất của MPLS là có thể điều khiển toàn bộ đường truyền gói tin mà không cần xác định cụ thể các bộ định tuyến trung gian. Điều đó được tạo ra bởi các đường hầm thông qua các bộ định tuyến trung gian có thể cách nhiều đoạn. Khái niệm này được sử dụng trong VPN dựa trên MPLS.

4.8. Các ứng dụng cảu MPLS:

Internet có ba nhóm ứng dụng chính: voice, data, video với các yêu cầu khác nhau. Voice yêu cầu độ trễ thấp, cho phép thất thoát dữ liệu để tăng hiếu quả. Video cho phép thất thoát dữ liệu ở mức chấp nhận được, mang tính thời gian thực (realtime). Data yêu cầu độ bảo mật và chính xác cao. MPLS giúp khai thác tài nguyên mạng đạt hiệu quả cao.

Một số ứng dụng đang được triển khai là:

MPLS VPN: Nhà cung cấp dịch cụ có thể tạo VPN lớp 3 dọc theo mạng đường trục cho nhiều khách hàng, chỉ dùng một cơ sở hạ tầng công cộng sẵn có, không cần các ứng dụng encrytion hoặc end-user.

MPLS Traggic Engineer: Cung cấp khả năng thiết lập một hoặc nhiều đường đi để điều khiển lưu lượng mạng và các đặc trưng thực thi cho một loại lưu lượng.

MPLS QoS (Quality of service): Dùng QoS các nhà cung cấp dịch vụ có thể cung cấp nhiều loại dịch vụ với sự đảm bảo tối đa về QoS cho khách hàng.

CHƯƠNG V  
THIẾT KẾ MẠNG CHO TRƯỜNG HỌC.

5.1. Tóm tắt mục tiêu hệ thống:

Hệ thống thiết kế cần đáp ứng những mục tiêu sau:

Xây dựng hệ thống mạng trục trên nền cáp đồngcho trường học theo mô hình chuẩn thiết kế phân cấp.

Kết nối toàn bộ các máy tính và máy chủ ứng dụng lại với nhau.

Triển khai hệ thống wifi internet chất lượng cao phục vụ cho nhu cầu sử dụng internet wifi của giáo viên và học sinh.

Đảm bảo tính bảo mật, khả năng dự phòng cao cho hệ thống mạng tại nhà trường. Hệ thống sẵn sàng đáp ứng tất cả những ứng dụng và khả năng truyền file với dung lượng lớn trên nền trục tốc độ 1GB.

Hệ thống Switch chuyển mạch đáp ứng về mặt kỹ thuật, tốc độ, độ tin cậy.

**Dễ quản lý:** Hệ thống được thiết kế trên tiêu chuẩn dễ quản lý, thuận tiện cho công tác quản lý và vận hành hệ thống.

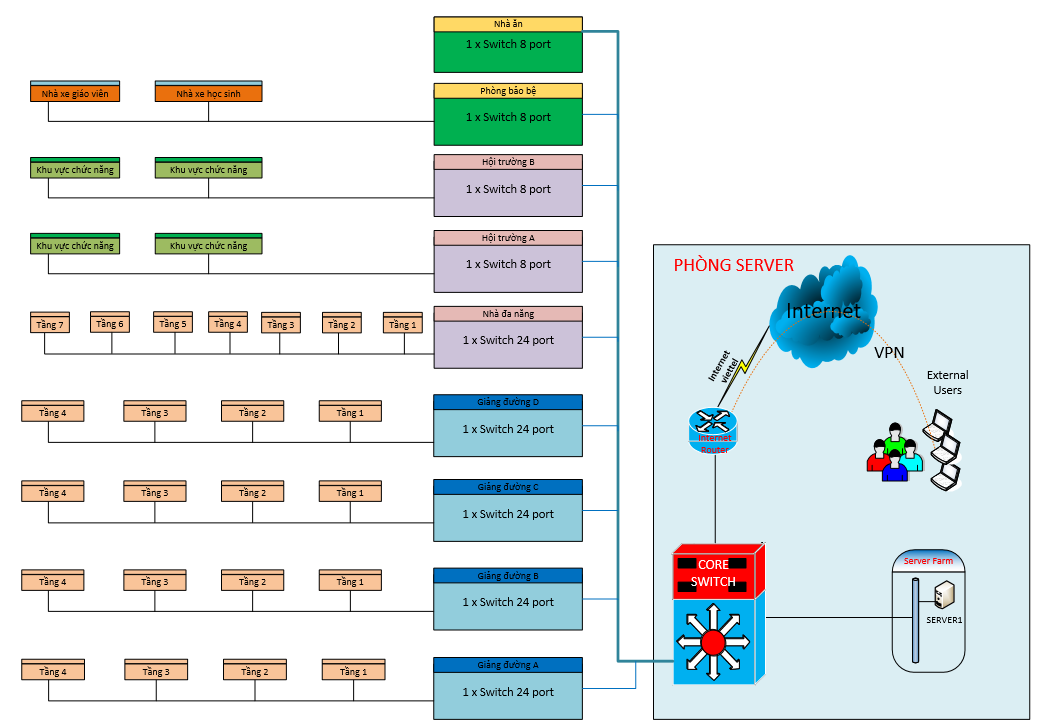
**Dễ dàng mở rộng:** Hệ thống cho phép dễ dàng thi công mở rộng khi có nhu cầu để đáp ứng cho công việc tại trường học.

**Dễ dàng lắp đặt, vận hành và sữa chữa:** Hệ thống phải cho phép dễ dàng và thuận tiện cho thi công và trong trường hợp có sự cố thì phải thuận tiện cho việc kiểm tra sữa chữa.

**Đáp ứng tốt các yâu cầu của công nghệ:** Hệ thống phải đáp ứng tốt các nhu cầu kỹ thuật hiện tại và các nhu cầu phát triển của công nghệ thông tin trong tương lai.

5.2. Hệ thống triển khai:

5.2.1. Sơ đồ mạng tổng thể triển khai cho trường học:



Hình 5.1: Sơ đồ nguyên lí hệ thống mạng.

5.2.2. Triển khai hệ thống mạng nội bộ:

Xác định rằng hệ thống mạng LAN chuyển mạch là cực kì quan trọng. Hệ thống mạng nếu thiết kế không tốt thì sẽ ảnh hưởng rất lớn đến các công tác quản trị, cũng như việc vận hành của toàn hệ thống trường học. Hệ thống mạng nội bộ đã triển khai cho trường học bao gồm những thiết bị:

* Switch Core trung tâm – CISCO 3750G-24TS\_L
* Switch access nhánh đặt tại các tầng – access switch CISCO WS-C2960S-48PS-L
* Thiết bị Router internet chuyên dụng – draytek 2960

Sau đây là các giải pháp thiết kế chi tiết cho các thiết bị để xây dựng 1 hệ thống mạng nội bộ hoàn chỉnh cho trường học.

Hệ thống mạng trường học được thiết kế theo mô hình phân cấp chuẩn với thiết bị mạng chuyên dụng của hãng CISCO. Các thành phần của mô hình này là lớp Core /Distribution và Lớp Access. Thiết bị ở lớp Core/Distribution - lớp trung tâm là họ sản phẩm CISCO Procure 3750G-24TS\_L được sử dụng phổ biến cho các doanh nghiệp vừa và lớn.

Switch access CISCO WS-C2960S-48PS-L đặt tại các tầng giúp tối ưu việc đi dây từ vị trí wifi, mạng tại các tầng. Bên cạnh đó các switch này sẽ được đấu nối 2 sợi uplink về coreswitch trung tâm. Sử dụng công nghệ **“ etherchannel”** nhằm mục đích tăng băng thông truy cập cho toàn bộ hệ thống mạng, tránh hiện tượng nghẽn cổ chai trong hệ thống mạng. Thiết kế này sẽ giúp tối ưu tốt nhất cho việc dự phòng của hệ thống, cũng như tăng gấp đôi băng thông truy cập trong mạng lên thành 2GB cho các kết nối uplink truy cập về core switch trung tâm. Trong trường hợp 1 tuyến cáp từ các switch tầng về switch trung tâm bị lỗi hệ thống vẫn làm việc bình thường. Không bị gián đoạn dịch vụ.

Cung cấp các cổng kết nối với tốc độ 10/100/1000 Mbps đến từng thiết bị của người dùng cũng như đến phân vùng server frame máy chủ. CISCO procure switch 3750G-24TS\_L có nhiều chức năng để quản lý lưu thông trên mạng luôn ở tốc độ cao và hiệu quả gigabit switching. Hệ thống mạng này còn hỗ trợ này còn hỗ trợ các dịch vụ mới như hệ thống điện thoại IP Phone, Video conferencing và các kết nối với hệ thống mạng không dây wireless LAN.

Trong giải pháp này, thiết bị CISCO Procure 3750G-24TS\_L được xếp ở lớp core/distribution, với nhiệm vụ chính là đảm bảo tốc độ truy cập tối đa cho mạng. Thực hiện việc chia các mạng riêng ảo vlan để tối ưu hóa băng thông trong mạng cũng như đảm bảo tính an toàn, bảo mật cho hệ thống mạng thông qua tính năng access list. Thiết bị đóng vai trò định tuyến traffic cho tất cả các vlan trong mạng. và cung cấp các kết nối đến các máy chủ chạy ở tốc độ 1000 Mbps sử dụng cáp UTP.

Với mô hình đề xuất hệ thống mạng của trường học có thể dễ dàng mở rộng với các kết nối switch lớp Access layer 2. Cung cấp các kết nối đến các máy trạm, các thiết bị mạng không dây Access Point … với tốc độ 100 Mbps.

Các máy chủ phục vụ cho hệ thống phần mềm tại trường học được nối thẳng vào switch CISCO Procure 3750G-24TS\_L trên 1 vlan riêng được thiết lập dành cho hệ thống server frame. Đáp ứng tốt tốc độ truy nhập từ mọi máy trạm trong mạng với tốc độ kết nối là 1000 Mbps, tất cả các kết nối trong mạng được thực hiện qua các đường cáp đồng UTP với giao tiếp RJ45 sẽ giúp tiết kiệm chi phí lớn hơn.

Ngoài ra để đảm bảo an ninh, an toàn cho hệ thống tất cả các thiết bị mạng sẽ được thiết lập một mạng quản trị riêng (Private Management Network).

Việc phân chia VLAN ở lớp 2 cũng sẽ được thiết lập trên bộ chuyển mạch trung tâm CISCO 3750G-24TS\_L để tạo thành các phân vùng độc lập tách rời các hệ thống máy chủ và hệ thống mạng nội bộ, hệ thống mạng riêng giành cho khách để tăng cường khả năng quản lý và an ninh mạng.

Để đảm bảo băng thông truy cập internet chúng tôi đề xuất thiết bị Router cân bằng tải chuyên dụng Draytek vigor 2960. Với việc thuê bao 2 đường truyền internet của nhà cung cấp Viettel giúp tăng băng thông truy cập internet cho hệ thống và dự phòng khi một đường truyền cung cấp bị lỗi. Đảm bảo đường truyền internet luôn luôn hoạt động 24/24 đáp ứng tốt nhất nhu cầu sử dụng của khách hàng.

Dễ dàng trong việc phát triển cũng như mở rộng hệ thống trong tương lai.

5.3. Vấn đề an ninh hệ thống:

5.3.1. Tường lửa:

Nguyên tắc chung khi thiết kế mạng cho một trung tâm dữ liệu là phải tạo hệ thống tường lửa hai lớp. Lớp trong cùng hoạt động tại khối core để bảo vệ các máy chủ của môi trường vận hành khỏi sự xâm nhập không được phép từ các môi trường kết nối khác. Lớp phía ngoài nằm ngay sau bộ định tuyến kết nối với các mạng diện rộng khác nhằm bảo vệ sự thâm nhập từ bên ngoài vào trong mạng của trung tâm.

5.3.2. Ngăn ngừa xâm nhập:

Hệ thống ngăn ngừa xâm nhập được đặt ở đoạn giữa của mạng cục bộ và các mạng diện rộng bên ngoài. Hệ thống này chủ yếu thiết lập các quy tắc lọc gói tin đã được thông qua tường lửa. Ví dụ, các dữ liệu ở cổng web (80) sẽ được chạy thông qua tường lửa và được lọc nội dung ở thiết bị ngăn ngừa thâm nhập.

5.3.3. Phòng chống virut:

Nguy cơ virus đến chủ yếu tập trung qua hai đường cổng internet và các máy trạm. Một giải pháp phòng chống tập trung theo mô hình client-server cộng với giải pháp quét ngăn ngừa mã độc hại qua kết nối internet có thể đáp ứng được nhu cầu.

KẾT LUẬN

Hiện nay, nhiều nhà cung cấp Internet đã và đang triển khai mạng Campus rộng khắp các trường học trên cả nước và mang lại hiệu quả đáng kể cho người sử dụng cũng như các nhà khai thác mạng. Campus cung cấp khả năng sử dụng đồng thời ba loại dịch vụ: thoại (voice) – dữ liệu (data) – hình ảnh (video) như: Truyền dữ liệu, Hội nghị truyền hình (Video Conference), Xem phim theo yêu cầu (Video ON Demand), Truyền hình cáp (CATV), Giáo dục từ xa, Chuẩn đoán bệnh từ xa, Điện thoại IP, Truyền hình IP, Truy cấp Internet tốc độ cao… Với băng thông cực rộng lên đến hàng Gbps, người sử dụng sẽ tiết kiệm được thời gian tải chương trình, nhất là đối với các cơ sở dữ liệu, hệ thống hình ảnh, phim… có dung lượng lớn. Campus giúp đơn giản hóa công tác quản lý cơ sở hạ tầng công nghệ thông tin, tiết kiệm chi phí và tối ưu hóa hệ thống công nghệ thông tin, dễ dàng triển khai các ứng dụng chuyên nghiệp và hiện đại nhất cũng như các dịch vụ cộng thêm; kết nối mạng liên tỉnh, quốc tế và băng thông rộng; kết nối với các nhà cung cấp nội dung thông tin để tăng tính đa dạng và hiệu quả khai thác mạng nội bộ. Cùng với sự phát triển của các công nghệ truy nhập mới như G-PON, E-PON, tốc độ truy nhập của thuê bao không ngừng được tăng lên, đem lại giải pháp truy nhập hiệu quả về môi trường cũng như về mặt kinh tế.

DANH MỤC TÀI LIỆU THAM KHẢO

1. Trung tâm khoa học tự nhiên và công nghệ quốc gia - viện công nghệ thông tin (2004), “Giáo Trình Thiết Kế Mạng LAN – WAN”.
2. Th.s Ngô Bá Hùng – Đại Học Cần Thơ – Khoa Công Nghệ Thông Tin (2005), Giáo Trình Thiết Kế & Cài Đặt Mạng.
3. Học viện mạng Quốc tế NETPRO - ITI Viện CNTT ( 2011) , Giáo trình Thiết kế và xây dựng mạng LAN và WAN, Hà Nội.
4. Võ Thị Hà (2009), Thiết kế mạng CAMPUS theo công nghệ CISCO
5. Nguyễn Hồng Sơn (2006), Giáo trình hệ thống mạng máy tính CCNA, Nhà xuất bản Lao động Xã hội.
6. Diane Teare (2005), “Campus Network Design Fundamentals Catherine Paquet Copyright©2006 Cisco Systems, Inc. Published by: Cisco Press.
7. Cisco Systems, Metro Ethernet WAN Service and Architecture, 2002.
8. Cisco Systems, Cisco-our NGN Perspective, Telecomp 2004.