ỦY BAN NHÂN DÂN HUYỆN CỦ CHI
TRƯỜNG TRUNG CẤP NGHỀ CỦ CHI

GIÁO TRÌNH

MÔ ĐUN: THIẾT KẾ VÀ XÂY DỰNG MẠNG LAN

NGHỀ: QUẢN TRỊ MẠNG MÁY TÍNH
TRÌNH ĐỘ: TRUNG CẤP NGHỀ

Ban hành kèm theo Quyết định số: 89/QĐ-TCNCC ngày 15 tháng 08 năm 2024 của Hiệu trưởng Trường Trung cấp nghề Củ Chi

TP. Hồ Chí Minh - Năm 2024

TUYÊN BỐ BẢN QUYỀN:

Tài liệu này thuộc loại sách giáo trình nên các nguồn thông tin có thể được phép dùng nguyên bản hoặc trích dùng cho các mục đích về đào tạo và tham khảo.

Mọi mục đích khác mang tính lệch lạc hoặc sử dụng với mục đích kinh doanh thiếu lành mạnh sẽ bị nghiêm cấm.

LỜI GIỚI THIỆU

Giáo trình "***Thiết kế và xây dựng mạng LAN***" được biên soạn theo Chương trình khung Quản trị mạng máy tính đã được Bộ Lao động – Thương binh và Xã hội ban hành.

Trong những năm qua, dạy nghề đã có những bước tiến vượt bậc cả về số lượng và chất lượng, nhằm thực hiện nhiệm vụ đào tạo nguồn nhân lực kỹ thuật trực tiếp đáp ứng nhu cầu xã hội. Cùng với sự phát triển của khoa học công nghệ trên thế giới, lĩnh vực Công nghệ thông tin nói chung và ngành Quản trị mạng ở Việt Nam nói riêng đã có những bước phát triển đáng kể.

Chương trình khung quốc gia nghề Quản trị mạng đã được xây dựng trên cơ sở phân tích nghề, phần kỹ thuật nghề được kết cấu theo các môđun. Để tạo điều kiện thuận lợi cho các cơ sở dạy nghề trong quá trình thực hiện, việc biên soạn giáo trình kỹ thuật nghề theo theo các môđun đào tạo nghề là cấp thiết hiện nay.

Nội dung chính của giáo trình được chia thành 07 bài, bao gồm các nội dung:

1. Bài mở đầu
2. Khảo sát chức năng mạng máy tính
3. Mạng cục bộ Ethernet
4. Cơ sở về định tuyến
5. Cơ sở về bộ chuyển mạch
6. Mạng cục bộ ảo
7. Xây dựng mạng LAN

Thiết kế và xây dựng mạng LAN là mô đun đào tạo nghề được biên soạn theo hình thức tích hợp lý thuyết và thực hành. Trong quá trình thực hiện, nhóm biên soạn đã tham khảo nhiều tài liệu Quản trị mạng trong và ngoài nước, kết hợp với kinh nghiệm trong thực tế. Mặc dầu có rất nhiều cố gắng, nhưng không tránh khỏi những khiếm khuyết, rất mong nhận được sự đóng góp ý kiến của độc giả để giáo trình được hoàn thiện hơn.

Xin chân thành cảm ơn!

Củ Chi, ngày … tháng … năm 2024

Nhóm biên soạn:

MỤC LỤC

BÀI 1. BÀI MỞ ĐẦU

1. Giới thiệu thời gian, vị trí, tính chất của mô đun:

- **Thời gian**: 90 giờ (Lý thuyết: 30 giờ; Thực hành: 56 giờ; Kiểm tra: 4 giờ).
- **Vị trí:** Mô đun được bố trí sau khi học sinh học xong các môn học chung và các môn học, mô đun đào tạo cơ sở nghề;
- **Tính chất:** Là mô đun đào tạo chuyên ngành.

2. Giới thiệu mục tiêu mô đun;

2.1 Mục tiêu mô đun:

- Về kiến thức
  + Trình bày được quy trình thiết kế một hệ thống mạng;
  + Đọc được các bảng vẽ thi công;
  + Phân biệt được các chuẩn kết nối mạng cục bộ;
  + Phân biệt, lựa chọn được các thiết bị mạng;
  + Trình bày được nguyên tắc hoạt động của bộ chọn đường bộ định tuyến;
  + Xây dựng được các địa chỉ IP cho một liên mạng;
- Về kỹ năng
  + Thiết kế được một mạng cục bộ;
  + Đọc được bảng vẽ thi công;
  + Cấu hình được bộ định tuyến;
  + Lập được hồ sơ thiết kế mạng;
  + Cài đặt được hệ điều hành;
  + Cài đặt và cấu hình được các dịch vụ mạng;
  + Bảo mật được dữ liệu cho hệ thống;
- Về năng lực tự chủ và trách nhiệm
  + Bố trí làm việc khoa học đảm bảo an toàn cho người và phương tiện học tập;
  + Rèn luyện ý thức kỷ luật trong học tập, tinh thần hợp tác, giúp đỡ lẫn nhau;
  + Thực hiện được các thao tác an toàn trong lao động.

3. Giới thiệu nội dung chi tiết của mô đun;

BÀI MỞ ĐẦU - THỜI GIAN: 1 GIỜ

- Giới thiệu thời gian, vị trí và tính chất của mô đun;
- Giới thiệu mục tiêu mô đun;
- Giới thiệu nội dung chi tiết của mô đun;
- Giới thiệu phương thức tổ chức môn học và phương pháp đánh giá kết quả học tập của mô đun;
- Giới thiệu tài nguyên học học tập (tài liệu, giáo trình, phần mềm, nguồn tìm kiếm và tham khảo, …)

BÀI 1. KHẢO SÁT CHỨC NĂNG MẠNG MÁY TÍNH - THỜI GIAN: 4 GIỜ

1. Mục tiêu của bài

- Liệt kê được các thành phần chính của mạng;
- Diễn dịch được mô hình mạng;
- Liệt kê được các chức năng chia sẻ tài nguyên chính và các ưu điểm của chúng;
- Liệt kê được 4 ứng dụng mạng và các ưu điểm của mỗi ứng dụng;
- Mô tả được ảnh hưởng của ứng dụng trên mạng;
- Liệt kê được loại đặc trưng dùng để mô tả các loại mạng khác nhau;
- So sánh được các loại mô hình vật lý và luận lý (physical & logical topologies);
- Liệt kê được đặc trưng của mô hình bus;
- Liệt kê được đặc trưng của mô hình sao & sao mở rộng;
- Liệt kê được đặc trưng của mô hình vòng đơn & vòng đôi;

- Liệt kê được đặc trưng của mô hình lưới đầy đủ và không đầy đủ;
- Mô tả được các phương pháp kết nối với mạng internet;

2. Nội dung bài

2.1 Khái niệm và chức năng của vi xử lý

2.2 Các ứng dụng mạng

2.3 Đặc trưng của mạng

2.4 Các loại mô hình mạng

BÀI 2. MẠNG CỤC BỘ ETHERNET - THỜI GIAN: 20 GIỜ

1. Mục tiêu của bài

- Định nghĩa được mạng cục bộ (LAN);
- Quan sát và mô tả được các thành phần của mạng cục bộ;
- Liệt kê được chức năng của mạng LAN;
- Định nghĩa được kích thước mạng LAN;
- Mô tả được quá trình phát triển của mạng Ethernet (IEEE 802.3);
- Mô tả được các chuẩn dùng trong Ethernet;
- Liệt kê được chức năng của card mạng (NIC) trong Ethernet;
- Liệt kê được các yêu cầu kết nối của Ethernet;
- Định nghĩa được các loại môi trường nối kết Ethernet;
- Liệt kê được đặc trưng của cáp xoắn đôi không bọc giáp (UTP);
- Phân biệt được điểm khác biệt giữa cáp thẳng và cáp chéo, giải thích cách sử dụng phù hợp cho từng loại;
- Định nghĩa và tìm được giới hạn của việc phân đoạn mạng LAN (LAN segments);
- Liệt kê được các tính chất và nhiệm vụ cuả HUB trong Ethernet LAN;
- Định nghĩa được việc đụng độ (collisions) trên LAN và liệt kê các điều kiện gây ra;
- Định nghĩa được việc miền xảy ra đụng độ trong Ethernet LAN;
- Liệt kê được danh sách các thuộc tính và nhiệm vụ cuả bridge trong việc làm giảm sự cố nghẽn mạng;
- Liệt kê được danh sách các thuộc tính và nhiệm vụ của switch;

2. Nội dung bài

2.1 Card mạng (Network Interface Card)

2.2 Môi trường truyền Ethernet

2.3 Cáp mạng, đầu nối RJ45, Giắc cắm RJ-45

2.4 Cáp thẳng, cáp chéo UTP

2.5 Các giới hạn về phân vùng mạng và mở rộng mạng cục bộ

2.6 Giải quyết các thách thức trong mạng với Công nghệ LAN Switched

2.7 Quy trình phân phối Packet (gói thông tin mạng)

BÀI 3. CƠ SỞ VỀ ĐỊNH TUYẾN - THỜI GIAN: 15 GIỜ

1. Mục tiêu của bài

- Mô tả được đặc tính vật lý của router và chức năng của router trong quá trình phân phối gói dữ liệu IP;
- Mô tả được phương pháp được sử dụng trong việc xác định đường truyền tối ưu để truyền dữ liệu;
- Liệt kê được những đặc tính của bảng định tuyến và chức năng của nó trong việc xác định đường;
- Mô tả được những đặc tính của những tuyến tĩnh (static route), tuyến động (dynamic route), tuyến kết nối trực tiếp (directly connected route) và tuyến mặc định (default route);

- Liệt kê được những đặc điểm của các giao thức định tuyến được dùng để xây dựng và duy trì bảng định tuyến một cách tự động;

2. Nội dung bài

2.1 Giới thiệu Router

2.2 Xây dựng bảng định tuyến

2.3 Giao thức định tuyến Distance Vector

2.4 Giao thức định tuyến Link-State

2.5 Cấu trúc địa chỉ mạng

2.6 Cấu hình Router cơ bản

2.7 Quá trình phân phối gói dữ liệu

2.8 Bảo mật trên Cisco Router

2.9 Sử dụng Cisco SDM

2.10 Sử dụng Cisco Router như một DHCP server

2.11 Kết nối mạng diện rộng

2.12 Cấu hình định tuyến tĩnh

2.13 Cấu hình RIP

2.14 Quản lý thiết bị Cisco

BÀI 4. CƠ SỞ VỀ BỘ CHUYỂN MẠCH - THỜI GIAN: 15 GIỜ

1. Mục tiêu của bài

- Khởi động được với một Cisco IOS switch;
- Nhận dạng được các đèn trên switch phản ánh điền kiện làm việc của switch;
- Mô tả được các kết qủa hiển thị của quá trình khởi độngtrên switch;
- Đăng nhập được vào Cisco IOS switch;
- Cấu hình được switch từ dòng lệnh;
- Kiểm định được hoạt động ban đầu của switch;
- Quản lý được bảng MAC bằng các lệnh Show tương ứng;

2. Nội dung bài

2.1 Khởi động Catalyst Switch

2.2 Đo lường bằng đèn LED trên Switch Catalyst 2960

2.3 Cấu hình Switch cơ bản

2.4 Kiểm tra cấu hình Switch

2.5 Bảo mật thiết bị Switch

2.6 Tối ưu hóa những tiện ích của Switch

2.7 Xử lý các sự cố của Switch

BÀI 5. MẠNG CỤC BỘ ẢO - THỜI GIAN: 15 GIỜ

1. Mục tiêu của bài

- Mô tả được chức năng của mạng ảo VLAN;
- Mô phỏng được vai trò của Switch trong VLAN;
- Trình bày được lợi ích của VLAN;
- Thiết lập được các VLAN;
- Triển khai được VTP, OSPF và EIGRP;

2. Nội dung bài

2.1 Triển khai VLANs và Trunks

2.2 Cải tiến hiệu suất với Spanning Tree

2.3 Định tuyến giữa các VLAN

2.4 Triển khai VTP

2.5 Triển khai OSPF

2.6 Chẩn đoán và xử lý lỗi OSPF

2.7 Triển khai EIGRP

2.8 Xử lý sự cố EIGRP

BÀI 6. XÂY DỰNG MẠNG LAN - THỜI GIAN: 20 GIỜ

1. Mục tiêu của bài

- Mô tả được quy trình thiết kế một hệ thống mạng;
- Xác định được cách đấu cáp cho các thiết bị phần cứng;
- Đọc được bảng vẽ thi công mạng;
- Cài đặt được hệ điều hành mạng;
- Cài đặt, cấu hình được các dịch vụ mạng;
- Cấu hình được các giao thức mạng;
- Xây dựng được các phương án bảo mật mạng;
- Lập được nhật kí thi công mạng;
- Thực hiện các thao tác an toàn với máy tính;

2. Nội dung bài

2.1 Các chi tiết cơ bản trên bảng vẽ thi công mạng (sử dụng microsoft visio)

2.2 Giám sát thi công mạng

2.3 Các kỹ thuật thi công công trình mạng

2.4 Các kỹ thuật đấu nối

2.5 Các bước tiến hành thi công

2.6 Đấu nối và cấu hình phần cứng

2.7 Nhật kí thi công

4. GIỚI THIỆU PHƯƠNG THỨC TỔ CHỨC MÔN HỌC VÀ PHƯƠNG PHÁP ĐÁNH GIÁ KẾT QUẢ HỌC TẬP CỦA MÔ ĐUN;

4.1 NỘI DUNG VÀ PHƯƠNG PHÁP ĐÁNH GIÁ:

4.1.1 NỘI DUNG

- Kiến thức
  + Mô tả được quy trình thiết kế một hệ thống mạng;
  + Mô phỏng được vai trò và chức năng của các thiết bị mạng;
  + Trình bày được cách thức truy nhập đường truyền;
  + Phân biệt được các loại mạng khác nhau;
  + Trình bày được nguyên tắc hoạt động của bộ định tuyến;
- Kỹ năng
  + Thiết kế được một mạng cục bộ;
  + Đọc được bảng vẽ thi công;
  + Cấu hình được bộ định tuyến bộ định tuyến;
  + Lập được hồ sơ thiết kế mạng;
  + Cài đặt được hệ điều hành;
  + Cài đặt và cấu hình được các dịch vụ mạng;
  + Bảo mật được dữ liệu cho hệ thống;
- Năng lực tự chủ và trách nhiệm
  + Bố trí làm việc khoa học đảm bảo an toàn cho người và phương tiện;
  + Rèn luyện ý thức kỷ luật trong học tập, tinh thần hợp tác, giúp đỡ lẫn nhau;

4.1.2 PHƯƠNG PHÁP, ĐÁNH GIÁ

- Học sinh được đánh giá qua cách thức thi **tích hợp**;
- Thời gian kiểm tra đánh giá: **90 phút**;

5. GIỚI THIỆU TÀI NGUYÊN HỌC HỌC TẬP (TÀI LIỆU, GIÁO TRÌNH, PHẦN MỀM, NGUỒN TÌM KIẾM VÀ THAM KHẢO, …)

5.1 NHỮNG TRỌNG TÂM CẦN CHÚ Ý

- Cấu hình cơ bản Router, Switch layer 3;
- Cấu hình định tuyến cơ bản và nâng cao;
- Cấu hình mạng riêng ảo cơ bản và nâng cao;
- Xây dựng bảng dự toán cho công trình xây dựng mạng LAN;

5.2 TÀI LIỆU THAM KHẢO

- [1]. KS. Nguyễn Công Sơn, *Hướng Dẫn Quản Trị Mạng Microsoft Windows Server 2003*, nhà xuất bản: Tổng Hợp TP. Hồ Chí Minh, năm 2005.
- [2]. Th.s Ngô Bá Hùng, Giáo trình thiết kế và cài đặt mạng, năm 2002.
- [3]. Giáo trình *Thiết kế và xây dựng mạng LAN và WAN*; Trung tâm Điện toán và Truyền số liệu KV1.
- [4].Website: https://vnpro.vn, https://quantrimang.com, https://cuongquach.com, và một số trang mạng khác.

BÀI 2. KHẢO SÁT CHỨC NĂNG MẠNG MÁY TÍNH

Giới thiệu:

Các thiết bị máy tính mạng làm nhiệm vụ khởi động, định tuyến và chấm dứt dữ liệu được gọi là các nút mạng. Các nút thường được xác định bởi địa chỉ mạng và có thể bao gồm máy chủ mạng như máy tính cá nhân, điện thoại và máy chủ, cũng như phần cứng mạng như bộ định tuyến và chuyển mạch. Hai thiết bị như vậy có thể được cho là được kết nối với nhau khi một thiết bị có thể trao đổi thông tin với thiết bị kia, cho dù chúng có kết nối trực tiếp với nhau hay không. Trong hầu hết các trường hợp, các giao thức truyền thông dành riêng cho ứng dụng được xếp lớp (nghĩa là mang theo trọng tải) so với các giao thức truyền thông chung khác.

1. Mục tiêu của bài

- Liệt kê được các thành phần chính của mạng;
- Diễn dịch được mô hình mạng;
- Liệt kê được các chức năng chia sẻ tài nguyên chính và các ưu điểm của chúng;
- Liệt kê được 4 ứng dụng mạng và các ưu điểm của mỗi ứng dụng;
- Mô tả được ảnh hưởng của ứng dụng trên mạng;
- Liệt kê được loại đặc trưng dùng để mô tả các loại mạng khác nhau;
- So sánh được các loại mô hình vật lý và luận lý (physical & logical topologies);
- Liệt kê được đặc trưng của mô hình bus;
- Liệt kê được đặc trưng của mô hình sao & sao mở rộng;
- Liệt kê được đặc trưng của mô hình vòng đơn & vòng đôi;
- Liệt kê được đặc trưng của mô hình lưới đầy đủ và không đầy đủ;
- Mô tả được các phương pháp kết nối với mạng internet;

2. Nội dung bài

2.1 Khái niệm và chức năng của vi xử lý

Vi xử lý vốn là một khái niệm đã quá quen thuộc với những người sử dụng máy tính hay những kĩ sư, lập trình viên. Tuy nhiên đây cũng là một khái niệm có một vài điểm cần lưu ý. Hôm nay trong giáo trình này sẽ khái quát lại một số những kiến thức liên quan đến vi xử lý nhé!

Với những tiến bộ của công nghệ hiện đại, vi xử lý ra đời và phát triển nhanh chóng theo thời gian. Những hãng sản xuất tên tuổi lần lượt đưa ra những vi xử lý với thương hiệu riêng của mình. Một số hãng tên tuổi với những sản phẩm hiện được bán rộng rãi như: Intel, Texas Instruments và Garett AiResearch. Đây cũng chính là ba hãng sản xuất đầu tiên cho ra đời những bộ vi xử lý hoàn chỉnh.

Vi xử lý (viết tắt là µP hay uP), đôi khi còn được gọi là bộ vi xử lý, là một linh kiện điện tử máy tính được chế tạo từ các tranzito thu nhỏ tích hợp lên trên một vi mạch tích hợp đơn. Khối xử lý trung tâm (CPU) là một bộ vi xử lý được nhiều người biết đến nhưng ngoài ra nhiều thành phần khác trong máy tính cũng có bộ vi xử lý riêng của nó, ví dụ trên card màn hình chúng ta cũng có một bộ vi xử lý. Trước khi xuất hiện các bộ vi xử lý, các CPU được xây dựng từ các mạch tích hợp cỡ nhỏ riêng biệt, mỗi mạch tích hợp chỉ chứa khoảng vào chục tranzito.

Sự tiến hóa của các bộ vi xử lý một phần nhờ vào việc chạy theo định luật Moore và hiệu suất của nó tăng lên một cách ổn định sau hàng năm. Vi xử lý chính là bộ xử lý trung tâm trong: máy tính (PC, Laptop,…), smartphone, thiết bị nhúng,... và đặc biệt trong công

nghiệp ngành điện với bộ điều khiển khả trình PLC và vi điều khiển để ứng dụng điều khiển các dây chuyền, hệ thống tự động,…

Để hiểu hơn về vi xử lý chúng ta sẽ tìm hiểu một vài thông tin chi tiết về CPU

Khái niệm CPU:

- CPU được gọi là bộ xử lý, bộ xử lý trung tâm, hoặc bộ vi xử lý, CPU viết tắt của Central Processing Unit là bộ xử lý trung tâm của máy tính. Nhiệm vụ chính của CPU là xử lý các chương trình và dữ kiện. CPU có nhiều kiểu dáng khác nhau. Ở hình thức đơn giản nhất, CPU là một con chip với vài chục chân. Phức tạp hơn, CPU được ráp sẵn trong các bộ mạch với hàng trăm con chip khác. CPU là một mạch xử lý dữ liệu theo chương trình được thiết lập trước. Nó là một mạch tích hợp phức tạp gồm hàng triệu transistor.

Cấu tạo:

- CPU được cấu tạo bởi 3 thành phần chính:
  + Bộ điều khiển: là các vi xử lí có nhiệm vụ thông dịch các lệnh của chương trình và điều khiển hoạt động xử lí, được điều tiết chính xác bởi xung nhịp đồng hồ hệ thống.
  + Bộ số học logic: có chức năng thực hiện lệnh của đơn vị điều khiển và xử lý tín hiệu. Bộ phận này thực hiện các phép tính số học hay các phép tính logic
  + Thanh ghi: Thanh ghi này có nhiệm vụ ghi mã lệnh trước khi xử lý và sau đó ghi kết quả đã xử lý.

Cách thức hoạt động:

- Với ba bước chính theo một quy trình, bao gồm: tìm nạp, giải mã, thực thi.
- Tìm nạp: Khi nhận lệnh, lênh được biểu diễn dưới dạng một chuỗi các số và chuyển tới CPU từ RAM. Mỗi lệnh chỉ là một phần nhỏ của bất kì thao tác nào vì vậy CPU cần biết lệnh nào đến tiếp theo.
- Giải mã: Khi một lệnh được tìm nạp và lưu trữ trong IR, CPU sẽ truyền lệnh tới một mạch gọi là bộ giải mã lệnh. Qua đây chuyển đổi lệnh thành các tín hiệu được chuyển qua phần khác để thực hiện hành động.
- Thực thi: Các lệnh được giải mã được gửi đến bộ phận liên quan của CPU để thực hiện. Các kết quả được ghi vào một CPU register, nơi chúng được tham chiếu bằng các lệnh sau đó.

2.2 Các ứng dụng mạng

Ngày nay, với sự phát triển của công nghệ, máy tính ngày càng trở nên quen thuộc. Hầu hết mọi lĩnh vực khoa học đều sử dụng mạng. Vậy mạng máy tính là gì? **Ứng dụng của mạng máy tính** trong đời sống hiện nay ra sao? Trong giáo trình này chúng ta cùng tìm hiểu nhé.

Mạng máy tính là gì?

- Mạng máy tính là một tập hợp các máy tính được kết nối với nhau theo một cấu trúc nào đó. Thông qua các đường truyền mà chúng có thể trao đổi dữ liệu qua lại với nhau.

Ứng dụng của mạng máy tính

- Ứng dụng của mạng máy tính có ở hầu hết mọi lĩnh vực trong cuộc sống. Từ khoa học, quân sự, quốc phòng cho đến y tế, giáo dục,… mạng máy tính đã trở nên quá quen thuộc và không thể thiếu trong cuộc sống hiện nay. Những ứng dụng mạng máy tính tạo nên những lợi ích to lớn như:

Ứng dụng của mạng máy tính đối với các cá nhân

- Đối với cá nhân, ứng dụng của mạng máy tính mang lại những sự tiện lợi như:
  + Truyền và nhận thông tin liên lạc cũng như dữ liệu từ người này qua người khác một cách dễ dàng
  + Giúp chúng ta liên lạc trực tiếp với nhau mà không cần gặp mặt trực tiếp
  + Cung cấp các trò chơi giải trí, phim ảnh,…
  + Giúp quan hệ giữa người với người trở nên dễ dàng và gần gũi hơn.

+ Xem thêm: Các loại mạng máy tính hiện nay

Ứng dụng của mạng máy tính đối với các doanh nghiệp

- Với những ứng dụng của mạng máy tính, các doanh nghiệp có thể:

+ Chia sẻ tài nguyên: Việc khai thác những **ứng dụng của mạng máy tính**, các doanh nghiệp có thể chia sẻ dữ liệu, các ứng dụng cũng như các tài nguyên khác.

+ Tăng độ tin cậy cũng như độ an toàn thông tin: **Ứng dụng của mạng máy tính** giúp thông tin gửi và nhận trên đường truyền chính xác hơn vì chúng được cập nhật theo thời gian thực. Khi một máy tính bị hỏng thì các máy còn lại vẫn hoạt động cũng như cung cấp dịch vụ bình thường, không gây ảnh hưởng đến việc truyền dữ liệu

+ Ứng dụng của mạng máy tính còn được coi là một phương tiện liên lạc hữu hiệu giữa các nhân viên trong mọi tổ chức.

Ngoài những ứng dụng kể trên, phải kể đến mặt hạn chế của mạng máy tính như:

+ Mạng máy tính càng lớn thì khả năng bị đánh cắp dữ liệu càng cao
+ Việc kiểm soát băng thông khó khăn
+ Nguy cơ lan truyền các phần mềm độc hại chứa virus dễ dàng xảy ra.

2.3 Đặc trưng của mạng

Một mạng máy tính có các đặc trưng kỹ thuật cơ bản như sau:

- Đường truyền

+ Là phương tiện dùng để truyền các tín hiệu điện tử giữa các máy tính. Các tín hiệu điệu tử đó chính là các thông tin, dữ liệu được biểu thị dưới dạng các xung nhị phân (ON_OFF), mọi tín hiệu truyền giữa các máy tính với nhau đều thuộc sóng điện từ, tuỳ theo tần số mà ta có thể dùng các đường truyền vật lý khác nhau

+ Đặc trưng cơ bản của đường truyền là giải thông nó biểu thị khả năng truyền tải tín hiệu của đường truyền.

+ Thông thuường người ta hay phân loại đường truyền theo hai loại:

+ Đường truyền hữu tuyến (các máy tính được nối với nhau bằng các dây dẫn).

+ Đường truyền vô tuyến: các máy tính truyền tín hiệu với nhau thông qua các sóng vô tuyến với các thiết bị điều chế/giải điều chế ở các đầu mút.

- Kỹ thuật chuyển mạch

+ Là đặc trưng kỹ thuật chuyển tín hiệu giữa các nút trong mạng, các nút mạng có chức năng hướng thông tin tới đích nào đó trong mạng, hiện tại có các kỹ thuật chuyển mạch như sau:

+ Kỹ thuật chuyển mạch kênh: Khi có hai thực thể cần truyền thông với nhau thì giữa chúng sẽ thiết lập một kênh cố định và duy trì kết nối đó cho tới khi hai bên ngắt liên lạc. Các dữ liệu chỉ truyền đi theo con đường cố định đó.

+ Kỹ thuật chuyển mạch thông báo: thông báo là một đơn vị dữ liệu của người sử dụng có khuôn dạng được quy định trước. Mỗi thông báo có chứa các thông tin điều khiển trong đó chỉ rõ đích cần truyền tới của thông báo. Căn cứ vào thông tin điều khiển này mà mỗi nút trung gian có thể chuyển thông báo tới nút kế tiếp trên con đường dẫn tới đích của thông báo

+ Kỹ thuật chuyển mạch gói: ở đây mỗi thông báo được chia ra thành nhiều gói nhỏ hơn được gọi là các gói tin (packet) có khuôn dạng qui định trước. Mỗi gói tin cũng chứa các thông tin điều khiển, trong đó có địa chỉ nguồn (người gửi) và địa chỉ đích (người nhận) của gói tin. Các gói tin của cùng một thông báo có thể được gửi đi qua mạng tới đích theo nhiều con đường khác nhau.

- Kiến trúc mạng

+ Kiến trúc mạng máy tính (network architecture) thể hiện cách nối các máy tính với nhau và tập hợp các quy tắc, quy ước mà tất cả các thực thể tham gia truyền thông trên mạng phải tuân theo để đảm bảo cho mạng hoạt động tốt.

+ Khi nói đến kiến trúc của mạng người ta muốn nói tới hai vấn đề là hình trạng mạng (Network topology) và giao thức mạng (Network protocol)

+ Network Topology: Cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là tô pô của mạng

+ Các hình trạng mạng cơ bản đó là: hình sao, hình bus, hình vòng

+ Network Protocol: Tập hợp các quy ước truyền thông giữa các thực thể truyền thông mà ta gọi là giao thức (hay nghi thức) của mạng

+ Các giao thức thường gặp nhất là: TCP/IP, NETBIOS, IPX/SPX,...

Hệ điều hành mạng

- Hệ điều hành mạng là một phần mềm hệ thống có các chức năng sau: Quản lý tài nguyên của hệ thống, các tài nguyên này gồm:

+ Tài nguyên thông tin (về phương diện lưu trữ) hay nói một cách đơn giản là quản lý tệp. Các công việc về lưu trữ tệp, tìm kiếm, xoá, copy, nhóm, đặt các thuộc tính đều thuộc nhóm công việc này

+ Tài nguyên thiết bị. Điều phối việc sử dụng CPU, các ngoại vi... để tối ưu hoá việc sử dụng

- Quản lý người dùng và các công việc trên hệ thống.
- Hệ điều hành đảm bảo giao tiếp giữa người sử dụng, chương trình ứng dụng với thiết bị của hệ thống.
- Cung cấp các tiện ích cho việc khai thác hệ thống thuận lợi (ví dụ FORMAT đĩa, sao chép tệp và thư mục, in ấn chung...)
- Các hệ điều hành mạng thông dụng nhất hiện nay là: WindowsNT, Windows9X, Windows 2000, Unix, Novell.

2.4 Các loại mô hình mạng

Một máy tính trên mạng có thể thuộc một trong ba loại như sau:

- *Máy trạm (Client):* Không cung cấp tài nguyên mà chỉ sử dụng tài nguyên từ mạng.
- *Máy chủ (Server):* Cung cấp tài nguyên và các dịch vụ cho các máy trên mạng.
- *Peer:* Sử dụng tài nguyên và đồng thời cũng cung cấp tài nguyên cho mạng.

Dựa vào cách mà các máy tính được nối vào mạng cũng như cách mà chúng tương tác với mạng và với nhau, mạng máy tính được chia làm ba mô hình cơ bản như sau:

Mô hình trạm-chủ (Client-Server):

- Các máy trạm được nối với các máy chủ, nhận quyền truy nhập mạng và tài nguyên mạng từ các máy chủ. Đối với Windows NT các máy được tổ chức thành các miền (domain). An ninh trên các domain được quản lý bởi một số máy chủ đặc biệt gọi là domain controller. Trên domain có một master domain controller được gọi là PDC (Primary Domain Controller) và một BDC (Backup Domain Controller) để đề phòng trường hợp PDC gặp sự cố.

Mô hình mạng ngang hàng (Peer-to-Peer):

- Mô hình này không có máy chủ, các máy trên mạng chia sẻ tài nguyên không phụ thuộc vào các máy khác trên mạng. Mạng ngang hàng thường được tổ chức thành các nhóm làm việc workgroup. Mô hình này không có quá trình đăng nhập tập trung, nếu đã đăng nhập vào mạng bạn có thể sử dụng tất cả tài nguyên trên mạng. Truy cập vào các tài nguyên phụ thuộc vào người đã chia sẻ các tài nguyên đó, do vậy bạn có thể phải biết mật khẩu để có thể truy nhập được tới các tài nguyên được chia sẻ.

Mô hình lai (Hybrid)

- Mô hình này là sự kết hợp giữa Client-Server và Peer-to-Peer. Phần lớn các mạng máy tính trên thực tế thuộc mô hình này.
- Trong các mô hình mạng nói trên, mỗi mô hình có những ưu, nhược điểm riêng đối với từng chỉ tiêu đánh giá như: tính bảo mật thông tin, sự cài đặt, khả năng mở rộng mạng... Sự so sánh giữa các mô hình mạng trên đối với một số chỉ tiêu đánh giá phổ biến được cho trong bảng sau:

Mô hình mạng / Chỉ tiêu đánh giá	Client-Server	Peer-to-Peer	Hybrid
Độ an toàn và tính bảo mật thông tin.	Có độ an toàn và bảo mật thông tin cao nhất. Quản trị mạng có thể điều chỉnh quyền truy nhập thông tin.	Độ an toàn và bảo mật kém, phụ thuộc vào mức truy nhập được chia sẻ.	Độ an toàn và bảo mật cao gần như Client-Server.
Khả năng cài đặt.	Khó cài đặt.	Dễ cài đặt.	Khó cài đặt.
Đòi hỏi về phần cứng và phần mềm.	Đòi hỏi có máy chủ, hệ điều hành mạng và các phần cứng bổ sung.	Không cần máy chủ, hệ điều hành mạng, phần cứng bổ sung rất ít.	Như Client-Server.
Quản trị mạng.	Phải có quản trị mạng.	Không cần có quản trị mạng.	Như Client-Server.
Xử lý và lưu trữ tập trung.	Có.	Không.	Không.
Chi phí cài đặt.	Cao.	Thấp.	Cao.

Trong mô hình mạng có máy chủ (server) không phải mọi máy chủ đều hoạt động như nhau mà chúng được dành riêng để thực hiện những nhiệm vụ chuyên biệt nhằm hỗ trợ các máy trạm trên mạng, một máy chủ có thể thực hiện toàn bộ các nhiệm vụ này hoặc cũng có thể có một số máy chủ sẽ thực hiện mộ nhiệm vụ riêng biệt nào đó, ví dụ như: Web server, FTP server, File server, Printer server…

Câu hỏi ôn tập

1. Liệt kê các thành phần chính của mạng;
2. Liệt kê 4 ứng dụng mạng và các ưu điểm của mỗi ứng dụng;
3. Mô tả ảnh hưởng của ứng dụng trên mạng;
4. Liệt kê đặc trưng của mô hình bus;
5. Liệt kê đặc trưng của mô hình sao & sao mở rộng;
6. Liệt kê đặc trưng của mô hình vòng đơn & vòng đôi;

7. Liệt kê đặc trưng của mô hình lưới đầy đủ và không đầy đủ;
8. Mô tả các phương pháp kết nối với mạng internet;

BÀI 3. MẠNG CỤC BỘ ETHERNET

Giới thiệu:

Ethernet đã dễ dàng trở thành công nghệ mạng LAN thành công nhất trong suốt 20 năm qua. Được phát triển vào giữa thập kỷ 1970 bởi các nhà nghiên cứu tại Xerox Palo Atlto Research Center (PARC), Ethernet là một ví dụ thực tiễn của loại mạng cục bộ sử dụng giao thức CSMA/CD.

1. Mục tiêu của bài

- Định nghĩa được mạng cục bộ (LAN);
- Quan sát và mô tả được các thành phần của mạng cục bộ;
- Liệt kê được chức năng của mạng LAN;
- Định nghĩa được kích thước mạng LAN;
- Mô tả được quá trình phát triển của mạng Ethernet (IEEE 802.3);
- Mô tả được các chuẩn dùng trong Ethernet;
- Liệt kê được chức năng của card mạng (NIC) trong Ethernet;
- Liệt kê được các yêu cầu kết nối của Ethernet;
- Định nghĩa được các loại môi trường nối kết Ethernet;
- Liệt kê được đặc trưng của cáp xoắn đôi không bọc giáp (UTP);
- Phân biệt được điểm khác biệt giữa cáp thẳng và cáp chéo, giải thích cách sử dụng phù hợp cho từng loại;
- Định nghĩa và tìm được giới hạn của việc phân đoạn mạng LAN (LAN segments);
- Liệt kê được các tính chất và nhiệm vụ cuả HUB trong Ethernet LAN;
- Định nghĩa được việc đụng độ (collisions) trên LAN, liệt kê các điều kiện gây ra;
- Định nghĩa được việc miền xảy ra đụng độ trong Ethernet LAN;
- Liệt kê được danh sách các thuộc tính và nhiệm vụ cuả bridge trong việc làm giảm sự cố nghẽn mạng;
- Liệt kê được danh sách các thuộc tính và nhiệm vụ của switch;

2. Nội dung bài

2.1 Card mạng (Network Interface Card)

2.1.1 Card mạng là gì ?

Card mạng là gì ? Card mạng hay còn gọi là card dùng để giao tiếp với internet là 1 loại bảng mạch giúp cho máy tính có thể giao tiếp với các máy khác, thông qua internet, nó có thể được gọi với tên LAN adapter, nó được sử dụng trong một khe cắm trong bo mạch chính của máy tính để bàn để có thể giúp PC giao tiếp và kết nối với môi trường mạng.

Card mạng được cắm vào các khe cắm như PCI hay qua ***cổng USB*** đều được và card mạng giao tiếp với cáp mạng bằng các chuẩn AUI, BNC, UTP…

Hình 3.1: Card mạng

2.1.2 Các chức năng cơ bản của card mạng

Card mạng giúp máy tính của bạn chuẩn bị dữ liệu để đưa lên mạng hay nhận dữ liệu từ mạng về máy tính, dữ liệu phải được chuyển đổi từ dạng byte và bit sang loại tín hiệu điện để truyền qua dây cáp và ngược lại nếu như máy tính muốn nhận dữ liệu từ mạng.

Nó giúp các máy tính giao tiếp vs nhau truyền dữ liệu qua lại giữa các máy tính kiểm soát thống kê thông tin dữ liệu từ cấp tới máy tính.

Mỗi card mạng cần có 1 địa chỉ MAC và địa chỉ đó là duy nhất không bị trùng lặp để nó phân biệt các ***card mạng*** với nhau trên mạng internet, địa chỉ MAC này được cung cấp bởi viện công nghệ điện và điện tử) và các nhà sản xuất card mạng cố định địa chỉ MAC do viện cung cấp đến các card mạng do mình tự sản xuất, địa chỉ MAC gồm 6 byte (48 bit) trong đó thì 3 byte là mã số của chính nhà sản xuất ra card mạng và 3 byte là số seri của các card mạng do hãng sản xuất, và những người am hiểu hay gọi là địa chỉ vật lý.

2.2 Môi trường truyền Ethernet

Ethernet được khám phá và phát minh đầu tiên bởi Robert Metcalfe và David Boggs của Công ty Xerox PARC vào những năng 1973 với tốc độ truyền tải ban đầu là 2.9Mbs. Sau này Metcalfe đã gia nhập vào hãng Digital và hợp tác với Intel và Xerox để phát triển công nghệ này. Và sau này khái niệm về Ethernet đã được tổ chức IEEE chuẩn hóa vào năm 1983.

Ethernet có khái niện như là một phương pháp truy cập mạng máy tính nội bộ (mạng LAN) được sử dụng đầu tiên và phổ biến nhất. Ethernet hình thành từ khái niệm chuẩn 802.3 của IEE, một tổ chức Quốc tế của nghành Điện và Điện tử có uy tín chuyên thiết lập các chuẩn cho máy tính và mạng truyền thông.

Ngày nay, mạng Lan đã hết sức phổ biến và được sử dụng rộng rãi trên toàn Thế giới và mỗi khi nhắc đến kết nối mạng là người ta nghĩ đến ngay mạng Ethernet.

Đơn giản hơn, mạng ethernet là một mạng lan có môi trường truyền thông được chia sẻ qua lại. Tất cả các trạm trên mạng lan đều chia nhau tổng số băng thông của mạng. Con số băng thông này có thể là 10Mbs, 100Mbs và 1000Mbs (Megibit per second = megabit/giây).

Ngoài ra còn có những khái niệm như Switch Ethernet đây là công nghệ mạng Ethernet sử dụng Switch để thay cho các thiết bị Hub. Với công nghệ này mỗi máy tính truyền và nhận tín hiệu sẽ có một đường truyền băng thông riêng với đầy đủ tần số bằng thông đầy đủ.

Các loại dây sử dụng trong mạng Ethernet

- Mạng Ethernet LAN có thể sử dụng các loại cáp để truyền tín hiệu như: cáp đồng trục, cáp mạng, cáp quang. Mạng ethernet sử dụng cả 2 cấu trúc tuyến tính và hình sao.

Hai chuẩn mạng Ethernet phổ biến

- Tất cả các máy tính trên cùng mạng Lan đều có khả năng truy cập mạng, tuy nhiên khi phát hiện sự va chạm của nhiều gói thông tin khác nhau trên mạng lan thì toàn bộ các gói thông tin đang truyền sẽ bị loại bỏ để truyền lại. Ngày nay chúng ta chỉ cần quan tâm tới 2 chuẩn Ethernet được sử dụng phổ biến nhất đó là:

+ **Tốc độ 10/100Mbs đây là tốc độ mạng đạt chuẩn Megabit** truyền tải ở nhu cầu phổ thông đa số các kết nối internet mà ta đang sử dụng đều có tốc độ đạt chuẩn giga này.

+ **Tốc độ 10/100/1000Mbs là tốc độ mạng đạt chuẩn Gigabit** truyền tải dành cho nhu cầu cao cấp hơn, thương bắt gặp ở các sever quán nét, hoặc các doanh nghiệp có tính chất công việc sử dụng kết nối internet nhiều.

2.3 Cáp mạng, đầu nối RJ45, Giắc cắm RJ-45

2.3.1 Dây cáp mạng là gì?

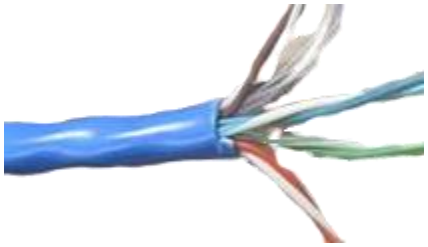
Dây cáp mạng được biết đến là dây dẫn dạng xoắn làm từ kim loại hay hợp kim được chia thành nhiều loại khác nhau nhưng chủ yếu là cáp đồng và cáp quang bao bọc bên ngoài là một lớp vỏ nhựa cách điện.

Cùng với sự phát triển của công nghệ hiện đại các thiết bị có khả năng kết nối mạng ngày càng nhiều nhưng chúng ta không nên bỏ qua sản phẩm thông minh này,dây mạng này được thiết kế nhỏ gọn, tiện dụng dễ dàng dàng trong việc vận chuyển và lắp đặt.giá thành lại hợp lí đáp ứng được các nhu cầu của người sử dụng.

Phân loại các loại dây cáp mạng

Trên thực tế có rất nhiều loại cáp khác nhau được tạo ra với các mục đích khác nhau, tuy nhiên có một số loại cáp cơ bản trên thị trường được nhiều người sử dụng nhất và có tính phổ biến cao. Đó chính là những loại cáp sau đây:

Cáp mạng CAT 5



Hình 3.2*: Dây cáp mạng CAT5*

- Cáp mạng CAT5 là loại cáp được sử dụng phổ biến nhất với giá thành rẻ nhất trên thị trường, được thiết kế đạt chuẩn. Sử dụng loại cáp này bạn sẽ thấy có hoặc không có bọc kim loại chống nhiễu bao quanh cáp bao quanh 8 sợi cáp trước khi được bọc lớp vỏ nhựa bên ngoài. Lõi của các dây cáp là 1 lõi đặc nhiều sợi bện giúp truyền tín hiệu tốt hơn. Tốc độ đường truyền dữ liệu tối đa là 100 Mbps.

Cáp mạng CAT 5E

- Cáp CAT 5E giống như cáp CAT 5 nhưng được sản xuất theo tiêu chuẩn kỹ thuật khắt khe và nổi trội hơn và hiệu quả sử dụng cũng tốt hơn rất nhiều. Gần đây hầu hết người dùng thường chọn cáp CAT 5E này để sử dụng bởi giá của cũng không chênh lệch nhiều so với những dây cáp khác mà tốc độ sử dụng thì được cải thiện hơn. Mặt khác cáp này cho phép truyền dữ liệu tốt hơn rất nhiều 1000 Mbps và giảm nhiễu trong quá trình truyền tín hiệu tốt hơn hẳn so với CAT 5.

Cáp mạng CAT 6

- Cáp CAT6 truyền dữ liệu ổn định và xa hơn các loại cáp bên trên. Cũng sở hữu cấu trúc chữ thập và các vỏ nhựa được gia cố dày hơn. với lớp vỏ chống nhiễu tối đa, chịu đựng điều kiện môi trường khắc nhiệt. Tốc độ đáp ứng với quãng đường xa hơn rất nhiều. Chính vì thế mà loại cáp này giá thành của cáp rất cao bên cạnh đó người dùng lại thường ít khai thác hết sức mạng của cáp nên không được sử dụng nhiều.

Hình 3.3*: Cáp mạng CAT 6 chống nhiễu*

- Trên đây là phân loại những dây cáp khác nhau với hiệu quả khác nhau, tìm hiểu những loại dây cáp này hi vọng bạn sẽ có sự lựa chọn đúng cho việc khai thác và sử dụng của mình.

Vai trò, ứng dụng của dây cáp mạng

- Dây cáp mạng có dây là sản phẩm thông dụng nhất mà bất cứ ai đang sử dụng internet đều biết đến, dây mạng phổ biến với chiều dài 100m kết nối mạng đến máy tính của chúng ta. Dây mạng đươc sử dụng trong nhiều thiết bị thông minh khác nhau từ các phòng máy đến các hệ thống mạng LAN, mạng khu vực hay thậm chí là các hệ thống mạng xuyên quốc gia.Tuy nhiên thực tế hơn hết vẫn là việc sử dụng dây mạng trong sinh hoạt hàng ngày từ việc kết nối Internet.Chỉ cần cắm đầu mạng vào thiết bị là bạn đã có thể kết nối mạng và sử dụng bất cứ lúc nào, việc **sử dụng dây cáp mạng** sẽ ổn định hơn, tốc độ đường truyền nhanh hơn và hiệu quả cho công việc hơn.
- Việc sử dụng dây cáp mạng sẽ đem lại hiệu quả tốt hơn nhiều so với việc sử dụng mạng không dây, có nghĩa là việc truy cập sử dụng mạng để tìm kiếm hay làm việc sẽ nhanh hơn rất nhiều.

2.3.2 Đầu nối RJ45

Đầu nối mạng LAN RJ45 giúp bạn dễ dàng kết nối tín hiệu Internet khi mà sợi dây cáp mạng không đủ độ dài để kết nối. Hỗ trợ tốc độ truyền tải tín hiệu lên tới 10Gbps.

Hình 3.4 Đầu nối mạng LAN RJ45

2.3.3 Giắc cắm RJ-45

RJ-45 là tên gọi tắt của một loại dây cáp được cấu tạo bởi 8 dây nhỏ chia làm 4 cặp với màu sắc khác nhau và còn có tên gọi khác là dây cáp mạng. Mỗi đầu dây mạng khi sử dụng được để kết nối với các thiết bị như Modem, Hub, Switch cần phải có một đầu bấm để kết nối, loại đầu bấm này được gọi là hạt mạng RJ-45.

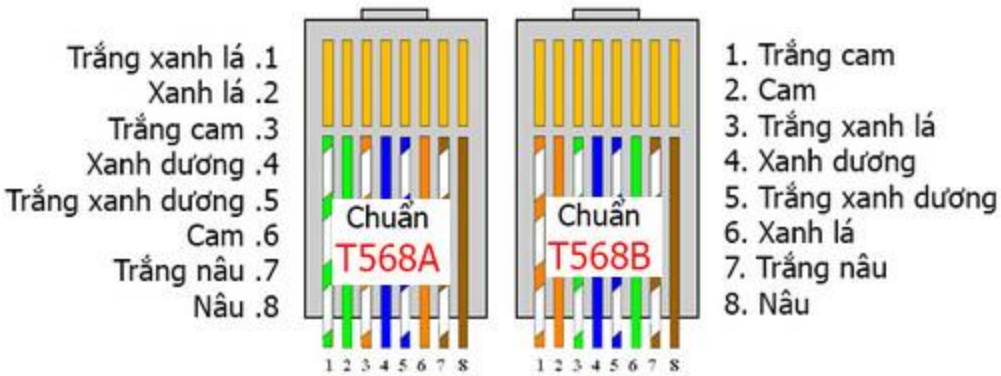
2.4 Cáp thẳng, cáp chéo UTP

Hiện nay có 2 chuẩn bấm cáp dây mạng là chuẩn **T568A** (gọi tắt là chuẩn A) và chuẩn **T568B** (gọi tắt là chuẩn B).

- Đối với mỗi chuẩn thì có cách sắp xếp màu các dây khác nhau:

+ **Chuẩn T568A**: Trắng xanh lá - Xanh lá - Trắng cam - Xanh dương - Trắng xanh dương - Cam - Trắng nâu - Nâu.

+ **Chuẩn T568B**: Trắng cam - Cam - Trắng xanh lá - Xanh dương - Trắng xanh dương - Xanh lá - Trắng nâu - Nâu.



Hình 3.5 Chuẩn T568A và T568B

- Trong một dây cáp đạt chuẩn qui định bao gồm tám sợi dây đồng trong đó mỗi hai sợi xoắn với nhau thành từng cặp theo qui định nâu - trắng nâu, cam - trắng cam, xanh lá -

trắng xanh lá, xanh dương - trắng xanh dương và 1 sợi dây kẽm. Sợi dây kẽm này chỉ có chức năng làm cho sợi dây cáp chắc chắn hơn. Sợi dây cáp này sẽ được nối với một đầu RJ45 để bấm dây mạng thì phải bấm tám sợi dây đồng vào các điểm tiếp xúc bằng đồng trong đầu RJ45.

2.4.1 Các kiểu bấm cáp dây mạng

Đối với hạt mạng loại RJ45 thì chúng ta sẽ có 2 kiểu bấm đó là kiểu bấm cáp thẳng (Straight through) và kiểu bấm cáp chéo (Crossover).

- Bấm cáp thẳng: là khi bạn bấm cả 2 đầu cùng 1 chuẩn, ví dụ như A–A hoặc B–B.
- Bấm cáp chéo: là khi bạn bạn bấm 1 đầu là chuẩn A và đầu còn lại là chuẩn B.

2.4.2 Cách dùng kiểu bấm thẳng và bấm chéo

Bấm cáp thẳng: Các bạn dùng kiểu này để kết nối từ máy tính đến hub/switch. Nối switch đến router, nối switch đến PC hoặc server, nối hub đến PC hoặc server…. Tóm lại là bạn sử dụng kiểu bấm cáp thẳng để kết nối giữa các thiết bị khác loại với nhau.

- Lý do: Đầu nhận của bên này là đầu gửi của bên kia rồi, nên kiểu bấm thẳng sẽ dùng nối 2 thiết bị khác loại.

Bấm cáp chéo: Các bạn dùng kiểu này để nối 2 máy tính lại với nhau mà không dùng hub/switch. Nối switch đến switch, nối switch đến hub, nối hub đến hub, nối router đến rounter, nối PC đến PC, nối router đến PC…Nói tóm lại là bạn sử dụng kiểu bấm cáp chéo để kết nối giữa các thiết bị cùng loại.

- Lý do: Đầu nhận của bên này là đầu nhận của bên kia luôn nên phải đảo chéo lại để nó có thể gửi nhận đúng.

2.5 Các giới hạn về phân vùng mạng và mở rộng mạng cục bộ

Nếu lấy khoảng cách địa lý làm yếu tố phân loại mạng thì ta có mạng cục bộ, mạng đô thị, mạng diện rộng, mạng toàn cầu. Mạng cục bộ (LAN - Local Area Network): là mạng được cài đặt trong phạm vi tương đối nhỏ hẹp như trong một toà nhà, một xí nghiệp...với khoảng cách lớn nhất giữa các máy tính trên mạng trong vòng vài km trở lại.

2.6 Giải quyết các thách thức trong mạng với Công nghệ LAN Switched

Mạng cục bộ (LAN) là hệ truyền thông tốc độ cao được thiết kế để kết nối các máy tính và các thiết bị xử lý dữ liệu khác cùng hoạt động với nhau trong một khu vực địa lý nhỏ như ở một tầng của toà nhà, hoặc trong một toà nhà Một số mạng LAN có thể kết nối lại với nhau trong một khu làm việc.

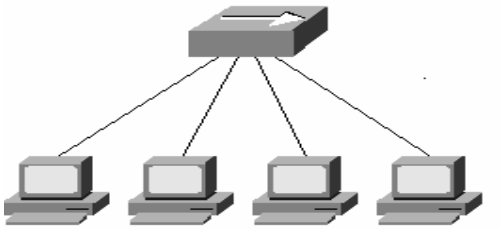
Các mạng LAN trở nên thông dụng vì nó cho phép những người sử dụng dùng chung những tài nguyên quan trọng như máy in, ổ đĩa CD-ROM, các phần mềm ứng dụng và những thông tin cần thiết khác. Trước khi phát triển công nghệ LAN các máy tính là độc lập với nhau, bị hạn chế bởi số lượng các chương trình tiện ích, sau khi kết nối mạng rõ ràng hiệu quả của chúng tăng lên gấp bội.

Cấu trúc tôpô của mạng

- Cấu trúc tôpô (network topology) của LAN là kiến trúc hình học thể hiện cách bố trí các đường cáp, sắp xếp các máy tính để kết nối thành mạng hoàn chỉnh. Hầu hết các mạng LAN ngày nay đều được thiết kế để hoạt động dựa trên một cấu trúc mạng định trước. Điển hình và sử dụng nhiều nhất là các cấu trúc: dạng hình sao, dạng hình tuyến, dạng vòng cùng với những cấu trúc kết hợp của chúng.

Mạng dạng hình sao (Star topology)

- Mạng dạng hình sao bao gồm một bộ kết nối trung tâm và các nút. Các nút này là các trạm đầu cuối, các máy tính và các thiết bị khác của mạng. Bộ kết nối trung tâm của mạng điều phối mọi hoạt động trong mạng.
- Mạng dạng hình sao cho phép nối các máy tính vào một bộ tập trung (Hub) bằng cáp, giải pháp này cho phép nối trực tiếp máy tính với Hub không cần thông qua trục bus, tránh được các yếu tố gây ngưng trệ mạng.



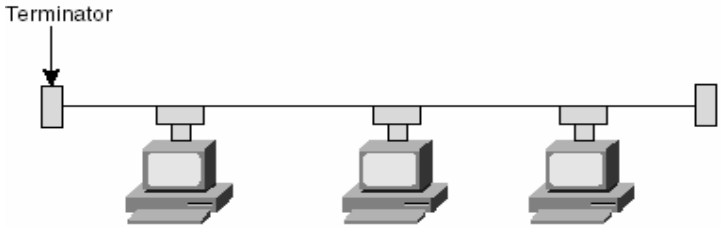
Hình 3.6 Cấu trúc mạng hình sao

Mô hình kết nối hình sao ngày nay đã trở lên hết sức phổ biến. Với việc sử dụng các bộ tập trung hoặc chuyển mạch, cấu trúc hình sao có thể được mở rộng bằng cách tổ chức nhiều mức phân cấp, do vậy dễ dàng trong việc quản lý và vận hành.

- Các ưu điểm của mạng hình sao:
  + Hoạt động theo nguyên lý nối song song nên nếu có một thiết bị nào đó ở một nút thông tin bị hỏng thì mạng vẫn hoạt động bình thường.
  + Cấu trúc mạng đơn giản và các thuật toán điều khiển ổn định.
  + Mạng có thể dễ dàng mở rộng hoặc thu hẹp.
- Những nhược điểm mạng dạng hình sao:
  + Khả năng mở rộng mạng hoàn toàn phụ thuộc vào khả năng của trung tâm.
  + Khi trung tâm có sự cố thì toàn mạng ngừng hoạt động.
  + Mạng yêu cầu nối độc lập riêng rẽ từng thiết bị ở các nút thông tin đến trung tâm. Khoảng cách từ máy đến trung tâm rất hạn chế (100m).

Mạng hình tuyến (Bus Topology)

- Thực hiện theo cách bố trí hành lang, các máy tính và các thiết bị khác - các nút, đều được nối về với nhau trên một trục đường dây cáp chính để chuyển tải tín hiệu. Tất cả các nút đều sử dụng chung đường dây cáp chính này.
- Phía hai đầu dây cáp được bịt bởi một thiết bị gọi là terminator. Các tín hiệu và dữ liệu khi truyền đi dây cáp đều mang theo địa chỉ của nơi đến.

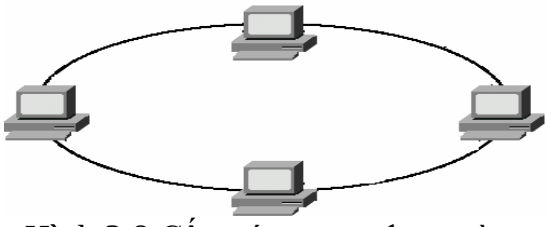


Hình 3.7 Cấu trúc mạng hình tuyến

- Ưu điểm:
  + Loại hình mạng này dùng dây cáp ít nhất, dễ lắp đặt, giá thành rẻ.
- Nhược điểm:
  + Sự ùn tắc giao thông khi di chuyển dữ liệu với lưu lượng lớn.
  + Khi có sự hỏng hóc ở đoạn nào đó thì rất khó phát hiện, một sự ngừng trên đường dây để sửa chữa sẽ ngừng toàn bộ hệ thống.
  + Cấu trúc này ngày nay ít được sử dụng.

Mạng dạng vòng (Ring Topology)

- Mạng dạng này, bố trí theo dạng xoay vòng, đường dây cáp được thiết kế làm thành một vòng khép kín, tín hiệu chạy quanh theo một chiều nào đó. Các nút truyền tín hiệu cho nhau mỗi thời điểm chỉ được một nút mà thôi. Dữ liệu truyền đi phải có kèm theo địa chỉ cụ thể của mỗi trạm tiếp nhận.
- Ưu điểm:
  + Mạng dạng vòng có thuận lợi là có thể nới rộng ra xa, tổng đường dây cần thiết ít hơn so với hai kiểu trên
  + Mỗi trạm có thể đạt được tốc độ tối đa khi truy nhập.
- Nhược điểm:
  + Đường dây phải khép kín, nếu bị ngắt ở một nơi nào đó thì toàn bộ hệ thống cũng bị ngừng.



Hình 3.8 Cấu trúc mạng dạng vòng

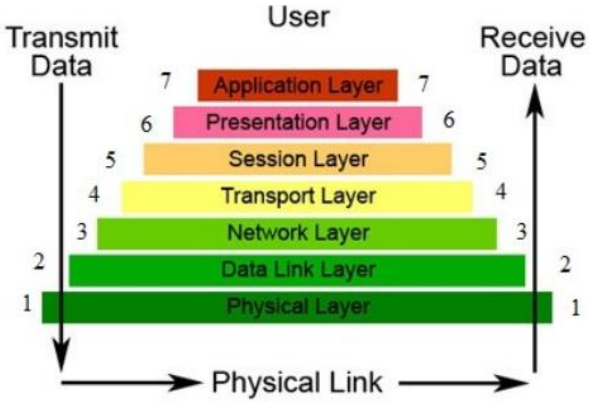
Mạng dạng kết hợp

- Kết hợp hình sao và tuyến (*Star/Bus Topology*): Cấu hình mạng dạng này có bộ phận tách tín hiệu (*spitter*) giữ vai trò thiết bị trung tâm, hệ thống dây cáp mạng có thể chọn hoặc *Ring Topology* hoặc *Linear Bus Topology*. Lợi điểm của cấu hình này là mạng có thể gồm nhiều nhóm làm việc ở cách xa nhau, ARCNET là mạng dạng kết hợp *Star/Bus Topology*. Cấu hình dạng này đưa lại sự uyển chuyển trong việc bố trí đường dây tương thích dễ dàng đối với bất cứ toà nhà nào.
- Kết hợp hình sao và vòng *(Star/Ring Topology)*. Cấu hình dạng kết hợp *Star/Ring Topology*, có một "thẻ bài" liên lạc (*Token*) được chuyển vòng quanh một cái HUB trung tâm. Mỗi trạm làm việc (*workstation*) được nối với HUB - là cầu nối giữa các trạm làm việc và để tăng khoảng cách cần thiết.

2.7 Quy trình phân phối Packet (gói thông tin mạng)

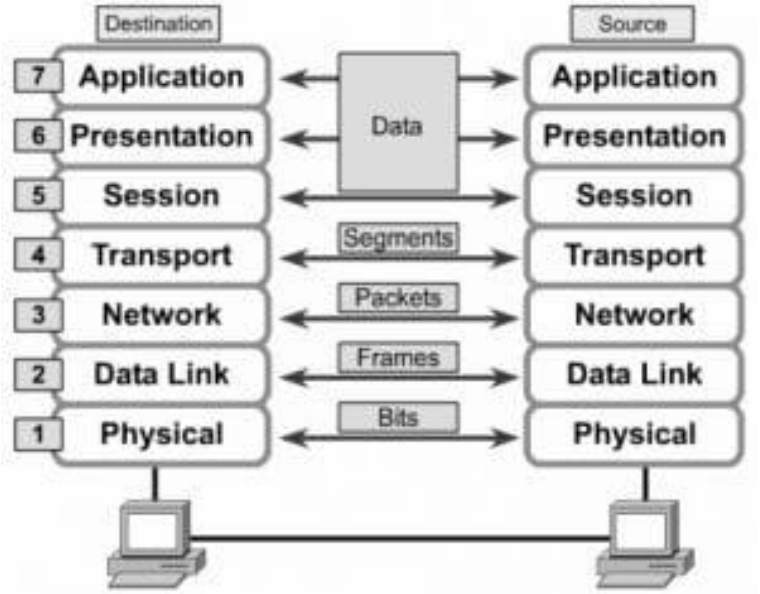
Trong thời đại công nghệ phát triển ngày nay, chắc hẳn ai trong số chúng ta đều đã sử dụng chức năng gửi 1 hình ảnh, email, bài hát,… cho một máy tính khác để đưa thông tin đến cho người nhận. Công việc tưởng chừng như rất đơn giản nhưng có khi nào các bạn thắc mắc vì sao 1 file nhac, 1 hình ảnh hay 1 thư điện tử lại có thể truyền đến cho người nhận không. Chắc hẳn các bạn đã nghĩ nó thật kì diệu. Trong giáo trình này sẽ giúp các bạn hình dung và hiểu rõ cơ chế hoạt động cũng như cách thức gửi nhận của một dữ liệu từ một máy tính này đến một máy tính khác các bạn nhé.

2.7.1 Tổng quan



Hình 3.9 Mô hình bảy lớp OSI

Theo sơ đồ ở trên thì mô hình OSI gồm có 7 tầng và được đánh số thứ tự từ dưới lên từ 1 đến 7. Và ở đây các bạn có thể thấy rằng có 2 trạng thái đó là "Transmit Data" và "Receive Data". Ở đây 2 trạng thái này có nghĩa là truyền dữ liệu và nhận dữ liệu. Các bạn có thể hiểu nôm na ở đây là bên người gửi dữ liệu, máy tính gửi còn bên kia là bên người nhận, máy tính nhận dữ liệu. Và như các đã thấy, bên phía người gửi thì gói tin sẽ đi từ tầng 7 xuống tầng 1 và ngược lại.

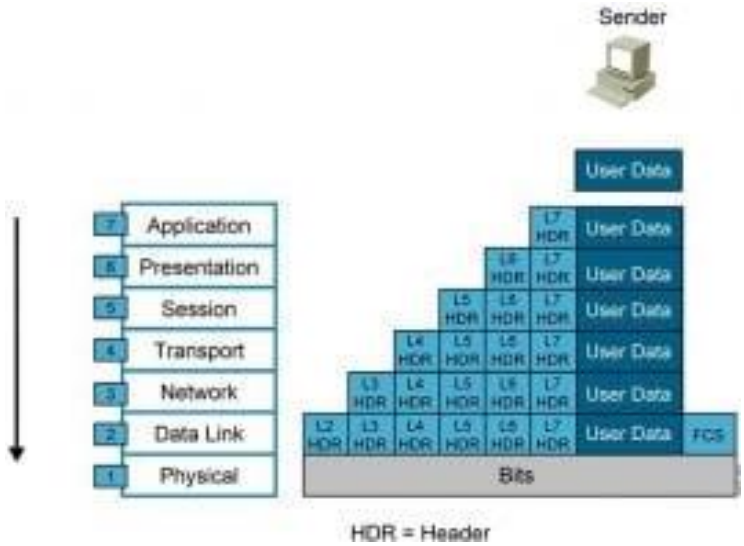


Hình 3.10 Data, Segments, Packets, Frames, Bits trong mô hình OSI

- Data, Segments, Packets, Frames, Bits là đơn vị truyền dữ liệu giữa các tầng.

Quy trình xử lý dữ liệu trong mô hình OSI

- **Phía máy gửi**



Hình 3.11 Mô phỏng dịch vụ người gởi qua mô hình OSI

+ Ở tầng Application (tầng 7), người dùng tiến hành đưa thông tin cần gửi vào máy tính. Các thông tin này thường có dạng như: hình ảnh, văn bản,…

+ Sau đó thông tin dữ liệu này được chuyển xuống tầng Presentation (tầng 6) để chuyển các dữ liệu thành một dạng chung để mã hóa dữ liệu và nén dữ liệu.

+ Dữ liệu tiếp tục được chuyển xuống tầng Session (Tầng 5). Tầng này là tầng phiên có chức năng bổ sung các thông tin cần thiết cho phiên giao dịch (gửi- nhận) này. Các bạn

có thể hiêu nôm na là tâng phiên cũng giống như các cô nhân viên ngân hàng làm nhiệm vụ xác nhận, bổ sung thông tin giao dịch khi bạn chuyển tiền tại ngân hàng.

+ Sau khi tầng Session thực hiện xong nhiệm vụ, nó sẽ tiếp tục chuyển dữ liệu này xuống tầng Transport (Tầng 4). Tại tầng này, dữ liệu được cắt ra thành nhiều Segment và cũng làm nhiệm vụ bổ sung thêm các thông tin về phương thước vận chuyển dữ liệu để đảm bảo tính bảo mật, tin cậy khi truyền trong mô hình mạng.

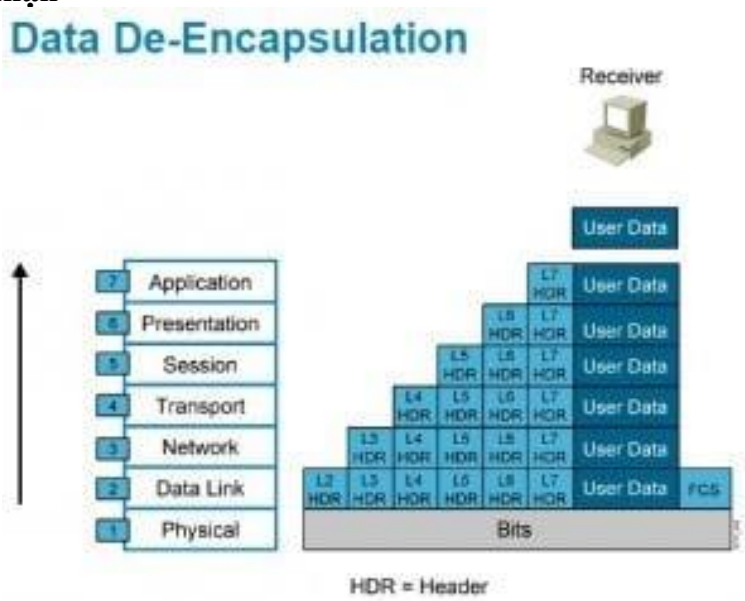
+ Tiếp đó, dữ liệu sẽ được chuyển xuống tầng Network (Tầng 3). Ở tầng này, các segment lại tiếp tục được cắt ra thành nhiều gói Package khác nhau và bổ sung thông tin định tuyến. Tầng Network này chức năng chính của nó là định tuyến đường đi cho gói tin chứa dữ liệu.

+ Dữ liệu tiếp tục được chuyển xuống tầng Data Link (tầng 2). Tại tầng này, mỗi Package sẽ được băm nhỏ ra thành nhiều Frame và bổ sung thêm các thông tin kiểm tra gói tin chứa dữ liệu để kiểm tra ở máy nhận.

+ Cuối cùng, các Frame này khi chuyển xuống tầng Physical (Tầng 1) sẽ được chuyển thành một chuỗi các bit nhị phân (0 1….) và được đưa lên cũng như phá tín hiệu trên các phương tiện truyền dẫn (dây cáp đồng, cáp quang,…) để truyền dữ liệu đến máy nhận.

+ Mỗi gói tin dữ liệu khi được đưa xuống các tầng thì được gắn các header của tầng đó, riêng ở tầng 2 (Data Link), gói tin được gắn thêm FCS.

- **Phía máy nhận**



Hình 3.12 Mô phỏng dịch vụ người nhận qua mô hình OSI

+ Tầng Physical (tầng 1) phía máy nhận sẽ kiểm tra quá trình đồng bộ và đưa các chuỗi bit nhị phân nhận được vào vùng đệm. Sau đó gửi thông báo cho tầng Data Link (Tầng 2) rằng dữ liệu đã được nhận.

+ Tiếp đó tầng Data Link sẽ tiến hành kiểm tra các lỗi trong frame mà bên máy gửi tạo ra bằng cách kiểm tra FCS có trong gói tin được gắn bên phía máy nhận. Nếu có lỗi xảy ra thì frame đó sẽ bị hủy bỏ. Sau đó kiểm tra địa chỉ lớp Data Link (Địa chỉ MAC Address) xem có trùng với địa chỉ của máy nhận hay không. Nếu đúng thì lớp Data Link sẽ thực hiện gỡ bỏ Header của tầng Data Link để tiếp tục chuyển lên tầng Network.

+ Tầng Network sẽ tiến hành kiểm tra xem địa chỉ trong gói tin này có phải là địa chỉ của máy nhận hay không. (Lưu ý: địa chỉ ở tầng này là địa chỉ IP). Nếu đúng địa chỉ máy nhận, tầng Network sẽ gỡ bỏ Header của nó và tiếp tục chuyển đến tầng Transport để tiếp tục qui trình.

+ Ở tầng Transport sẽ hỗ trợ phục hồi lỗi và xử lý lỗi bằng cách gửi các gói tin ACK, NAK (gói tin dùng để phản hồi xem các gói tin chứa dữ liệu đã được gửi đến máy nhận hay chưa?). Sau khi phục hồi sửa lỗi, tầng này tiếp tục sắp xếp các thứ tự phân đoạn và đưa dữ liệu đến tầng Session.

+ Tầng Session làm nhiệm vụ đảm bảo các dữ liệu trong gói tin nhận được toàn vẹn. Sau đó tiến hành gỡ bỏ Header của tầng Session và tiếp tục gửi lên ầng Presentation.

+ Tầng Presentation sẽ xử lý gói tin bằng cách chuyển đổi các định dạng dữ liệu cho phù hợp. Sau khi hoàn thành sẽ tiến hành gửi lên tầng Application.

+ Cuối cùng, tầng Application tiến hành xử lý và gỡ bỏ Header cuối cùng. Khi đó ở máy nhận sẽ nhận được dữ liệu của gói tin được truyền đi.

Như vậy:

Quá trình truyền và nhận một gói tin được thực hiện trong mô hình mạng máy tính được thực hiện một cách trình tự. Hi vọng qua giáo trình này, các bạn có thể hình dung cụ thể đường đi của một gói tin khi chúng ta tiến hành gửi một dữ liệu nào đó. Để qua đó có thể hiểu rõ hơn những công nghệ mà chúng ta đang được sử dụng trong xã hội ngày nay không phải là một thứ gì đó quá mơ hồ, mà tất cả đều dựa trên một qui trình và công nghệ do con người làm chủ và tạo ra chúng.

Câu hỏi ôn tập

1. Định nghĩa mạng cục bộ (LAN);
2. Mô tả các thành phần của mạng cục bộ (LAN);
3. Liệt kê chức năng của mạng LAN;
4. Mô tả các chuẩn dùng trong Ethernet;
5. Liệt kê chức năng của card mạng (NIC) trong Ethernet;
6. Liệt kê các yêu cầu kết nối của Ethernet;
7. Định nghĩa các loại môi trường nối kết Ethernet;
8. Liệt kê đặc trưng của cáp xoắn đôi không bọc giáp (UTP);
9. Điểm khác biệt giữa cáp thẳng và cáp chéo, giải thích cách sử dụng phù hợp cho từng loại;
10. Liệt kê tính chất và nhiệm vụ của HUB trong Ethernet LAN;

BÀI 4. CƠ SỞ VỀ ĐỊNH TUYẾN

Giới thiệu:

Trong ngành mạng máy tính, **định tuyến** (tiếng Anh: *routing* hay *routeing*) là quá trình chọn lựa các đường đi trên một mạng máy tính để gửi dữ liệu qua đó. Việc định tuyến được thực hiện cho nhiều loại mạng, trong đó có mạng điện thoại, liên mạng, Internet, mạng giao thông. Vì vậy việc xây dựng bảng định tuyến, được tổ chức trong bộ nhớ của router, trở nên vô cùng quan trọng cho việc định tuyến hiệu quả.

1. Mục tiêu của bài

- Mô tả được đặc tính vật lý của router và chức năng của router trong quá trình phân phối gói dữ liệu IP;
- Mô tả được phương pháp được sử dụng trong việc xác định đường truyền tối ưu để truyền dữ liệu;
- Liệt kê được những đặc tính của bảng định tuyến và chức năng của nó trong việc xác định đường;
- Mô tả được những đặc tính của những tuyến tĩnh (static route), tuyến động (dynamic route), tuyến kết nối trực tiếp (directly connected route) và tuyến mặc định (default route);
- Liệt kê được những đặc điểm của các giao thức định tuyến được dùng để xây dựng và duy trì bảng định tuyến một cách tự động;

2. Nội dung bài

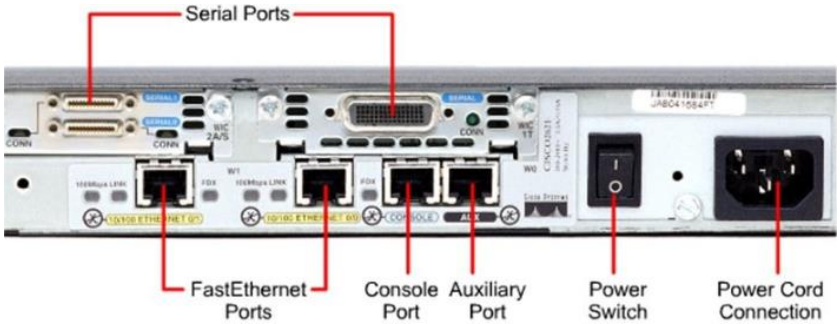
2.1 Giới thiệu Router

2.1.1 Phần cứng và cấu trúc của Router

Phần cứng: phần cứng của Router gần tương đồng về các thành phần với PC

Router	PC
Main	Main
CPU	CPU
RAM: là nơi chạy file Runingconfig. Bao gồm: bảng định tuyến, MAC, NAT, ACL	RAM
+ NVRAM: là bộ nhớ lưu file cấu hình: Startup config + Flash: là bộ nhớ lưu file IOS	HDD

Cổng kết nối:



Hình 4.1 Các cổng kết nối của Router

- Chúng ta có thể truy cập và điều khiển từ máy tính tới Router bằng các đường:

+ **Đường console:** kết nối trực tiếp từ máy tính tới Router bằng cáp Console (một đầu cắm vào cổng com trên máy tính, một đầu cổng console của Router hoặc Switch). Cáp console có tốc độ thấp 56kb/s nên chỉ được dùng thiết lập ban đầu

+ **Telnet or SSH:** kết nối tới Router hoặc Switch thông qua cổng mạng. Kết nối này có tốc độ cao và cho phép truy cập từ xa. Trong đó telnet có tốc độ nhanh hơn. Nhưng không hỗ trợ bảo mật. SSH hỗ trợ bảo mật nhưng tốc độ truyền chậm hơn. Vì vậy người ta thường dùng SSH trong những khu vực không an toàn, và Telnet trong những khu vực mạng an toàn.

+ **AUX:** Chỉ hỗ trợ trên Router: cũng cho phép kết nối tới Router từ xa, thông qua đường truyền Modem. Tuy nhiên loại kết nối này thường không được sử dụng.

IOS (Internetwork Operating System): Hệ điều hành của thiết bị Cisco

Tương tự như một máy tính, một router hoặc switch hoạt động thì phải có hệ điều hành. Cisco Internetwork Operating System (IOS) là phần mềm hệ thống trong các thiết bị của Cisco. Nó là công nghệ cốt lõi được mở rộng trên hầu hết các dòng sản phẩm của Cisco

+ Cisco IOS cung cấp cho các thiết bị với các dịch vụ mạng sau đây:
+ => Chức năng định tuyến và chuyển mạch
+ => Tin cậy và truy cập bảo mật vào tài nguyên mạng
+ => Khản năng mở rộng hệ thống.

- Chú ý về IOS:
  + => Hệ điều hành hoạt động là khác nhau trên từng thiết bị (Router hoặc Switch)
  + => Các thiết bị đều truy cập bằng lệnh
  + => File os nặng khoảng 40M. Nó được lưu trong bộ nhớ Flash. Bộ nhớ flash cung cấp lưu trữ không mất dữ liệu.
  + => Sử dụng Flash memory có thể copy vào là chạy

Quá trình khởi động của Router:

- Bước 1: Khi bật Router điện sẽ được nạp vào ROM
- Bước 2: ROM sẽ thực hiện quá trình kiểm tra các thiết bị phần cứng gọi là POST (Power on self test)
- Bước 3: Sau khi kiểm tra phần cứng chạy ổn định sẽ chuyển sang Bootstrap. Bootstrap sẽ liên lạc với IOS, IOS sẽ được load từ bộ nhớ Flash (bootstrap cho phép hệ điều hành nào khở động trước nếu có nhiều IOS).
- Bước 4: tiếp theo file cấu hình (Start up config) được copy từ bộ nhớ NVRAM
- Bước 5: IOS và Startup Config được load vào RAM tạo thành file chạy Running config.

2.2 Xây dựng bảng định tuyến

Các giao thức định tuyến

Trong ngành mạng máy tính, định tuyến (tiếng Anh: routing hay routeing) là quá trình chọn lựa các đường đi trên một mạng máy tính để gửi dữ liệu qua đó. Việc định tuyến được thực hiện cho nhiều loại mạng, trong đó có mạng điện thoại, liên mạng, Internet, mạng giao thông.

Routing chỉ ra hướng, sự di chuyển của các gói (dữ liệu) được đánh địa chỉ từ mạng nguồn của chúng, hướng đến đích cuối thông qua các node trung gian; thiết bị phần cứng chuyên dùng được gọi là router (bộ định tuyến). Tiến trình định tuyến thường chỉ hướng đi dựa vào bảng định tuyến, đó là bảng chứa những lộ trình tốt nhất đến các đích khác nhau trên mạng. Vì vậy việc xây dựng bảng định tuyến, được tổ chức trong bộ nhớ của router, trở nên vô cùng quan trọng cho việc định tuyến hiệu quả.

Routing khác với bridging (bắc cầu) ở chỗ trong nhiệm vụ của nó thì các cấu trúc địa chỉ gợi nên sự gần gũi của các địa chỉ tương tự trong mạng, qua đó cho phép nhập liệu một bảng định tuyến đơn để mô tả lộ trình đến một nhóm các địa chỉ. Vì thế, routing làm việc

tốt hơn bridging trong những mạng lớn, và nó trở thành dạng chiếm ưu thế của việc tìm đường trên mạng Internet.

Các mạng nhỏ có thể có các bảng định tuyến được cấu hình thủ công, còn những mạng lớn hơn có topo mạng phức tạp và thay đổi liên tục thì xây dựng thủ công các bảng định tuyến là vô cùng khó khăn. Tuy nhiên, hầu hết mạng điện thoại chuyển mạch chung (public switched telephone network - PSTN) sử dụng bảng định tuyến được tính toán trước, với những tuyến dự trữ nếu các lộ trình trực tiếp đều bị nghẽn. Định tuyến động (dynamic routing) cố gắng giải quyết vấn đề này bằng việc xây dựng bảng định tuyến một cách tự động, dựa vào những thông tin được giao thức định tuyến cung cấp, và cho phép mạng hành động gần như tự trị trong việc ngăn chặn mạng bị lỗi và nghẽn.

Định tuyến động chiếm ưu thế trên Internet. Tuy nhiên, việc cấu hình các giao thức định tuyến thường đòi hỏi nhiều kinh nghiệm; đừng nên nghĩ rằng kỹ thuật nối mạng đã phát triển đến mức hoàn thành tự động việc định tuyến. Cách tốt nhất là nên kết hợp giữa định tuyến thủ công và tự động.

Những mạng trong đó các gói thông tin được vận chuyển, ví dụ như Internet, chia dữ liệu thành các gói, rồi dán nhãn với các đích đến cụ thể và mỗi gói được lập lộ trình riêng biệt. Các mạng xoay vòng, như mạng điện thoại, cũng thực hiện định tuyến để tìm đường cho các vòng (ví dụ như cuộc gọi điện thoại) để chúng có thể gửi lượng dữ liệu lớn mà không phải tiếp tục lặp lại địa chỉ đích.

Định tuyến IP truyền thống vẫn còn tương đối đơn giản vì nó dùng cách định tuyến bước kế tiếp (next-hop routing), router chỉ xem xét nó sẽ gửi gói thông tin đến đâu, và không quan tâm đường đi sau đó của gói trên những bước truyền còn lại. Tuy nhiên, những chiến lược định tuyến phức tạp hơn có thể được, và thường được dùng trong những hệ thống như MPLS, ATM hay Frame Relay, những hệ thống này đôi khi được sử dụng như công nghệ bên dưới để hỗ trợ cho mạng IP.

Thuật toán vector (distance-vector routing protocols)

Thuật toán này dùng thuật toán Bellman-Ford. Phương pháp này chỉ định một con số, gọi là chi phí (hay trọng số), cho mỗi một liên kết giữa các node trong mạng. Các node sẽ gửi thông tin từ điểm A đến điểm B qua đường đi mang lại tổng chi phí thấp nhất (là tổng các chi phí của các kết nối giữa các node được dùng).

Thuật toán hoạt động với những hành động rất đơn giản. Khi một node khởi động lần đầu, nó chỉ biết các node kề trực tiếp với nó, và chi phí trực tiếp để đi đến đó (thông tin này, danh sách của các đích, tổng chi phí của từng node, và bước kế tiếp để gửi dữ liệu đến đó tạo nên bảng định tuyến, hay bảng khoảng cách). Mỗi node, trong một tiến trình, gửi đến từng "hàng xóm" tổng chi phí của nó để đi đến các đích mà nó biết. Các node "hàng xóm" phân tích thông tin này, và so sánh với những thông tin mà chúng đang "biết"; bất kỳ điều gì cải thiện được những thông tin chúng đang có sẽ được đưa vào các bảng định tuyến của những "hàng xóm" này. Đến khi kết thúc, tất cả node trên mạng sẽ tìm ra bước truyền kế tiếp tối ưu đến tất cả mọi đích, và tổng chi phí tốt nhất.

Khi một trong các node gặp vấn đề, những node khác có sử dụng node hỏng này trong lộ trình của mình sẽ loại bỏ những lộ trình đó, và tạo nên thông tin mới của bảng định tuyến. Sau đó chúng chuyển thông tin này đến tất cả node gần kề và lặp lại quá trình trên. Cuối

cùng, tất cả node trên mạng nhận được thông tin cập nhật, và sau đó sẽ tìm đường đi mới đến tất cả các đích mà chúng còn tới được.

Thuật toán trạng thái kết nối (Link-state routing protocols)

Khi áp dụng các thuật toán trạng thái kết nối, mỗi node sử dụng dữ liệu cơ sở của nó như là một bản đồ của mạng với dạng một đồ thị. Để làm điều này, mỗi node phát đi tới tổng thể mạng những thông tin về các node khác mà nó có thể kết nối được, và từng node góp thông tin một cách độc lập vào bản đồ. Sử dụng bản đồ này, mỗi router sau đó sẽ quyết định về tuyến đường tốt nhất từ nó đến mọi node khác.

Thuật toán đã làm theo cách này là Dijkstra, bằng cách xây dựng cấu trúc dữ liệu khác, dạng cây, trong đó node hiện tại là gốc, và chứa mọi noded khác trong mạng. Bắt đầu với một cây ban đầu chỉ chứa chính nó. Sau đó lần lượt từ tập các node chưa được thêm vào cây, nó sẽ thêm node có chi phí thấp nhất để đến một node đã có trên cây. Tiếp tục quá trình đến khi mọi node đều được thêm.

Cây này sau đó phục vụ để xây dựng bảng định tuyến, đưa ra bước truyền kế tiếp tốt ưu,… để từ một node đến bất kỳ node khác trên mạng.

So sánh các thuật toán định tuyến

Các giao thức định tuyến với thuật toán vector tỏ ra đơn giản và hiệu quả trong các mạng nhỏ, và đòi hỏi ít (nếu có) sự giám sát. Tuy nhiên, chúng không làm việc tốt, và có tài nguyên tập hợp ít ỏi, dẫn đến sự phát triển của các thuật toán trạng thái kết nối tuy phức tạp hơn nhưng tốt hơn để dùng trong các mạng lớn. Giao thức vector kém hơn với rắc rối về đếm đến vô tận.

- Ưu điểm

  + Chính của định tuyến bằng trạng thái kết nối là phản ứng nhanh nhạy hơn, và trong một khoảng thời gian có hạn, đối với sự thay đổi kết nối. Ngoài ra, những gói được gửi qua mạng trong định tuyến bằng trạng thái kết nối thì nhỏ hơn những gói dùng trong định tuyến bằng vector. Định tuyến bằng vector đòi hỏi bảng định tuyến đầy đủ phải được truyền đi, trong khi định tuyến bằng trạng thái kết nối thì chỉ có thông tin về "hàng xóm" của node được truyền đi. Vì vậy, các gói này dùng tài nguyên mạng ở mức không đáng kể.

- Khuyết điểm

  + Chính của định tuyến bằng trạng thái kết nối là nó đòi hỏi nhiều sự lưu trữ và tính toán để chạy hơn định tuyến bằng vector.

- Giao thức được định tuyến và giao thức định tuyến

  + Sự nhầm lẫn thường xảy ra giữa "giao thức được định tuyến" và "giao thức định tuyến" ("routed protocols" và "routing protocols").

Giao thức được định tuyến (routed protocols hay routable protocols)

Một giao thức đã được định tuyến là bất kỳ một giao thức mạng nào cung cấp đầy đủ thông tin trong địa chỉ tầng mạng của nó để cho phép một gói tin được truyền đi từ một máy chủ (host) đến máy chủ khác dựa trên sự sắp xếp về địa chỉ, không cần biết đến đường đi tổng thể từ nguồn đến đích. Giao thức đã được định tuyến định nghĩa khuôn dạng và mục đích của các trường có trong một gói. Các gói thông thường được vận chuyển từ hệ thống cuối đến một hệ thống cuối khác. Hầu như tất cả giao thức ở tầng 3 các giao thức khác ở các tầng trên đều có thể được định tuyến, IP là một ví dụ. Nghĩa là gói tin đã được định hướng (có địa chỉ rõ ràng)giống như lá thư đã được ghi địa chỉ rõ chỉ còn chờ routing (tìm đường đi đến địa chỉ đó)

Các giao thức ở tầng 2 như Ethernet là những giao thức không định tuyến được, vì chúng chỉ chứa địa chỉ tầng liên kết, không đủ để định tuyến: một số giao thức ở tầng cao dựa trực tiếp vào đây mà không có thêm địa chỉ tầng mạng, như NetBIOS, cũng không định tuyến được.

Giao thức định tuyến (routing protocols)

Giao thức định tuyến được dùng trong khi thi hành thuật toán định tuyến để thuận tiện cho việc trao đổi thông tin giữa các mạng, cho phép các router xây dựng bảng định tuyến một cách linh hoạt. Trong một số trường hợp, giao thức định tuyến có thể tự chạy đè lên giao thức đã được định tuyến: ví dụ, BGP chạy đè trên TCP: cần chú ý là trong quá trình thi hành hệ thống không tạo ra sự lệ thuộc giữa giao thức định tuyến và đã được định tuyến.

Danh sách các giao thức định tuyến

- Giao thức định tuyến trong
  + Router Information Protocol (RIP)
  + Open Shortest Path First (OSPF)
  + Intermediate System to Intermediate System (IS-IS)
  + Hai giao thức sau đây thuộc sở hữa của Cisco, và được hỗ trợ bởi các router Cisco hay những router của những nhà cung cấp mà Cisco đã đăng ký công nghệ:
  + Interior Gateway Routing Protocol (IGRP)
  + Enhanced IGRP (EIGRP)
- Giao thức định tuyến ngoài
  + Exterior Gateway Protocol (EGP)
  + Border Gateway Protocol (BGP)
  + Constrained Shortest Path First (CSPF)
  + Thông số định tuyến (Routing metrics)

Một thông số định tuyến bao gồm bất kỳ giá trị nào được dùng bởi thuật toán định tuyến để xác định một lộ trình có tốt hơn lộ trình khác hay không. Các thông số có thể là những thông tin như băng thông (bandwidth), độ trễ (delay), đếm bước truyền, chi phí đường đi, trọng số, kích thước tối đa gói tin (MTU - Maximum transmission unit), độ tin cậy, và chi phí truyền thông. Bảng định tuyến chỉ lưu trữ những tuyến tốt nhất có thể, trong khi cơ sở dữ liệu trạng thái kết nối hay topo có thể lưu trữ tất cả những thông tin khác.

Router dùng tính năng phân loại mức tin cậy (administrative distance -AD) để chọn đường đi tốt nhất khi nó "biết" hai hay nhiều đường để đến cùng một đích theo các giao thức khác nhau. AD định ra độ tin cậy của một giao thức định tuyến. Mỗi giao thức định tuyến được ưu tiên trong thứ tự độ tin cậy từ cao đến thấp nhất có một giá trị AD. Một giao thức có giá trị AD thấp hơn thì được tin cậy hơn, ví dụ: OSPF có AD là 110 sẽ được chọn thay vì RIP có AD là 120.

Bảng sau đây cho biết sự sắp xếp mức tin cậy được dùng trong các router Cisco

Giao thức	Administrative distance
Nối trực tiếp	0
Static route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90

Giao thức	Administrative distance
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
ODR	160
External EIGRP	170
Internal BGP	200
Không xác định	255

Các lớp giao thức định tuyến

Dựa vào quan hệ của các dòng router với các hệ thống tự trị, có nhiều lớp giao thức định tuyến như sau:

- **Giao thức định tuyến trong mạng Ad-hoc** xuất hiện ở những mạng không có hoặc ít phương tiện truyền dẫn.
- **Interior Gateway Protocols (IGPs)** trao đổi thông tin định tuyến trong một AS. Các ví dụ thường thấy là:
  + IGRP (Interior Gateway Routing Protocol)
  + EIGRP (Enhanced Interior Gateway Routing Protocol)
  + OSPF (Open Shortest Path First)
  + RIP (Routing Information Protocol)
  + IS-IS (Intermediate System to Intermediate System)
  + Chú ý: theo nhiều tài liệu của Cisco, EIGRP không phân lớp như giao thức trạng thái kết nối.
  + Exterior Gateway Protocols (EGPs) định tuyến giữa các AS. EGPs gồm:
  + EGP (giao thức cũ để nối mạng Internet trước đây, bây giờ đã lỗi thời)
  + BGP (Border Gateway Protocol: phiên bản hiện tại, BGPv4, có từ khoảng năm 1995)

Giao thức định tuyến nội vùng RIP

RIP (tiếng Anh: Routing Information Protocol) là một giao thức định tuyến nội vùng sử dụng thuật toán định tuyến Distance-vector.

- Các đặc điểm:
  + Là giao thức định tuyến theo vector khoảng cách (Distance Vector), tức là RIP sẽ cập nhật toàn bộ hoặc 1 phần bảng định tuyến của mình cho các Router láng giềng kết nối trực tiếp với nó. Bảng định tuyến gồm các thông tin như: địa chỉ của router kế tiếp trên đường đi, tổng chi phí từ chính router đó đến mạng đích…
  + Là giao thức định tuyến theo kiểu classful (tức định tuyến theo lớp địa chỉ) vì rip k mang theo thông tin subnet mask đi kèm (FLSM)
  + Chọn đường đi dựa vào thông số định tuyến là hop count (số router) hay còn nói metric của RIP là hop count, dùng simple routing metric. Chính vì thế mà đôi lúc có 1 số đường mà rip chọn k phải là đường tối ưu nhất đến mạng đích. Nếu 1 packet đến mạng đích có số lượng hop vượt quá 15 thì nó sẽ bị drop. Do cái tính khó chịu này của RIP nên mới nó được cho là khó mở rộng, phù hợp với mạng nhỏ (nhưng mèo thấy nó không nhỏ đâu đối với vn)

+ Update định kì 30s (thay đổi bằng câu lệnh update-timers). Ngoài ra RIP còn các giá trị thời gian khác như invalid, holdown và flush timer set bằng câu lệnh sau timers basic update invalid holdown flush

+ Administrative Distance (AD) = 120, thông số này càng nhỏ thì càng ưu tiên

+ Load balacing (chia tải) maximum là 6 đường, default là 4 đường có thể set lại bằng câu lệnh maximum-paths. Việc chia tải ở đây đòi hỏi các đường phải có chi phí (cost)bằng nhau mới được nhé hay còn gọi là equal-cost mà cost của rip là hop count vì thế nếu tốc độ của 2 đường khác nhau như 1 đường là dial-up và 1 đường là T1 thì cũng như vậy thôi.

- Các cơ chế chống Loop

+ Count to infinity (định nghĩa giá trị tối đa) khi trong mạng xảy ra loop, gói tin chạy lòng vòng hoài trong mạng cho đến khi có tiến trình nào đó cắt đứt vòng lặp gọi là đếm vô hạn.Với rip metric là hop count vì thế mỗi khi thông tin cập nhật được "đi qua" 1 router thì số lượng hop sẽ tăng lên 1. Bản thân rip sẽ khắc phục tình trạng đếm đến vô hạn bằng cách cứ thông số định tuyến mà vượt quá 15 thì packet đó sẽ bị drop

+ Route poisioning (poison reverse): thường thì khi 1 đường mạng nào đó có thông số định tuyến tăng dần lên thì đã bị tình nghi là loop rồi nhé. Lúc đó router sẽ phát đi 1 thông tin poison reverse để xóa đi đường đó và cho nó vào trạng thái holddown.

+ Triggered update (câu lệnh ip rip triggered): vì rip cập nhật thông tin định tuyến 30s 1 lần vì thế khi có 1 mạng thay đổi thì phải chờ đến hết 1 chu kỳ 30s thì các router khác trong mạng mới biết được sự thay đổi đó. Cơ chế triggered update này giúp router cập nhật ngay sự thay đổi trong mạng mà k cần phải đợi hết chu kỳ đó. Kết hợp cơ chế này cùng poison reverse là ok.

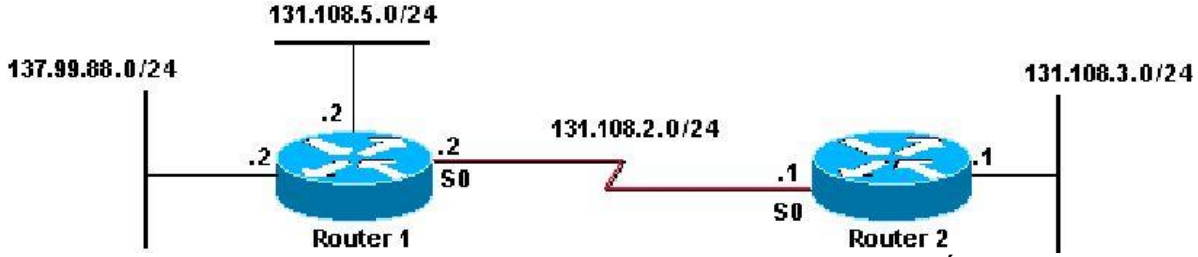
+ Holdown timer:khi router A nhận được 1 thông tin về 1 mạng X từ 1 router B nói rằng mạng X bị đứt thì router A sẽ set holddown timer. Trong suốt thời gian holddown này, router sẽ không cập nhật bất kì thông tin định tuyến nào về mạng X từ các router khác trong mạng, chẳng hạn router C cập nhật cho A nói, mạng X còn sống thì router A sẽ phớt lờ thông tin đó đi. Trừ phi router B nói với nó là mạng X sống lại rồi thì router A mới cập nhật nhé

+ Split Horizon tức là khi router gửi thông tin định tuyến ra 1 interface, thì router sẽ k gửi ngược trở lại các thông tin định tuyến mà nó học được từ cổng đó. Cơ chế này chỉ tránh được loop giữa 2 router

+ Kết hợp Split horizon với poision reverse: nếu đọc phớt qua, các bạn sẽ thấy 2 anh này trái ngược nhau, chắc là 2 cơ chế này đố kị nhau đây. Nhưng thực ra khi kết hợp lại sẽ hữu dụng trong khi mạng gặp sự cố, hình như mặc định là nó k dùng cơ chế này hay nói cách khác 2 cơ chế này tách riêng không làm chung vì sợ làm tăng kích thước của bảng định tuyến. Khi router A học được 1 mạng X bị die từ router B từ cổng S0/0 chẳng hạn, thì A sẽ advertise lại mạng X đó ra cổng s0/0 tiếp tục với hop count là 16

Quá trình gửi và nhận thông tin định tuyến

- Mô hình minh họa



Hình 4.2 Quá trình gửi và nhận thông tin định tuyến

Lúc gửi thông tin định tuyến: Trước khi gửi update (về đường mạng 131.108 và 131.99) cho router 2 thì router 1 phải check rằng

Đường mạng 131.108.5.0/24 có cùng major net với 131.108.2.0/24 hay không?

Trong trường hợp này là có, Router 1 mới check típ 131.108.5.0 và 131.108.2.0 có cùng subnet mask hay không?

Nếu trùng, Router 1 sẽ quảng bá đường mạng này.

Nếu k trùng, router 1 sẽ drop packet đó

Đường mạng 137.99.88.0/24 có cùng major net với 131.108.2.0/24 hay không?

Nếu không thì router 1 sẽ làm động tác là tổng hợp (summarize) 137.99.88.0/24 tại major net boundary thành 137.99.0.0 và quảng bá nó.

Trong mô hình này thì ta nhận được kết quả như thế này trong khi thi hành lệnh debug ip rip

```
RIP: sending v1 update to 255.255.255.255 via Serial0 (131.108.2.2)
     subnet 131.108.5.0, metric 1
     network 137.99.0.0, metric 1
```

Nhận update:

- Lúc này debug ip rip ngay trên router 2 thì ta thấy như thế này

```
RIP: received v1 update from 131.108.2.2 on Serial0
     131.108.5.0 in 1 hops
     137.99.0.0 in 1 hops
```

- Router 2 sẽ check để xem nên apply mask nào cho đường mạng 131 và 137 này đây:
- 131.108.5.0 và 131.108.2.0 (xét trên interface mà nhận update vào) có cùng 1 major net không?

Nếu có thì apply thẳng mask của interface mà nó nhận update, trong trường hợp này là apply /24). Nếu mạng được quảng bá tức 131.108 mà /32 thì router 2 sẽ apply /32 và tiếp tục quảng bá cho các router khác là /32(điều này nó khác với IGRP nhé)

- 131.108.5.0 và 137.99.0.0 có cùng major net không?

Nếu không xét tiếp, trong bảng định tuyến có subnet nào hay mạng con của major net này mà nó học từ các interface khác không?

Nếu không thì router 2 sẽ apply thẳng classful subnet mask là /16 luôn vì 137 là mạng lớp B. Chú ý ở đây nó sẽ apply host mask nếu như giữa 2 router là 1 unnumbered link và chứa thông tin về subnet (tức là khi đó các bit trong phần portion của network được set).

Ngược lại thì router sẽ ignore thông tin định tuyến này đi

Lúc này show ip route thử xem

```
R       137.99.0.0/16 [120/1] via 131.108.2.2, 00:00:07, Serial0
     131.108.0.0/24 is subnetted, 3 subnets
R       131.108.5.0 [120/1] via 131.108.2.2, 00:00:08, Serial0
C       131.108.2.0 is directly connected, Serial0
C       131.108.3.0 is directly connected, Ethernet0
```

Do ripv2 phát triển từ ripv1 nên nó cũng còn thừa hưởng những đặc điểm của ripv1 như:

Là giao thức định tuyến theo vector khoảng cách

Cost của nó là hop count. Ở đây cho mèo sử dụng từ cost thay cho metric nhé. Vì nếu lỡ có ai xem qua BGP rùi thì sẽ bị lộn 1 tí. Maximum hop count vẫn là 15

Cũng sử dụng các cơ chế chống lặp vòng như ripv1

Nhưng Ripv2 có các điểm cải tiến khác version 1 như

Nhiều thông tin định tuyến hơn như có gửi subnet mask đi kèm với địa chỉ mạng trong thông tin mà nó update.

Hỗ trợ VLSM (Variable length subnet mask) subnet mask khác nhau, CIDR (Classless Interdomain Routing) và route summarization

Có cơ chế xác thực thông tin khi nhận được bằng plaintext hoặc mã hóa MD5. Gởi thông tin định tuyến theo địa chỉ multicast là 224.0.0.9 bằng với 01-00-5E-00-00-09

Giao thức định tuyến động OSPF

- Tổng Quan Về OSPF

+ OSPF là một giao thức định tuyến theo trạng thái đường liên kết được triển khai dựa trên các chuẩn mở. OSPF được mô tả trong nhiều chuẩn của IETF (Internet Engineering Task Force). Chuẩn mở ở đây có nghĩa là OSPF hoàn toàn mở với công cộng, không có tính độc quyền.

+ Nếu so sánh với RIPv1 và RIPv2 là một giao thức nội thì IGP tốt hơn vì khả năng mở rộng của nó. RIP chỉ giới hạn trong 15 hop, hội tụ chậm và đôi khi còn chọn đường có tốc độ chậm vì khi quyết định chọn đường nó không quan tâm đến các yếu quan trọng khác như băng thông chẳng hạn. OSPF khắc phục được các nhược điểm của RIP vì nó là một giao thức định tuyến mạnh, có khả năng mởi rộng, phù hợp với các hệ thống mạng hiện đại. OSPF có thể cấu hình đơn vùng để sử dụng cho các mạng nhỏ.

- So Sánh OSPF Với Giao Thức Định Tuyến Theo Distance Vector

+ Router định tuyến theo trạng thái đường liên kết có một cơ sở đầy đủ về cấu trúc hệ thống mạng. Chúng chỉ thực hiện trao đổi thông tin về trạng thái đường liên kết lúc khởi động và khi hệ thống mạng có sự thay đổi. Chúng không phát quảng bá bảng định tuyến theo định kỳ như các router định tuyến theo distance vector. Do đó, các router định tuyến theo trạng thái đường liên kết sử dụng ít băng thông hơn cho hoạt động duy trì bảng định tuyến.

+ RIP phù hợp với các mạng nhỏ và đường tốt nhất đối với RIP là đường có số hop ít nhất. OSPF thì phù hợp với mạng lớn, có khả năng mở rộng, đường đi tốt nhất của OSPF được xác định dựa trên tốc độ của đường truyền. RIP cũng như các giao thức định tuyến theo distance vector khác đều sử dụng thuật toán chọn đường đơn giản. Còn thuật toán SPF thì phức tạp. Do đó, nếu router chạy theo giao thức định tuyến theo distance vector thì sẽ ít tốn bộ nhớ và cần năng lực xử lý thấp hơn so với khi chạy OSPF.

+ OSPF chọn đường dựa trên chi phí được tính từ tốc độ của đường truyền. Đường truyền có tốc độ càng cao thì chi phí OSPF tương ứng càng thấp.

+ OSPF chọn đường tốt nhất từ cây SPF.

+ OSPF bảo đảm không bị định tuyến lặp vòng. Còn giao thức định tuyến theo distance vector vẫn có thể bị loop.

+ Nếu một kết nối không ổn định, chập chờn, việc phát liên tục các thông tin về trạng thái của đường kiên kết này sẽ dẫn đén tình trạng các thông tin quảng cáo không đồng bộ làm cho kết quả chọn đường của các router bị đảo lộn.

+ OSPF giải quyết được các vấn đề sau:

+ Tốc độ hội tụ.

+ Hỗ trợ VLSM (Variable Length Subnet Mask).

+ Kích cỡ mạng.

+ Chọn đường.

+ Nhóm các thành viên.

+ Trong một hệ thống mạng lớn, RIP phải mất ít nhất vài phút mới có thể hội tụ được vì mỗi router chỉ trao đổi bảng định tuyến với các router láng giềng kết nối trực tiếp với

mình mà thôi. Còn đối với OSPF sau khi đã hội tụ vào lúc khởi động, khi có thay đổi thì việc hội tụ sẽ rất nhanh vì chỉ có thông tin về sự thay đổi được phát ra cho mọi router trong vùng.

+ OSPF có hỗ trợ VLSM nên nó được xem là một giao thức định tuyến không theo lớp địa chỉ. RIPv1 không hỗ trợ VLSM, nhưng RIPv2 thì có.

+ Đối với RIP, một mạng đích cách xa hơn 15 router xem như không thể đến được vì RIP có số lượng hop giới hạn là 15. Điều này làm kích thước mạng của RIP bị giới hạn trong phạm vi nhỏ. OSPF thì không giới hạn về kích thước mạng, nó hoàn toàn có thể phù hợp với mạng vừa và lớn.

+ Khi nhận được từ router láng giềng các báo cáo về số lượng hop đến mạng đích, RIP sẽ cộng thêm 1 vào thông số hop này và dựa vào số lượng hop đó để chọn đường đến mạng đích. Đường nào có khoảng cách ngắn nhất hay nói cách khác là có số lương hop ít nhất sẽ là đường tốt nhất đối với RIP. Nhận xét thấy thuật toán chọn đường như vậy là rất đơn giản và không đòi hỏi nhiều bộ nhớ và năng lực xử lý của router. RIP không hề quan tâm đến băng thông đường truyền khi quyết định chọn đường.

+ OSPF thì chọn đường dựa vào chi phí được tính từ băng thông của đường truyền. Mọi OSPF đều có thông tin đầy đủ về cấu trúc của hệ thống mạng và dựa vào đó để chọn đường đi tốt nhất. Do đó, thuật toán chọn đường này rất phức tạp, đòi hỏi nhiều bộ nhớ và năng lực xử lý của router cao hơn so với RIP.

+ RIP sử dụng cấu trúc mạng dạng ngang hàng. Thông tin định tuyến được truyền lần lượt cho mọi router trong cùng một hệ thống RIP. Còn OSPF sử dụng khái niệm về phân vùng. Một mạng OSPF có thể chia các router thành nhiều nhóm. Bằng cách này, OSPF có thể giới hạn lưu thông trong từng vùng. Thay đổi trong vùng này không ảnh hưởng đến hoạt động của các vùng khác. Cấu trúc phân lớp như vậy cho phép hệ thống mạng có khả năng mở rộng một cách hiệu quả.

- Thuật Toán Chọn Đường Ngắn Nhất

+ Theo thuật toán này, đường tốt nhất là đường có chi phí thấp nhất. Thuật toán được sử dụng là Dijkstra, thuật toán này xem hệ thống mạng là mọt tập hợp các nodes được kết nối với nhau bằng kết nối point-to-point. Mỗi kết nối này có một chi phí. Mỗi nodes có một tên. Mỗi nodes có đầy đủ cơ sở dữ liệu về trạng thái của các đường liên kết. Do đó, chúng có đầy đủ thông tin về cấu trúc vật lý của hệ thống mạng. Tất cả các cơ sở dữ liệu này điều giống nhau cho mọi router trong cùng một vùng.

- Các Loại Mạng OSPF

Các OSPF phải thiết lập mối quan hệ láng giềng để trao đổi thông tin định tuyến. Trong mỗi mạng IP kết nối vào router. Nó đều cố gắng ít nhất là trở thành một láng giềng hoặc là một láng giềng thân mật với một router khác, router OSPF quyết định chọn router nào làm láng giềng thân mật là tùy thuộc vào từng loại mạng kết nối với nó. Có một số router có thể cố gắng trở thành láng giềng thân mật với mọi router láng giềng khác. Có một số router khác lại có thể chỉ cố gắng trở thành láng giềng thân mật với một hoặc hai router láng giềng thôi. Một khi mối quan hệ láng giềng thân mật đã được thiết lập giữa hai láng giềng với nhau thì thông tin về trạng thái đường liên kết mới được trao đổi.

Giao thức OSPF nhận biết các loại mạng sau:

Mạng quảng bá đa truy cập, ví dụ mạng Ethernet.

Mạng point-to-point.

Mạng không quảng bá đa truy cập (NBMA – NonBroadcast Multil-Access), ví dụ Frame Relay.

Mạng Point-to-Multipoint có thể được nhà quản trị mạng cấu hình cho một cổng của router.

Trong mạng đa truy cập không thể biết được là có bao nhiêu router sẽ có thể được kết nối vào mạng.

Trong mạng point-to-point thì chỉ có hai router được kết nối với nhau.

Trong mạng quảng bá đa truy cập có rất nhiều router kết nối vào. Nếu mỗi router đều thiết lập mối quan hệ thân mật với mọi router khác và thực hiện trao đổi thông tin về trạng thái đường liên kết với mọi router láng giềng thì sẽ quá tải. Nếu có 10 router thì sẽ cần 45 mối liên hệ thân mật, nếu có n router thì sẽ có n*(n-1)/2 mối quan hệ láng giềng cần thiết lập.

Giải pháp cho vấn đề quá tải trên là bầu ra một router làm đại diện (DR- Designated Router). Router này sẽ thiết lập mối quan hệ thân mật với mọi router khác trong mạng quản bá. Mọi router còn lại sẽ chỉ gởi thông tin về trạng thái đường liên kết cho DR. Sau đó DR sẽ gởi các thông tin này cho mọi router khác trong mạng bằng địa chỉ multicast 224.0.0.5 DR đóng vai trò như một người phát ngôn chung.

Việc bầu DR rất có hiệu quả nhưng cũng có một nhược điểm. DR trở thành một tâm điểm nhạy cảm đối với sự cố. Do đó, cần có một router thứ hai được bầu ra để làm đại diện dự phòng (BDR – Backup Designated Router), router này sẽ đảm trách vai trò của DR nếu DR bị sự cố. Để đảm bảo cả DR và BDR đều nhận được thông tin về trạng thái đường liên kết từ mọi router khác trong cùng một mạng, địa chỉ multicast 224.0.0.6 cho các router đại diện.

Trong mạng point-to-point chỉ có 2 router kết nối với nhau nên không cần bầu ra DR và DBR. Hai router này sẽ thiết lập mối quan hệ láng giềng thân mật với nhau.

- Loại Mạng Các Đặc Tính Bầu DR

Broadcast, Multi-Access Ethernet,ToKen Ring,FĐI	Có
NonBroadcast Multi-Access Frame Relay,X25,SMDS	Có
Point-to-Point PPP,HDLC	Không
Point-to-Multipoint Được cấu hình bởi Administrator	Không

- Giao Thức OSPF Hello

Khi router bắt đầu khởi động tiến trình định tuyến OSPF trên một cổng nào đó thì nó sẽ gởi một gói hello ra cổng đó và tiếp tục gởi hello theo định kỳ. Giao thức hello đưa ra các nguyên tắc quản lý việc trao đổi các gói OSPF hello.

Ở lớp 3 của mô hình OSI, gói hello mang địa chỉ multicast 224.0.5.0 địa chỉ này chỉ đến tất cả các OSPF router. OSPF router sử dụng gói hello để thiết lập một quan hệ láng giềng thân mật mới và để xác định là router láng giềng có còn hoạt động hay không. Mặc định hello được gởi đi 10 giây một lần trong mạng quảng bá đa truy cập và mạng Point-to-Point. Trên cổng nói vào mạng NBMA, ví dụ như Frame Relay, chu trình mặc định của hello là 30 giây.

Trong mạng đa truy cập, giao thức hello tiến hành bầu DR và BDR.

Mặc dù gói hello rất nhỏ nhưng nó cũng bao gồm cả phần header của gói OSPF. Cấu trúc của phần header trong gói OSPF được thể hiện như hình sau. Nếu gói hello thì trường Type sẽ có giá trị là một.

Các thông điệp Hello trong OSPF thực hiện ba chức năng chính:

Tìm ra những router chạy OSPF khác trên cùng một mạng chung.

Kiểm tra sự tương thích trong các thông số cấu hình.

Giám sát tình trạng của láng giềng để phản ứng nếu láng giềng bị fail.

Để tìm ra những router láng giềng, OSPF lắng nghe những thông điệp Hello được gửi đến 224.0.0.5. Đây là địa chỉ multicast tượng trưng cho tất cả các router OSPF, trên bất cứ cổng nào đã bật OSPF. Các gói Hello sẽ lấy nguồn từ địa chỉ primary trên cổng, nói cách khác, Hello không dùng địa chỉ phụ. (OSPF router sẽ quảng bá các địa chỉ phụ nhưng nó sẽ không gửi Hello từ những địa chỉ này và không bao giờ hình thành mối quan hệ dùng địa chỉ phụ.

Khi hai router tìm ra nhau thông qua các gói Hello, các router thực hiện các phép kiểm tra các thông số như sau:

Các router phải vượt qua tiến trình xác thực.

Các router phải trong cùng địa chỉ mạng primary, phải có cùng subnetmask.

Phải trong cùng OSPF area.

Phải có cùng kiểu vùng OSPF. Không có trùng RID.

OSPF Hello và Deadtimer phải bằng nhau.

Nếu bất kỳ điều kiện nào nêu trên không thỏa mãn, hai router đơn giản sẽ không hình thành quan hệ láng giềng. Cũng lưu ý rằng một trong những điều kiện quan trọng nhất mà hai bên không cần giống là chỉ số ID của tiến trình OSPF, như được cấu hình trong câu lệnh router ospf process-id. Bạn cũng nên lưu ý rằng giá trị MTU phải bằng nhau để các gói tin DD được gửi thành công giữa những láng giềng nhưng thông số này không được kiểm tra trong tiến trình Hello.

Chức năng thứ ba của Hello là để duy trì liên lạc giữa những láng giềng. Các láng giềng gửi Hello ở mỗi chu kỳ hello interval; nếu router không nhận được Hello trong khoảng thời gian dead interval sẽ làm cho router tin rằng láng giềng của nó đã fail. Khoảng thời gian hello interval mặc định bằng 10 giây trên những cổng LAN và 30 giây trong những đường T1 hoặc đường thấp hơn T1. Thời gian dead interval mặc định bằng bốn lần thời gian hello interval.

2.2.1 Xây dựng bảng định tuyến trong OSPF

Sau khi trao đổi LSDB giữa các OSPF router xong, thì chúng bắt đầu tính toán đường đi ngắn nhất và tốt nhất cho cho các gói tin lưu thông trong Area của mình. Để làm được điều này các OSPF router sử dụng thuật toán tìm đường đi ngắn nhất Shortest Path Firts (Distrakj). Các bước phân tích để tìm ra routes tốt nhất có thể tóm gọn lại như sau:

- Phân tích LSDB để tìm ra routes có thể đến được với subnet.
- Với mỗi routes như vậy sẽ gán một giá trị Cost cho tất cả các outgoing interfaces trên đường đó.
- Tiến hành lấy các routes với tổng số Cost là thấp nhất.

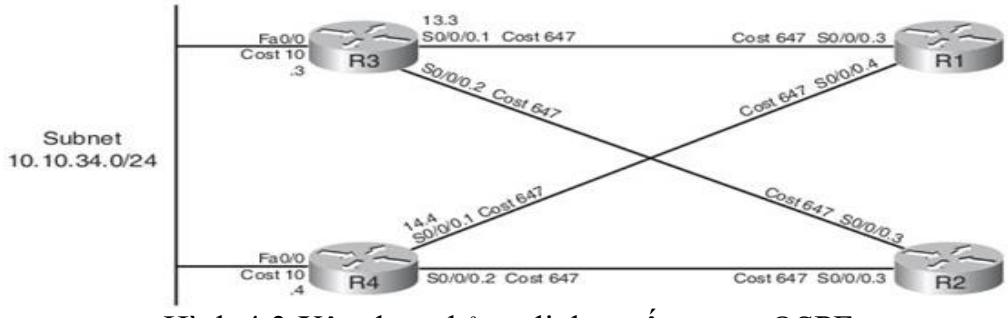
Tính toán Cost cho các routes bên trong Area. Việc tính cost có thể được chia làm 3 mảng chính:

- Intra area routes: trong cùng một area.
- Inter area routes: Giữa các area với nhau.
- Và cả 2 trường hợp trong cùng một subnet.

+ Intra area routes: Sau khi phân tích LSDB để tìm ra các routes có thể đến được với subnet, thì công việc tiếp theo của nó là:

+ Tìm ra các subnet trong cùng area.
+ Chạy SPF để tìm đường đi đến mỗi subnet

Tính toán cost cho mỗi outgoing interfaces và sẽ chọn routes nào mà có cost thấp nhất.



Hình 4.3 Xây dựng bảng định tuyến trong OSPF

Ví dụ: Trong mô hình mạng trên thì các Router đều nằm chung một area 34. Trong mô hình đã mô tả về interfaces number và cost. Bây giờ ta sẽ xét xem các bước để R1 có thể học về thông tin mạng 10.10.10.0/24.

Bước 1: R1 nó có thể xác định subnet 10.10.10.0/24 tồn tại trong area 34, nó biết được thông tin nhận được từ DR

Bước 2: R1 chạy SPF để tìm routes đến subnet 10.10.10.0/24, và nó tìm được 4 đường

+ 1: R1-R4
+ 2: R1-R3
+ 3: R1-R4-R2-R3
+ 4: R1-R2-R3-R4

Bước 3: Thực hiện một số phép tính đơn giản, bằng cách thêm cost ở mỗi out – going trên mỗi interface.

- R1-R3: thêm cost của s0/0/0.3 của R1 là 647 và cost của fa0/0 của R3 là 10. Tổng là 657.

- R1-R4: thêm cost của s0/0/0.4 của R1 là 647 và cost của fa0/0 của R4 là 10. Tổng là 657. Với thiết lập mặc định số route tối đa đến một subnet là 4 thì R1 sẽ thêm cả 2 routes trên vào routing table của nó.

OSPF hỗ trợ khả năng cân bằng tải (load balancing) trên các routes có cost bằng nhau nhưng không hỗ trợ cân bằng trên với các routes có cost khác nhau.

Tính toán cost cho các inter-area routes: Ta sẽ tiếp tục với việc tính toán cost cho các interarea routes. Việc này cũng tương tự như intra-area đó là lấy thông tin cost của outgoing-interface mà Router thu thập được. Sau đó sử dụng SPF để tính toán route nào là tối ưu. Nhưng đối với inter-area thì có một vài điểm khác biệt. Đối với interarea, ta sẽ xem xét một khái niệm là ABRs (Area Border Routers) - các Router biên. Router biên là Router tham gia vào nhiều area thay vì chỉ tham gia vào 1 area. ABR đóng vai trò là nơi trao đổi thông tin cho các areas. Chúng duy trì, lưu trữ một LSDB cho mỗi area mà chúng tham gia.

2.3 Giao thức định tuyến Distance Vector

Các giao thức định tuyến thuộc loại này như: RIP, IGRP, … Hoạt động theo nguyên tắc Neighbor, nghĩa là mỗi router sẻ gửi routing-table của mình cho tất cả các router được nối trực tiếp với nó. Các router đó sau đó so sánh với bảng routing-table mà mình hiện có và kiểm tra lại các tuyến đường của mình với các tuyến đường mới nhận được, tuyến đường nào tối ưu hơn sẻ được đưa vào routing-table. Các gói tin update sẽ được gửi theo định kỳ (30 giây với RIP, 90 giây đối với IGRP).

- Ưu điểm:
  + Dễ cấu hình, router không phải xử lý nhiều nên không tốn nhiều dung lượng bộ nhớ và CPU có tốc độ xử lý nhanh hơn.
- Nhược điểm:
  + Hệ thống metric quá đơn giản (như rip chỉ là hop-count) dẫn đến việc các tuyến đường được chọn vào routing-table chưa phải tuyến đường tốt nhất
  + Vì các gói tin update được gửi theo định kỳ nên một lượng bandwidth đáng kể sẻ bị chiếm (mặc dù mạng không gì thay đổi nhiều).
- Do Router hội tụ chậm, dẫn đến việc sai lệch trong bảng định tuyến gây nên hiện tượng loop.

2.4 Giao thức định tuyến Link-State

Các giao thức định tuyến thuộc loại này như OSPF, IS-IS. Link State không gửi bảng định tuyến của mình, mà chỉ gửi tình trạng của các đường link trong linkstate-database của mình đi cho các router khác, các router sẽ áp dụng giải thuật SPF (shortest path first), để tự xây dựng routing-table riêng cho mình. Khi mạng đã hội tụ, Link State protocol sẽ không gửi update định kỳ mà chỉ gởi khi nào có một sự thay đổi trong mạng (1 line bị down, cần sử dụng đường back-up)

- Ưu điểm:
  + Có thể thích nghi được với đa số hệ thống, cho phép người thiết kế có thể thiết kế mạng linh hoạt, phản ứng nhanh với tình huống xảy ra.
  + Do không gởi interval-update, nên link state bảo đảm được bandwidth cho các đường mạng.
- Nhược điểm:
  + Do router phải sử lý nhiều, nên chiếm nhiều bộ nhớ, tốc độ CPU chậm hơn nên tăng delay
  + Link State khá khó cấu hình để chạy tốt.

2.5 Cấu trúc địa chỉ mạng

Chúng ta cũng biết là mạng máy tính nội bộ nói riêng và mạng máy tính trên internet nói chung, địa chỉ IP (viết tắt **Internet Protocol Address)** là một con số duy nhất dùng để xác định một thiết bị đầu cuối (ví dụ: máy tính, router….). Địa chỉ IP giống như số nhà của chúng ta, nó là duy nhất. Địa chỉ IP cho phép các máy tính có thể truyền tải thông tin, giao tiếp với nhau, và chúng đảm bảo cho các thiết bị có thể hiểu được và chia sẻ dữ liệu với nhau.

Lớp trong địa chỉ IP.

- Hiện tai chúng ta có 2 phiên bản IPv4 và IPv6, nhưng IPv6 còn khá mới và chưa nắm hết vì thế trong giáo trình này sẽ không giới thiệu về IPv6 mà chỉ tập trung nói về IPv4. Ở Phiên bản IPv4, địa chỉ IP được chia thành 5 lớp, mỗi lớp có miền địa chỉ và cấu trúc khác

nhau. Khi các bạn chuyển đổi IP sang hệ nhị phân (0 và 1). Một địa chỉ IP luôn có hai phần **Network** và **Host**.

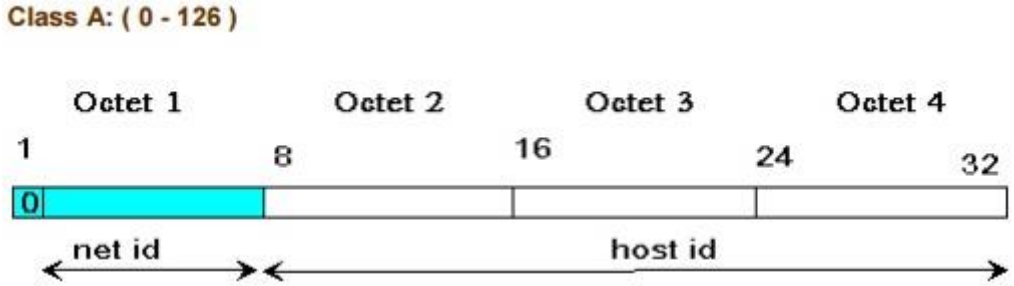
- Mỗi một lớp có thành phần Network và Host khác nhau. Thành phần Network quy định trong một lớp có bao nhiêu mạng và trong phần Host quy định số địa chỉ IP khả thi trong một đường mạng. Ở dạng nhị phân, địa chỉ IP là một số 32 bits và được chia thành 4 phần, mỗi phần được gọi là một Octet, mỗi Octet là 8bits.

- 192.168.1	- 10
- Network	- Host

Cấu trúc tổng quát của một địa chỉ IP.

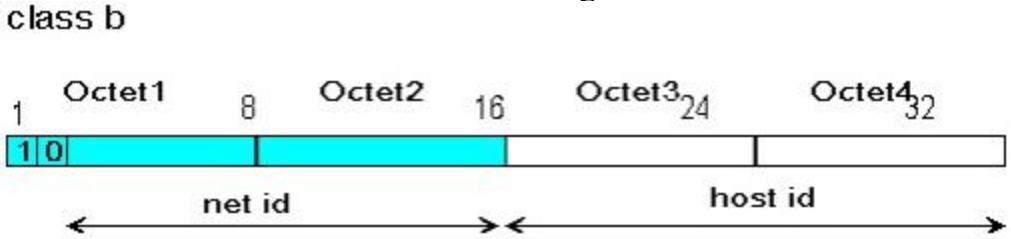
- Địa chỉ IP lớp A.

+ Bit đầu tiên của một Octet thứ nhất được đặt là 0 để nhận dạng lớp A,7 bits kế tiếp xác định địa chỉ mạng, 24 bit của 3 Octet còn lại xác định địa chỉ máy tính.ở Lớp A sẽ có 2^7-2 = 126 đường mạng (từ 1 – 126) và 2^24-2 = 16.777.214 địa chỉ IP trên mỗi đường mạng



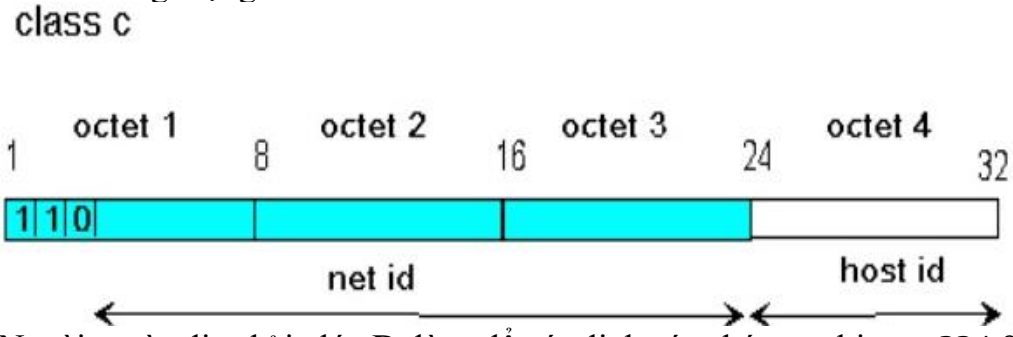
- Địa chỉ IP lớp B.

+ Ở lớp B, 32 bits được chia đôi cho phần NetWork và phân Host.Do vậy, hai bit đầu tiên được đặt 10 để nhân dạng lớp B, 14 bits còn lại của phân Network xác định địa chỉ mạng và 16 bits còn lại danh cho phần Host. Lớp B có 2^14-2=16.382 mạng (128-191) và 2^16-2 = 65.534 địa chỉ IP dành cho mỗi mạng.



- Địa chỉ IP lớp C.

+ Ở lớp C, 24 bits của 3 octet đầu được dành cho phần network, 8 bits của octet cuối cùng được dành cho phần Host. Trong 24 bits của phần Network, người ta dành ra 3 bits đầu tiên và đặt là 110 để nhân dạng lớp C, 21 bits còn lại là dung để xác định đường mạng. Do vậy, số đường mạng của địa chỉ IP lớp C là 2^21 – 2 = 2.097.150 (192–223), số máy tính trên mỗi đường mạng là 2^8-2=254



+ Ngoài ta còn địa chỉ ip lớp D dùng để xác định các nhóm multicast 224.0.0.0/4 và địa chỉ lớp mạng E chỉ được dùng để nghiên cứu, không áp dụng trên thực tế.

- **Tóm lại:**
  + Địa chỉ lớp A: Địa chỉ mạng ít và địa chỉ máy chủ trên từng mạng nhiều.
  + Địa chỉ lớp B: Địa chỉ mạng và địa chỉ máy chủ trên từng mạng vừa phải.
  + Địa chỉ lớp C: Địa chỉ mạng nhiều, địa chỉ máy chủ trên từng mạng ít.
  + Ngoài ra lớp D có 4 bit đầu tiên để nhận dạng là 1110, còn lớp E có 5 bít đầu tiên để nhận dạng là 11110.
  + Lớp A Từ 0.0.0.0 đến 127.0.0.0 126 16777214
  + Lớp B Từ 128.0.0.0 đến 191.255.0.0 16382 65534
  + Lớp C Từ 192.0.0.0 đến 223.255.255.0 2097150 254
  + Lớp D Từ 224.0.0.0 đến 240.0.0.0 Không phân
  + Lớp E Từ 241.0.0.0 đến 255.0.0.0 Không phân

2.6 Cấu hình Router cơ bản

Các Mode lệnh trong IOS: có 4 mode lệnh

- Router> ----------> Mode User (Mode có quyền thấp nhất)
- Router# ----------> Mode Previlidge (Mode quản trị)
- Router (config)#----------> Mode cấu hình
- Router (config-if)#----------> Mode vào cổng

Các lệnh cấu hình Cơ bản Router:

- Router#configure terminal
- Router(config)#----------=> Mode config | Mode global (Mode cấu hình)
- Router(config)#**hostname R1** => Đặt tên cho Router
- R1(config)#
- R1(config)#**enable password cisco** => Đặt pass enable là cisco (khi chuyển từ Mode người dùng sang Mode quản trị sẽ yêu cầu mật khẩu).
- R1(config)#**enable secret aptech** => Đặt pass enable secret là aptech (pass này sẽ được dùng khi câu lệnh này được thực hiện. Cao hơn pass của enable)
- R1(config)#
- R1(config)#line console 0
- R1(config-line)#**password aptech** => Đặt pass khi truy nhập vào Router bằng đường Console.
- R1(config-line)#**login**
- R1(config-line)#
- R1(config-line)#**line vty 0 4**
- R1(config-line)#**password aptech** => Đặt pass khi truy nhập vào Router bằng đường telnet
- R1(config-line)#**login**
- R1(config-line)#**exit**
- R1(config)#
- R1(config)#**banner motd !Hello!** => Đặt lời chào cho Router/Switch, lưu ý ký tự bắt đầu và ký tự kết thúc của lời chào phải giống nhau.
- R1(config)#
- R1(config)#interface f0/0
- R1(config-if)#----------=> Mode Interface (mode cấu hình địa chỉ cổng)
- R1(config-if)#**no shut** => Bật cổng của Rotuer lên
- R1(config-if)#**ip address 192.168.1.1 255.255.255.0** => Đặt địa chỉ IP cho cổng của Router.
- R1(config-if)#
- R1(config-if)#**interface s0/0**

- R1(config-if)#**no shut**
- R1(config-if)#ip address 172.16.0.1 255.255.255.252
- R1(config-if)#**clock rate 64000** (bật xung nhịp đối với đầu DCE)
- R1(config)#
- R1(config)#**exit**
- R1#**show running-config** => Kiểm tra file cấu hình đang chạy.
- R1#**copy running-config startup-config | write** => ghi file cấu hình đang chạy vào NVRAM.
- R1#**show startup-config** => Kiểm tra file cấu hình xem đã có những thông tin đang chạy chưa?

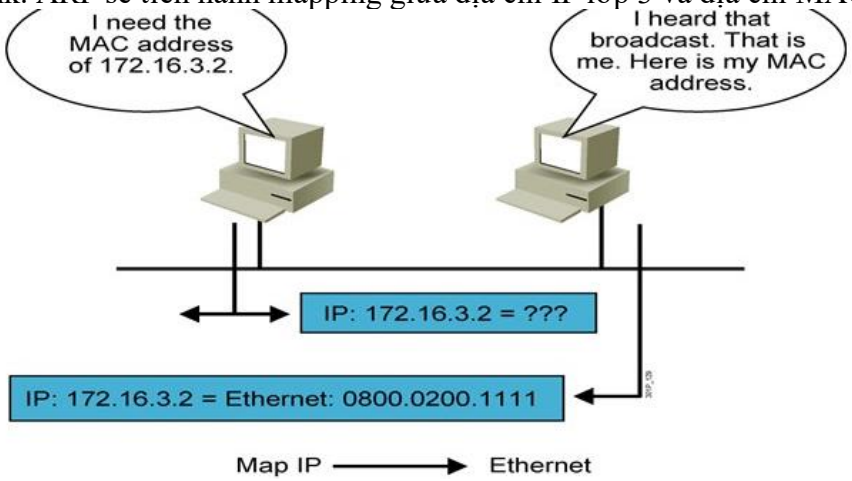
Chú ý:

- => R1(config-if)#**clock rate 64000** => Clock rate là xung nhịp của các bít truyền. Bít này cách bít kia là 64000 micro/giây

2.7 Quá trình phân phối gói dữ liệu

Nhớ lại nguyên lý hoạt động của mô hình OSI thì dữ liệu từ bên trên đi xuống khi đi tới một lớp sẽ được đóng vào trong header của lớp đó. Khi đi tới layer 7 sẽ được đóng vào trong layer 7 header, xuống layer 6 sẽ được đóng vào trong layer 6 header tương tự với các lớp 5, 4, 3 và 2, và khi nghiên cứu về Network thì sẽ tập trung vào các lớp 4, 3, 2, và 1.

Vậy thì dữ liệu xuống layer 4 Transport, thông tin cần chú ý sẽ là cặp source port và destination port, xuống lớp 3 Network lại quan tâm đến cặp địa chỉ source IP và destination IP rồi xuống lớp 2 Data-Link sẽ được đóng vào trong layer 2 header với cặp thông tin source MAC và destination MAC tương ứng với source IP và destination IP bên trên, thì lúc này sẽ phải có 1 cái gì đó đứng ra đảm nhiệm việc tìm cho ra cặp thông tin source MAC và destination MAC tương ứng với IP ở lớp bên trên, và cái gì đó chính là giao thức ARP – giao thức phân giải địa chỉ giữa lớp Network và lớp Data-Link. ARP sẽ tiến hành mapping giữa địa chỉ IP lớp 3 và địa chỉ MAC lớp 2.



Hình 4.4 ARP mapping địa chỉ lớp 3 Network và địa chỉ lớp 2 Data-Link

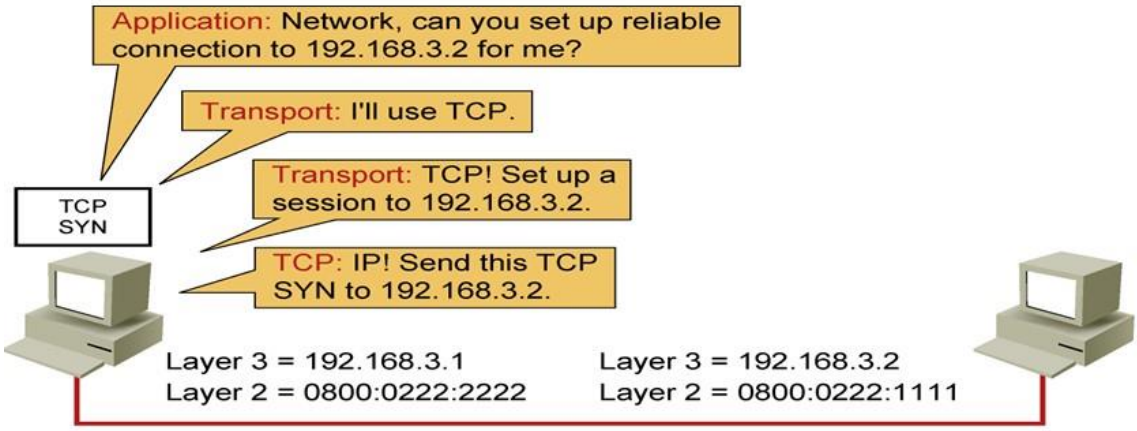
Ví dụ 1 máy A có địa chỉ 172.16.3.1 muốn gửi dữ liệu đến máy B có địa chỉ 172.16.3.2 thì máy A cần phải biết địa chỉ MAC tương ứng với 172.16.3.2 là bao nhiêu để gửi xuống lớp 2 Data-Link. Thì lúc này ARP của máy A hoạt động và đi tìm MAC của 172.16.3.2. ARP máy A sẽ tìm dữ liệu trong bảng ARP local của nó nhưng nếu không có trong dữ liệu thì phải broadcast lên đi tìm, khi máy B nhận được broadcast hỏi địa chỉ MAC của 172.16.3.2 biết là hỏi mình thì trả lời lại máy A, máy A nhận được địa chỉ MAC thì đóng gói dữ liệu rồi truyền đi.

Vậy ARP hoạt động như thế nào, minh hoạ quá trình trao đổi gói tin giữa hai máy trong mạng dưới đây sẽ nói rõ điều này. Minh hoạ này sẽ chia làm 3 giai đoạn:

Quá trình TCP bắt tay 3 bước thiết lập kết nối

Quá trình ARP hoạt động phân giải địa chỉ

Quá trình data được gửi và nhận

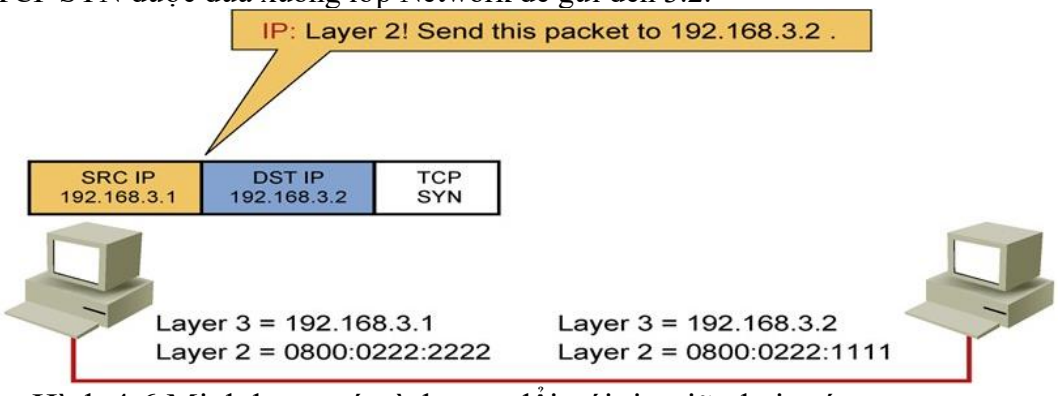


Hình 4.5 Minh hoạ quá trình trao đổi gói tin giữa hai máy trong mạng

Ví dụ có 2 máy 1 và 2 đang trao đổi dữ liệu với nhau qua hệ thống mạng, máy 1 có IP là 192.168.3.1 (viết tắt là 3.1) địa chỉ MAC là 0800:0222:2222 (viết tắt là 2222); máy 2 có IP là 192.168.3.2 (viết tắt là 3.2) địa chỉ MAC là 0800:0222:1111 (viết tắt là 1111).

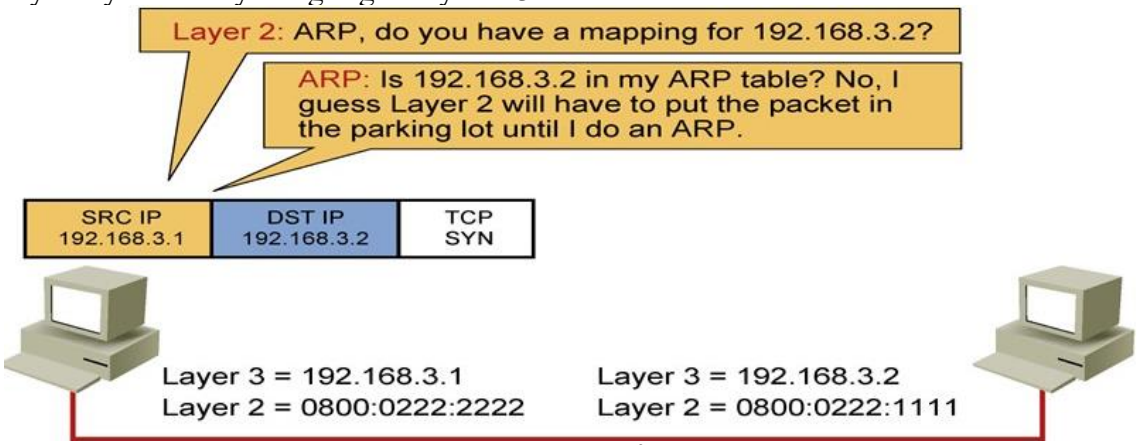
Giai đoạn 1: Quá trình TCP bắt tay 3 bước thiết lập kết nối.

Đầu tiên tầng ứng dụng Application yêu cầu 1 dịch vụ từ lớp bên dưới nó là Network, hãy thiết lập 1 kết nối tin cậy đến địa chỉ 3.2 dùm cho tôi được hay không, yêu cầu này đi xuống dưới đến Transport, Transport nhìn thấy yêu cầu kết nối tin cậy thì biết mình phải dùng TCP và nói TCP thiết lập 1 phiên kết nối tới 3.2 đi, TCP nhận được yêu cầu thì thực hiện quá trình bắt tay 3 bước và gói TCP SYN được đưa xuống lớp Network để gửi đến 3.2.



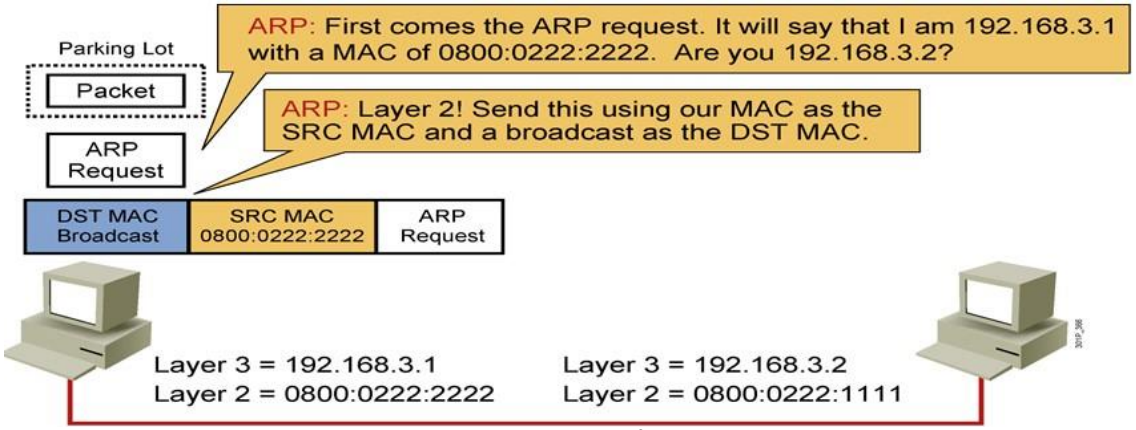
Hình 4.6 Minh hoạ quá trình trao đổi gói tin giữa hai máy trong mạng

Gói TCP SYN này đi xuống lớp 3 Network được đóng vào trong layer 3 header với cặp địa chỉ source IP và destination IP, source IP từ chính bản thân máy 1 là 3.1 còn destination IP thì từ yêu cầu của lớp Transport bên trên, khi đã có đủ cặp chỉ source IP và destination IP thì gửi xuống layer 2 yêu cầu layer 2 gửi gói này đến 3.2.



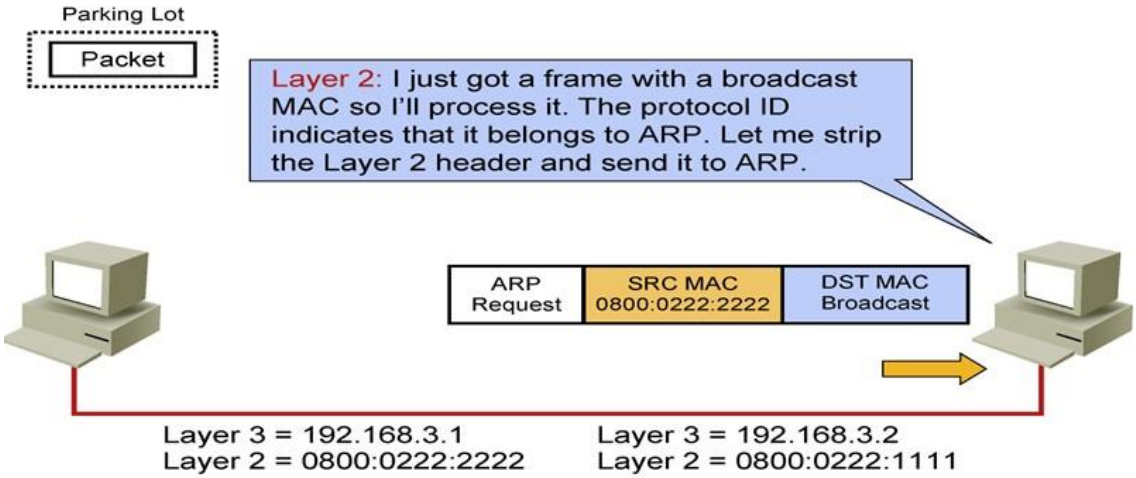
Hình 4.7 Minh hoạ quá trình trao đổi gói tin giữa hai máy trong mạng

Đến lớp 2 Data-Link thì sẽ phải đóng vào layer 2 header với cặp địa chỉ source MAC và destination MAC tương ứng. Source MAC từ chính Card mạng của máy 1 là 2222, còn destination MAC của 3.2 là bao nhiêu, nó sẽ phải dùng ARP để tìm. Nó sẽ tra trong bảng ARP của nó là có MAC của 3.2 chưa thì phát hiện là chưa có nên tạm thời nó sẽ để gói TCP SYN qua 1 bên (đưa vào Parking Lot) và tiến hành gửi ARP đi tìm MAC của 3.2 trước.
Giai đoạn 2: Quá trình ARP hoạt động phân giải địa chỉ



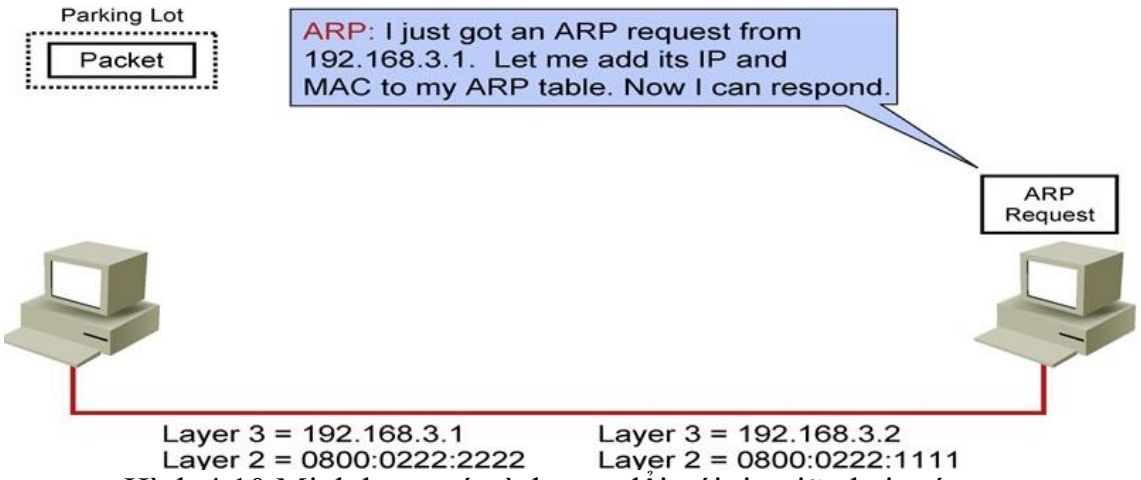
Hình 4.8 Minh hoạ quá trình trao đổi gói tin giữa hai máy trong mạng

Khi máy 1 thực hiện ARP đi tìm MAC của 3.2 thì đầu tiên phải gửi gói ARP request mang các thông tin như thể máy 1 đang nói rằng tôi là 3.2, tôi có địa chỉ mac là 2222, anh có phải là 3.1 hay không. và sẽ broadcast gói này đi đến từng nhà từng nhà để hỏi anh có phải là 3.2 không. Gói ARP request này sẽ có source MAC là chính nó 2222 và destination MAC ở dạng broadcast layer 2 tương ứng với tất cả các bit bật lên bằng 1 thành 12 chữ F. Sau đó đưa xuống lớp 1 Physical chuyển thành các bit nhị phân rồi truyền đi. Vì destination là Broadcast nên gói ARP request này sẽ đi đến tất cả các máy có trong mạng và tất nhiên sẽ đến được tay máy 2.



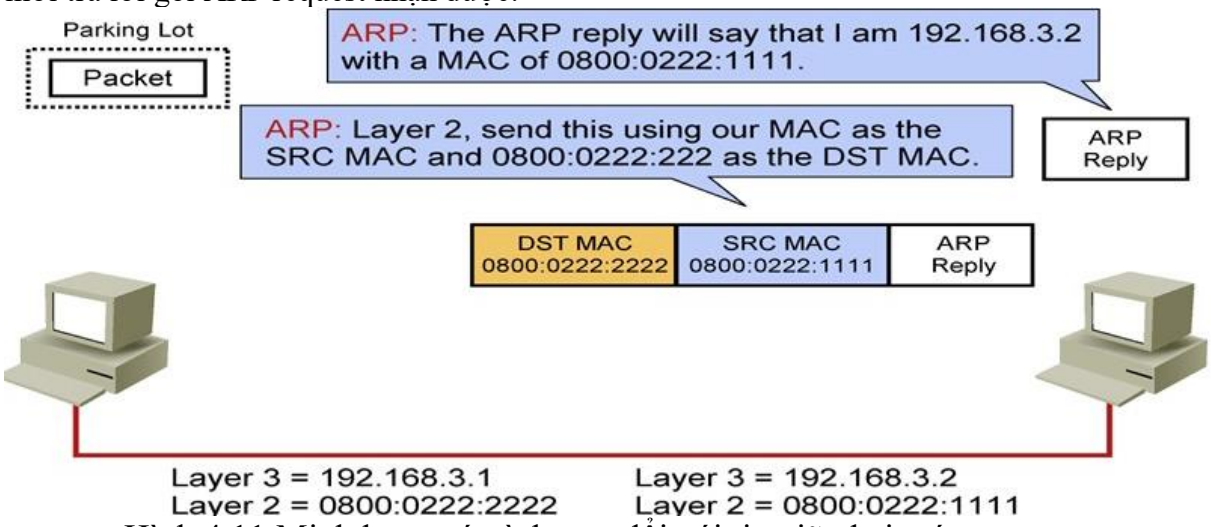
Hình 4.9 Minh hoạ quá trình trao đổi gói tin giữa hai máy trong mạng

Lớp Physical của máy 2 nhận được dãy bit nhị phân đưa lên lớp 2 Data-Link thì chuyển thành frame phát hiện đây là gói broadcast thì xử lý gói này, đọc vào protocol ID của header thì biết nó là ARP thì máy 2 gọi ARP ra nhận và xử lý gói tin này.



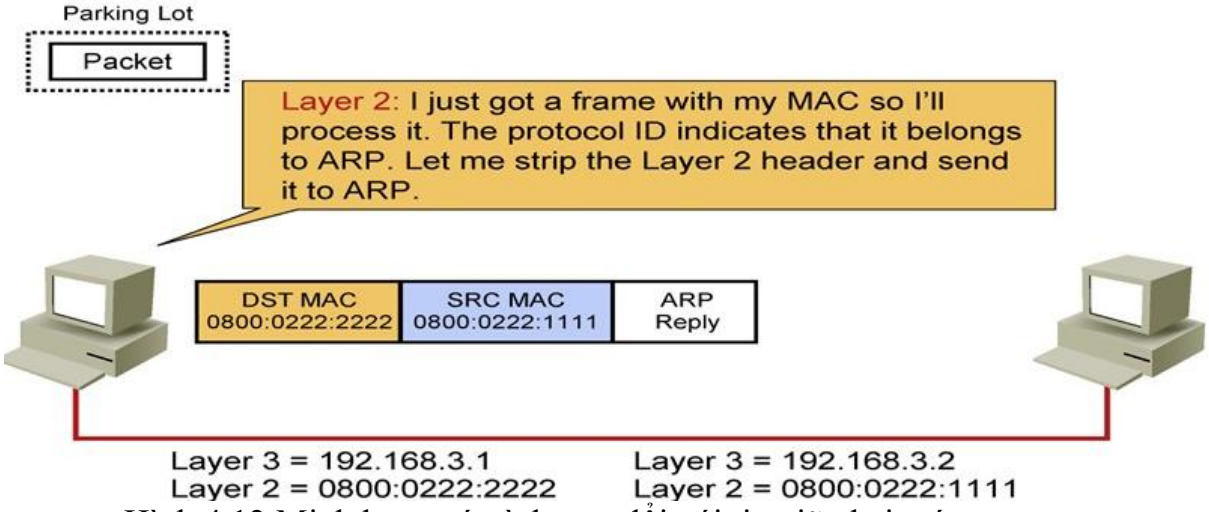
Hình 4.10 Minh hoạ quá trình trao đổi gói tin giữa hai máy trong mạng

Khi ARP mở gói này ra xem thì thấy đây là 1 ARP request được gửi từ 3.1 với MAC 2222 và hỏi phải 3.2 không, máy 2 nhận ra 3.2 chính là mình thì mình trả lời và trước khi trả lời, máy 2 sẽ lưu thông tin 3.1 có MAC là 2222 vào bảng ARP của nó trước để sau này có khi dùng tới sau đó mới trả lời gói ARP request nhận được.



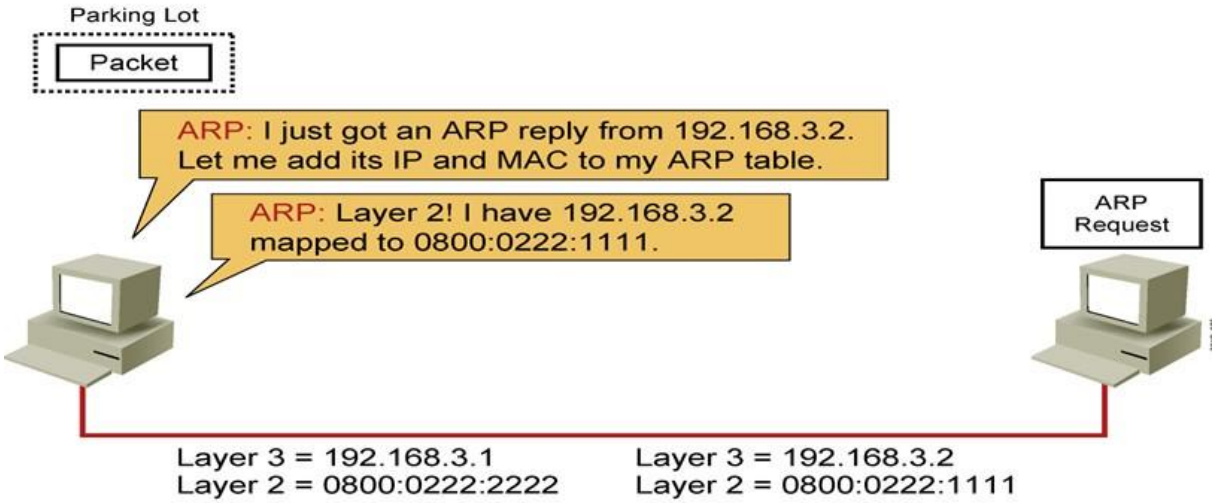
Hình 4.11 Minh hoạ quá trình trao đổi gói tin giữa hai máy trong mạng

Máy 2 sẽ dùng gói ARP Reply mang các thông tin như tôi là 3.2 đây, tôi có địa chỉ MAC là 1111.Và lúc này gói ARP reply sẽ đảo cặp địa chỉ source MAC và destination MAC lại, source MAC của chính máy 2 là 1111, destination MAC là 2222, đóng thành gói ARP reply chuyển xuống lớp Physical và trả về đúng máy 1.



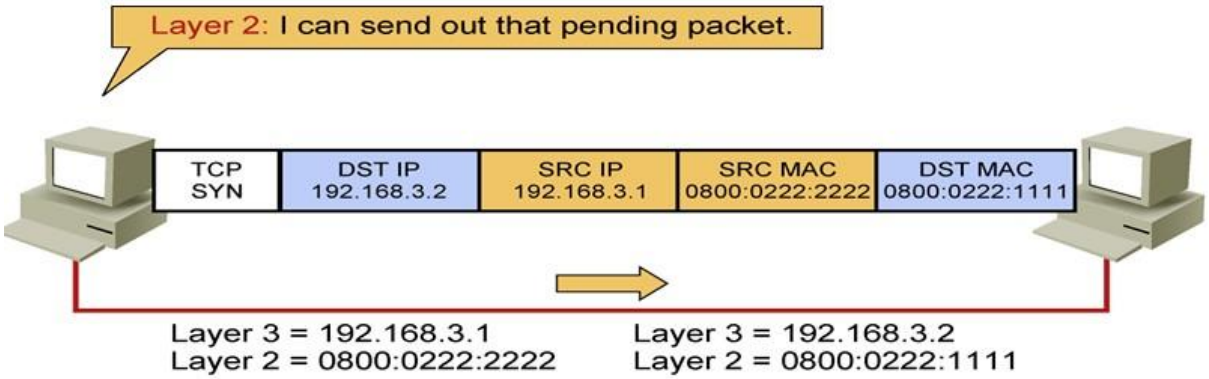
Hình 4.12 Minh hoạ quá trình trao đổi gói tin giữa hai máy trong mạng

Lớp Physical của máy 1 nhận được cũng đưa lên trên chuyển thành frame, thấy frame này gửi cho mình thì xử lý nó, đọc vào protocol ID của header thì biết nó là ARP thì máy 1 gọi ARP ra nhận và xử lý gói tin này.



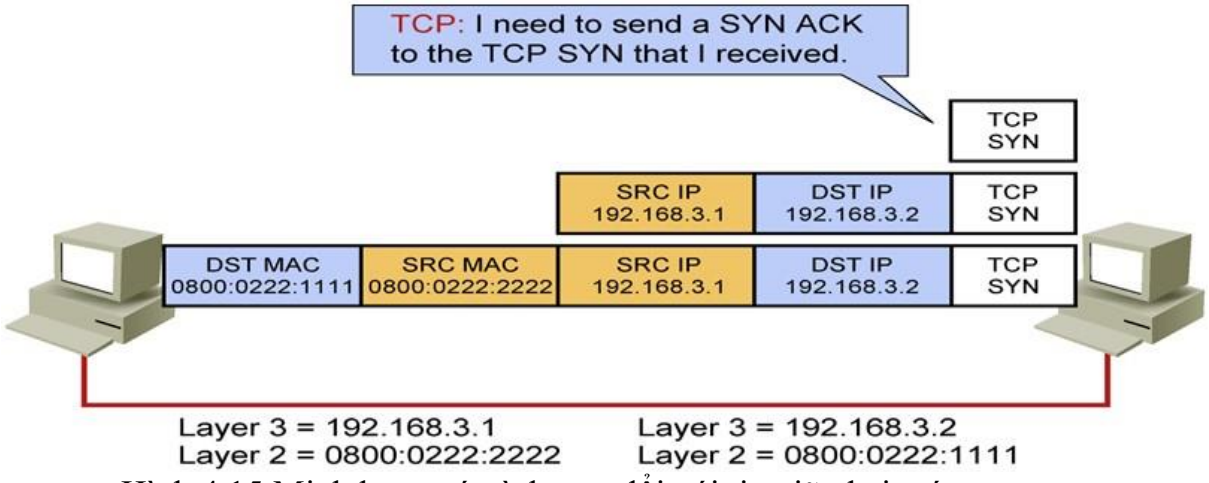
Hình 4.13 Minh hoạ quá trình trao đổi gói tin giữa hai máy trong mạng

Máy 1 mở ra thì thấy đây là gói ARP reply từ 3.2 với địa chỉ MAC là 1111, thì máy 1 lưu 1111 vào bảng ARP của nó. Khi đó máy 1 đã có được MAC của 3.2 thì thông báo cho layer 2 biết rằng đã có địa chỉ MAC tương ứng của 3.2 rồi, bây giờ gửi gói tin đi. Lúc này giai đoạn 2 ARP phân giải địa chỉ mới hoàn tất.



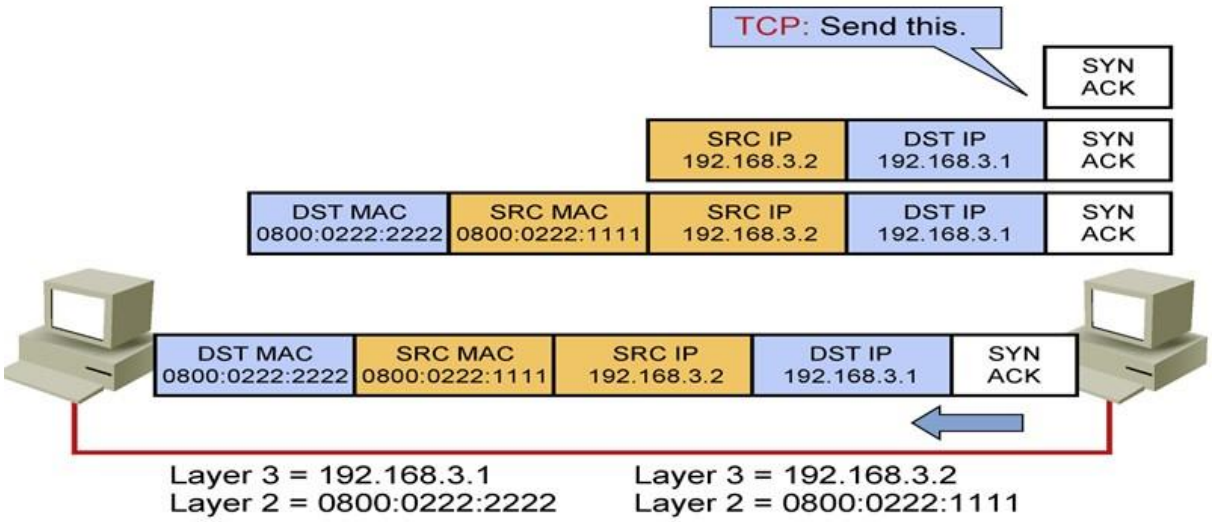
Hình 4.14 Minh hoạ quá trình trao đổi gói tin giữa hai máy trong mạng

Lúc này máy 1 mới bắt đầu lấy gói TCP SYN đang chứa trong Parking Lot để đóng gói lại với đầy đủ cặp source IP, destination IP, source MAC, destination MAC đưa xuống lớp Physical chuyển thành các bit nhị phân và gửi qua máy 2.



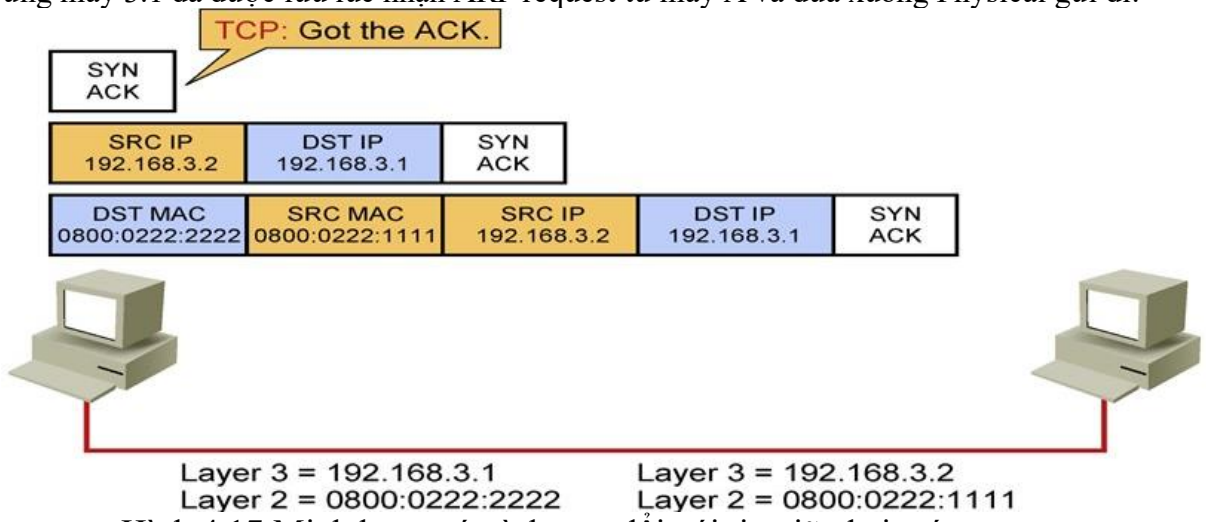
Hình 4.15 Minh hoạ quá trình trao đổi gói tin giữa hai máy trong mạng

Physical của máy 2 nhận được cũng đưa lên trên chuyển thành frame thấy destination MAC gửi cho mình thì xử lý nó, gỡ bỏ layer 2 header đưa lên trên, có được cặp source IP và destination IP, gỡ layer 3 header có được gói TCP SYN, khi nhận được TCP SYN thì máy 2 sẽ trả lời lại SYN ACK.



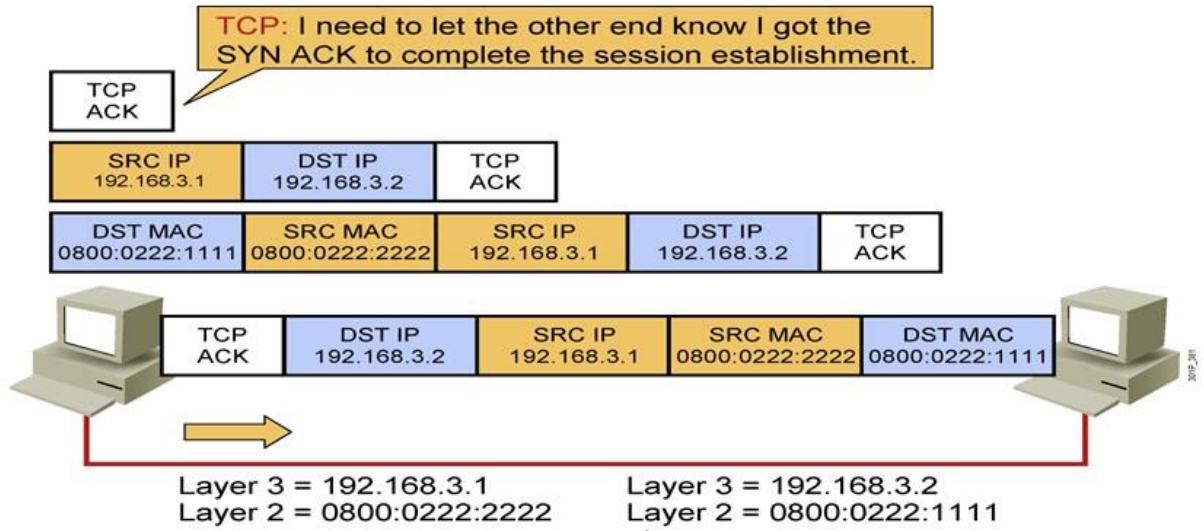
Hình 4.16 Minh hoạ quá trình trao đổi gói tin giữa hai máy trong mạng

Gói TCP SYN ACK được gửi xuống lớp 3 thì đóng vào layer 3 header với cặp source IP và destination IP đảo ngược lại là 3.2 và 3.1, gửi xuống lớp 2 đóng vào layer 2 header với cặp source MAC và destination MAC, source MAC của máy 2 1111, destination MAC 2222 tương ứng máy 3.1 đã được lưu lúc nhận ARP request từ máy A và đưa xuống Physical gửi đi.



Hình 4.17 Minh hoạ quá trình trao đổi gói tin giữa hai máy trong mạng

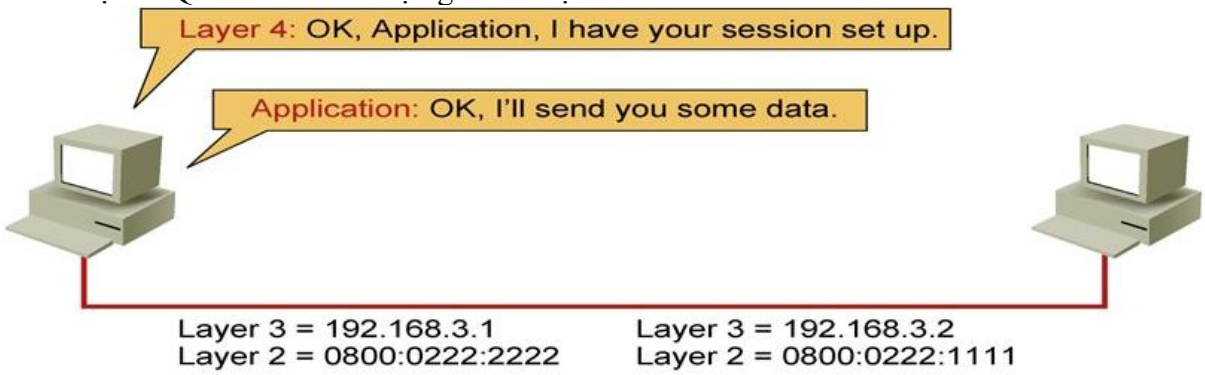
Máy 1 nhận được cũng làm tương tự, chuyển thành frame, gở bỏ các header của lớp 2, lớp 3 và nhận được gói TCP SYN ACK



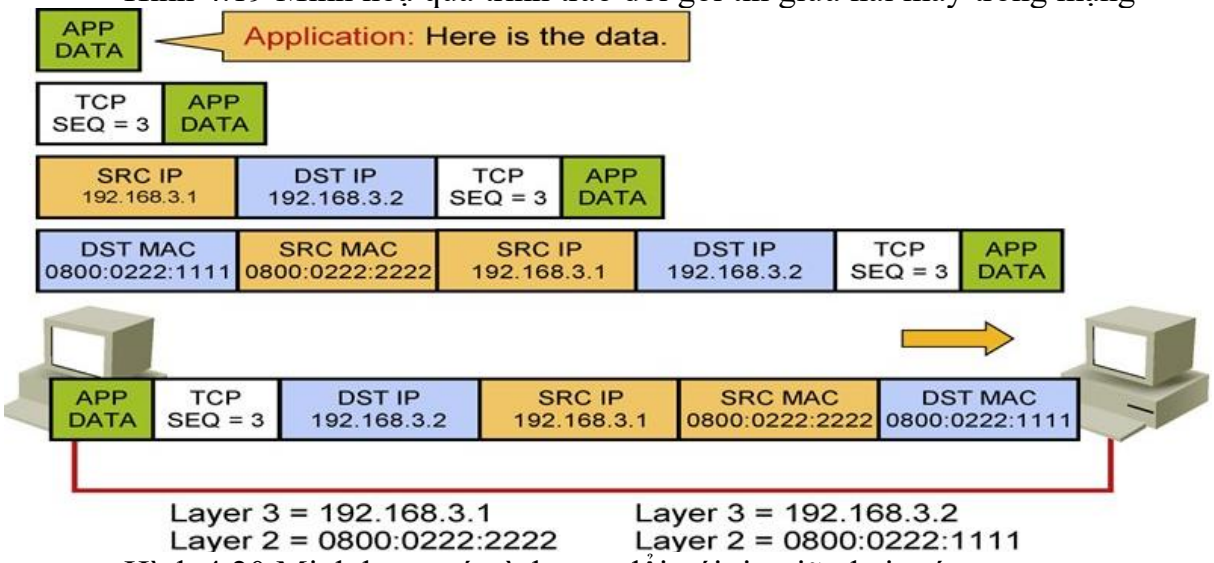
Hình 4.18 Minh hoạ quá trình trao đổi gói tin giữa hai máy trong mạng

Nhận được TCP SYN ACK thì phải trả lời lại ACK để biết mà kết thúc quá trình bắt tay 3 bước thiết lập kết nối trước khi truyền data. Lúc này giai đoạn 1 TCP bắt tay 3 bước thiết lập kết nối mới hoàn tất.

Giai đoạn 3: Quá trình data được gửi và nhận



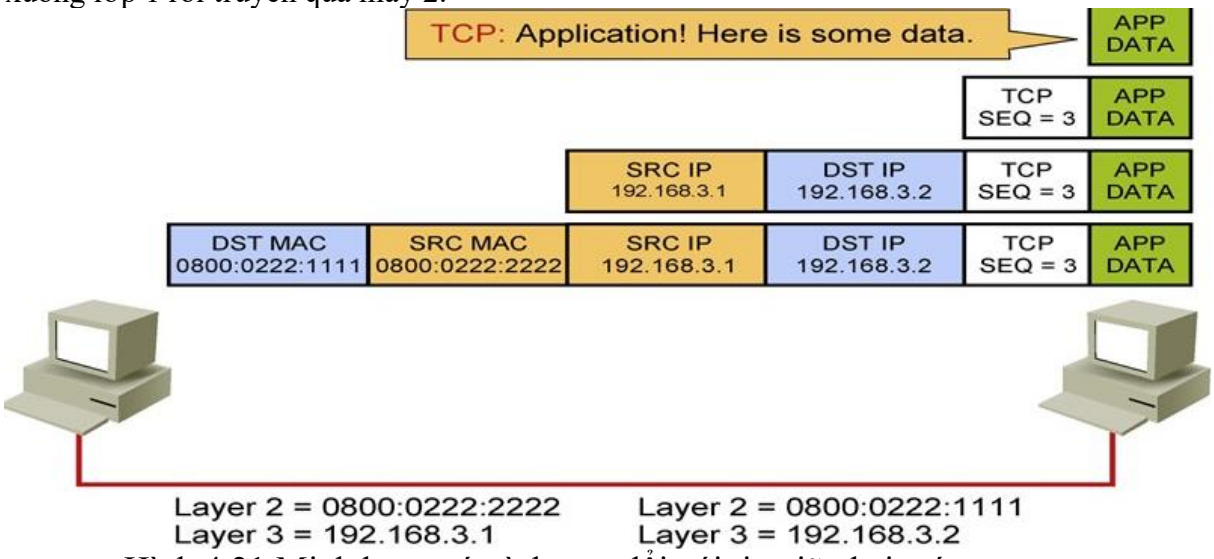
Hình 4.19 Minh hoạ quá trình trao đổi gói tin giữa hai máy trong mạng



Hình 4.20 Minh hoạ quá trình trao đổi gói tin giữa hai máy trong mạng

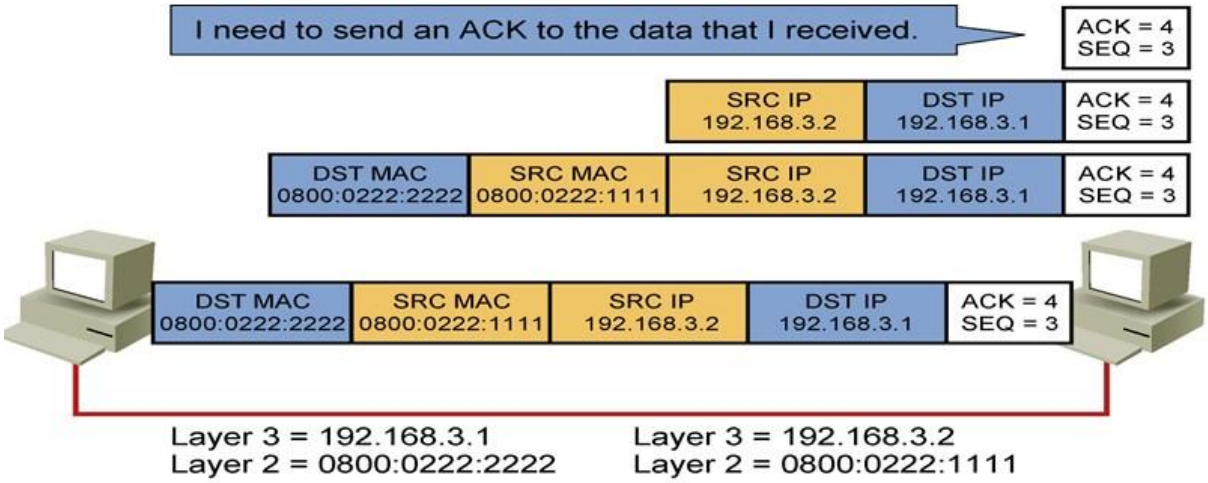
Layer 4 ở máy 1 báo rằng đã thiết lập xong 1 kết nối rồi, Applicatiion hãy bắt đầu truyền data đi, Application bắt đầu đưa data của mình xuống lớp bên dưới, xuống tới Transport bọc thêm header của nó vào và giao thức lúc đầu thiết lập cho kết nối an toàn là TCP nên nó sẽ gắn TCP vào và bắt đầu đánh số thứ tự sequence number cho quá trình truyền ví dụ trường hợp này đánh sequence là 3 rồi gửi xuống lớp Network, ở đây tương tự như quá trình bắt tay 3 bước sẽ đóng

layer 3 header với source IP, destination IP, xuống lớp 2 là source MAC và destination MAC rồi xuống lớp 1 rồi truyền qua máy 2.



Hình 4.21 Minh hoạ quá trình trao đổi gói tin giữa hai máy trong mạng

Máy 2 nhận được chuyển thành frame, gỡ bỏ các header ở các lớp 2, 3, 4… và trả về data cho Application.



Hình 4.22 Minh hoạ quá trình trao đổi gói tin giữa hai máy trong mạng

Và đương nhiên, dùng TCP thì khi máy 2 nhận được sẽ phải trả lời lại cho máy 1 biết, nên đóng gói tin ACK với sequence là 3, ACK là 4 với ý là đã nhận được gói thứ 3 rồi còn gói thứ 4 nữa không, gửi thêm gói thứ 4 đi. Nếu máy 1 không gửi dữ liệu nữa thì đến đây, giai đoạn 3 quá trình data được gửi và nhận hoàn tất.

Lúc này quá trình phân phối gói tin giữa 2 máy 1 và 2 trong mạng kết thúc.

2.8 Bảo mật trên Cisco Router

2.8.1 Cấu hình Firewall Cisco

FireWall Cisco một dòng sản phẩm được đông đảo khách hàng trên thị trường ưa chuộng, sử dụng. Trong giáo trình này chúng tôi sẽ gửi tới quý bạn đọc các cấu hình cơ bản Firewall Cisco. Xin mời các bạn cũng tìm hiểu.

Tóm tắt nội dung trong giáo trình này sẽ gửi đến các bạn những nội dung cơ bản như:

- Cấu hình Hostname, Domain Name và Passwords
- Đặt ngày và giờ
- Cấu hình cụm mật khẩu chính
- Cấu hình máy chủ DNS

Chúng ta sẽ bắt tay ngay vào với các Config cơ bản là thay đổi mật khẩu đăng nhập, thay đổi kích hoạt mật khẩu.

Cấu hình Hostname, Domain Name và Passwords

- Để thay đổi mật khẩu bạn có thể sử dụng câu lệnh
  + **{ passwd | mật khẩu } mật khẩu**
  + Mật khẩu đăng nhập ở đây được sử dụng cho các kết nối Telnet và SSH.
- Các bạn lưu ý là với các thiết bị chưa Config thì mặc định mật khẩu sẽ là "Cisco", đặc điểm này thường được áp dụng với các thiết bị chính hãng của Cisco.
- Bạn có thể nhập password hoặc mật khẩu. Mật khẩu là mật khẩu có phân biệt chữ hoa chữ thường lên đến 16 ký tự chữ và số và ký tự đặc biệt. Bạn có thể sử dụng bất kỳ ký tự nào trong mật khẩu ngoại trừ dấu chấm hỏi hoặc dấu cách.
- Mật khẩu được lưu trong cấu hình dưới dạng mã hóa, vì vậy bạn không thể xem mật khẩu ban đầu sau khi nhập mật khẩu. Sử dụng lệnh không có mật khẩu để khôi phục mật khẩu về cài đặt mặc định.

Thay đổi và kích hoạt mật khẩu

- Bạn sử dụng dòng lệnh
  + **hostname (config) # passwd Pa $$ w0rd**
- Mục đích của dòng lệnh này chính là thay đổi mật khẩu cho phép, cho phép bạn vào chế độ EXEC đặc quyền. Theo mặc định, mật khẩu cho phép trống.
- Đối số mật khẩu là mật khẩu phân biệt chữ hoa chữ thường lên đến 16 ký tự chữ và số và ký tự đặc biệt. Bạn có thể sử dụng bất kỳ ký tự nào trong mật khẩu ngoại trừ dấu chấm hỏi hoặc dấu cách.
- Lệnh này thay đổi mật khẩu cho cấp đặc quyền cao nhất. Nếu bạn định cấu hình ủy quyền lệnh cục bộ, bạn có thể đặt bật mật khẩu cho từng cấp đặc quyền từ 0 đến 15. Mật khẩu được lưu trong cấu hình dưới dạng mã hóa, vì vậy bạn không thể xem mật khẩu ban đầu sau khi nhập mật khẩu. Nhập lệnh bật mật khẩu mà không có mật khẩu để đặt mật khẩu thành mặc định, để trống.

Đặt tên máy chủ cho thiết bị: hostname tên

- Ví dụ:
  + **hostname (config)# hostname farscape**
  + **farscape (config) #**

Chỉ định tên máy chủ cho ASA hoặc cho ngữ cảnh.

+ Tên này có thể lên đến 63 ký tự. Tên máy chủ phải bắt đầu và kết thúc bằng một chữ cái hoặc chữ số và có ký tự bên trong chỉ chữ cái, chữ số hoặc dấu gạch ngang.
+ Khi bạn đặt tên máy chủ cho ASA, tên đó xuất hiện trong lời nhắc dòng lệnh. Nếu bạn thiết lập phiên cho nhiều thiết bị, tên máy chủ sẽ giúp bạn theo dõi vị trí bạn nhập lệnh. Tên máy chủ mặc định tùy thuộc vào nền tảng của bạn.
+ Đối với nhiều chế độ ngữ cảnh, tên máy chủ mà bạn đặt trong không gian thực hiện hệ thống xuất hiện trong lời nhắc dòng lệnh cho tất cả các ngữ cảnh. Tên máy chủ mà bạn tùy ý đặt trong ngữ cảnh không xuất hiện trong dòng lệnh, nhưng có thể được sử dụng bởi lệnh biểu ngữ $ (tên máy chủ) mã thông báo.

Đặt tên miền cho thiết bị: miền tên tên

- Ví dụ:
  + **tên máy chủ (config) # tên miền-example.com**
- Chỉ định tên miền cho ASA. ASA gắn thêm tên miền dưới dạng hậu tố cho các tên không đủ tiêu chuẩn. Ví dụ: nếu bạn đặt tên miền thành "example.com" và chỉ định máy chủ syslog theo tên không đủ tiêu chuẩn của "jupiter", thì ASA đủ điều kiện tên thành "jupiter.example.com".
- Tên miền mặc định là default.domain.invalid.

- Đối với nhiều chế độ ngữ cảnh, bạn có thể đặt tên miền cho mỗi ngữ cảnh, cũng như trong không gian thực thi hệ thống.

Đặt ngày và giờ

Sự khác biệt trong phần này có lẽ chính là việc lựa chọn sử dụng và đặt phạm vi ngày giờ khác nhau.

- Đặt phạm vi ngày giờ theo múi giờ và múi giờ tiết kiệm ánh sáng ban ngày
- Đặt ngày và giờ bằng máy chủ NTP
- Đặt ngày và giờ theo cách thủ công

Để thực hiện những điều đó bạn hãy làm theo các bước sau:

- Bước 1: **đồng hồ múi giờ khu [–] giờ [phút]**
  + **Ví dụ: tên máy chủ (config) # múi giờ đồng hồ PST -8**
- Mục đích chính đó là đặt múi giờ. Theo mặc định, múi giờ là UTC và phạm vi ngày giờ tiết kiệm ánh sáng ban ngày là từ 2:00 sáng vào Chủ nhật đầu tiên trong tháng 4 đến 2:00 sáng vào Chủ nhật cuối cùng trong tháng 10.
- Trong trường hợp khu vực xác định múi giờ như là một chuỗi, ví dụ, PST cho Giờ chuẩn Thái Bình Dương.
- Giá trị giờ [–] thiết lập số giờ bù đắp từ UTC. Ví dụ, PST là -8 giờ. Các phút giá trị thiết lập số phút của bù đắp từ UTC.
- Bước *2*: Để thay đổi phạm vi ngày cho thời gian tiết kiệm ánh sáng ban ngày từ mặc định, hãy nhập một trong các lệnh sau. Phạm vi ngày lặp lại mặc định là từ 2:00 sáng vào Chủ Nhật thứ hai trong tháng 3 đến 2:00 sáng vào Chủ nhật đầu tiên của tháng 11. Đồng hồ mùa hè thời gian khu vực ngày {ngày tháng | ngày tháng} năm hh:mm {ngày tháng | ngày tháng} năm hh: mm [bù trừ].
  + Ví dụ: **hostname (config) # đồng hồ giờ mùa hè PDT 1 tháng 4 năm 2010 2:00 60**

Đặt ngày bắt đầu và ngày kết thúc cho thời gian tiết kiệm ánh sáng ban ngày làm ngày cụ thể trong một năm cụ thể. Nếu bạn sử dụng lệnh này, bạn cần đặt lại ngày tháng mỗi năm.
Các khu vực có giá trị xác định múi giờ như là một chuỗi, ví dụ, PDT cho Pacific Daylight Time.
Các ngày giá trị đặt ngày trong tháng, từ 1 đến 31. Bạn có thể nhập ngày tháng như 01 tháng 4 hoặc 01 tháng tư, ví dụ, tùy thuộc vào định dạng ngày tháng tiêu chuẩn của bạn.
Các tháng giá trị đặt tháng như là một chuỗi. Bạn có thể nhập ngày và tháng vào ngày 1 tháng 4 hoặc ngày 1 tháng 4, tùy thuộc vào định dạng ngày chuẩn của bạn.
Các năm giá trị đặt năm sử dụng bốn chữ số, ví dụ, năm 2004. Phạm vi năm là năm 1993 đến năm 2035.
Các hh: mm giá trị đặt giờ và phút trong thời gian 24 giờ.
Các bù đắp giá trị đặt số phút để thay đổi thời gian cho tiết kiệm thời gian ban ngày.
Theo mặc định, giá trị là 60 phút.
Đồng hồ mùa hè thời gian khu định kỳ [tuần tuần tháng hh:hh mm tuần tuần tháng:mm] [bù đắp]
Ví dụ: hostname (config) # đồng hồ thời gian mùa hè PDT định kỳ đầu tiên Thứ Hai Tháng Tư 2:00 60
Chỉ định ngày bắt đầu và ngày kết thúc cho thời gian tiết kiệm ánh sáng ban ngày, dưới dạng ngày và giờ trong tháng và không phải là ngày cụ thể trong một năm.
Lệnh này cho phép bạn đặt phạm vi ngày lặp lại mà bạn không cần phải thay đổi hàng năm. Các khu vực có giá trị xác định múi giờ như là một chuỗi, ví dụ, PDT cho Pacific Daylight Time.
Các tuần giá trị quy định cụ thể trong tuần của tháng là một số nguyên từ 1 đến 4 hoặc là những lời đầu tiên hoặc cuối cùng. Ví dụ: nếu ngày có thể rơi vào tuần thứ năm một phần, thì hãy chỉ định cuối cùng.
Các ngày trong tuần giá trị xác định ngày trong tuần: Thứ Hai, Thứ Ba, Thứ Tư,… Các tháng giá trị đặt tháng như là một chuỗi. Các hh: mm giá trị đặt giờ và phút trong thời gian 24 giờ.

Các bù đắp giá trị đặt số phút để thay đổi thời gian cho thời gian tiết kiệm ánh sáng ban ngày. Theo mặc định, giá trị là 60 phút.

Đặt ngày và giờ bằng máy chủ NTP

Để thực hiện đặt ngày và giờ bằng máy chủ NTP bạn cần thực hiện theo các bước sau.

- **Bước 1: NTP xác thực**
  - + Ví dụ: **hostname (config) # ntp xác thực**
  - + Bật xác thực với máy chủ NTP.
- **Bước 2: NTP tin cậy-key KEY_ID**
  - + **Ví dụ: tên máy chủ (config) # ntp khóa tin cậy 1**
  - + Chỉ định ID khóa xác thực là khóa đáng tin cậy, được yêu cầu để xác thực bằng máy chủ NTP.
  - + Đối số key_id là giá trị từ 1 đến 4294967295. Bạn có thể nhập nhiều khóa tin cậy để sử dụng với nhiều máy chủ.
- **Bước 3: Khóa xác thực ntp key_id md5 chính**
  - + **Ví dụ: tên máy chủ (config) # ntp khóa xác thực 1 md5 aNiceKey**

Đặt khóa để xác thực bằng máy chủ NTP.

+ Đối số key_id là ID bạn đã đặt trong Bước 2 bằng cách sử dụng lệnh khóa tin cậy ntp và đối số khóa là chuỗi dài tối đa 32 ký tự.

Bước 4: máy chủ ntp ip_address [key key_id] [source interface_name] [thích]

+ **Ví dụ: hostname (config) # ntp máy chủ 10.1.1.1 phím 1 thích**

Xác định máy chủ NTP

Đối số key_id là ID bạn đã đặt trong Bước 2 bằng cách sử dụng lệnh khóa đáng tin cậy ntp.
Các nguồn interface_name cặp từ khóa luận xác định outgoing interface cho các gói NTP nếu bạn không muốn sử dụng giao diện mặc định trong bảng định tuyến. Bởi vì hệ thống không bao gồm bất kỳ giao diện nào trong nhiều chế độ ngữ cảnh, hãy chỉ định tên giao diện được xác định trong ngữ cảnh quản trị.
Các thích bộ từ khóa NTP server này như máy chủ ưa thích nếu nhiều máy chủ có độ chính xác tương tự. NTP sử dụng thuật toán để xác định máy chủ nào chính xác nhất và đồng bộ hóa với máy chủ đó. Nếu máy chủ có độ chính xác tương tự, thì từ khóa ưu tiên chỉ định máy chủ nào sẽ sử dụng các máy chủ đó.
Tuy nhiên, nếu máy chủ chính xác hơn đáng kể so với máy chủ ưu tiên, ASA sử dụng máy chủ chính xác hơn. Ví dụ, ASA sử dụng một máy chủ của tầng 2 trên một máy chủ của tầng 3 được ưa thích.
Lưu ý Trong chế độ nhiều ngữ cảnh, chỉ đặt thời gian trong cấu hình hệ thống.

Đặt ngày và giờ theo cách thủ công

- Sử dụng dòng lệnh để đặt đồng hồ theo cách thủ công đồng hồ bộ hh:
  - + **mm: ss { month day | ngày tháng } năm**
  - + Ví dụ: **hostname # clock set 20:54:00 ngày 1 tháng 4 năm 2004**
  - + Các hh: mm: ss luận đặt giờ, phút và giây trong thời gian 24 giờ. Ví dụ: nhập 20:54:00 cho 8:54 tối.
  - + Các ngày giá trị đặt ngày trong tháng, từ 1 đến 31. Bạn có thể nhập ngày tháng như 01 tháng 4 hoặc 01 tháng tư, ví dụ, tùy thuộc vào định dạng ngày tháng tiêu chuẩn của bạn.
  - + Các tháng giá trị đặt tháng. Tùy thuộc vào định dạng ngày chuẩn của bạn, bạn có thể nhập ngày và tháng như tháng tư 1 hoặc là ngày 1 tháng 4.
  - + Các năm giá trị đặt năm sử dụng bốn chữ số, ví dụ, năm 2004. Phạm vi năm là từ năm 1993 đến năm 2035.
  - + Múi giờ mặc định là UTC. Nếu bạn thay đổi múi giờ sau khi bạn nhập lệnh đặt đồng hồ bằng lệnh múi giờ đồng hồ, thời gian sẽ tự động điều chỉnh theo múi giờ mới.

+ Lệnh này đặt thời gian trong chip phần cứng và không tiết kiệm thời gian trong tệp cấu hình. Lần này sẽ khởi động lại. Không giống như các lệnh đồng hồ khác, lệnh này là một lệnh EXEC đặc quyền. Để đặt lại đồng hồ, bạn cần đặt thời gian mới bằng lệnh đặt đồng hồ.

Cấu hình máy chủ DNS

- Một số tính năng ASA yêu cầu sử dụng máy chủ DNS để truy cập các máy chủ bên ngoài theo tên miền; ví dụ, tính năng Lọc lưu lượng truy cập Botnet yêu cầu máy chủ DNS truy cập vào máy chủ cơ sở dữ liệu động và để giải quyết các mục nhập trong cơ sở dữ liệu tĩnh.
- Các tính năng khác, chẳng hạn như lệnh ping hoặc traceroute, cho phép bạn nhập tên mà bạn muốn ping hoặc traceroute và ASA có thể giải quyết tên bằng cách liên lạc với máy chủ DNS. Nhiều SSL VPN và lệnh chứng chỉ cũng hỗ trợ tên.
- Để biết thông tin về DNS động, hãy xem phần "Định cấu hình DDNS".
- Đảm bảo rằng bạn định cấu hình định tuyến thích hợp cho bất kỳ giao diện nào mà bạn bật tra cứu tên miền DNS để bạn có thể tiếp cận máy chủ DNS. Xem phần "Thông tin về định tuyến" để biết thêm thông tin về định tuyến.

Chi tiết các bước thực hiện

- Bước 1: **dns domain-lookup interface_name**
  + Ví dụ: **hostname (config) # dns domain-lookup bên trong**
  + Cho phép ASA gửi yêu cầu DNS tới máy chủ DNS để thực hiện tra cứu tên cho các lệnh được hỗ trợ.
- Bước 2: **nhóm máy chủ dns DefaultDNS**
  + Ví dụ: **hostname (config) # dns máy chủ nhóm**
  + **DefaultDNS**
  + Chỉ định nhóm máy chủ DNS mà ASA sử dụng cho các yêu cầu gửi đi.
  + Các nhóm máy chủ DNS khác có thể được cấu hình cho các nhóm đường hầm VPN. Xem lệnh nhóm-đường hầm trong tham chiếu lệnh để biết thêm thông tin.
- Bước 3: **name-server ip_address [ip_address2] […] [ip_address6]**
  + Ví dụ: **tên máy chủ (config-dns-server-group) #**
  + **name-server 10.1.1.5 192.168.1.67**
  + **209.165.201.6**
  + Chỉ định một hoặc nhiều máy chủ DNS. Bạn có thể nhập tất cả sáu địa chỉ IP trong cùng một lệnh, được phân tách bằng dấu cách hoặc bạn có thể nhập riêng từng lệnh. ASA cố gắng mỗi máy chủ DNS theo thứ tự cho đến khi nó nhận được phản hồi.

Theo dõi bộ nhớ cache DNS

- ASA cung cấp một bộ nhớ cache địa phương của thông tin DNS từ các truy vấn DNS bên ngoài được gửi cho một số SSL VPN clientless và các lệnh chứng chỉ. Mỗi yêu cầu dịch DNS lần đầu tiên được tìm trong bộ đệm cục bộ. Nếu bộ nhớ cache cục bộ có thông tin, địa chỉ IP kết quả sẽ được trả về.
- Nếu bộ nhớ cache cục bộ không thể giải quyết yêu cầu, một truy vấn DNS sẽ được gửi đến các máy chủ DNS khác nhau đã được cấu hình. Nếu một máy chủ DNS bên ngoài giải quyết yêu cầu, địa chỉ IP kết quả được lưu trữ trong bộ nhớ cache cục bộ với tên máy chủ tương ứng của nó.

Lệnh theo dõi bộ nhớ cache DNS

- Để theo dõi bộ nhớ cache DNS, hãy nhập lệnh sau:
  + Hiển thị dns-hosts: Hiển thị bộ nhớ cache DNS, bao gồm các mục được học tự động từ máy chủ DNS cũng như tên và địa chỉ IP được nhập theo cách thủ công bằng cách sử dụng lệnh tên.

2.9 Sử dụng Cisco SDM

2.9.1 Giới thiệu:

SDM (Security Device Manager) là công cụ để quản lý thiết bị Router thông qua công nghệ JAVA. SDM sử dụng để cấu hình Router thông qua các interface HTTP hoặc HTTPs giúp chúng ta cấu hình LAN, WAN và các tính năng bảo mật khác của Router (ACLs, VPN,…). SDM được thiết kế cho người quản trị mạng hay reseller SMB mà không yêu cầu người sử dụng có kinh nghiệm nhiều trong việc cấu hình Router.

2.9.2 Cài đặt:

Software:

- Download SDM (Security Device Manager): www.cisco.com/go/sdm hoặc http://www.mediafire.com/?zw3h7cahyycdflb
- Sun Java Run Time Environment (JRE): http://download.cnet.com/Java-Runtime-Environment-JRE/3000-2356_4-10009607.html

Cài đặt:

Bước 1:

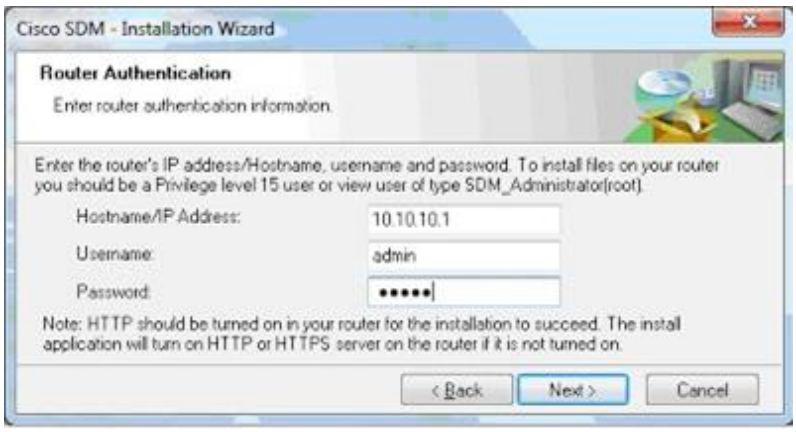
- Kết nối Console vào router thực hiện cấu hình cơ bản
  + Router>enable
  + Router#conf t
  + Router(config)#
- Cấu hình http server
  + Router(config)#ip http server
  + Router(config)#ip http secure-server
  + Router(config)#ip http authentication local
- Tạo user privilege level 15
  + Router(config)#username admin privalege 15 password admin
- Cấu hình telnet và ssh
  + Router(config)#line vty 0 4
  + Router(config-line)#privilege level 15
  + Router(config-line)#login local
  + Router(config-line)#transport input telnet
  + Router(config-line)#transport input telnet ssh
  + Router(config-line)#exit

Bước 2: Cài đặt SDM (Security Device Manager)

- Chạy cài đặt setup.exe. Chọn Both (computer and router). Sau đó chọn Next

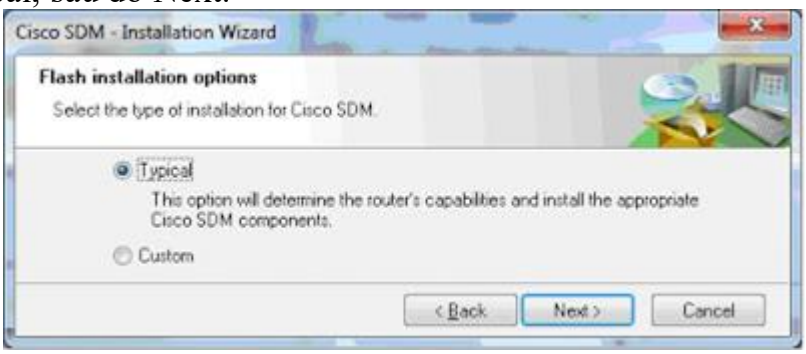
Hình 4.23 Cài đặt SDM (Security Device Manager)

- Nhập địa chỉ IP Router và username password. Chọn Next.



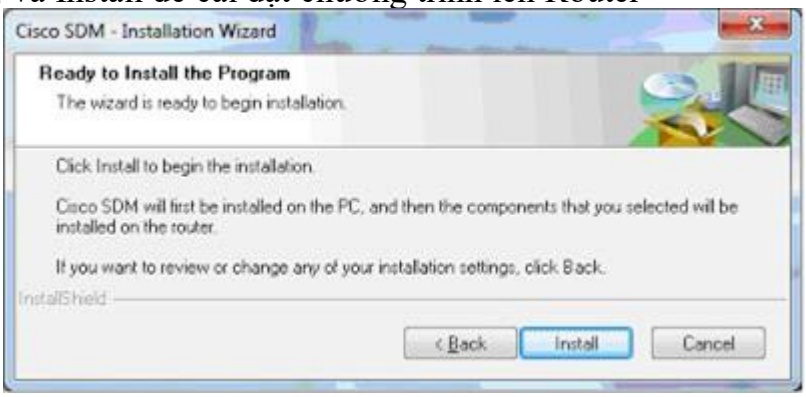
Hình 4.24 Cài đặt SDM (Security Device Manager)

- Chọn Typical, sau đó Next.



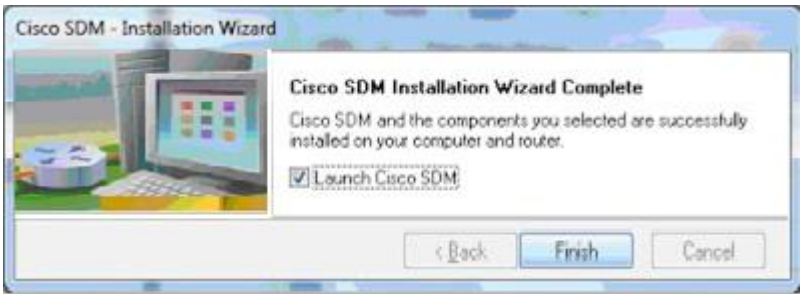
Hình 4.25 Cài đặt SDM (Security Device Manager)

- Chọn Next, và Install để cài đặt chương trình lên Router



Hình 4.26 Cài đặt SDM (Security Device Manager)

- Nhấn Finish

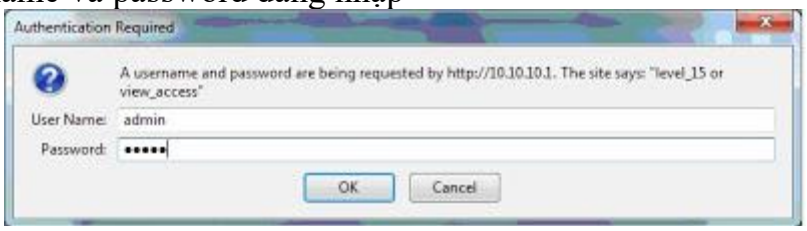


Hình 4.27 Cài đặt SDM (Security Device Manager)

- Kết nối đến Router thông qua địa chỉ 10.10.10.1

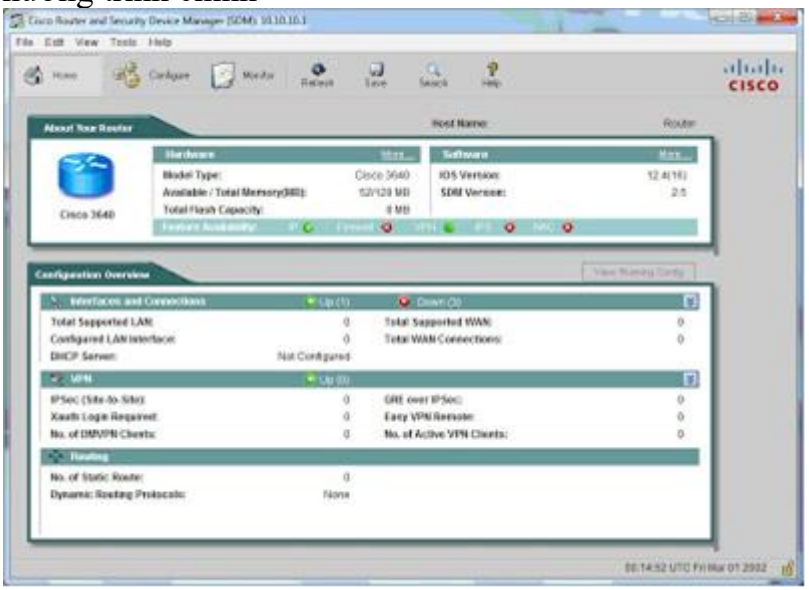
Hình 4.28 Cài đặt SDM (Security Device Manager)

- Nhập username và password đăng nhập



Hình 4.29 Cài đặt SDM (Security Device Manager)

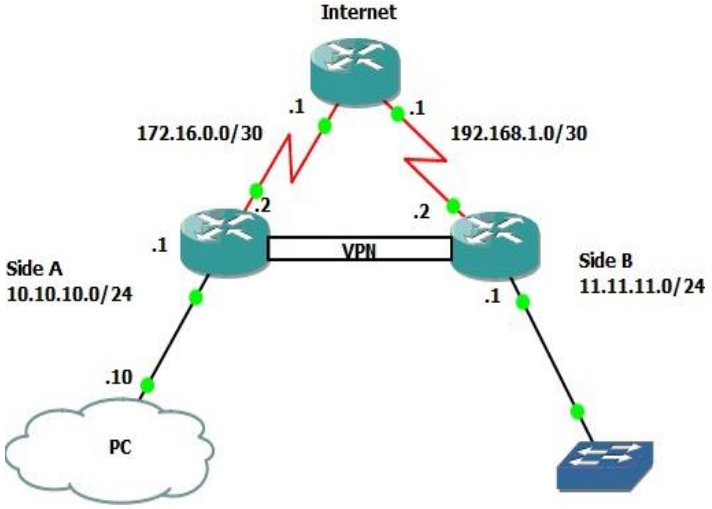
- Giao diện chương trình chính



Hình 4.30 Giao diện chương trình SDM

2.9.3 Chức năng

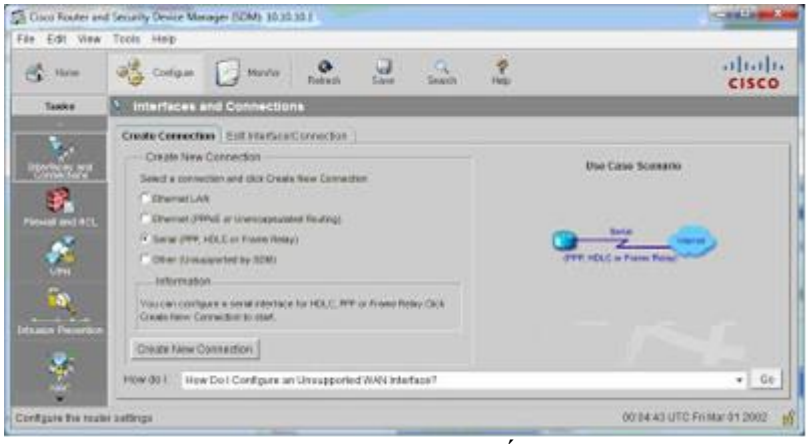
Các chức năng được mô tả dựa cho sơ đồ mạng bên dưới.



Hình 4.31 Mô tả các chức năng

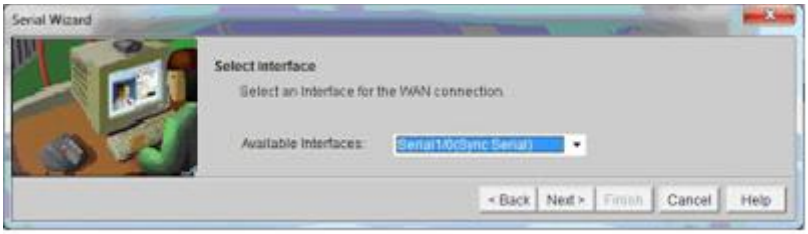
2.9.3.1. Cấu hình Interfaces

- Configure > Interfaces and Connections > Create New Connection



Hình 4.32 Giao diện cấu hình

Chọn Interface cần cấu hình (Serial 1/0). Sau đó Next

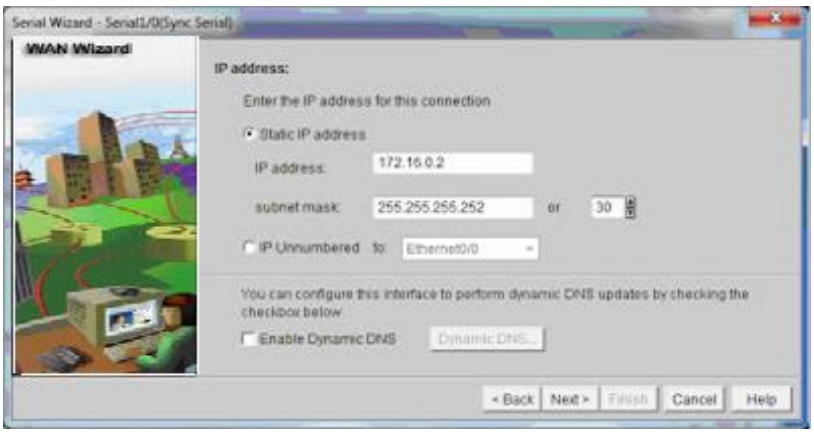


Hình 4.33 Giao diện cấu hình

Chọn type Encapsulation cho Serial Interface. Sau đó Next

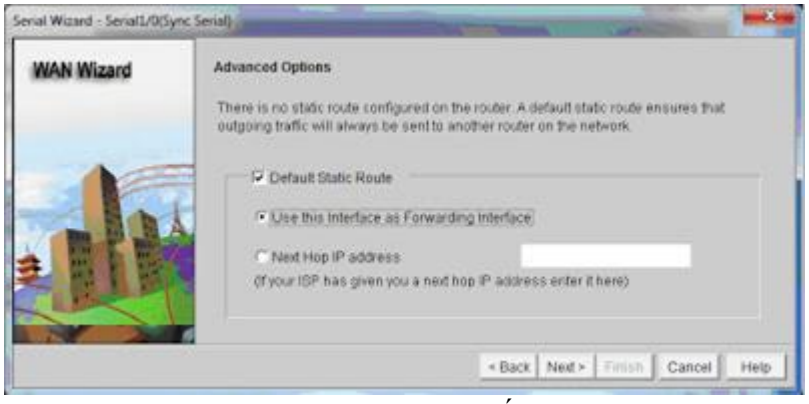
Hình 4.34 Giao diện cấu hình

Nhập địa chỉ IP cho Interface



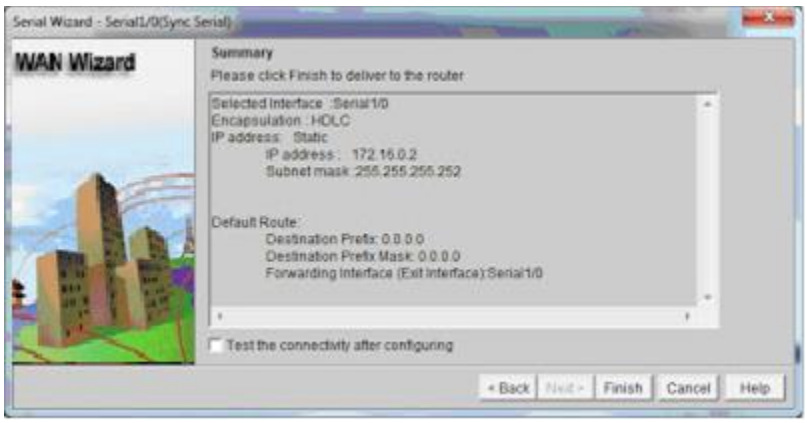
Hình 4.35 Giao diện cấu hình

Chọn Exit Interface hoặc IP Next Hop



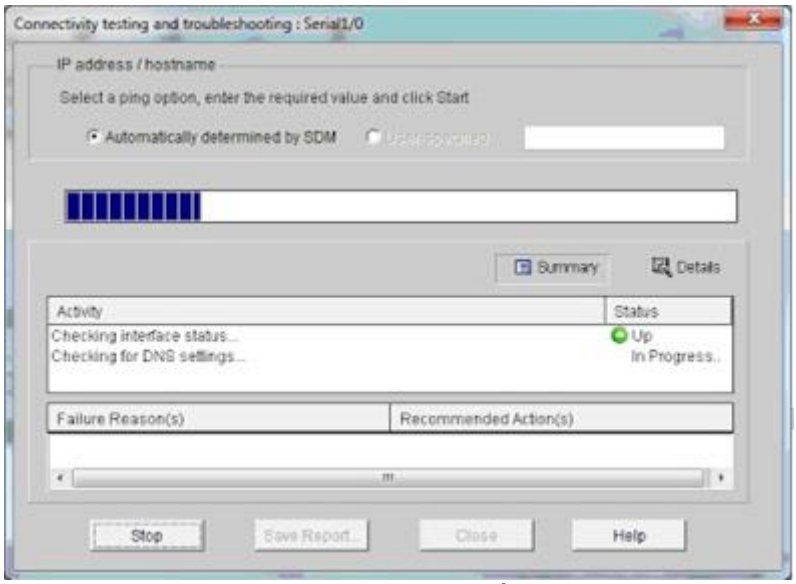
Hình 4.36 Giao diện cấu hình

Chọn Test the connectivity after configuring để kiểm tra kết nối.



Hình 4.37 Giao diện cấu hình

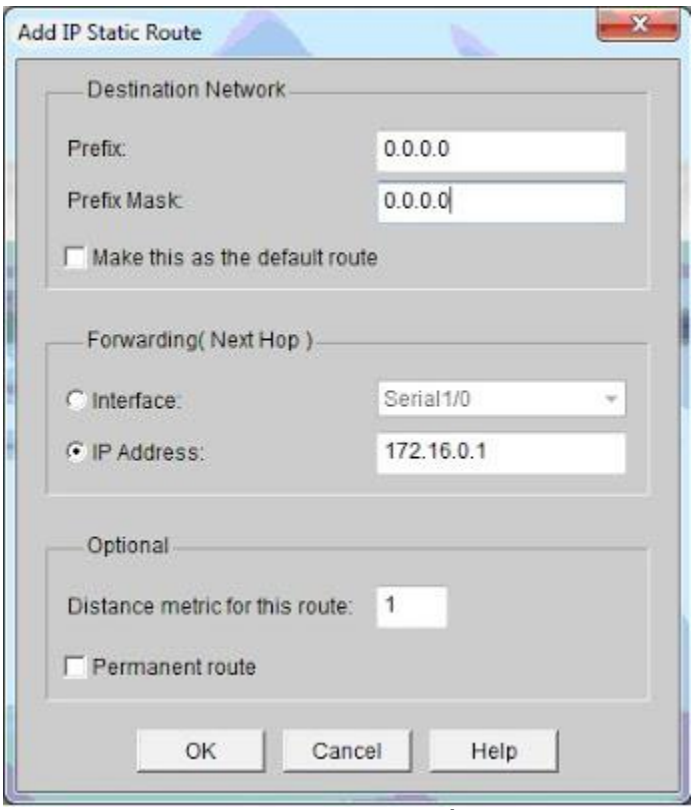
Chọn Start để kiểm tra



Hình 4.38 Giao diện cấu hình

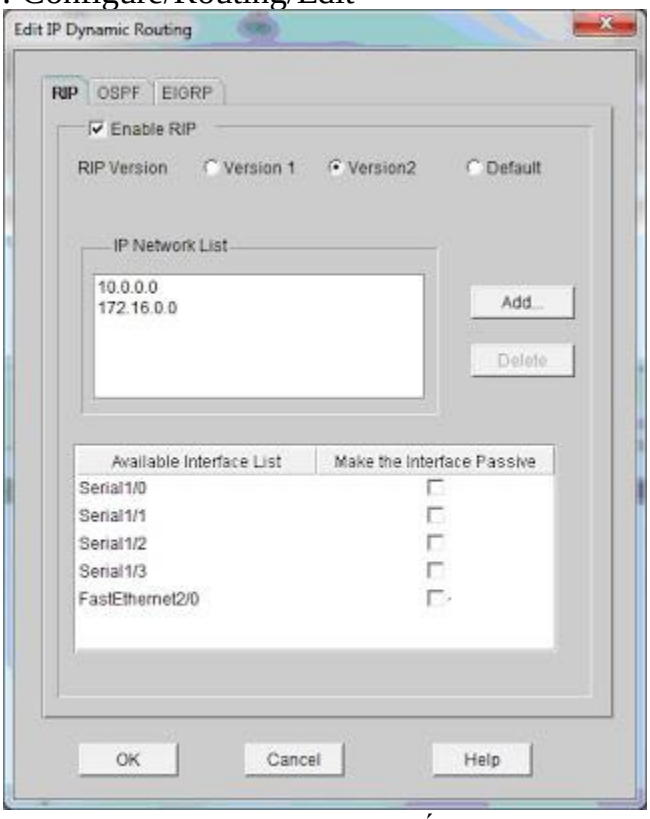
Định tuyến

- Static Route: Configure/Routing/Add

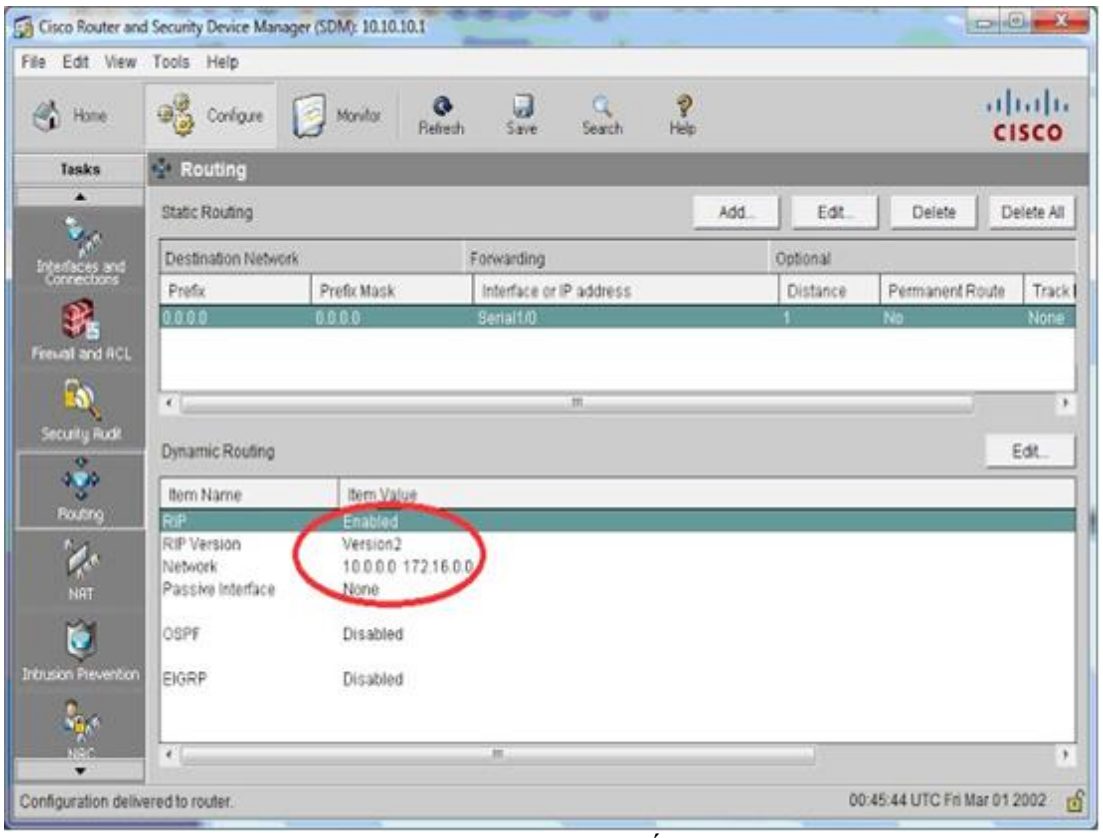


Hình 4.39 Giao diện cấu hình

- Dynamic Route: Configure/Routing/Edit



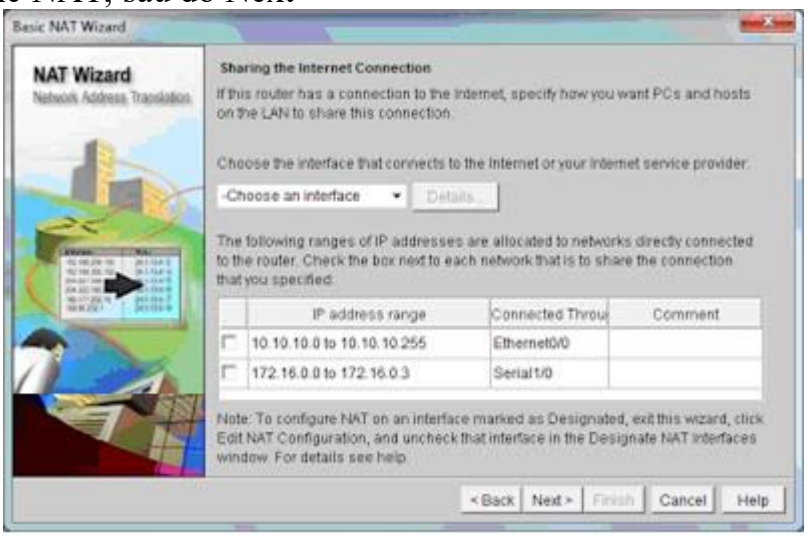
Hình 4.40 Giao diện cấu hình



Hình 4.41 Giao diện cấu hình

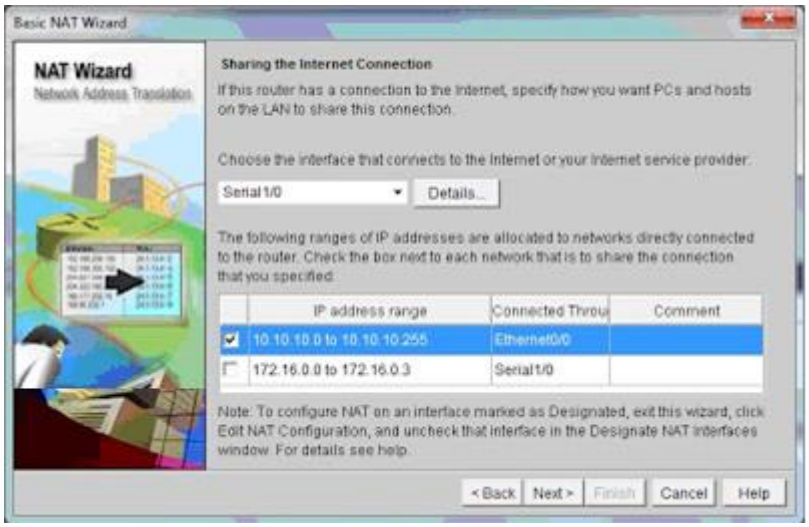
- NAT

- Chọn Basic NAT, sau đó Next



Hình 4.42 Giao diện cấu hình

- Chọn Interface kết nối với Internetvà ranges địa chỉ cần NAT

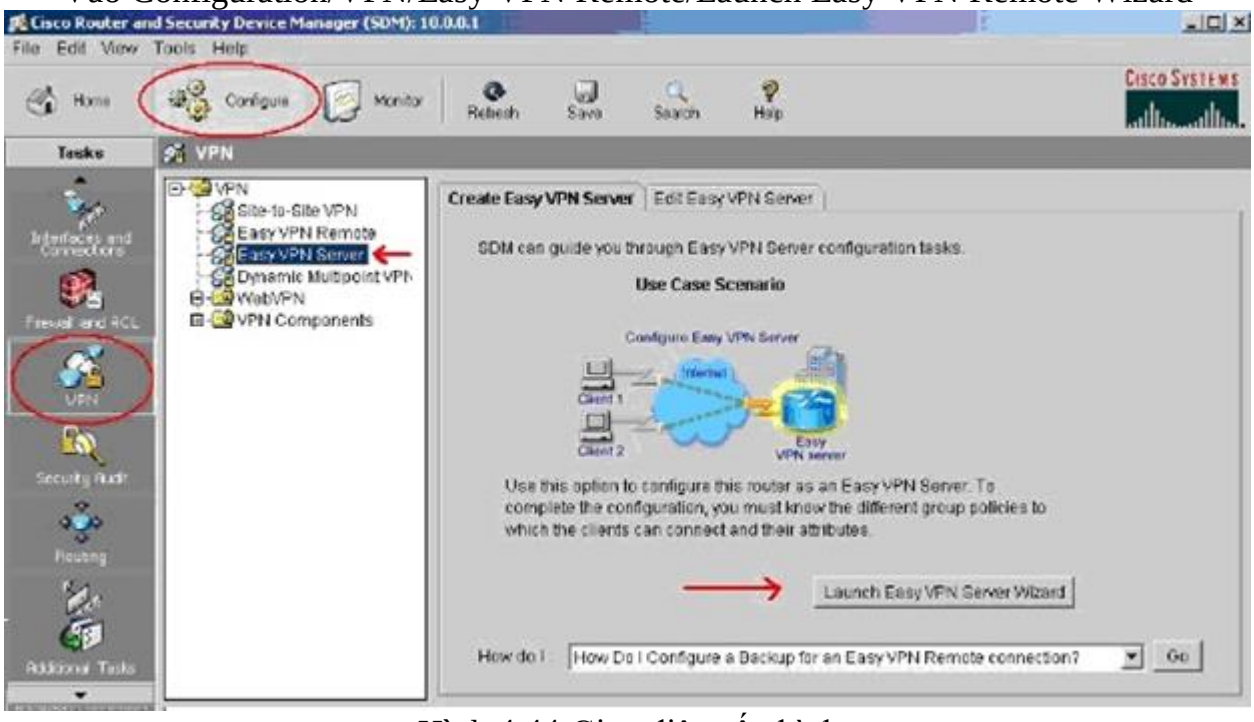


Hình 4.43 Giao diện cấu hình

+ Nhấn Finish

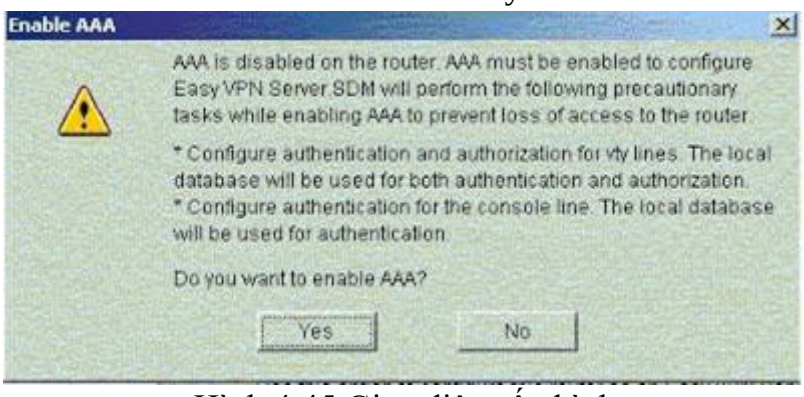
VPN (Virtual Private Network)

Vào Configuration/VPN/Easy VPN Remote/Launch Easy VPN Remote Wizard



Hình 4.44 Giao diện cấu hình

Enable AAA trên Router trước khi cấu hình Easy VPN Server



Hình 4.45 Giao diện cấu hình

Chọn Interface và kiểu chứng thực

Hình 4.46 Giao diện cấu hình

Chọn Next để cấu hình Internet Key Exchange (IKE)

Hình 4.47 Giao diện cấu hình

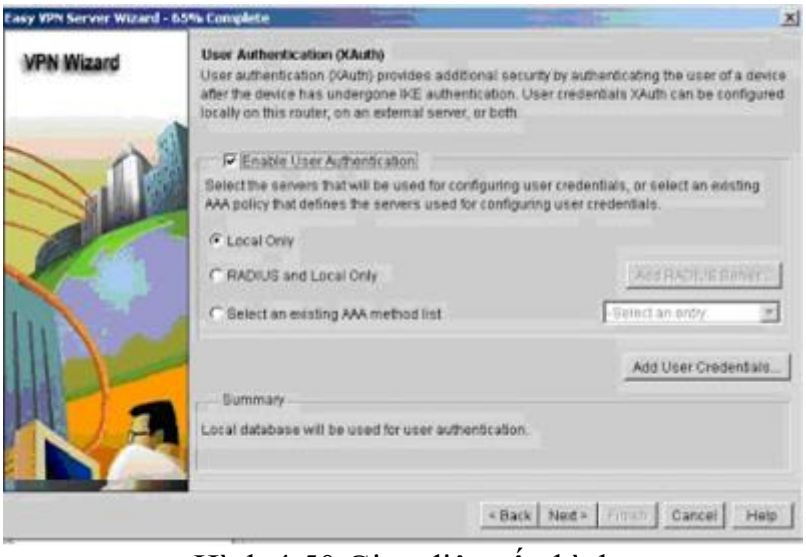
Chọn default transfrom set để thiết lập kiểu mã hóa và chứng thực mặc định

Hình 4.48 Giao diện cấu hình

Chọn Next để tạo mới AAA

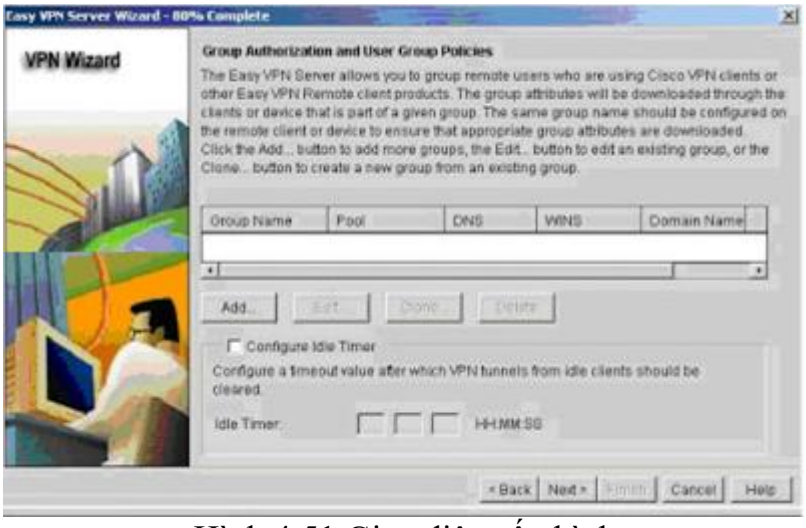
Hình 4.49 Giao diện cấu hình

Cấu hình chứng thực trên Easy VPN Server



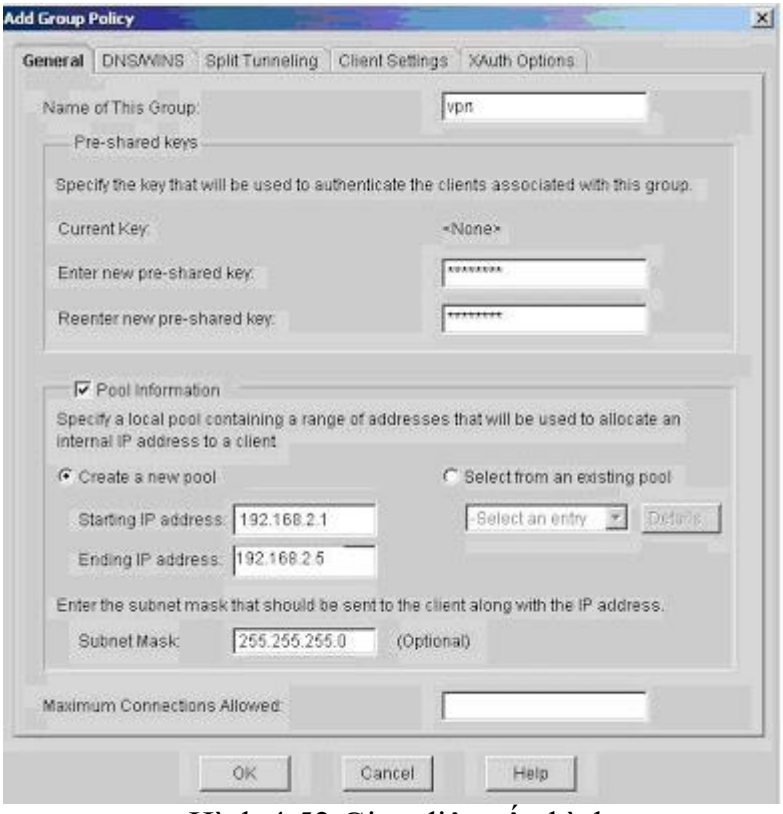
Hình 4.50 Giao diện cấu hình

Add gourp remote users. Chọn Add để thêm group



Hình 4.51 Giao diện cấu hình

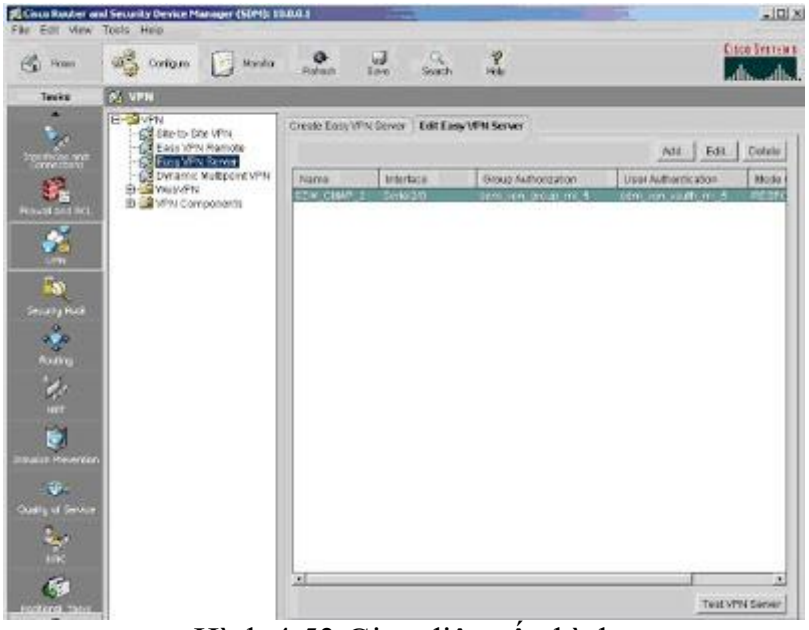
Đặt tên Tunnel Group Name.Cung cấp khóa và thông tin chứng thực và cấp phát vùng IP cho VPN Clients.



Hình 4.52 Giao diện cấu hình

Sau đó Chọn Finish để hoàn thành

+ Kết quả sau khi cấu hình



Hình 4.53 Giao diện cấu hình

+ Ngoài ra SDM còn hỗ trợ cấu hình QoS (Quality of Service), IPS (Intrusion Prevention), NAC, Security Audit, Firewall and AC…

2.10 Sử dụng Cisco Router như một DHCP server

2.10.1 Cấu Hình DHCP Server

Router1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#service dhcp
Router1(config)#ip dhcp pool 192.168.6.128/25
Router1(dhcp-config)#network 192.168.6.128 255.255.255.128
Router1(dhcp-config)#default-router 192.168.6.200
Router1(dhcp-config)#dns-server 210.245.31.130
Router1(dhcp-config)#lease 2
Router1(dhcp-config)#exit
Router1(config)#ip dhcp excluded-address 192.168.6.129 192.168.6.140
Router1(config)#ip dhcp excluded-address 192.168.6.200 192.168.6.254
Router1(config)#end
Router1#

Ở đây:

- Service DHCP: khởi tạo dịch vụ DHCP Server.
- IP DHCP Pool: Xác định khoảng địa chỉ mà DHCP server sẽ cấp cho Client. cú pháp là địa chỉ Network liền với /Subnetmask bits. Có thể thay bằng tên Pool rồi xác định khoảng địa chỉ bằng lệnh Network (ngay sau trong ví dụ)
- Các Options: Default-router tương đương Default-gateway, và DNS server
- Ip dhcp excluded-address: bỏ lại 1 số địa chỉ cho các mục đích sử dụng khác, như các Server – đăng ký riêng địa chỉ tĩnh, địa chỉ của DHCP Server… là để tránh xung đột về địa chỉ sau này.
- Lease: Thời gian cliet giữ ip add, mặc định là 1 ngày. có thể thay đổi. trên ví dụ là để 2 ngày. Tối đa là 365 ngày 23 giờ 59 phút, tối thiểu là 1 phút.
    + Cú pháp: **Lease [ngày] [giờ] [phút]:** giờ và phút là các options có hay ko cũng được.
- Các Options
    + Các options thường được cấu hình là: default-router (Default-gateway),
    + DNS-server, Lease…. đã có trên ví dụ.
- Sau đây là 1 vài options thêm. (Chỉ config options được khi ở trong mode DHCP-config – đã vào trong pool)
    + Router1(dhcp-config)#domain-name [tên domain]
    + Router1(dhcp-config)#netbios-name-server [tên Wins Server]
    + Router1(dhcp-config)#netbios-node-type [loại node-type]
    + **Router1(dhcp-config)#client-name** [Tên client là chỉ sử dụng khi đăng ký riêng địa chỉ tĩnh cho client]
    + Router1(dhcp-config)#host [địa chỉ đăng ký riêng cho client và Subnetmask]

Ngoài tên options, các options này còn được định số thứ tự để tiện cấu hình. Một số options cơ bản và số thứ tự của options:

- VD: như trên ví dụ trên cùng ta có thể thay:
    + Router1(dhcp-config)#default-router 192.168.6.200
    + Router1(dhcp-config)#dns-server 210.245.31.130
    + Router1(dhcp-config)#lease 2

  Bằng:
    + Router1(dhcp-config)#option 3 ip 192.168.6.200
    + Router1(dhcp-config)#option 6 ip 210.245.31.130
    + Router1(dhcp-config)#option 58 2

Một số options khác:

- Router1(dhcp-config)#option 66 ip 10.1.1.1
- Router1(dhcp-config)#option 33 ip 192.0.2.1 172.25.1.3
- Router1(dhcp-config)#option 31 hex 01

+ Option 66: TFTP server, Option 33: static routes, và option 31 buộc Client sử dụng ICMP Router Discovery Protocol (IRDP).

Một Số Điểm Cần Lưu Ý:

- DHCP sử dụng port 67 và 68, nếu hệt thống có xài tường lửa thì phải mở các port này.
- Một số options có thể gán nhiều hơn 1 giá trị. VD là default-router và dns-server. nhưng với option 3 (default-router) chỉ nên đặt 1 giá trị.
- Các options có tính thừa kế (Inherited). bởi vậy khi cấu hình nhiều pool cấp địa chỉ cho nhiều subnet thì nên tạo 1 pool " Cha " bao gồm các pool " con " rồi cấu hình các options chung. sau đó tạo các pool con – có địa chỉ nằm trong pool cha. các options sẽ tự động được thừa kế.
- Nếu pool co có cấu hình cùng options nhưng khác value với pool cha. cấu hình của pool con được ưu tiên hơn.
- Có một option duy nhất không được thừa kế, đó là Lease. bởi vậy nếu pool con không cấu hình Lease. option này trả về giá trị mặc định là 1 (ngày).
- Không nên để giá trị Lease lâu: vì các cập nhật options mới từ DHCP server sẽ chậm được triển khai đến Client. Cũng không nên đặt quá ngắn là tăng lưu lượng mạng. Giá trị mặc định =1 được nhiều người chấp nhận.

2.10.2 Cấu Hình DHCP Client

Việc cấu hình DHCP Client đơn giản hơn nhiều. đơn giản là Set interface của router ở trạng thái DHCP Client là xong. Tuy nhiên, việc này không được khuyên dung cho Router. đơn giản là Router làm nhiều việc quan trọng, nên set địa chỉ tĩnh. vả lại, Client thì nhiều chứ Router thì có bao nhiêu?

Trong 1 số trường hợp, DHCP Server gởi luôn 1 DF route cho Client với AD cao à Client. Router sẽ sử dụng khi Destination không có trong routing table.Nhưng đã nói ở trên, không nên cho Router làm DHCP client nên options này không quan trọng lắm.

Điểm nữa là hiện tại các router làm DHCP client không coi được mình đã nhận được các options gì từ DHCP Server. các IOS sau này có hay không thì chưa biết

```
Router1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#interface Ethernet0
Router1(config-if)#ip address dhcp client-id Ethernet0
Router1(config-if)#no shut
Router1(config-if)#end
Router1#
Interface Ethernet0 assigned DHCP address 192.168.6.141, mask 255.255.255.128
Router1#
```

Thông tin về interface sẽ có dạng sau:

```
Router1#show ip interface e0
Ethernet0 is up, line protocol is up
Internet address is 192.168.6.141/25
Broadcast address is 255.255.255.255
```

Address determined by DHCP

MTU is 1500 bytes

<removed for brevity>

2.10.3 Cấu Hình DHCP Relay Agent bằng lệnh IP Helper-address

Trong mô hình mạng nhiều Subnet, các client không cùng Network với DHCP Server. cần cấu hình DHCP relay Agent để forward DHCP discover đến DHCP Server.

Mô hình DHCP Server cùng net với client, mạng đơn giản thì không cần làm việc này. Cú pháp cũng rất đơn giản:

- Trong ví dụ này sẽ cấu hình Router làm DHCP Server có địa chỉ F0/0 là 192.168.6.201
  + Router1#configure terminal
  + Enter configuration commands, one per line. End with CNTL/Z.
  + Router1(config)#interface Ethernet0
  + Router1(config-if)#ip helper-address 192.168.6.201
  + Router1(config-if)#end
  + Router1#

Một số điểm cần lưu ý:

- Interface E0 là interface cùng Lan với DHCP Server.
- Khi 1 Client gởi DHCP Discover, nó dùng địa chỉ Source là 0.0.0.0 và địa chỉ Destination là 255.255.255.255 (broadcast)
- Khi DHCP Relay Agent nhận được tín hiệu DHCP Discover, nó sẽ thay địa chỉ source của gói tin thành chính nó và địa chỉ đích là DHCP Server xác định trong lệnh ip helper-address. Địa chỉ MAC vẫn là của DHCP Client.
- DHCP Server sẽ nhận ra được Subnet mà Client đang ở thông qua địa chỉ mà DHCP relay Agent gán vào. Nó sẽ chọn địa chỉ phù hợp và gởi lại cho DHCP relay agent (tín hiệu unicast). DHCP RA sẽ gởi lại cho client (qua Mac add trong gói tin)
- Có thể chỉ định nhiều DHCP Server (mỗi lệnh ip helper-add chỉ định 1 DHCP server). khi đó tín hiệu DHCP Discover sẽ được forward đi nhiều hướng. Khi có nhiều hơn Response cho 1 DHCP discover, Client sẽ nhận địa chỉ IP trả về sớm hơn.
- Để coi thông tin về các IP helper-add đã xác định: coi trong output của: sh ip int [int].
- Một lưu ý quan trọng là " IP helper-add" không chỉ forward DHCP Discover đến DHCP server, các tín hiệu UDP khác cũng sẽ được forward theo ảnh hưởng đến hoạt động của DHCP Server. các tín hiệu UDP được forward bởi IP heler-add:
- Các client chạy Windows phát khá nhiều tín hiệu Netbios, những tín hiệu khác ít xảy ra hơn. Nếu không chặn hết thì nên chặn tín hiệu Netbios không thôi.
  + Router1#configure terminal
  + Enter configuration commands, one per line. End with CNTL/Z.
  + Router1(config)#no ip forward-protocol udp netbios-ns
  + Router1(config)#no ip forward-protocol udp netbios-dgm
  + Router1(config)#no ip forward-protocol udp tftp
  + Router1(config)#no ip forward-protocol udp nameserver
  + Router1(config)#no ip forward-protocol udp domain
  + Router1(config)#no ip forward-protocol udp time
  + Router1(config)#no ip forward-protocol udp tacacs
  + Router1(config)#end
  + Router1#
- Có thể thay tên bằng số Port tương ứng phía trên.

2.10.4 Cấu hình địa chỉ đăng ký riêng (Static assign)

Việc này cũng thường phải làm để gán IP cho các Server cần ip static.

Một số lưu ý trước khi cấu hình:

- Đương nhiên là việc gán này dựa theo địa chỉ MAC. điểm khác biệt là router cisco xài Client-identifier có gán thêm giá trị 01 trước MAC add (giá trị 01 được gán cho các interface chạy tốc độ 10/100/1000)
- Địa chỉ MAC có thể viết liền nhau, router tự tìm cách ra.
- Phải tạo Pool riêng cho mỗi lần đăng ký địa chỉ tĩnh.
- Nên Exclue sẵn 1 số địa chỉ trong Root Pool cho việc này (như ví dụ trên cùng)
- Các options sẽ được thừa hưởng từ pool cha, nếu thấy được thì khỏi config nữa.

+ Trong ví dụ này sẽ lấy địa chỉ MAC card mạng của mình là 009099169EFC. tên là WebServer, ip 6.199, DF GW 6.200, DNS 210.245.31.130, Lease 5 (option này không được thừa kế).

+ Router1(config)#ip dhcp pool WEB
+ Router1(dhcp-config)#host 192.168.6.199 255.255.255.128
+ Router1(dhcp-config)#client-identifier 01009099169EFC
+ Router1(dhcp-config)#client-name WebServer
+ Router1(dhcp-config)#default-router 192.168.6.200
+ Router1(dhcp-config)#domain-name **hohoho.com**
+ Router1(dhcp-config)#dns-server 210.245.31.130
+ Router1(dhcp-config)#lease 5
+ Router1(dhcp-config)#end
+ Router1#

2.10.5 Lưu trữ DHCP Database

DHCP database được lưu trong RAM -> mất đi khi reload. nếu không có lưu trữ về database ở một điểm khác. Sau khi Reload, DHCP Server bắt đầu như trạng thái mới hoạt động là sẽ cấp những địa chỉ mà client còn đang sử dụng (vì nó có biết ai đang xài địa chỉ gì của nó đâu?) gây ra xung đột (Conflic IP) mạng

- Việc cấu hình như ví dụ trên, ở đây ta lấy FTP Server, TFTP Server và RCP Server đều là 192.168.6.199. đây là những dịch vụ được hỗ trợ, với TFTP (Có lẽ thông dụng và dễ sử dụng nhất) thì nhớ bật sẵn TFTP Server lên chờ.

FTP:

Router1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#ip dhcp database ftp://dhcp:bindsave@192.168.6.199/dhcp-r2a (tên tùy thích)

Router1(config)#end

Router1#

(dhcp:bindsave: user + Pass)

TFTP:

Router1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#ip dhcp database tftp://192.168.6.199/dhcp-r2a

Router1(config)#end

Router1#

RCP:

Router1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#ip dhcp database rcp://dhcp@192.168.6.199/dhcp-r2a

Router1(config)#end

Router1#

- Khi đã up data lên data server, một khi reload, DHCP server sẽ tự lấy lại data và hoạt động tiếp tục một cách bình thường.
- Cấu hình địa chỉ tĩnh đăng ký cho các server nằm trong NVRAM và không bị ảnh hưởng, reload thoải mái không sao.

2.10.6 Cấu hình nhiều DHCP trên 1 Subnet

- Bình thường như cấu hình 1 DHCP Server trên 1 subnet vậy thôi. chẳng qua là làm trên 2 cái Router
- Lưu ý một chút là vì trên cùng Subnet, Pool giống nhau là đương nhiên; do đó, cần exclue đi một phần cho DHCP Server bên kia cấp. Tránh việc 2 DHCP cấp cùng 1 khoảng địa chỉ là Conflic IP ngay.
- Khi up data lên Data Server, đặt tên sao cho dễ nhận ra data nào là của DHCP nào, tiện việc sau này.

2.10.7 Theo dõi trạng thái DHCP Server

- Dùng các lệnh:
  + **SH ip DHCP Binding** : thông tin về các địa chỉ đã cấp, các Mac add của địa chỉ được cấp, thời hạn còn lại.
  + **SH ip DHCP Conflic** : Tìm coi thằng nào đang xung đột với thằng nào
  + **SH ip DHCP Database** : thông tin về các lần up data lên server
  + **SH ip DHCP Server Statistics** : Chi tiết tỉ mỉ các thứ còn lại
- Không muốn DHCP Server ghi lại các sự kiện về xung đột địa chỉ: dùng lệnh
  + Router(config)#no ip dhcp conflict logging
- Xóa binding database:
  + Router#clear ip dhcp binding *
  + Có thể thay * bằng địa chỉ ip nếu muốn xóa một entry nào đó thôi.

2.10.8 Debugging DHCP

Có 2 lệnh thôi:

- Router1#debug ip dhcp server events (output thí dụ)

Router1#debug ip dhcp server events

Sep 15 00:58:17.218: DHCPD: returned 172.25.1.51 to address pool COOKBOOK

Sep 15 00:58:22.566: DHCPD: assigned IP address 172.25.1.51 to client 0100.0103.85e9.87.

Sep 15 0115.056: DHCPD: writing bindings to ftp://dhcp:bindsave@172.25.1.1/dhcp-leases-rtr1.

Sep 15 0115.132: DHCPD: writing address 172.25.1.51.

Sep 15 0115.148: DHCPD: wrote automatic bindings to ftp://dhcp:bindsave@172.25.1.1/dhcp-leases-rtr1.

Sep 15 0158.816: DHCPD: checking for expired leases.

Sep 15 01:03:58.841: DHCPD: checking for expired leases.

Sep 15 0158.859: DHCPD: checking for expired leases.

Sep 15 0158.874: DHCPD: checking for expired leases.

Sep 15 01:09:58.885: DHCPD: checking for expired leases.

Sep 15 01:09:58.885: DHCPD: the lease for address 172.25.1.51 has expired.
Sep 15 01:09:58.885: DHCPD: returned 172.25.1.51 to address pool COOKBOOK.

- Router1#debug ip dhcp server packet (output thí dụ)

Router1#debug ip dhcp server packet
Sep 15 01:19:41.211: DHCPD: DHCPDISCOVER received from client 0100.0103.85e9.87 on interface FastEthernet0/0.1.
Sep 15 01:19:43.212: DHCPD: Sending DHCPOFFER to client 0100.0103.85e9.87 (172.25.1.51).
Sep 15 01:19:43.212: DHCPD: creating ARP entry (172.25.1.51, 0001.0385.e987).
Sep 15 01:19:43.212: DHCPD: unicasting BOOTREPLY to client 0001.0385.e987 (172.25.1.51).
Sep 15 01:19:43.216: DHCPD: DHCPREQUEST received from client 0100.0103.85e9.87.
Sep 15 01:19:43.216: DHCPD: Sending DHCPACK to client 0100.0103.85e9.87 (172.25.1.51).
Sep 15 01:19:43.216: DHCPD: creating ARP entry (172.25.1.51, 0001.0385.e987).
Sep 15 01:19:43.216: DHCPD: unicasting BOOTREPLY to client 0001.0385.e987 (172.25.1.51).
Router1#

2.11 Kết nối mạng diện rộng

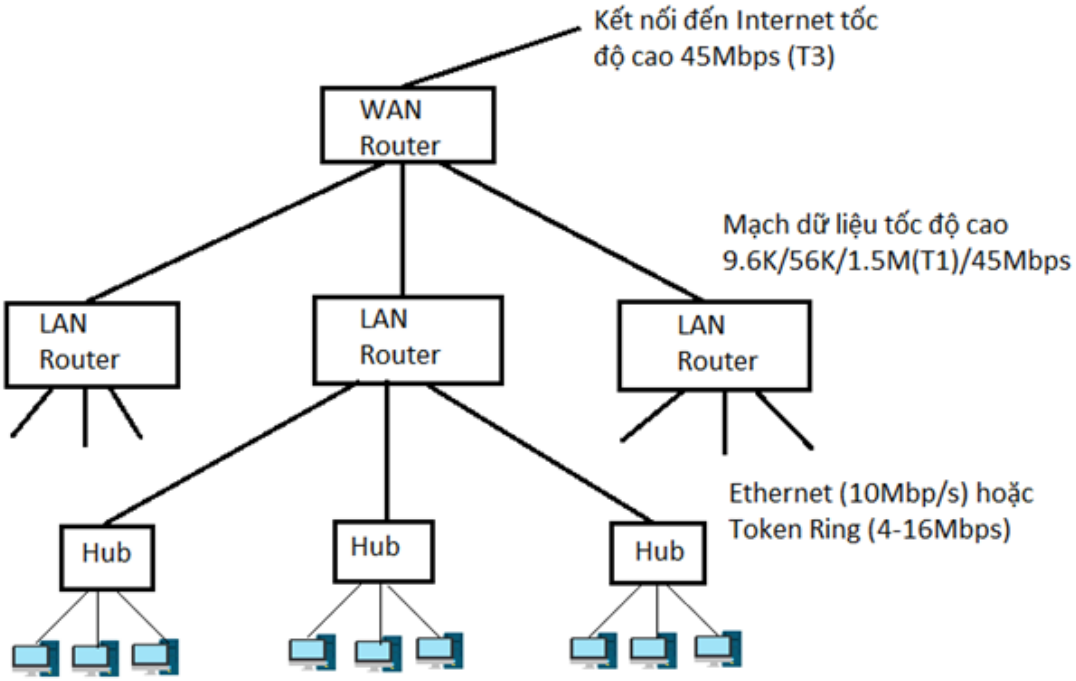
Như chúng ta đã biết mạng cục bộ (LAN) sử dụng để kết nối các thiết bị gần nhau với nhau. Tốc độ truyền dữ liệu trong mạng cục bộ vì thế thường khá cao. Mạng WAN, trái lại, kết nối các thiết bị xa cách nhau về mặt địa lý và do đó công nghệ mạng WAN cũng khác với công nghệ mạng LAN.

Mạng WAN sử dụng phương thức truyền dẫn, phần cứng và giao thức khác mạng LAN. Tốc độ truyền dữ liệu trong mạng WAN cũng thấp hơn nhiều khi so với mạng LAN. Chúng ta sẽ nghiên cứu tổng quan về các công nghệ của mạng WAN dưới một số góc độ.

Mạng WAN sử dụng hạ tầng truyền dẫn của một nhà cung cấp dịch vụ bên thứ 3, chủ yếu là các công ty điện thoại, để cung cấp dịch vụ kết nối khoảng cách xa. Cấu hình phổ biến nhất của một mạng WAN bao gồm các thành phần như hình dưới. Một thông điệp được khởi tạo từ phía khách hàng và được gửi đi bởi một thiết bị gọi là DTE[1] tới nhà cung cấp dịch vụ mạng WAN. Các thiết bị DCE[2] ở văn phòng trung tâm của nhà cung cấp dịch vụ sẽ "đẩy" gói tin tới mạng WAN, sau đó đi qua các thiết bị chuyển mạch để tới đích. Các thiết bị tương tự ở phía đầu nhận sẽ kết thúc hành trình.

[1] **DTE:** ***Data Terminal Equipment***, hay **Thiết bị cuối xử lý số liệu** (hoặc dữ liệu). Từ này ám chỉ đến một thiết bị cuối (*end instrument*) sử dụng để biến tư liệu sang tín hiệu truyền thông, hoặc biến những tín hiệu thu được sang tư liệu. Thiết bị cuối xử lý số liệu (DTE) giao thông với thiết bị kết cuối kênh số liệu (*Data Circuit-terminating Equipment* - DCE).

[2] Thiết bị kết cuối kênh số liệu (*Data Circuit-terminating Equipment* - DCE)



Hình 4.54 Mạng WAN điển hình

Thiết bị đầu cuối dữ liệu (DTE - Data Terminal Equipment): Thiết bị ở phía lề của liên kết mạng WAN có chức năng gửi và nhận dữ liệu. DTE được đặt tại vị trí của người thuê bao, chính là điểm kết nối giữa mạng LAN của thuê bao và mạng WAN của nhà cung cấp dịch vụ. DTE thông thường là một bộ định tuyến (router), nhưng trong một số trường hợp có thể là một máy tính hay một bộ dồn kênh (multiplexer). Các DTE ở đầu bên này sẽ thực hiện việc truyền thông với thiết bị DTE tương ứng ở đầu bên kia.

Điểm ranh giới (Damarcation Point): Điểm kết nối giữa đường dây điện thoại của công ty điện thoại với đường dây của thuê bao. Điểm ranh giới còn được gọi là giao diện mạnghay điểm hiện diện (point of presence). Thông thường, khách hàng sẽ chịu trách nhiệm cho tất cả các thiết bị bên trong điểm ranh giới và công ty viễn thông sẽ chịu trách nhiệm về tất cả các thiết bị ở phía bên kia.

Cáp nối chặng cuối (Local Loop): Cáp nối từ Điểm ranh giới tới Văn phòng trung tâm của công ty điện thoại. Thông thường đó là cáp đôi xoắn (UTP), nhưng cũng có thể là kết hợp cáp đôi xoắn, cáp sợi quang và các loại phương tiện truyền dẫn khác.

Văn phòng trung tâm (Central Office): Trạm tổng đài gần nhất,cũng là điểm cung cấp dịch vụ mạng WAN gần nhất với người thuê bao. Văn phòng trung tâm cung cấp điểm vàocho các cuộc gọi đi vào "đám mây mạng WAN" và cung cấp các điểm ra cho các cuộc gọi từ đám mây mạng WAN tới người sử dụng điện thoại.Ngoài ra, nó còn đóng vai trò như một điểm chuyển mạng để chuyển các gói dữ liệu tới các văn phòng trung tâm khác. Nó cũng cung cấp dòng điện một chiều ổn định cho hệ thống cáp nối chặng cuối để thiết lập mạch điện.

Thiết bị đóng mạch dữ liệu (DCE – Data Circuit-terminating Equipment)

Thiết bị truyền thông với cả DTE và đám mây mạng WAN. DCE thông thường là một bộ định tuyến của nhà cung cấp dịch vụ có chức năng chuyển tiếp dữ liệu giữa khách hàng và đám mây mạng WAN.Theo nghĩa hẹp, DTE là bất cứ thiết bị nào cung cấp tín hiệu xung

cho DTE. DCE cũng có thể là một thiết bị tương tự DTE (thường là một bộ định tuyến) ngoại trừ mỗi loại thiết bị đóng một vai trò riêng.

Đám mây mạng WAN (WAN cloud): Một loạt các trung kế, tổng đài và văn phòng trung tâm tạo thành hạ tầng truyền dẫn của công ty điện thoại. Nó được thể hiện trong hình như một đám mây bởi vì có cấu trúc vật lý thay đổi thường xuyên và chỉ những người có trách nhiệm quản trị mạng mới biết dữ liệu sẽ đi tới đâu tại các tổng đài. Đối với khách hàng, điều quan trọng là dữ liệu đã được chuyển qua đường dây để tới đích.

Tổng đài chuyển mạch gói (Packet-switching exchange): Các tổng đài chuyển mạch trên mạng chuyển mạch gói của công ty viễn thông. PSE là các điểm trung gian trong đám mây mạng WAN.

Dữ liệu truyền trên mạng LAN chủ yếu được gửi từ một thiết bị số (máy tính) tới một thiết bị số khác thông qua kết nối trực tiếp. Trong khi đó, bởi vì một số mạng WAN sử dụng mạng điện thoại tương tự sẵn có, nên việc truyền số liệu có thể sử dụng một hay kết hợp những phương pháp dưới đây:

Truyền tín hiệu tương tự

Các tín hiệu tương tự thường được thể hiện dưới dạng sóng. Cường độ và tần số của tín hiệu tương tự thay đổi liên tục nên nó có thể thể hiện một cách chính xác sự chuyển động liên tục hay âm thanh hay những chuyển động đa trạng thái. Cường độ và tần số của tín hiệu tăng lên và giảm xuống tương ứng với cao độ và cường độ của âm thanh. Các tín hiệu tương tự thường dùng để biểu diễn các dữ liệu thời gian thực. Truyền thanh, điện thoại và các phương tiện truyền thông thường sử dụng tín hiệu tương tự.

Truyền tín hiệu số

Thay vì dòng thay đổi liên tục, các tín hiệu số chỉ sử dụng 2 trạng thái, 0 và 1, để biểu diễn các bit dữ liệu. Đây là phương pháp truyền tín hiệu lý tưởng cho các mạng máy tính. Các máy tính sẽ cần tới modem, thiết bị chuyển đổi tín hiệu số của máy tính thành tín hiệu tương tự để truyền dữ liệu qua đường dây điện thoại tương tự.

Lưu ý: Trước đây, mạng điện thoại PSTN là mạng tương tự hoàn toàn. Các tín hiệu tương tự từ máy điện thoại tới công ty viễn thông và sẽ tiếp tục được chuyển qua các hệ thống sử dụng tín hiệu tương tự để tới đích. Ngày nay, các hệ thống điện thoại hiện nay sử dụng kết hợp hai phương pháp. Phần lớn các mạng chuyển mạch (swithced network) kết nối mạng của các công ty viễn thông đều đã được số hoá, riêng chặng cuối nối phần lớn hộ gia đình và một số doanh nghiệp vẫn sử dụng tín hiệu tương tự. Sơ đồ dưới đây cho ta thấy hai máy tính số có thể được kết nối qua mạng WAN có cả các thành phần số và thành phần tương tự. Khi một máy tính gửi tín hiệu qua mạng WAN, modem sẽ chuyển tín hiệu số thành tín hiệu tương tự để chuyển tín hiệu tới công ty điện thoại. Modem của công ty điện thoại sẽ lại chuyển dữ liệu thành dạng số để truyền qua mạng chuyển mạch. Tín hiệu lại được chuyển ngược trở lại thành tín hiệu tương tự tại phía đầu đích của công ty viễn thông để chuyển tới modem của máy tính nhận dữ liệu. Cuối cùng, modem này sẽ chuyển tín hiệu tương tự thành dạng số cho máy tính.

Các loại hình kết nối trong mạng WAN

Khi một thông điệp di chuyển qua đám mây mạng WAN, cách thức nó di chuyển từ điểm này tới điểm khác trên đường đi của nó sẽ khác nhau phụ thuộc vào kết nối vật lý và giao thức sử dụng. Các kết nối mạng WAN thường được phân thành những dạng sau:

Kết nối dành riêng (Dedicated Connection)

Đây là kết nối mang tính thường trực, kết nối trực tiếp một thiết bị với một thiết bị khác. Kết nối dành riêng có tính ổn định và nhanh nhưng có thể rất đắt. Thuê một đường dây từ nhà cung cấp dịch vụ mạng WAN có nghĩa là bạn phải trả tiền kết nối ngay cả khi bạn không sử dụng nó. Hơn nữa, bởi vì các đường dây dành riêng thiết lập kết nối trực tiếp chỉ giữa 2 điểm, nên số đường dây cần thiết sẽ tăng theo hàm số mũ các vị trí cần kết nối. Ví dụ, nếu bạn muốn kết nối 2 vị trí, bạn cần một đường dây nhưng muốn kết nối 4 vị trí bạn sẽ cần tới 6 đường dây.

Các đặc trưng của kết nối dành riêng:

- Luôn luôn sẵn có
- Sử dụng đường dây người thuê bao thuê của nhà cung cấp dịch vụ mạng WAN
- Đắt hơn so với các giải pháp mạng WAN khác
- Sử dụng các kết nối riêng biệt giữa các điểm
- Sử dụng kết nối dành riêng khi:
  + Có lưu lượng cao dữ liệu luân chuyển qua mạng LAN
  + Cần kết nối thường xuyên
  + Có ít địa điểm cần kết nối với nhau
  + Mạng chuyển mạch (circuit- switched network)
- Mạng chuyển mạch cho bạn một giải pháp thay thế đối với đường thuê riêng (kết nối dành riêng), cho phép bạn sử dụng các đường dây dùng chung. Mạng chuyển mạch làm việc hai chiều, cho phép thiết lập cả các kết nối quay số vào (dial-in) và quay số ra (dial-out).

Khi bạn sử dụng mạng chuyển mạch:

- Máy tính gửi dữ liệu quay số vào đường dây và kết nối được thiết lập
- Máy tính nhận dữ liệu gửi xác nhận và khoá đường dây
- Máy tính gửi dữ liệu truyền dữ liệu qua kết nối được thiết lập
- Sau khi hoàn tất việc truyền dữ liệu, kết nối được giải phóng cho những người sử dụng khác.
- Mạng chuyển mạch sử dụng các mạch ảo chuyển mạch (SVC – switched virtual circuit). Một đường truyền dữ liệu dành riêng được thiết lập khi bắt đầu quá trình truyền thông nhờ một loạt các bộ chuyển mạch điện tử. Con đường riêng này sẽ còn cho tới khi kết thúc quá trình truyền thông).
- Hệ thống điện thoại công cộng là một mạng chuyển mạch. Khi bạn thực hiện một cuộc gọi, PSTN sử dụng các bộ chuyển mạch để tạo ra một kết nối vật lý, trực tiếp và dành riêng cho suốt thời gian diễn ra cuộc gọi. Khi bạn ngưng cuộc gọi, các bộ chuyển mạch giải phóng đường dây cho những người sử dụng khác. Các máy tính kết nối qua mạng làm việc theo cách thức tương tự như vậy. Khi máy tính quay số vào mạng, trước tiên con đường qua mạng được thiết lập để sau đó dữ liệu sẽ được chuyển qua con đường dành riêng tạm thời này.

Mạng chuyển mạch gói (packet-swiched)

- Mạng chuyển gói không yêu cầu một đường thuê riêng hay đường dành riêng tạm thời. Thay vào đó, đường đi của thông điệp được thiết lập một cách cơ động khi dữ liệu chuyển qua mạng. Kết nối chuyển mạch gói là kết nối thường xuyên bật. Điều đó có nghĩa

là bạn không cần quan tâm tới việc thiết lập kết nối hay giữ riêng đường dây. Mỗi gói tin bao gồm cả thông tin cần thiết để tới đích.

Mạng chuyển mạch gói có những đặc trưng sau đây:

- Thông điệp được chia thành những đơn vị nhỏ, gọi là gói
- Các gói được chuyển độc lập qua liên mạng (có thể theo những con đường khác nhau)
- Các gói được sắp xếp lại theo thứ tự ban đầu tại nơi nhận
- Thiết bị gửi và thiết bị nhận mặc định xem kết nối là thường trực (không cần quay số)
- Mạng chuyển mạch gói sử dụng các mạch ảo thường trực (PVC- permanent virtual circuit). Mặc dù PVC giống như kết nối dành riêng, trực tiếp, con đường mỗi gói tin đi trong liên mạng có thể khác nhau.

Các dịch vụ mạng diện rộng

PSTN

- Mạng điện thoại chuyển mạch công cộng là mạng lâu đời nhất và có qui mô lớn nhất có thể sử dụng cho truyền thông mạng WAN. Các đặc trưng của PSTN bao gồm:
- Đây là mạng chuyển mạch, có phạm vi toàn cầu. Giao diện với PSTN là tương tự, vì vậy các máy tính sử dụng modem để kết nối với PSTN
- Tốc độ trên PSTN thường bị giới hạn ở ngưỡng 56 Kbit/s
- Bạn có thể sử dụng PSTN khi có nhu cầu (on demand) hay thuê một mạch riêng

Đường thuê riêng (Leased Line)

- Đối với một số công ty, lợi ích của một đường thuê riêng có thể cao hơn rất nhiều so với chi phí phải bỏ ra. Đường thuê riêng là đường độc lập và có tốc độ cao hơn so với đường PSTN thông thường. Tuy nhiên nó khá đắt nên thường chỉ có các công ty lớn sử dụng. Các đặc trưng khác của đường thuê riêng bao gồm:
- Cung cấp kết nối thường xuyên, chất lượng ổn định
- Bạn có thể bỏ thêm chi phí để nâng cấp đường thuê riêng

X.25

- X.25 ra đời vào những năm 1970. Mục đích ban đầu của nó là kết nối các máy chủ lớn (mainframe) với các máy trạm (terminal) ở xa. Ưu điểm của X.25 so với các giải pháp mạng WAN khác là nó có cơ chế kiểm tra lỗi tích hợp sẵn. Chọn X.25 nếu bạn phải sử dụng đường dây tương tự hay chất lượng đường dây không cao.
- X.25 là chuẩn của ITU-T cho truyền thông qua mạng WAN sử dụng kỹ thuật chuyển mạch gói qua mạng điện thoại. Thuật ngữ X.25 cũng còn được sử dụng cho những giao thức thuộc Lớp vật lý và Lớp liên kết dữ liệu để tạo ra mạng X.25. Theo thiết kế ban đầu, X.25 sử dụng đường dây tương tự để tạo nên một mạng chuyển mạch gói, mặc dù mạng X.25 cũng có thể được xây dựng trên cơ sở một mạng số. Hiện nay, giao thức X.25 là một bộ các qui tắc xác định cách thức thiết lập và duy trì kết nối giữa các DTE và DCE trong một mạng dữ liệu công cộng (PDN – public data network). Nó qui định các thiết bị DTE/DCE và PSE (Packet-swiching exchange) sẽ truyền dữ liệu như thế nào.
- Bạn cần phải trả phí thuê bao khi sử dụng mạng X.25
- Khi sử dụng mạng X.25, bạn có thể tạo kết nối tới PDN qua một đường dây dành riêng
- Mạng X.25 hoạt động ở tốc độ 64 Kbit/s (trên đường tương tự)
- Kích thước gói tin (gọi là frame) trong mạng X.25 không cố định
- Giao thức X.25 có cơ chế kiểm tra và sửa lỗi rất mạnh nên nó có thể làm việc tương đối ổn định trên hệ thống đường dây điện thoại tương tự có chất lượng thấp
- X.25 hiện đang được sử dụng rộng rãi ở nhiều nước trên thế giới nơi các mạng số chưa phổ biến cũng như chất lượng đường dây còn thấp

Frame Relay

- Frame Relay hiệu quả hơn so với X.25 và đang dần dần thay thế chuẩn này. Khi sử dụng Frame Relay, bạn trả phí thuê đường dây tới node gần nhất trên mạng Frame Relay. Bạn gửi dữ liệu qua đường dây của bạn và mạng Frame Relay sẽ định tuyến nó tới node gần nhất với nơi nhận và chuyển dữ liệu xuống đường dây của người nhận. Frame Relay nhanh hơn so với X.25
- Frame Relay là một chuẩn cho truyền thông trongmạng WAN chuyển mạch gói qua các đường dây số chất lượng cao. Một mạng Frame Relay có các đặc trưng sau:
  + Có nhiều điểm tương tự như khi triển khai một mạng X.25
  + Có cơ chế kiểm tra lỗi nhưng không có cơ chế khắc phục lỗi
  + Tốc độ truyền dữ liệu có thể lên tới 1.54 Mbit/s
  + Cho phép nhiều kích thước gói tin khác nhau
  + Có thể kết nối như một kết nối đường trục tới mạng LAN
  + Có thể triển khai qua nhiều loại đường kết nối khác nhau (56K, T-1, T-3)
  + Hoạt động tại Lớp Vật lý và Lớp Liên kết dữ liệu trong mô hình OSI.
- Khi đăng ký sử dụng dịch vụ Frame Relay, bạn được cam kết về mức dịch vụ gọi là CIR (Committed Information Rate). CIR là tốc độ truyền dữ liệu tối đa được cam kết bạn nhận được trên một mạng Frame Relay. Tuy nhiên, khi lưu lượng trên mạng thấp, bạn có thể gửi dữ liệu ở tốc độ nhanh hơn CIR. Khi lưu lượng trên mạng cao, ưu tiên sẽ dành cho những khách hàng có mức CIR cao.

ISDN (Intergrated Services Digital Network)

- Một trong những mục đích của ISDN là cung cấp khả năng truy nhập mạng WAN cho các hộ gia đình và doanh nghiệp sử dụng đường cáp đồng điện thoại. Vì lý do đó, các kế hoạch triển khai ISDN đầu tiên đã đề xuất thay thế các đường dây tương tự đang có bằng đường dây số. Hiện nay, việc chuyển đổi từ tương tự sang số đang diễn ra mạnh mẽ trên thế giới. ISDN cải thiện hiệu năng vận hành so với phương pháp truy nhập mạng WAN qua đường quay số và có chi phí thấp hơn so với Frame Relay.
- ISDN định ra các tiêu chuẩn cho việc sử dụng đường dây điện thoại tương tự cho cả việc truyền dữ liệu số cũng như truyền dữ liệu tương tự. Các đặc điểm của ISDN là:
- Cho phép phát quảng bá nhiều kiểu dữ liệu (thoại, video, đồ hoạ...)
- Tốc độ truyền dữ liệu và tốc độ kết nối cao hơn so với kết nối quay số truyền thống

ATM

- ATM (Asynchronous Transfer Mode – Chế độ truyền không đồng bộ) là hệ thống chuyển mạch gói tiên tiến, có thể truyền đồng thời dữ liệu, âm thanh và hình ảnh số hoá trên cả mạng LAN và mạng WAN.
- Đây là một trong những phương pháp kết nối mạng WAN nhanh nhất hiện nay, tốc độ đạt từ 155 Mbit/s đến 622 Mbit/s. Trên thực tế, theo lý thuyết nó có thể hỗ trợ tốc độ cao hơn khả năng hiện thời của các phương tiện truyền dẫn hiện nay. Tuy nhiên, tốc độ cao có nghĩa là chi phí cũng cao hơn, ATM đắt hơn nhiều so với ISDN, X25 hoặc FrameRelay. Các đặc trưng của ATM bao gồm:
- Sử dụng gói dữ liệu (cell) nhỏ, có kích thước cố định (53 byte), dễ xử lý hơn so với các gói dữ liệu có kích thước thay đổi trong X.25 và Frame Relay.
- Tốc độ truyền dữ liệu cao, theo lý thuyết có thể đạt 1,2 Gbit/s
- Chất lượng cao, độ nhiễu thấp nên gần như không cần đến việc kiểm tra lỗi
- Có thể sử dụng với nhiều phương tiện truyền dẫn vật lý khác nhau (cáp đồng trục, cáp dây xoắn, cáp sợi quang)
- Có thể truyền đồng thời nhiều loại dữ liệu

Phần cứng mạng WAN

- Phần cứng mạng WAN bạn sử dụng phụ thuộc vào dịch vụ mạng WAN bạn muốn kết nối tới. Mỗi giao thức mạng WAN có các đặc tả và yêu cầu khác nhau đối với phần cứng và phương tiện truyền dẫn. Tuy nhiên, với sự lựa chọn của bạn, có nhiều phần cứng có thể tương thích với nhiều dịch vụ mạng WAN khác nhau.
- Nhà cung cấp dịch vụ mạng WAN là người chịu trách nhiệm về mạng WAN và cung cấp Cáp nối chặng cuối (local loop) tới Điểm ranh giới (Demarc) (xem Internet thật là đơn giản số 2/2004). Cáp nối chặng cuối thường là dây cáp đồng, cùng một loại dây sử dụng cho dịch vụ điện thoại.

Thiết lập đường dây điện thoại

- Nhiều hộ gia đình và doanh nghiệp hiện nay sử dụng cáp 4 dây gồm 2 cặp dây xoắn đồng: cặp thứ nhất sử dụng cho điện thoại và cặp thứ hai làm dự phòng. Điều này cho phép các doanh nghiệp mới có thể sẵn sàng kết nối mạng WAN mà không cần phải lắp đặt thêm hệ thống đường dây mới. Một đường tín hiệu tương tự sử dụng hai dây đồng và một đường tín hiệu số có thể sử dụng hai dây hay cả 4 dây đồng của Cáp nối chặng cuối tuỳ thuộc vào loại hình kết nối mạng WAN. Các công ty điện thoại cần phải sửa đổi bộ chuyển mạch đường truyền (line switching) ở Văn phòng trung tâm để có thể truyền tín hiệu số trên Cáp nối chặng cuối.
- Dây dẫn đồng được phân loại theo băng thông. Băng thông, đến lượt nó, lại quyết định lượng dữ liệu bạn có thể gửi và tín hiệu truyền là tương tự hay tín hiệu số. Dưới đây chúng ta sẽ nghiên cứu về hai phương pháp phân loại băng thông trên cáp đồng.

Plain Old Telephone Service (POTS)

- Hệ thống điện thoại tương tự chỉ gửi một tín hiệu tương tự trên mỗi cặp dây: mỗi tín hiệu riêng biệt này được coi là một kênh. Sử dụng POTS và modem để gửi tín hiệu tương tự cung cấp cho bạn một kênh 64Kbit/s, trong đó chỉ 56Kbit/s băng thông dành cho truyền dữ liệu. Modem và đường dây điện thoại truyền thống khá phù hợp cho mục đích sử dụng Internet để gửi thư điện tử và một số công việc thông thường khác. Tuy nhiên, nếu cần gửi và nhận một khối lượng dữ liệu lớn thì sẽ mất khá nhiều thời gian.

Dịch vụ POTS có những đặc điểm sau đây:

- Các đường dây hiện thời chỉ sử dụng hai cặp dây xoắn
- Tín hiệu trên Cáp nối chặng cuối là tín hiệu tương tự.
- Cần tới modem để chuyển tín hiệu số thành tín hiệu tương tự
- Tốc độ hiệu quả của đường dây bị giới hạn ở ngưỡng 56 Kbit/s

T-Carries

- Lớp vật lý của nhiều hệ thống mạng WAN ở Mỹ dựa trên công nghệ T-Carrier do công ty Bell/AT&T phát triển. Các đường dây T-1 sử dụng cả 4 dây đồng: một cặp để gửi và một cặp để nhận dữ liệu. Chúng không sử dụng đường dây vật lý bổ sung (additional wire) mà thiết lập các kênh ảo (virtual channel). Cáp sợi quang và các loại đường truyền khác sử dụng cho Cáp nối chặng cuối cho phép tốc độ truyền dữ liệu đạt cao hơn.
- Công nghệ T-carries có các đặc điểm sau đây:
- Sử dụng hai cặp cáp dây xoắn đồng
- Sử dụng tín hiệu số
- Hỗ trợ nhiều kênh 64 Kbit/s trên một dây
- Các đường dây T-carrier được phân loại dựa trên số kênh mà nó có thể hỗ trợ
- T1 (24 kênh, sử dụng ở Mỹ)
- E1 (31 kênh, sử dụng ở châu Âu)
- Các đường T-carrier cũng được phân theo loại dữ liệu sẽ được truyền tải trên đường dây (ví dụ dữ liệu thuần tuý, âm thanh số hoá, hình ảnh số hoá...). Hơn nữa, người sử dụng

có thể đăng ký một phần dịch vụ của đường T1 và sử dụng một số trong số các kênh sẵn có của nó.

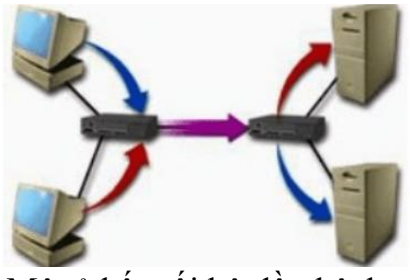
- Lưu ý: Các loại đường T-carrier được phân ra nhằm mục đích miêu tả băng thông, đây không phải là các giao thức mạng WAN. Ví dụ, ISDN là một dịch vụ mạng WAN sử dụng phương pháp truyền tín hiệu số qua 4 dây. Băng thông của ISDN phụ thuộc vào bao nhiêu dung lượng của đường T1 được sử dụng.

Basic Rate ISDN (BRI)

- Basic Rate ISDN gồm 2 kênh 64Kbit/s (gọi là các kênh B) và một kênh 16 Kbit/s (gọi là kênh D). Vì vậy nó còn được gọi là 2B+D. Các kênh B truyền tải dữ liệu, âm thanh và hình ảnh số hoá. Kênh D là kênh dịch vụ sử dụng cho cả dữ liệu và thông tin điều khiển. ISDN BRI rất hợp lý cho các hộ gia đình và doanh nghiệp nhỏ cần tốc độ truyền dữ liệu cao hơn so với modem truyền thống.
- Dưới đây là 2 trường hợp sử dụng ISDN BRI điển hình nhất:
- Một kênh B được dùng cho thoại, kênh kia được dùng cho dữ liệu
- Cả hai kênh được dùng cho truyền dữ liệu với tốc độ tổng cộng là 128 Kbit/s
- Lưu ý: Băng thông tổng cộng của ISDN BRI là 144 Kbit/s (2 kênh B và 1 kênh D) trong khi [/i]tốc độ truyền dữ liệu tổng cộng là 128 Kbit/s (dữ liệu chỉ được gửi qua 2 kênh B)
- Primary Rate ISDN(PRI)
- Tại Mỹ, Primary Rate ISDN sử dụng toàn bộ đường T1, hỗ trợ 23 kênh B 64 Kbit/s và một kênh D 64 Kbit/s, vì vậy nó được gọi là 23B+D. ISDN PRI sử dụng trong các doanh nghiệp yêu cầu kết nối tốc độ cao, thường xuyên bật.
- Tại châu Âu, Primary Rate thường được gọi là 30B+D bởi vì nó sử dụng toàn bộ đường E-1 để hỗ trợ 30 kênh B và 1 kênh D1.
- Ngoài đường truyền, bạn cần phần cứng để kết nối tới mạng WAN và định dạng chính xác tín hiệu cho loại hình kết nối bạn sử dụng. Ví dụ, phần cứng có thể là những modem chuyển tín hiệu số sang tín hiệu tương tự. Bạn sẽ sử dụng một hoặc hai loại thiết bị phần cứng dưới đây cho các mạng số hoàn toàn.

Multiplexer (Bộ dồn kênh)

- Như hình 4.55 dưới đây, bộ dồn kênh hoạt động tại hai đầu của đường truyền. Tại đầu gửi tín hiệu, bộ dồn kênh là thiết bị kết hợp tín hiệu từ hai hay nhiều thiết bị khác để truyền trên một đường truyền. Tại đầu nhận, một bộ dồn kênh với chức năng giải kênh sẽ tách tín hiệu kết hợp thành tín hiệu riêng rẽ như ban đầu. Nhiều bộ định tuyến trên mạng WAN có tích hợp sẵn các bộ dồn kênh.



Hình 4.55 Mô tả kết nối bộ dồn kênh trong WAN

- Bộ dồn kênh thống kê (Statistical multiplexer): Sử dụng các kênh ảo riêng biệt trên cùng một đường truyền vật lý để gửi đồng thời những tín hiệu khác nhau. (các tín hiệu được chuyển cùng một lúc trên đường truyền).
- Bộ dồn kênh phân chia theo thời gian (Time-division multiplexer): Gửi các gói dữ liệu của các tín hiệu khác nhau ở những khoảng thời gian khác nhau. Thay vì chia đường truyền vật lý thành các kênh, nó cho phép các dòng dữ liệu sử dụng đường truyền ở những

“khe” thời gian xác định (các tín hiệu lần lượt được sử dụng đường truyền trong những khoảng thời gian ngắn).

CSU/DSU (Chanel Service Unit/Data Service Unit)

- Đây là thiết bị kết nối các mạng với đường truyền tốc độ cao như T-1. Thiết bị này định dạng các dòng dữ liệu thành các khuôn dạng khung (framing) và xác định mã đường truyền cho các đường truyền số. Một số CSU/DSU còn là các bộ dồn kênh, hoặc được tích hợp sẵn trong các bộ định tuyến. Bạn cũng có thể nghe nói về CSU/DSU là một dạng modem số nhưng điều này không hoàn toàn chính xác. Modem chuyển dữ liệu từ dạng tương tự sang dạng số và ngược lại trong khi đó CSU/DSU chỉ định dạng lại các dữ liệu từ dạng số đã có.
- CSU nhận tín hiệu và truyền tín hiệu nhận được tới đường dây mạng WAN, phản xạ tín hiệu trả lời khi các công ty điện thoại cần kiểm tra thiết bị và ngăn nhiễu điện từ.
- DSU tương tự như một modem giữa DTE và CSU. Nó chuyển các khung dữ liệu từ định dạng sử dụng trong mạng LAN thành định dạng sử dụng trên đường T-1 và ngược lại. Nó còn quản lý đường dây, lỗi phân chia thời gian và tái tạo tín hiệu.

Các giao thức giao diện

- Có các loại giao thức “giao diện” khác nhau cho kết nối mạng WAN. “Giao diện”, trong ngữ cảnh này, liên quan tới định dạng của các khung tầng vật lý hoặc các phương pháp xác lập tín hiệu bit (định dạng các xung điện từ).

Các giao thức nối tiếp đồng bộ (Synchronous Serial Protocols)

- Các giao thức nối tiếp đồng bộ sử dụng tín hiệu đồng hồ chính xác giữa DCE và DTE để truyền dữ liệu theo thời gian. Trong truyền thông đồng bộ, một số lượng lớn khung dữ liệu được gửi đi khi đồng hồ đồng bộ và tốc độ truyền dữ liệu được xác lập từ trước. Đây là phương pháp truyền thông sử dụng băng thông rất hiệu quả.
- Các giao thức truyền tín hiệu đồng bộ bao gồm:
  + V.35
  + RS -232 (EAI/TIA)
  + X.21
  + RS-449
  + RS-530
- Mặc dù mỗi giao thức “giao diện” sử dụng một loại bộ kết nối riêng, phần lớn các bộ kết nối có thể được sử dụng cho nhiều giao diện khác nhau. Thông thường, loại phần cứng bạn có sẽ quyết định bộ kết nối nào được sử dụng. Trong thực tế, hãy kiểm tra số đầu cắm trong bộ kết nối để chắc chắn nó phù hợp với cổng nối tiếp của thiết bị. Những loại bộ kết nối phổ biến gồm (các số thể hiện số chân cắm trong bộ kết nối): DB60, DB25, DB15, DB9.

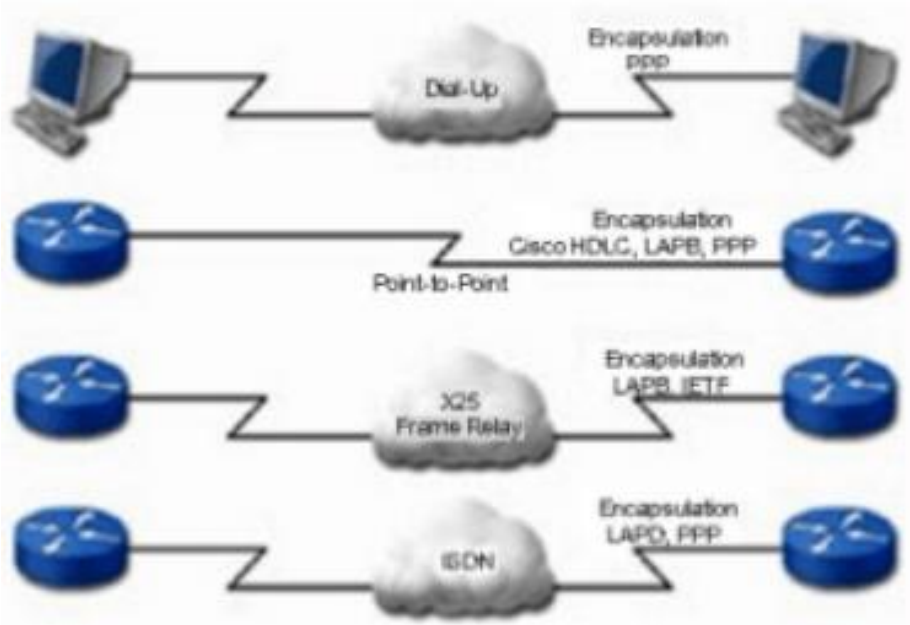
Các giao thức không đồng bộ (Asynchronous Protocol)

- Các giao thức truyền không đồng bộ sẽ đưa thêm các bít bắt đầu (start bit) và bit kết thúc (stop bit) vào mỗi gói tin để truyền thin, thay vì bắt buộc thiết bị gửi và thiết bị nhận sử dụng thoả thuận trước về nhịp đồng hồ. Truyền tín hiệu không đồng bộ thường được sử dụng giữa 2 modem. Tuy nhiên, đây là phương pháp truyền có phụ phí vì các bit phụ thêm sẽ làm chậm tốc độ truyền dữ liệu.
- Các giao thức không đồng bộ được sử dụng để thiết lập chuẩn cho truyền thông của các modem tương tự. Một modem bạn mua về có thể hỗ trợ một hoặc nhiều chuẩn truyền thông không đồng bộ khác nhau. Các giao thức truyền thông không đồng bộ bao gồm: V.92, V.45, V.35, V.34, V.32, V.32 bis, V.32 turbo, V.22.
- Truyền tín hiệu không đồng bộ sử dụng đường dây điện thoại và jack cắm chuẩn. Các bộ kết nối có thể là: RJ-11 (2 dây), RJ-45 (4 dây), RJ-48.

Hình 4.56 truyền dữ liệu đồng bộ (bên trái) và không đồng bộ (bên phải)

Các phương pháp đóng gói dữ liệu trong mạng WAN

- Các giao thức lớp vật lý của mạng WAN sẽ xác định phần cứng và phương pháp truyền tín hiệu bit. Các giao thức thuộc lớp liên kết dữ liệu sẽ kiểm soát những chức năng sau:
  + Kiểm tra và sửa lỗi
  + Thiết lập liên kết
  + Tổ chức các trường (field) của khung dữ liệu
  + Điều khiển luồng điểm tới điểm (point-to-point flow control)
- Các giao thức lớp liên kết vật lý còn xác định phương pháp đóng gói dữ liệu hoặc định dạng của khung dữ liệu. Phương pháp đóng gói dữ liệu trong mạng WAN thường được gọi là HDLC (high-level data link control - điều khiển liên kết dữ liệu mức cao). Thuật ngữ này vừa là tên chung cho các giao thức Liên kết Dữ liệu vừa là tên của một giao thức trong bộ giao thức và dịch vụ mạng WAN. Tuỳ thuộc vào dịch vụ mạng WAN và phương pháp kết nối, bạn có thể sử dụng một trong những phương pháp đóng gói dữ liệu sau đây:
  + Cisco HDLC cho kết nối đồng bộ, điểm tới điểm với các bộ định tuyến Cisco khác.
  + LAPB cho mạng X.25
  + LAPD, sử dụng kết hợp với các giao thức khác cho các kênh B trong mạng ISDN.
  + Cisco/IETF cho các mạng Frame Relay



Hình 4.57 Các phương pháp đóng gói dữ liệu trong mạng WAN

- Hình trên cho chúng ta thấy những phương pháp đóng gói dữ liệu thông thường nhất và cách thức sử dụng cho các loại kết nối mạng WAN điển hình. Như có thể thấy trong hình vẽ, PPP là phương pháp linh hoạt có thể sử dụng cho nhiều loại kết nối mạng WAN.

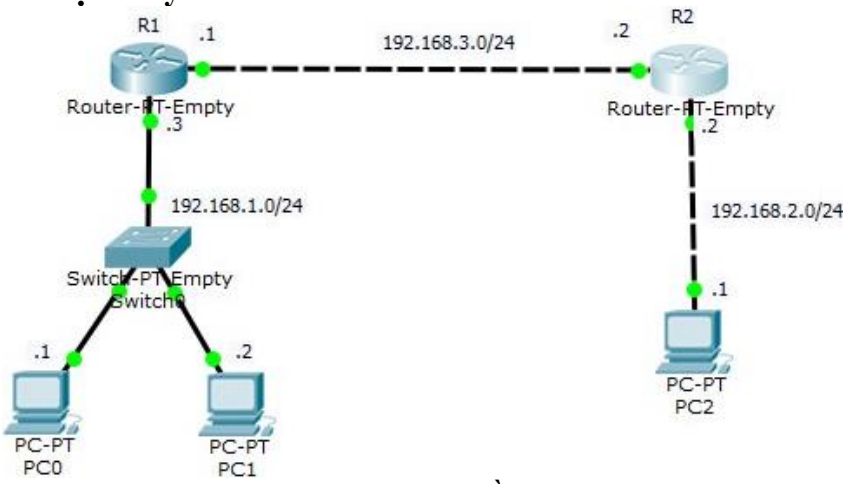
Nói chung, sử dụng phương pháp nào sẽ phụ thuộc vào loại của dịch vụ mạng WAN, chẳng hạn Frame Relay hay ISDN, và cả phương pháp đóng gói dữ liệu của nhà cung cấp dịch vụ mạng.

2.12 Cấu hình định tuyến tĩnh

- Định tuyến tĩnh là quá trình router thực hiện chuyển gói dữ liệu tới địa chỉ mạng đích dựa vào địa chỉ IP đích của gói dữ liệu. Để chuyển được gói dữ liệu đến đúng đích thì router phải học thông tin về đường đi tới các mạng khác. Thông tin về đường đi tới các mạng khác sẽ được người quản trị cấu hình cho router. Khi cấu trúc mạng thay đổi, người quản trị mạng phải tự thay đổi bảng định tuyến của router.
- Kỹ thuật định tuyến tĩnh đơn giản, dễ thực hiện, ít hao tốn tài nguyên mạng và CPU xử lý trên router (do không phải trao đổi thông tin định tuyến và không phải tính toán định tuyến). Tuy nhiên kỹ thuật này không hội tụ với các thay đổi diễn ra trên mạng và không thích hợp với những mạng có quy mô lớn (khi đó số lượng route quá lớn, không thể khai báo bằng tay được).

- Ưu điểm:
  + Sử dụng ít bandwidth hơn định tuyến động.
  + Không tiêu tốn tài nguyên để tính toán và phân tích gói tin định tuyến.
- Nhược điểm:
  + Không có khả năng tự động cập nhật đường đi.
  + Phải cấu hình thủ công khi mạng có sự thay đổi.
  + Phù hợp với mạng nhỏ, rất khó triển khai trên mạng lớn.
- Một số tình huống bắt buộc dùng định tuyến tĩnh:
  + Đường truyền có băng thông thấp
  + Người quản trị mạng cần kiểm soát các kết nối.
  + Kết nối dùng định tuyến tĩnh là đường dự phòng cho đường kết nối dùng giao thức định tuyến động.
  + Chỉ có một đường duy nhất đi ra mạng bên ngoài (mạng stub).
  + Router có ít tài nguyên và không thể chạy một giao thức định tuyến động.
  + Người quản trị mạng cần kiểm soát bảng định tuyến và cho phép các giao thức classful và classless.

2.12.1. Cấu hình định tuyến tĩnh



Hình 4.58 Sơ đồ ví dụ

- Hình trên là hai router, R1 sử dụng cổng f0/0 đấu xuống mạng LAN có subnet 192.168.1.0/24. Tương tự, R2 sử dụng cổng f0/0 đấu xuống PC có subnet 192.168.2.0/24. Subnet sử dụng cho kết nối leased-line nối giữa hai router là 192.168.3.0/24. Đầu tiên, chúng ta phải cấu hình đặt địa chỉ IP cho các cổng của router, cũng như IP và Default-

gateway cho các PC. Default-gateway hiểu đơn giản là IP của cổng của router gần nhất mà PC đó kết nối trực tiếp đến.

- Cấu hình định tuyến tĩnh trên router Cisco được thực hiện bằng cách sử dụng lệnh có cú pháp như sau: Router (config) # ip route *destination_subnet subnetmask {IP_next_hop|output_*interface} [AD]
- Trong đó:
  + *destination_subnet:* mạng đích đến.
  + *subnetmask:* subnet – mask của mạng đích.
  + *IP_next_hop:* địa chỉ IP của trạm kế tiếp trên đường đi.
  + *output_interface:* cổng ra trên router.
  + *AD:* chỉ số AD của route khai báo, sử dụng trong trường hợp có cấu hình dự phòng.
- Trong ví dụ hình trên, từ R1 muốn đi đến mạng 192.168.2.0/24 thì phải đi ra khỏi cổng f1/0. Để thể hiện điều đó vào bảng định tuyến phải thực hiện cấu hình:
  + *R1 (config) # ip route 192.168.2.0 255.255.255.0 f1/0*

hoặc

  + *R1 (config) # ip route 192.168.2.0 255.255.255.0 192.168.3.2*
  + R2 muốn đi đến mạng 192.168.1.0/24 thì phải đi ra khỏi cổng f1/0:
  + *R2 (config) # ip route 192.168.1.0 255.255.255.0 f1/0*

hoặc

  + *R2 (config) # ip route 192.168.1.0 255.255.255.0 192.168.3.1*
- Sau khi đã cấu hình xong các route cho các mạng 192.168.1.0/24 và 192.168.2.0/24, kiểm tra bảng định tuyến trên mỗi router: Bảng định tuyến của R1:
  + *R1#show ip route*
  + *C 192.168.1.0/24 is directly connected, FastEthernet0/0*
  + *S 192.168.2.0/24 [1/0] via 192.168.3.2*
  + *C 192.168.3.0/24 is directly connected, FastEthernet1/0*

Bảng định tuyến của R2:

  + *R2#show ip route*
  + *S 192.168.1.0/24 [1/0] via 192.168.3.1*
  + *C 192.168.2.0/24 is directly connected, FastEthernet0/0*
  + *C 192.168.3.0/24 is directly connected, FastEthernet1/0*
- Kí tự "S" ở đầu dòng thể hiện rằng các thông tin định tuyến này được học vào bảng định tuyến thông qua định tuyến tĩnh và các dòng mô tả các mạng kết nối trực tiếp được ký hiệu bởi kí tự "C" – connected – kết nối trực tiếp.

2.12.2 Default route

- Được dùng để định tuyến mặc định tất cả dữ liệu đến một mạng bất kỳ đi theo đường nào đó. Nhưng nếu mạng đó đã có đường đi trong bảng định tuyến, thì gói tin sẽ ưu tiên đi theo đường đi rõ ràng trước.
- *Router (config) # ip route 0.0.0.0 0.0.0.0 {ip next-hop | exit interface}*

2.13 Cấu hình RIP

- **RIP** là giao thức định tuyến Vector khoảng cách lâu đời nhất, mặc dù cách hoạt động chưa tối ưu nhưng RIP được cấu hình 1 cách đơn giản và phổ biến.
- Bộ định tuyến duy trì một bảng định tuyến (vector) cung cấp khoảng cách tốt nhất được biết đến mỗi đích (thường là bộ định tuyến). Thông tin của bảng này thường xuyên được cập nhật bằng cách trao đổi thông tin với các bộ định tuyến lân cận.
- **C**ó thể là bước nhảy, thời gian trễ đo bằng ms, Thông thường sử dụng thời gian trễ.
- RIP có 2 phiên bản: RIPv1 và RIPv2

Giải thuật Định tuyến theo vector khoảng cách (RIP)

[1] Bộ định tuyến tính khoảng cách từ nó đến các bộ định tuyến lân cận bằng cách gửi gói tin ECHO.

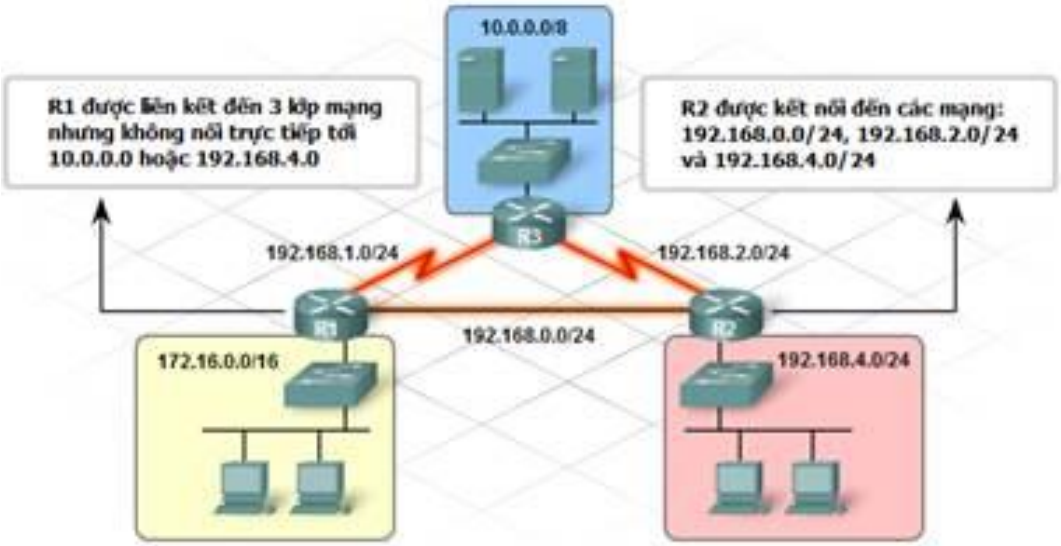
[2] Cứ sau T ms mỗi bộ định tuyến lại truyền đến bộ định tuyến lân cận một danh sách các khoảng cách ước lượng cho mỗi đích và nó cũng nhận từ các bộ lân cận khác.

[3] Cập nhật bảng định tuyến với khoảng cách tốt nhất.

Đặc điểm RIPv1

- Rip là gia thức định tuyến Vector khoảng cách
- Rip sử dụng Hop Count để lựa chọn đường đi
- Quảng bá tuyến đường đi với số Hop Count lớn hơn 15 là không truy cập được
- Thông điệp được broadcast mỗi 30 giây
- Giới hạn của RIPv1
- Các giao thức định tuyến classful không bao gồm mặt nạ mạng con với địa chỉ mạng trong quá trình cập nhật bảng định tuyến
- Khi đó có thể gây ra vấn đề với mạng con bị phân chia hoặc các mạng có sử dụng Variable-Length Subnetmask

⇨ RIPv2

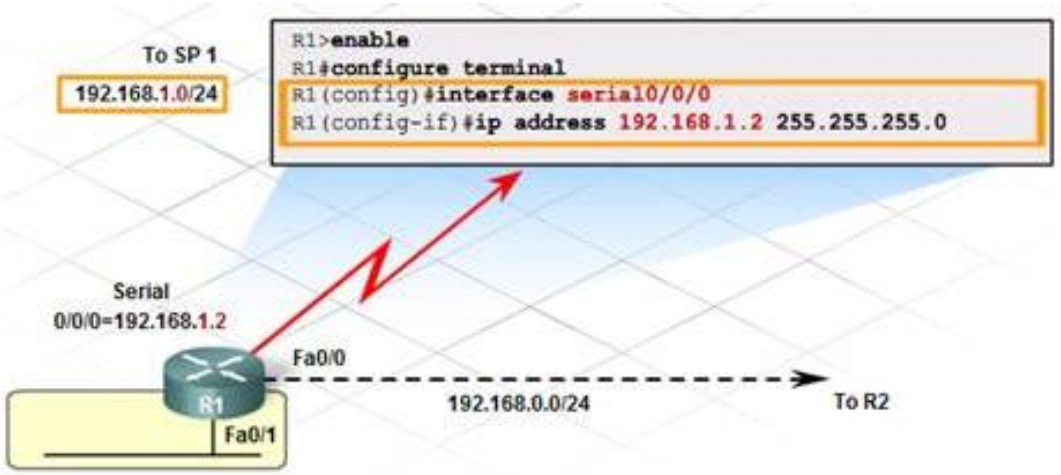


Hình 4.59 Mô hình RIP

Thực hiện theo yêu cầu sau:

- Cấu hình sao cho các mạng giao tiếp được với nhau với giao thức RIPv1/v2

Cấu hình định tuyến trên R1:

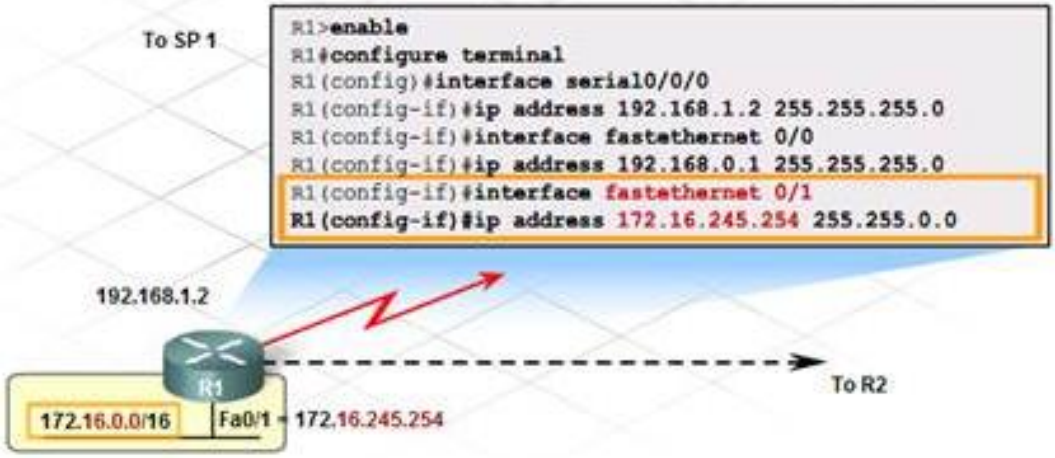


Hình 4.60 Cấu hình mô hình RIP

- Bước 1: Cấu hình địa chỉ serial interface nối với router R3
- Bước 2: Cấu hình địa chỉ IP cho fastethernet 0/0 interface

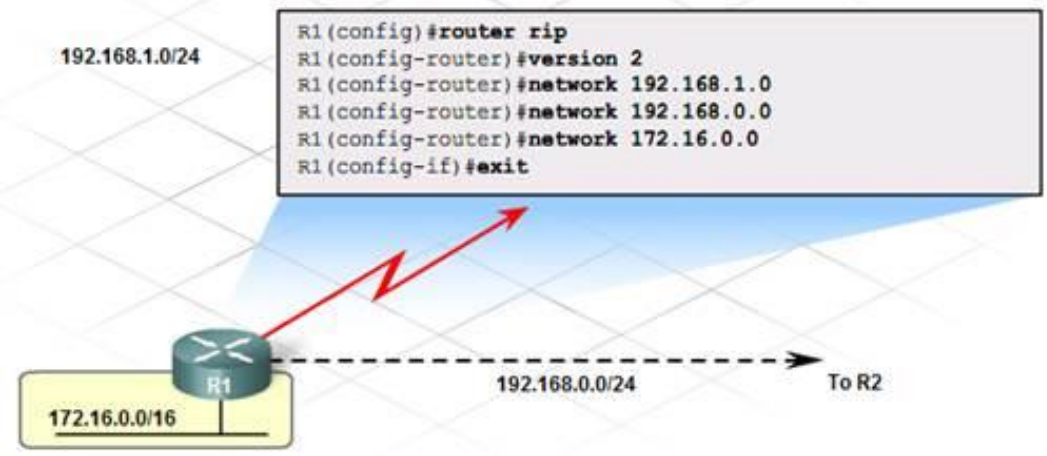
Hình 4.61 Cấu hình mô hình RIP

- Bước 3: Cấu hình địa chỉ IP fastethernet 0/1 interface



Hình 4.62 Cấu hình mô hình RIP

- Bước 4: Cấu hình RIP



Hình 4.63 Cấu hình mô hình RIP

Cấu hình tương tự trên các Router R2, R3:

2.14 Quản lý thiết bị Cisco

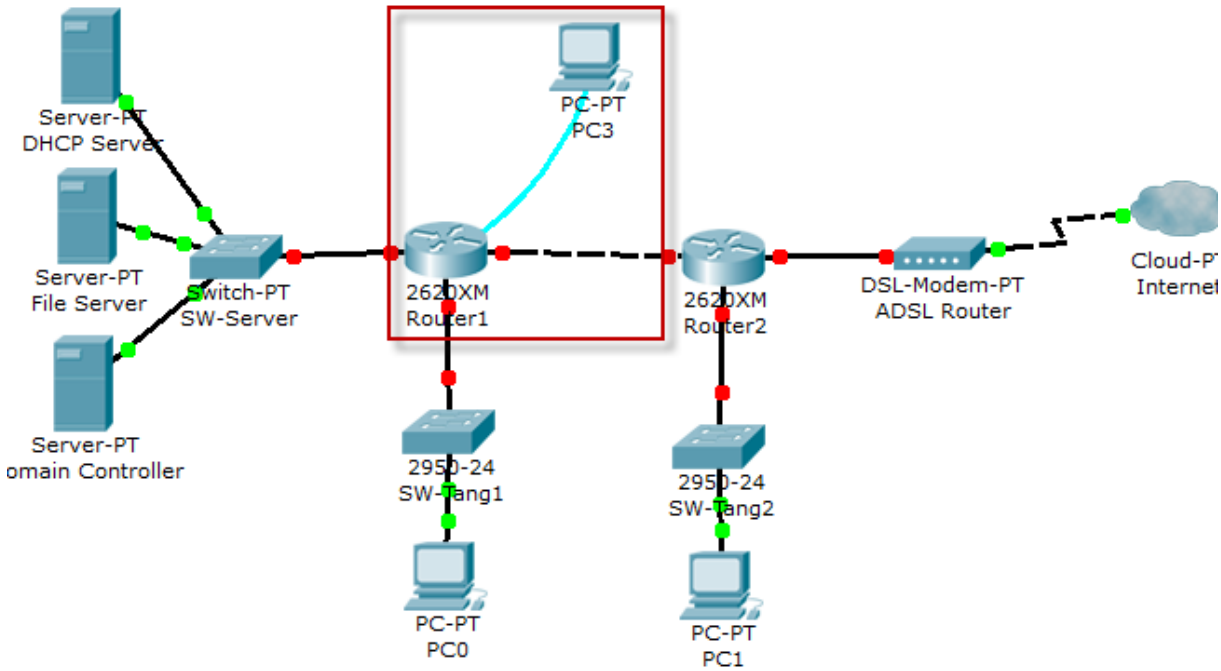
Hệ thống quản lý thiết bị định tuyến Cisco 12000/10720 cung cấp tính năng quản lý phần tử mạng ở cấp độ nhà khai thác cho các triển khai Giao thức IP và MPLS của thiết bị định tuyến dòng Cisco 12000 và Cisco 10720. Là một thành viên của họ sản phẩm hệ quản lý phần tử mạng của Cisco, Quản lý thiết bị định tuyến Cisco 12000/10720 cung cấp khả

năng quản lý lỗi, cấu hình, kế toán, hiệu năng và an ninh (FCAPS) đặc thù thiết bị cho các sản phẩm của Cisco. Nó còn bao gồm các tính năng vận hành và quản lý để xử lý các sự cố của mạng truyền tải MPLS.

Hệ quản lý thiết bị định tuyến Cisco 12000/10720 là phần mềm quản lý phần tử mạng ở cấp độ nhà cung cấp dựa trên giao diện GUI giúp tăng năng suất vận hành mạng. Với khả năng nhận dạng thiết bị thời gian thực, phần mềm giúp triển khai các thiết bị kết nối mạng của Cisco nhanh chóng hơn và cung cấp dịch vụ phần tử đầy đủ để giải quyết nhanh các vấn đề mạng.

Câu hỏi ôn tập

- Cài đặt cấu hình định tuyến tĩnh trên các Router Cisco sau:



Yêu cầu như sau:

1. Chuẩn bị sơ đồ mạng
2. Cấu hình các thông số cơ bản cho router
   + Cấu hình hostname cho router
   + Tắt cơ chế phân giải tên miền của router
   + Cấu hình các password cho router
   + Enable password: ccna
   + Enable secret: ccnp
   + Console password: cisco
   + Telnet password: telnet
3. Cấu hình địa chỉ IP cho các thiết bị như bảng mô tả địa chỉ bên trên
4. Kiểm tra cấu hình ban đầu
5. Test kết nối
6. Cấu hình static routing cho các đường mạng trong sơ đồ thông nhau
7. Cấu hình static default route để cho các máy trong mạng Lan có thể ra internet. Giả sử trên router R3 có một kết nối ra internet tại cổng fastethernet0/1.
8. Cấu hình static summary route

BÀI 5. CƠ SỞ VỀ BỘ CHUYỂN MẠCH

Giới thiệu:

Switch là một thiết bị **chuyển mạch** tối quan trọng trong mạng, dùng để kết nối các đoạn mạng với nhau theo mô hình hình sao (Star). Trong mô hình này, switch đóng vai trò trung tâm và tất cả các thiết bị vệ tinh khác kể cả máy tính đều được kết nối **về** đây, từ đó định tuyến tạo đường nối tạm trung **chuyển** dữ liệu đi

1. Mục tiêu của bài

- Khởi động được với một Cisco IOS switch;
- Nhận dạng được các đèn trên switch phản ánh điền kiện làm việc của switch;
- Mô tả được các kết qủa hiển thị của quá trình khởi độngtrên switch;
- Đăng nhập được vào Cisco IOS switch;
- Cấu hình được switch từ dòng lệnh;
- Kiểm định được hoạt động ban đầu của switch;
- Quản lý được bảng MAC bằng các lệnh Show tương ứng;

2. Nội dung bài

2.1 Khởi động Catalyst Switch

Switch cisco là thiết bị không thể thiếu trong mỗi hạ tầng mạng của công ty và doanh nghiệp, việc lắp đặt thiết bị và cấu hình chúng yêu cầu những thợ kỹ thuật am hiểu và có trình độ. Và để nắm rõ được trình tự hoạt động của các thiết bị chuyên mạch này là điều tối thiểu cần có ở người kỹ sư lắp đặt và quản lý mạng.

Trong giáo trình này sẽ giới thiệu sơ lược quy trình **các bước khởi động Switch** và hoạt động của thiết bị, mời bạn đọc cùng tham khảo.

Khởi động switch cisco nhanh chóng và chính xác nhất

Dưới đây chúng tôi sẽ chia sẻ đến các bạn **cách thức khởi động lại Switch** đơn giản hơn bao giờ hết.

- **Bước 1:** Bước đầu tiên switch sẽ tự động tải một chương trình tự kiểm tra (POST) được lưu trữ trong ROM. POST sẽ kiểm tra trình tự các hệ thống con CPU, DRAM, và phần cứng của thiết bị Flash tạo nên hệ thống các tệp flash.
- **Bước 2:** Bước tiếu theo, Switch sẽ tải tiếp nên phần mềm trình nạp khởi động, trình này là một chương trình cũng được lưu trữ trong ROM và sẽ tự động chạy ngay khi POST chạy thành công
- **Bước 3:** Switch Cisco sẽ bắt đầu khởi động CPU cấp thấp, nó khởi tạo các thanh ghi CPU kiểm soát nơi bộ nhớ vật lý được ánh xạ, số lượng của bộ nhớ và tốc độ của nó.
- **Bước 4:** Tới bước này Switch sẽ khởi tạp hệ thống tệp flash trên bảng hiển thị hệ thống.
- **Bước 5:** Định vị và tải một đĩa ảnh phần mềm ở hệ điều hành IOS
- Khi đã tiến hành xong 2 bước kể trên thì thiết bị chuyển mạch sẽ tự động định vị đồng thời tải một đĩa ảnh phần mềm ở hệ điều hành IOS. Thông qua quy trình sau mà switch cisco có thể tìm thấy file Cisco IOS:

- Trong môi trường BOOT, thiết bị chuyển mạch sẽ tìm kiếm thông tin.
- Nếu nó không có sẵn, bắt buộc bạn phải tải và tìm kiếm tệp đầu tiên trong hệ thống tệp flash. Lúc này, hệ điều hành IOS sẽ tự động khởi tạo các giao diện sử dụng các lệnh của cisco switch.
- Như vậy, bạn đã có thể khởi tạo lại switch cisco nhanh chóng và chính xác.

Các bước khôi phục hệ thống khi gặp sự cố

Trình nạp quá trình khởi động cung cấp quyền truy cập vào chuyển đổi, nếu bạn không thể dụng hệ điều hành vì các tệp hệ thống đã bị lỗi hoặc mất thì hãy tham khảo quá trình khắc phục này. Bộ tải khởi động sẽ cung cấp một dòng lệnh giúp truy cập vào các tệp lưu trữ sẵn trong flash của thiết bị.

- **Bước 1**: Để kết nối với switch cisco, bạn kết nối cáp điều khiển từ máy tính đến cổng Console và phần mềm Terminal .
- **Bước 2**: Rút dây nguồn thiết bị, sau đó kết nối lại dây nguồn và công tắc. Bấm và giữ nút Mode trong khoảng từ 10 đến 15 giây khi mà đèn nhấp nháy tín hiệu màu xanh lá cây.
- **Bước 3**: Tiếp tục ấn và giữ nút Mode cho đến khi tín hiệu đèn chuyển từ màu hổ phách sang màu xanh lá cây.
- **Bước 4**: Trình điều khiển sẽ xuất hiện trong phần mềm mô phỏng ở đầu và cuối PC.

Bài viết trên đây đã giới thiệu sơ lược quy trình các bước khởi động và hoạt động của thiết bị Switch Cisco, hi vọng sẽ mang tới cho quý khách hàng những thông tin hữu ích.

2.2 Đo lường bằng đèn LED trên Switch Catalyst 2960

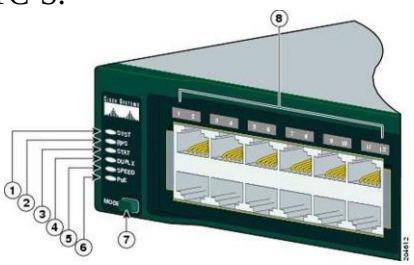
Đèn led báo trạng thái của dòng switch mạng cisco là một trong những thông tin quan trọng mà bắt buộc người quản lý thiết bị này phải hiểu và nắm rõ. Vậy có bao nhiêu thuật ngữ và chế độ đèn khác nhau, mời bạn đọc cùng tham khảo

Đèn LED trạng thái của Switch sẽ hiển thị cũng như thông báo tới người sử dụng rằng thiết bị đang hoạt động có ổn định không, đã kết nối đúng tiêu chuẩn chưa và khi nào cần nâng cấp hay bảo trì. Vì thế việc nắm rõ được các **quy tắc hiển thị đèn LED báo trạng thái** của dòng Switch chia cổng 2960 của Cisco là điều rất cần thiết đối với những ai đang sử dụng thiết bị.

Giáo trình này xin gửi tới các bạn đọc đang quan tâm tới thiết bị này một loạt các hướng dẫn hay thủ thuật để có thể nắm rõ từng khái niệm hiển thị đèn LED của Switch.

Khách hàng có thể quản lý thiết bị với hiệu suất tốt hơn, tất cả các đèn led hiển thị thông qua các ứng dụng quản lý GUI[3]. Trợ lý mạng cho nhiều nút chuyển và trình quản lý thiết bị cho một nút chuyển. Hướng dẫn cấu hình phần mềm chuyển đổi mô tả cách sử dụng CLI[4] để cấu hình và giám sát các chuyển mạch riêng lẻ và chuyển đổi các cụm. Chỉ có thiết bị chuyển mạch Catalyst 2960 PoE có đèn LED PoE.

Bốn thiết bị chuyển mạch Catalyst 2960 8 cổng và các mô hình này không có đầu nối RPS hoặc đèn LED RPS: Catalyst 2960-24-S, Catalyst2960-Plus 24TC-S, 2960-24TC-S, 2960-48TT-S, 2960 -Plus 48TC-S, 2960-48TC-S.



Hình 5.1 Đèn LED trên Switch Catalyst 2960

1. Đèn LED hệ thống	5.Đèn LED tốc độ
2. LED RPS	6.Đèn LED PoE
3.Đèn LED trạng thái	7.Nút điều chỉnh chế độ
4.Đèn LED kép	8.Đèn LED cổng

Lưu ý:Đèn LED PoE chỉ sáng ở trên công tắc Catalyst 2960 PoE.

Cách đọc trạng thái của đèn LED hệ thống (LED SYS)

Các Đèn LED hệ thống cho biết hệ thống có đang nhận nguồn và đang hoạt động bình thường không. Bảng kê dưới đây sẽ liệt kê các màu LED và ý nghĩa của chúng.

Màu đèn	**Trạng thái**
Tắt	Thiết bị đang tắt

[3] **Giao diện đồ họa người dùng** trong tiếng Anh gọi tắt là **GUI** (*Graphical User Interface*) là một thuật ngữ trong ngành công nghiệp máy tính

[4] **Giao diện dòng lệnh** (*Command-Line Interface* - **CLI**) là phương tiện tương tác với chương trình máy tính

Xanh lá	Thiết bị hoạt động bình thường
Hổ phách	Thiết bị có điện vào nhưng hoạt động không đúng cách

Cách đọc trạng thái của đèn LED RPS

Lưu ý: Thiết bị chuyển mạch Catalyst 2960 8 cổng, và Catalyst 2960-24-S, 2960-Plus 24TC-S, 2960+24TC-S, 2960-Plus 48TC-S, 2960-48TC-S và 2960-48TT-S công tắc không có đèn LED RPS.

Màu	Trạng thái RPS
Tắt	RPS bị tắt hoặc không được kết nối đúng cách.
Màu xanh lá	RPS được kết nối và sẵn sàng cung cấp điện dự phòng, nếu cần.
Xanh lục nhấp nháy	RPS được kết nối nhưng không khả dụng vì nó đang cấp nguồn cho thiết bị khác (dự phòng đã được cấp phát cho một thiết bị lân cận).
Hổ phách	RPS đang ở chế độ chờ hoặc trong tình trạng lỗi. Nhấn nút Chờ/ Hoạt động trên RPS và đèn LED sẽ chuyển sang màu xanh lục. Nếu không, quạt RPS có thể đã thất bại. Liên hệ với Cisco Systems.
Hổ phách nhấp nháy	Nguồn điện bên trong trong một công tắc không thành công, và RPS đang cấp nguồn cho công tắc (sự dư thừa đã được cấp cho thiết bị này).

Để biết thêm thông tin về Cisco RPS 2300 hoặc Cisco RPS 675, xem hướng dẫn cài đặt phần cứng liên quan cho hệ thống điện đó.

Cách đọc trạng thái của đèn LED cổng và chế độ

Các đèn LED cổng, như một nhóm hoặc riêng lẻ, hiển thị thông tin về công tắc và về các cổng riêng lẻ

LED chế độ được chọn	Chế độ cổng	Mô tả
STAT	Trạng thái cổng	Trạng thái cổng. Đây là chế độ mặc định
DUPLX	Chế độ song công cổng	Cổng chế độ song công: full duplex hoặc half duplex.
TỐC ĐỘ (1)	Tốc độ cổng	Tốc độ hoạt động của cổng: 10, 100 hoặc 1000 Mb / s.
PoE3 (2)	PoE cổng điện	Trạng thái PoE.

(1) Khi được cài đặt trong thiết bị chuyển mạch Catalyst 2960, mô-đun SFP 1000BASE-T có thể hoạt động ở mức 10, 100 hoặc 1000 Mb / s ở chế độ song công hoặc ở mức 10 hoặc 100 Mb / s ở chế độ bán song công.

(2) Đèn LED PoE chỉ ở trên công tắc Catalyst 2960 PoE.

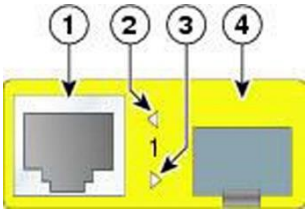
Ngay cả khi Chế độ PoE không được chọn, đèn LED PoE hiển thị các sự cố PoE khi chúng được phát hiện trong hình bên dưới. Đèn LED PoE chỉ áp dụng cho thiết bị chuyển mạch Catalyst 2960 hỗ trợ PoE.

Màu	Trạng thái PoE
Tắt	Chế độ PoE không được chọn. Không có cổng 10/100 PoE nào bị từ chối điện hoặc đang trong tình trạng lỗi.
Màu xanh lá	Chế độ PoE được chọn và trạng thái PoE được hiển thị trên đèn LED cổng.
Màu hổ phách nhấp nháy	Chế độ PoE không được chọn. Ít nhất một trong các cổng PoE 10/100 đã bị từ chối điện, hoặc ít nhất một trong các cổng có lỗi PoE.

Để chọn hoặc thay đổi một chế độ, hãy bấm phím Nút chế độ cho đến khi chế độ mong muốn được tô sáng. Khi bạnthay đổi chế độ cổng, ý nghĩa của màu sắc cổng LED cũng thay đổi. Bảng thông tin bên dưới giải thích cách diễn giải màu LED cổng ở các chế độ cổng khác nhau.

Cách đọc trạng thái của đèn 2 chế độ

Các đèn LED trên cổng hai mục đích cho biết đầu nối RJ-45 có được kết nối với cổng hay không hoặc nếu một mô-đun SFP được lắp vào khe. Xem ví dụ trong Hình 1-24 . Bạn có thể cấu hình mỗi cổng như mộtCổng 10/100/1000 thông qua đầu nối RJ-45 hoặc như một mô-đun SFP, nhưng không phải cả hai cùng một lúc. Các đèn LED hiển thị cách cổng được sử dụng (mô-đun Ethernet hoặc SFP).



Hình 5.2 Đèn LED trên Switch Catalyst 2960

1	Đầu nối RJ-45	3	Đèn LED sử dụng cổng mô-đun SFP
2	Cổng LED sử dụng trong RJ-45	4	Khe cắm mô-đun SFP

Trên đây là tổng hợp cách **cách đọc thông tin trạng thái đèn led** của switch mạng cisco dòng switch 2960 catalyst. Bạn đọc có thể dựa vào bảo hướng dẫn để đoán bệnh cũng như làm chủ thiết bị chuyển mạch của mình một cách tốt hơn. Bài viết được tổng hợp và việt hóa thông tin từ cisco.com độc quyền.

2.3 Cấu hình Switch cơ bản

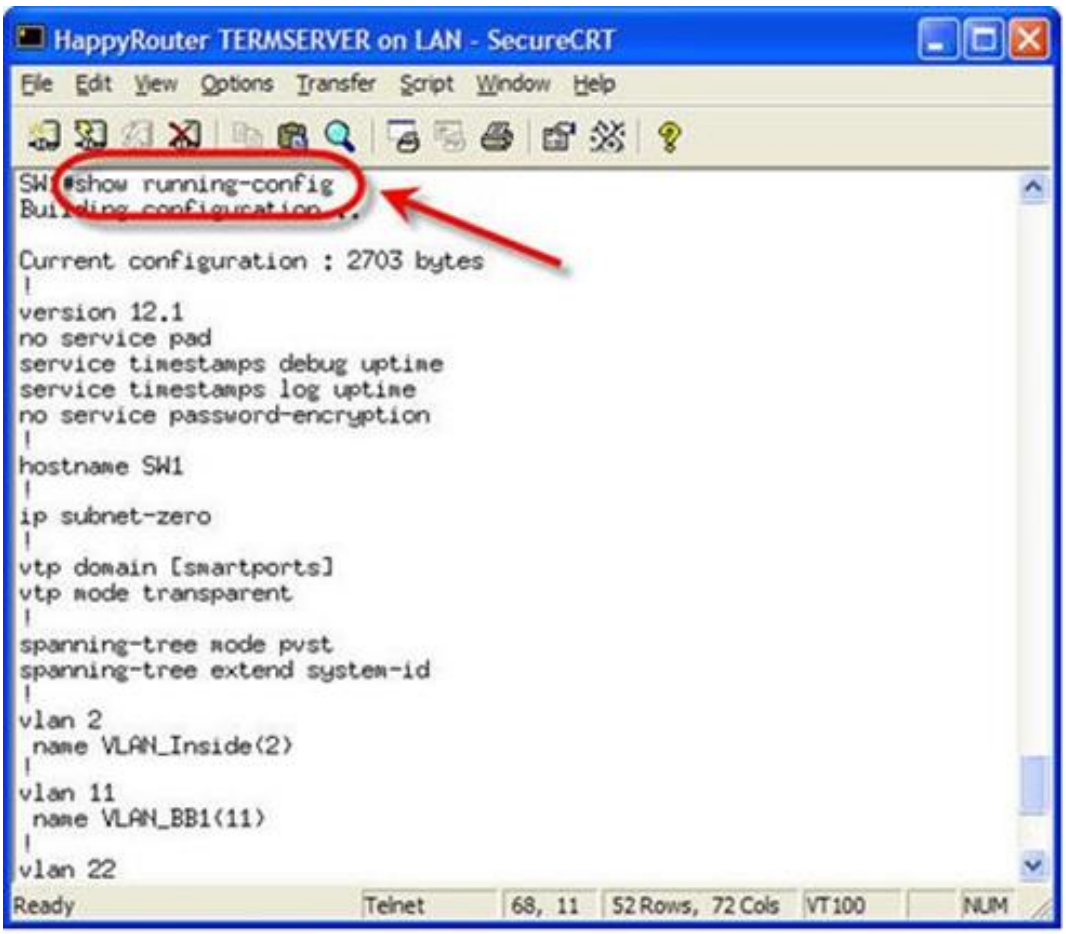
Switch chia mạng ngày nay không còn trở nên quá xa lạ với người sử dụng Việt Nam, đây là thiết bị được sử dụng rất nhiều ở các văn phòng, nhà xưởng, trường học đòi hỏi tính bảo mật cũng như sự ổn định trong hệ thống mạng LAN cũng như trong hệ thống mạng thông thường. Trên thị trường ngày nay, Switch chia mạng cũng vô cùng phong phú đến từ các thương hiệu khác nhau để người sử dụng có thể đa dạng hơn trong lựa chọn phù hợp với từng nhu cầu của bản thân. Trong đó Cisco là một trong những thương hiệu uy tín và chất lượng bậc nhất trong dòng sản phẩm này. Switch chia mạng Cisco luôn được kỹ thuật viên tin tưởng sử dụng và là sự lựa chọn số một trong các công trình mạng có yêu cầu về sự ổn định và tốc độ khắt khe.
Đôi khi, trong một số trường hợp, quý vị sẽ phải cấu hình một cổng switch hoặc tìm địa chỉ MAC trên mỗi cổng. Có thể, đây là công việc của kỹ thuật viên nhưng trong giáo trình này xin được chia sẻ những bước căn bản nhất trong việc quản trị Switch Cisco để giúp các bạn đọc có kiến thức tối thiểu để khắc phục một số vấn đề phát sinh có thể xảy ra.

Đăng nhập

- Trước khi quý vị có thể quản trị **Switch Cisco**, quý vị cần có một số thông tin cơ bản nhất như:
  + Cổng Ethernet của switch
  + Địa chỉ IP của switch gì? DNS là gì?
  + Tên đăng nhập và mật khẩu bạn có thể đăng nhập?
- Một cách khác để có thể cấu hình switch là cấu hình trực tiếp trên giao diện web. Cấu hình một cách cơ bản không khó và cũng không cần trợ giúp nhiều. Trong giao diện dòng lệnh CLI (command-line interface) ta có thể thực hiện bất kì kiểu cấu hình nào. Vì vậy, chúng ta nên sử dụng giao diện dòng lệnh IOS. Trong giáo trình này sẽ giúp các bạn thực hiện những bước cơ bản trong quản lý switch bằng Cisco IOS giao diện dòng lệnh (CLI) .

Hiển thị cấu hình switch

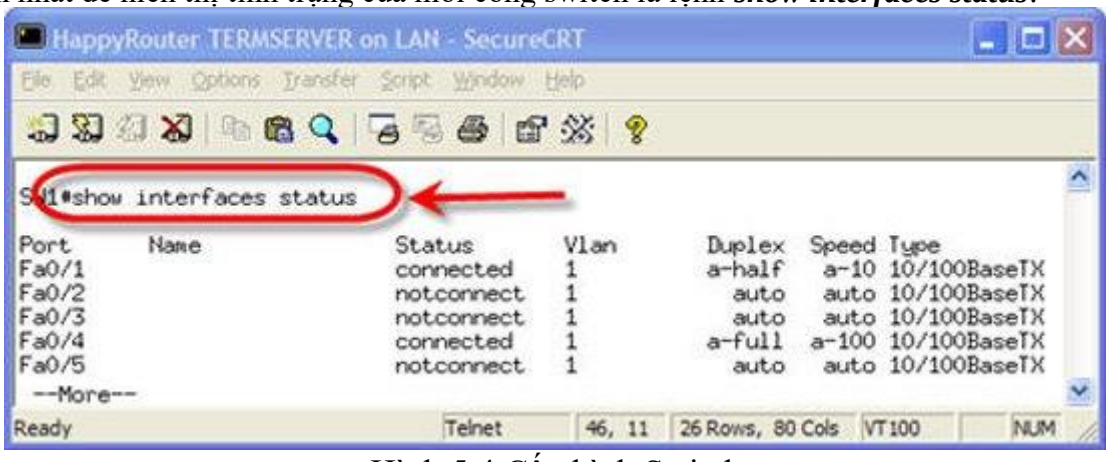
- Cũng giống như trên router, lệnh IOS được dùng để hiển thị cấu hình switch với tất cả những cổng Ethernet. Để biết được cấu hình switch, chỉ cần đánh ***show running-config*** như sau:



Hình 5.3 Cấu hình Switch

Hiển thị tình trạng các cổng của Sitch Cisco

Hầu như mỗi khi phải khắc phục sự cố cổng switch hoặc thay đổi cấu hình cổng switch, cách nhanh nhất để hiển thị tình trạng của mỗi cổng switch là lệnh ***show interfaces status***:

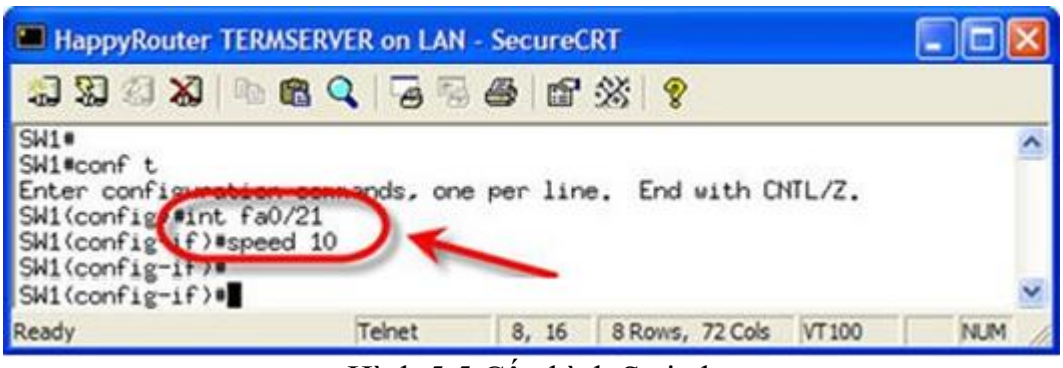


Hình 5.4 Cấu hình Switch

Lệnh này cho biết: nếu cổng kết nối với thiết bị, VLAN là IN, cùng với đó là hiển thị tốc độ, kiểu mẫu của cổng. Đây chính là cách nhanh và tốt nhất để có thể biết được tình trạng của từng trên cổng switch Cisco.

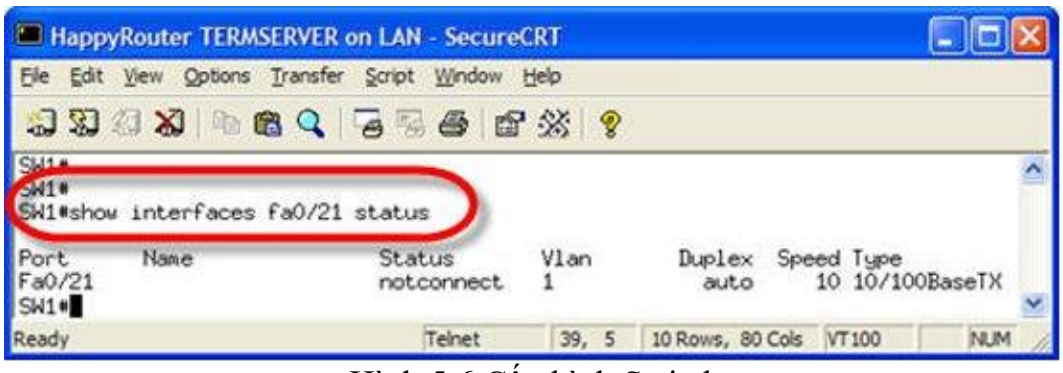
Thay đổi tốc độ và duplex của interface

Giao diện Fa0/21 với tốc độ được tự động đặt là auto. Tuy nhiên, tốc độ này cần phải được cài đặt là 10Mb/sec. Để thay đổi tốc độ của các cổng, bạn phải chuyển tới chế độ cấu hình interface và sử dụng lệnh ***speed***:



Hình 5.5 Cấu hình Switch

Trên switch này, tốc độ của 10/100 cổng Ethernet được đặt là auto. Trên cổng Gigabit Ethernet bạn chỉ có thể điều chỉnh switch với tốc độ của cổng là: có thể hoặc không thể tự động dò tìm tốc độ. Một khi tốc độ được cấu hình 10Mb, bạn hoàn toàn có thể kiểm tra lại interface Fa0/21 giống như:

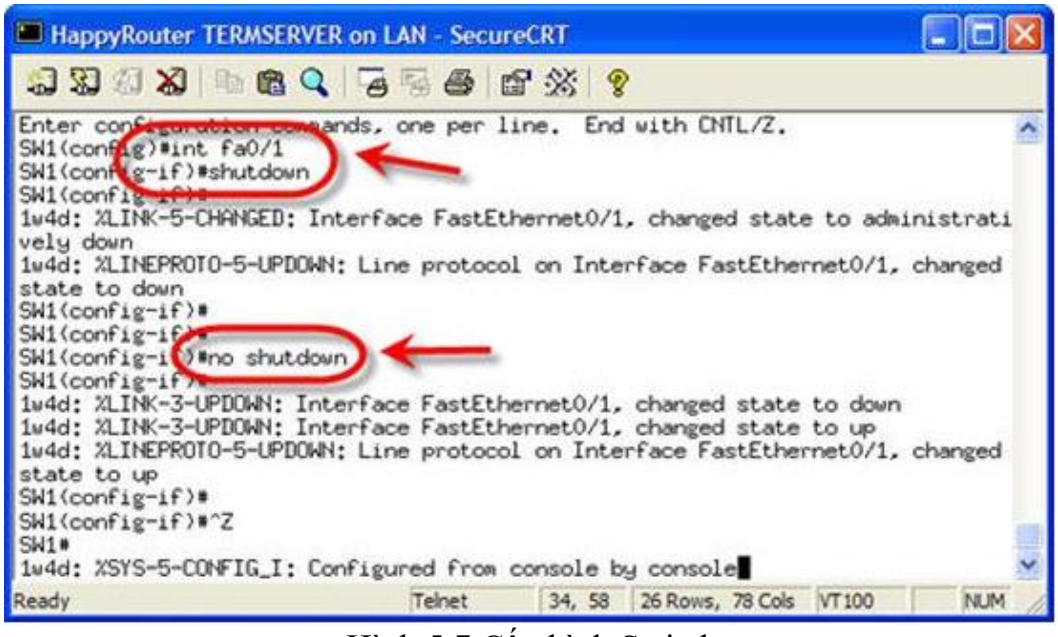


Hình 5.6 Cấu hình Switch

Như vậy ta thấy, tốc độ đã được đặt là 10. Và để có thay đổi tốc độ cả 2 chiều của cổng, bạn thực hiện các bước tương tự, nhưng trong trường hợp này cần sử dụng lệnh ***duplex***. Duplex có thể đặt là ***auto***, ***full*** hoặc ***half***.

Tắt và bật các interface

Để có thể tắt hoặc bật các interface, bạn có thể sử dụng lệnh ***no shutdown/shutdown*** trong chế độ cấu hình interface.



Hình 5.7 Cấu hình Switch

Chú ý khi cổng của switch bị shutdown, tin nhắn giao tiếp xuất hiện sẽ báo tình trạng quản lý đã được chuyển thành ***down***, line protocol cũng được chuyển thành ***down***. Khi cổng được bật trở

lại, line protocol sẽ chuyển thành ***up***. Giờ đây bạn có thể hiển thị tình trạng interface để thấy tình trạng của nó.

2.4 Kiểm tra cấu hình Switch

Switch là gì? là câu hỏi mà với đại đa số người dùng bình dân hiện nay. (có thể chính người dùng đang đọc giáo trình này) luôn có một câu trả lời khá đơn giản. nó chính là một bộ chia cổng mạng tại nhà, cơ quan, cửa hàng khi họ đang có nhu cầu chia sẻ kết nối mạng có dây cho nhiều thiết bị máy tính, laptop hơn.

Vai trò của Switch trong mạng LAN

- **Switch** đóng một vai trò vô cùng quan trọng trong mọi hệ thống mạng, nó giữ vai trò kết nối các thiết bị trong mạng LAN với nhau, đồng thời cũng là điểm trung gian để kết nối các thiết bị mạng LAN với Router để kết nối với Internet.
- Switch làm việc như một Bridge nhiều cổng. Khác với Hub nhận tín hiệu từ một cổng rồi chuyển tiếp tới tất cả các cổng còn lại, switch nhận tín hiệu vật lý, chuyển đổi thành dữ liệu, từ một cổng, kiểm tra địa chỉ đích rồi gửi tới một cổng tương ứng.

Thiết bị chuyển mạch Switch được phân chia thành các Layer (các tầng hoặc các lớp) gồm:

Switch layer 1: (Tầng 1 hoặc Lớp 1) là lớp cơ bản và là mô hình cổ nhất của thiết bị chuyển mạch. ở thời kỳ sơ khai nó được gọi là Hub (bridge – bộ lặp). Một hub (một cổng vào, nhiều cổng ra), hoặc bộ lặp (một cổng vào, một cổng ra), là những thiết bị mạng đơn giản không quản lý bất kỳ lưu lượng truy cập nào đến qua nó. Bất kỳ gói tin nào được đưa vào **Switch Layer 1** từ một cổng sẽ được "lặp lại" và được chuyển tới tất cả các thiết bị trong mạng qua các cổng khác ngoại trừ cổng nhập vào.

Vì mỗi gói được lặp lại và truyền trên tất cả các cổng khác do đó nó gây ra ảnh ảnh hưởng và làm giảm băng thông trên toàn bộ hệ thống mạng LAN (nội bộ), điều này gây nên sự giới hạn dung lượng chung của **Switch Layer 1**. Bộ lặp được dùng để bù suy hao tín hiệu bằng cách chuyển tiếp tất cả các tín hiệu điện đến từ cổng vào tới cổng ra sau khi đã khuếch đại. Trong khi một hub được dùng để nối với nhiều thiết bị ethernet.

Switch layer 2: về cơ bản là một cầu nối với nhiều port, mỗi port là một đoạn trong Ethernet LAN, biệt lập với các port còn lại. Việc truyền gói tin dựa hoàn toàn vào địa chỉ MAC hoặc địa chỉ IP chứa trong gói, nó sẽ không được truyền đi khi chưa biết được địa chỉ gốc.

Việc truyền các gói tin trong **Switch Layer 2** diễn ra như sau: gói tin được gửi từ một Host với một đích đến được đánh dấu bằng một địa chỉ MAC hoặc địa chỉ IP của máy đích. gói tin được gửi đến **Switch Layer 2** và được lưu trong bộ nhớ tạm của Switch. **Switch Layer 2** sẽ đọc thông tin đích đến là địa chỉ MAC hoặc địa chỉ IP của máy đích, sau đó nó sẽ lọc dữ liệu từ một bảng địa chỉ MAC và địa chỉ IP có sẵn để biết máy đích nằm ở cổng nào và sẽ chuyển tiếp gói tin này đến đúng cổng có địa chỉ MAC của máy đích.

Việc thu thập và tạo bảng địa chỉ MAC và địa chỉ IP của Switch Layer 2 diễn ra như sau: Khi mạng được khởi chạy, **Switch layer 2** sẽ bắn một gói tin Broadcast tới tất cả host trong mạng. các host này sẽ có quyền tiếp nhận hoặc không tiếp nhận gói tin Broadcast trên. nếu Host tiếp nhận, sau đó bắn trả lại một gói tin trả về cho **Switch layer 2** thì Switch sẽ thu thập được các thông tin như địa chỉ IP, địa chỉ MAC của Host này và lưu trữ chúng lại trên một bảng với mục đích sử dụng để truy xuất dữ liệu về địa chỉ IP hoặc địa chỉ MAC cho các lần truyền tiếp gói tin trong mạng.

Switch layer 2 là gì, Ích lợi của Switch Layer 2:

- Các thiết bị kết nối gián tiếp thông qua các port của **switch Layer 2**
- **Switch Layer 2** làm cho các host có thể hoạt động ở chế độ song công (có thể đọc – ghi, nghe – nói) cùng lúc.
- Không cần phải chia sẻ băng thông. Các port của switch sẽ quyết định băng thông truyền đi như thế nào.
- Giảm tỷ lệ lỗi trong frame. Frame sẽ được kiểm tra lỗi. Các gói tin tốt khi được nhận sẽ được lưu lại trước khi chuyển đi (công nghệ store-and-forward).

- Có thể giới hạn lưu lượng truyền đi ở một mức ngưỡng nào đó.
- Một **Switch Layer 2** đi kèm với các loại giao diện khác nhau như 10Mbps, 100Mbps, 1Gbps, 10Gbps… và nó cũng hỗ trợ giao tiếp full-duplex trên mỗi cổng của nó. Nó cũng tạo điều kiện mở rộng mạng và kết nối với phần còn lại của mạng thông qua các cổng tốc độ cao được gọi là các cổng uplink có thể được kết nối với các thiết bị chuyển mạch L2 khác hoặc các bộ định tuyến L3.

Switch layer 3: về cơ bản, là sự kết hợp khả năng định tuyến của Router và thêm vào **Switch layer 2** tiêu chuẩn. Sự khác biệt chính giữa hoạt động chuyển tiếp gói tin của một bộ định tuyến và sự chuyển đổi lớp 3 là thực thi thực tế. Trong các router có mục đích chung, việc chuyển tiếp thường được thực hiện trong phần mềm chạy trên bộ vi xử lý hoặc bộ xử lý mạng , trong khi đó công tắc lớp 3 thực hiện cùng một hoạt động bằng phần cứng mạch tích hợp dành riêng cho ứng dụng chuyên dụng (ASIC).

Hoạt động của **Switch Layer 3** chỉ dựa trên địa chỉ IP (đích) được lưu trữ trong tiêu đề của IP datagram. Sự khác biệt giữa chuyển đổi của **Switch layer 3** và bộ định tuyến là cách thiết bị đang đưa ra quyết định định tuyến. Theo truyền thống, bộ định tuyến sử dụng bộ vi xử lý để đưa ra quyết định chuyển tiếp trong phần mềm, trong khi chuyển đổi chỉ thực hiện chuyển mạch gói dựa trên phần cứng (bằng ASIC chuyên dụng với sự trợ giúp của bộ nhớ địa chỉ).Tuy nhiên, một số bộ định tuyến truyền thống có thể có các chức năng phần cứng tiên tiến cũng như trong một số mô hình cao cấp hơn.

Ưu điểm của Switch layer 3

Ưu điểm chính của **switch layer 3** là tiềm năng cho độ trễ mạng thấp hơn vì gói tin có thể được định tuyến mà không cần phải thực hiện thêm bước nhảy mạng cho router. Ví dụ, kết nối hai phân đoạn riêng biệt (ví dụ VLAN) với một bộ định tuyến cho một chuyển đổi lớp 2 tiêu chuẩn yêu cầu chuyển frame đến switch (L2 lớp đầu tiên), sau đó đến router (L2 lớp thứ hai), nơi gói tin bên trong khung được định tuyến (L3 hop) và sau đó quay trở lại công tắc (thứ ba L2 hop). Chuyển đổi lớp 3 hoàn thành nhiệm vụ tương tự mà không cần router (và do đó bổ sung) bằng cách tự định tuyến định tuyến, tức là gói được định tuyến đến mạng con khác và chuyển sang cổng mạng đích đồng thời.

- Bởi vì nhiều **thiết bị chuyển mạch layer 3** cung cấp chức năng tương tự như các bộ định tuyến truyền thống, chúng có thể được sử dụng như thay thế độ trễ thấp hơn, rẻ hơn trong một số mạng. **Switch layer 3** có thể thực hiện các thao tác sau cũng có thể được thực hiện bởi các bộ định tuyến:
  + Xác định đường dẫn dựa trên địa chỉ logic
  + Chạy lớp 3 tổng kiểm tra (chỉ trên tiêu đề)
  + Sử dụng thời gian để sống (TTL)
  + Xử lý và trả lời bất kỳ thông tin tùy chọn nào
  + Cập nhật các trình quản lý Giao thức quản lý mạng đơn giản (SNMP) với thông tin Cơ sở thông tin quản lý (MIB)
  + Cung cấp bảo mật

Những lợi ích của Switch Layer 3 bao gồm:

- Chuyển tiếp gói phần cứng nhanh
- Chuyển mạch gói hiệu suất cao
- Khả năng mở rộng tốc độ cao
- Thấp độ trễ
- Chi phí mỗi cổng thấp hơn
- Kế toán dòng chảy
- Chất lượng dịch vụ (QoS)

Có bao nhiêu loại Switch ?

Với nhu cầu sử dụng ngày càng đa dạng của khách hàng, các nhà cung cấp thiết bị mạng cũng ngày một đa dạng hoá và liên tục tích hợp thêm nhiều tính năng và thiết bị chuyển mạch Switch.

nhưng về cơ bản ở thời điểm hiện tại, chúng ta có thể phân loại Thiết bị chuyển mạch theo các nhóm sau:

Phân loại Switch theo lớp

- Như đã nói ở đầu bài viết **Switch là gì**, chúng ta có thể phân loại Switch theo lớp hoạt động đó là:
  + Switch Layer 1
  + Switch Layer 2
  + Switch Layer 3

Phân loại Switch theo số cổng

- Cũng như chúng tôi đã nói ở phần **Switch Là Gì**. Thông thường, với những người dùng không quá am hiểu về CNTT hoặc không đòi hỏi gì nhiều về tính năng. họ chỉ đơn giản là tìm kiếm thiết bị chuyển mạch. và khi đó họ chỉ quan tâm tới số cổng của switch để tìm một thiết bị chuyển mạch đáp ứng được số lượng user tại nhà hoặc cơ quan của họ. switch có các loại có số cổng như sau:
  + Switch 4 port
  + Switch 8 port
  + Switch 12 port
  + Switch 16 port
  + Switch 24 port
  + Switch 48 port

Phân loại theo công nghệ:

- Switch Ethernet 10/100
- Switch Ethernet 10/100/1000 (Switch Gigabit)
- Switch Ethernet POE
- Switch cổng Quang

Phân loại Switch theo vị trí hoạt động

- Switch Công nghiệp
- Core Switch
- Access Switch

Phân loại Switch theo hãng sản xuất

- Trên thị trường hiện nay có hàng trăm hãng sản xuất thiết bị chuyển mạch Switch. tuy nhiên, trong số đó có những cái tên không thể không nhắc đến như: Các thương hiệu switch hàng đầu, với các thương hiệu dẫn đầu thị trường chúng ta có thể kể tới:
  + **Switch Cisco**
  + Switch Linksys
  + Switch Juniper
  + Switch HP, …
- Trong số các hãng sản xuất trên thì cái tên CISCO luôn là Tập Đoàn dẫn đầu về công nghệ cũng như chất lượng. Đây là tập đoàn chuyên sản xuất **Thiết Bị Chuyển Mạch – Switch Cisco**. cái tên mà bất cứ một người có chút kiến thức về CNTT đều muốn sở hữu. đây là dòng sản phẩm mà Cisco chính hãng đang phân phối bao gồm:
  + **Switch Cisco 2960**
  + **Switch Cissco 2960-L**
  + **Switch Cisco 2960-X**
  + **Switch Cisco 3650**
  + **Switch Cisco 3850**

Các Thương Hiệu giá rẻ

- Hiện tại trên thị trường có rất nhiều các thương hiệu giá rẻ bao gồm:

+ Switch Planet
+ Switch TP-Link
+ Switch D-Link
+ Switch 3Com
+ Switch 3onedata
+ Switch Netgear
+ Switch Wintop
+ Switch Micronet, …

Kết luận

Qua giáo trình này (Thiết bị chuyển mạch là gì? Switch là gì? Tìm hiểu về Switch) hy vọng đã đưa đến cho bạn đọc cái nhìn tổng quan về thiết bị chuyển mạch – Switch và chúng tôi hy vọng sau bài học này, bạn đọc có thể trả lời được câu hỏi Switch là gì? hay thiết bị chuyển mạch là gì?

2.5 Bảo mật thiết bị Switch

Switch C2960-L là một thiết bị mạng nổi bật với nhiều tính năng mới, đem lại nhiều giải pháp mạng hoàn hảo cho các doanh nghiệp. Vì thế thiết bị này hiện tại được rất nhiều các doanh nghiệp vừa và nhỏ lựa chọn.

Hình 5.8 Switch C2960-L

Trong giáo trình này chúng ta cùng tham khảo tính năng bảo mật của nó

Cũng giống như các dòng sản phẩm khác của Cisco, C2960-L mang tính bảo mật cao và được hỗ trợ trên nhiều nền tảng ứng dụng. Cụ thể như sau:

Hệ thống bảo mật thông qua xác thực cổng IEEE802.1x

- Việc xác thực dựa trên cổng IEEE 802.1x giúp ngăn chặn các thiết bị trái phép truy cập vào mạng. Các tính năng 802.1x được hỗ trợ:

+ Xác thực đa miền (MDA) cho phép các thiết bị dữ liệu và thiết bị thoại, chẳng hạn như điện thoại IP (có thể là Cisco hoặc không phải Cisco), để xác thực độc lập trên cùng một cổng chuyển đổi hỗ trợ IEEE 802.1x.

+ Dynamic virtual virtual LAN (VLAN) cho MDA để cho phép một VLAN thoại động trên một cổng được kích hoạt MDA.

+ Phân bổ VLAN để hạn chế người dùng được xác thực 802.1x đến một VLAN được chỉ định.

+ Hỗ trợ cho việc gán VLAN trên một cổng được cấu hình cho chế độ multi-auth. RADIUS gán VLAN cho máy chủ đầu tiên để xác thực trên cổng và các máy chủ tiếp theo sử dụng cùng một VLAN. Phân bổ VLAN thoại được hỗ trợ cho một điện thoại IP.

+ Bảo mật cổng để kiểm soát quyền truy cập vào các cổng 802.1x.

+ Voice VLAN cho phép điện thoại IP của Cisco truy cập VLAN thoại bất kể trạng thái được phép hoặc không được phép của cổng.

+ Tăng cường phát hiện điện thoại IP để phát hiện và nhận diện một điện thoại IP của Cisco.

+ Khách VLAN cung cấp dịch vụ hạn chế cho người dùng không tuân thủ 802.1x.

+ Hạn chế VLAN để cung cấp các dịch vụ hạn chế cho người dùng tuân thủ 802.1x, nhưng không có thông tin xác thực để xác thực thông qua các quy trình chuẩn 802.1x.

802.1x kế toán để theo dõi việc sử dụng mạng.

- Kiểm tra sẵn sàng 802.1x để xác định mức độ sẵn sàng của các máy chủ kết thúc được kết nối trước khi định cấu hình IEEE 802.1x trên công tắc.
- Nhận biết bảo mật 802.1x bằng giọng nói chỉ áp dụng các hành động vi phạm giao thông trên VLAN mà vi phạm bảo mật xảy ra.
- Bỏ qua xác thực MAC (MAB) để ủy quyền cho khách hàng dựa trên địa chỉ MAC của máy khách.
- Kiểm soát truy nhập mạng (NAC) Lớp 2 Xác nhận 802.1x điều kiện chống vi-rút hoặc tư thế của hệ thống điểm cuối hoặc ứng dụng khách trước khi cấp quyền truy cập mạng của thiết bị.
- Hỗ trợ Cấu trúc liên kết truy cập mạng (NEAT) để thay đổi chế độ máy chủ cổng và áp dụng cấu hình cổng tiêu chuẩn trên cổng chuyển đổi trình xác thực.
- Xác thực MAC dựa trên VLAN-ID để sử dụng thông tin VLAN và địa chỉ MAC kết hợp để xác thực người dùng nhằm ngăn chặn truy cập mạng từ các VLAN trái phép.
- MAC di chuyển để cho phép máy chủ (bao gồm cả các máy chủ kết nối phía sau một điện thoại IP) để di chuyển qua các cổng trong cùng một chuyển đổi mà không có bất kỳ hạn chế nào để cho phép di chuyển. Khi di chuyển MAC, nút chuyển sẽ xử lý lại sự xuất hiện của cùng một địa chỉ MAC trên một cổng khác giống như địa chỉ MAC hoàn toàn mới.
- Hỗ trợ 3DES và AES với phiên bản 3 của Giao thức quản lý mạng đơn giản (SNMPv3). Bản phát hành này bổ sung hỗ trợ cho Chuẩn mã hóa dữ liệu ba chiều 168 bit (3DES) và các thuật toán mã hóa tiên tiến 128 bit, 192 bit và 256 bit (AES) cho SNMPv3.
- Hỗ trợ giao thức Cisco TrustSec SXP. Tính năng này không được hỗ trợ trên hình ảnh LanLite.

Tính năng bảo mật của Switch C2960-L

- Thiết bị chuyển mạch Switch hỗ trợ hình ảnh cơ sở LAN hoặc hình ảnh Lite LAN với bộ tính năng gồm:
  + Xác thực Web - Cho phép một máy khách (client) không hỗ trợ chức năng IEEE 802.1x được xác thực bằng trình duyệt web.
  + Biểu ngữ xác thực web cục bộ - Biểu ngữ tùy chỉnh hoặc tệp hình ảnh được hiển thị trên màn hình đăng nhập xác thực web.
  + Xác thực IEEE 802.1x với ACL và thuộc tính Id bộ lọc RADIUS
  + Quyền truy cập được bảo vệ bằng mật khẩu (truy cập chỉ đọc và ghi đọc) vào giao diện quản lý (trình quản lý thiết bị, Trợ lý mạng và CLI) để bảo vệ chống lại các thay đổi cấu hình trái phép
  + Bảo mật đa cấp cho lựa chọn cấp độ bảo mật, thông báo và hành động kết quả
  + Địa chỉ MAC tĩnh để đảm bảo an ninh
  + Tùy chọn cổng được bảo vệ để hạn chế chuyển tiếp lưu lượng truy cập đến các cổng được chỉ định trên cùng một nút chuyển
  + Tùy chọn bảo mật cổng để hạn chế và xác định địa chỉ MAC của các trạm được phép truy cập cổng
  + Tùy chọn bảo mật cổng VLAN để tắt VLAN trên cổng khi xảy ra vi phạm thay vì tắt toàn bộ cổng.
  + Port lão hóa an ninh để thiết lập thời gian lão hóa cho các địa chỉ an toàn trên một cổng.
  + Giao thức bảo vệ bão để kiểm soát tốc độ lưu lượng giao thức đến một chuyển đổi bằng cách thả các gói vượt quá tốc độ xâm nhập được chỉ định.

+ BPDU bảo vệ để tắt một cổng Port được cấu hình nhanh khi một cấu hình không hợp lệ xảy ra.

+ Danh sách điều khiển truy cập IP tiêu chuẩn và mở rộng (ACL) để xác định chính sách bảo mật trong nước trên giao diện Lớp 2 (cổng ACL).

+ Mở rộng các danh sách điều khiển truy cập MAC để xác định các chính sách bảo mật theo hướng gửi đến trên các giao diện Lớp 2.

+ ACLs nguồn và đích dựa trên MAC để lọc lưu lượng truy cập không phải IP.

+ DHCP snooping để lọc các tin nhắn DHCP không đáng tin cậy giữa các máy chủ không tin cậy và các máy chủ DHCP.

+ Bảo vệ nguồn IP để hạn chế lưu lượng trên các giao diện không được định trước bằng cách lọc lưu lượng dựa trên cơ sở dữ liệu DHCP snooping và các ràng buộc nguồn IP.

+ Kiểm tra ARP động để ngăn chặn các cuộc tấn công nguy hiểm trên switch bằng cách không chuyển tiếp các yêu cầu ARP không hợp lệ và các phản hồi tới các cổng khác trong cùng một VLAN.

Kết luận

Qua các thông tin mà giáo trình này mới chia sẻ tới bạn đọc, hi vọng giúp bạn biết các tính năng bảo mật của ***Switch C2960-L***, từ đó có cái nhìn mới mẻ hơn.

2.6 Tối ưu hóa những tiện ích của Switch

Giao diện quản lý Web được tích hợp trong thiết bị giúp người dùng dễ dàng quản lý và sử dụng. Chức năng Bluetooth để thực hiện các truy cập không dây cũng là một điểm khác biệt của dòng sản phẩm này.

- Virtual Stacking để quản lý nhóm thiết bị chuyển mạch dưới dạng một thực thể. Có thể cấu hình và quản lý tối đa tám bộ chuyển mạch bằng một địa chỉ IP duy nhất. Chuyển mạch trong một ngăn xếp ảo có thể được cấu hình từ một bộ chuyển mạch duy nhất.

Tất cả các thiết bị chuyển mạch trong ngăn xếp ảo có thể được quản lý bằng CLI, SNMP hoặc giao diện người dùng web.

Quản lý mạng C2960-L

Thiết bị chuyển mạch Cisco **Catalyst 2960-L** cung cấp một CLI cao cấp cho cấu hình và quản trị chi tiết. Các switch cũng được hỗ trợ bởi đầy đủ các giải pháp quản lý mạng của Cisco.

- Cơ sở hạ tầng của **Cisco 2960-L** cung cấp quản lý vòng đời mạng toàn diện, bao gồm thư viện mở rộng các tính năng dễ sử dụng để tự động hóa việc quản lý ban đầu và hàng ngày của mạng Cisco của bạn. Công nghệ Cisco Prime tích hợp chuyên môn nền tảng phần cứng và phần mềm và trải nghiệm hoạt động vào một bộ công cụ quản lý, theo dõi, khắc phục sự cố, báo cáo và quản trị mạnh mẽ.

PoE + thông minh

- **Cisco Catalyst 2960-L** bộ chuyển mạch hỗ trợ cả hai chuẩn IEEE 802.3af PoE và IEEE 802.3at PoE + (lên đến 30W mỗi cổng) để cung cấp một tổng chi phí sở hữu thấp cho các triển khai có kết hợp điện thoại IP của Cisco, Cisco Aironet điểm truy cập không dây, hoặc các tiêu chuẩn khác

- Thiết bị đầu cuối PoE loại bỏ sự cần thiết phải cung cấp điện tường cho các thiết bị hỗ trợ PoE và loại bỏ chi phí thêm cáp điện và các mạch mà nếu không sẽ cần thiết trong việc triển khai điện thoại IP và WLAN.

Thiết bị chuyển mạch Cisco Catalyst **Switch 2960-L** PoE cấp điện năng động, và ánh xạ năng lượng lên đến tối đa 370W công suất PoE +. Quản lý nguồn thông minh cho phép phân bổ nguồn linh hoạt trên tất cả các cổng. Với PoE vĩnh viễn, công suất PoE + được duy trì trong quá trình nạp lại bộ chuyển mạch. Điều này rất quan trọng đối với các thiết bị đầu cuối quan trọng như thiết bị y tế và cho các điểm cuối IoT như đèn hỗ trợ PoE, do đó không có sự gián đoạn trong khi khởi động lại bộ chuyển mạch.

Bảo mật mạng an toàn hơn với C2960-L

Bên cạnh các giao diện quản lý, bảo mật cũng là một yếu tố được đánh giá cao ở bộ chuyển đổi này và **Cisco Catalyst 2960-L** cung cấp một loạt các tính năng bảo mật để hạn chế quyền truy cập vào mạng và giảm thiểu các mối đe dọa, bao gồm:
- Tính năng 802.1X toàn diện để kiểm soát truy cập vào mạng, bao gồm xác thực linh hoạt, chế độ màn hình 802.1X và thay đổi quyền của RADIUS.
- Hỗ trợ 802.1x với Cấu trúc liên kết truy cập mạng (NEAT) mở rộng xác thực danh tính cho các khu vực bên ngoài tủ đấu dây (chẳng hạn như phòng hội nghị).
- Phân phối người dùng IEEE 802.1x cho phép bạn cân bằng tải người dùng với cùng một tên nhóm trên nhiều VLAN khác nhau.
- Vô hiệu hóa việc học tập trên mỗi VLAN MAC quản lý không gian bảng địa chỉ MAC có sẵn bằng cách kiểm soát giao diện hoặc VLAN nào tìm hiểu địa chỉ MAC.
- Xác thực đa miền để cho phép điện thoại IP và máy tính xác thực trên cùng một cổng chuyển mạch trong khi được đặt trên các VLAN thoại và dữ liệu thích hợp.
- Danh sách điều khiển truy cập (ACLS) cho các thành phần bảo mật IPv6 và IPv4 và các thành phần ACL chất lượng dịch vụ (QoS).
- Các cổng ACL dựa trên cổng cho giao diện Lớp 2 để cho phép các chính sách bảo mật được áp dụng trên các cổng chuyển đổi riêng lẻ.
- SSH, Kerberos và SNMPv3 để cung cấp bảo mật mạng bằng cách mã hóa lưu lượng truy cập của quản trị viên trong các phiên Telnet và SNMP. SSH, Kerberos và phiên bản mã hóa của SNMPv3 yêu cầu một hình ảnh phần mềm mật mã đặc biệt vì các hạn chế xuất khẩu của Hoa Kỳ.
- SPAN, với hỗ trợ dữ liệu hai chiều, để cho phép hệ thống phát hiện xâm phạm của Cisco (IDS) thực hiện hành động khi phát hiện kẻ xâm nhập.
- TACACS + và xác thực RADIUS để tạo điều kiện tập trung chuyển đổi và hạn chế người dùng trái phép thay đổi cấu hình.
- Thông báo địa chỉ MAC để thông báo cho quản trị viên về người dùng được thêm vào hoặc bị xóa khỏi mạng.
- Bỏ qua xác thực MAC và Webauth với ACL tải xuống cho phép ACL cho mỗi người dùng được tải xuống từ Máy chủ điều khiển truy cập của Cisco (ACS) như thực thi chính sách sau khi xác thực bằng MAB hoặc xác thực Web ngoài IEEE 802.1X.
- Chuyển hướng xác thực web cho phép mạng chuyển hướng người dùng khách đến URL mà họ đã yêu cầu ban đầu.
- Bảo mật đa cấp trên truy cập bảng điều khiển để ngăn người dùng trái phép thay đổi cấu hình chuyển đổi.
- BPDU bảo vệ để tắt các giao diện mở rộng PortFast-tree khi BPDU được nhận để tránh các vòng cấu trúc liên kết ngẫu nhiên.
- IP Source Guard hạn chế lưu lượng IP trên các giao diện không có lớp, Lớp 2 bằng cách lọc lưu lượng dựa trên cơ sở dữ liệu ràng buộc DHCP snooping hoặc cấu hình thủ công các ràng buộc nguồn IP.
- SSHv2 cho phép sử dụng chứng chỉ số để xác thực giữa người dùng và máy chủ.
- Spanning-Tree Root Guard (STRG) để ngăn chặn các thiết bị cạnh không nằm trong sự kiểm soát của quản trị mạng trở thành các nút gốc của giao thức Spanning Tree Protocol (STP).
- Bộ lọc giao thức quản lý nhóm Internet (IGMP) để cung cấp xác thực đa hướng bằng cách lọc ra những người không đăng ký và giới hạn số lượng các luồng phát đa hướng đồng thời có sẵn trên mỗi cổng.
- Phân bổ VLAN động thông qua việc thực hiện khả năng của máy khách VLAN Membership Policy Server để cung cấp sự linh hoạt trong việc gán các cổng cho các VLAN. Dynamic VLAN tạo điều kiện cho việc gán nhanh các địa chỉ IP.

Hiện tại Saigoncisco đang phân phối các bộ chuyển mạch Switch Cisco chính hãng với đầy đủ giấy tờ CO,CQ, Bảo hành 12 tháng.

2.7 Xử lý các sự cố của Switch

Bạn đã từng gặp sự cố trong quá trình sử dụng mạng và bối rối không biết nguyên nhân cũng như cách khắc phục ra sao? Bạn phải tốn rất nhiều thời gian lên mạng tìm hiểu nhưng vẫn không thể biết chính xác lỗi và nguyên nhân gặp phải? Trong giáo trình này chia sẻ danh sách bảy sự cố mà người dùng cũng như các kỹ thuật viên mạng thường gặp nhất, nguyên nhân và giải pháp cho từng sự cố.

2.7.1 Không thể lấy địa chỉ IP

Dấu hiệu:

- Biểu tượng mạng trên máy tính hoặc laptop hiển thị tình trạng không hoạt động. Hệ điều hành cảnh báo không nhận được địa chỉ IP từ máy chủ DHCP. Khi kiểm tra trạng thái của cổng mạng, không thấy địa chỉ nào được gán ngoài địa chỉ 169.254.x.x (đây là địa chỉ của hệ điều hành Windows tự cấp cho máy tính khi không nhận được IP).
- Mất mạng gây cảm giác ức chế cho người sử dụng

Nguyên nhân:

- Có thể nguyên nhân do máy chủ DHCP hết quỹ địa chỉ, dịch vụ DHCP ở máy chủ đã bị vô hiệu hóa, hay yêu cầu DHCP được gửi từ thiết bị đầu cuối không đến được tới máy chủ.

Giải pháp:

Bạn cần phải lưu ý xem lỗi này xảy ra với tất cả các máy hay chỉ duy nhất một máy bị. Nếu chỉ một người bị lỗi, nên kiểm tra cấu hình DHCP trên máy trạm. Sau đó, kiểm tra cổng mạng tương ứng đang thuộc VLAN nào trên switch. Kiểm tra thiết bị của người dùng trên VLAN tương ứng có nhận được địa chỉ IP hay không. Nếu không nhận được, sự cố này có thể là do router không chuyển tiếp các yêu cầu DHCP tới máy chủ. Nếu các máy trạm lại thuộc nhiều VLAN khác nhau cùng bị lỗi, nguyên nhân lúc này là do chính máy chủ DHCP. Máy chủ có thể lúc này chưa chạy dịch vụ DHCP, hoặc không còn quỹ địa chỉ. Nếu tổ chức có nhiều máy chủ DHCP, lỗi này có thể do một trong số những máy chủ được cấu hình không phù hợp với hệ thống. Ngoài ra, cũng có trường hợp do một AP (Access Point) giả mạo, do người dùng tự ý mang đến và cắm vào hệ thống mạng và cung cấp dịch vụ DHCP giả mạo cho hệ thống mạng.

2.7.2 Hiệu suất ứng dụng thấp

Dấu hiệu:

- Các ứng dụng hoạt động trở nên chậm chạp. Màn hình của người dùng có thể bị đơ, bị đứng, không hoạt động hay bị ngăn chặn khi truy xuất dữ liệu. Thông thường khi gặp phải lỗi này, người dùng sẽ có xu hướng đổ lỗi cho hệ thống mạng hoạt động quá chậm hoặc kém chất lượng

Nguyên nhân:

- Người dùng thường lầm tưởng và đổi tại chất lượng hệ thống mạng. Để tránh việc đổ lỗi cho hệ thống mạng, các nhân viên IT cần phải chẩn đoán, cô lập và xác định được chính xác vùng xảy ra sự cố.
- Việc ứng dụng hoạt động không tốt có thể xuất phát từ rất nhiều nguyên nhân, thường gặp nhất là do máy cầu thực hiện tiến hành sao lưu dữ liệu trong giờ làm việc, từ đó chiếm lượng lớn tài nguyên của hệ thống mạng, làm giảm tốc độ truy suất cơ sở dữ liệu của máy chủ và còn gây mất gói trên hệ thống mạng.
- Đứng trên góc độ kỹ thuật viên, cần xác định chính xác được nguyên nhân sự cố là do máy chủ hay do hệ thống mạng? Để làm được điều này, cần thu thập dữ liệu các gói tin của ứng dụng và tìm xem có hoạt động truyền lại nào giữa máy trạm và máy chủ không? Trong trường hợp có, đồng nghĩa với việc mất gói tin trên đường truyền chính là nguyên nhân ảnh hưởng tới hiệu suất ứng dụng. Còn nếu không xuất hiện tình trạng truyền lại, kết nối giữa máy trạm và máy chủ vẫn được thiết lập bình thường, nguyên nhân có thể từ các vấn đề tại máy chủ.

Giải pháp:

- Dù rất khó tìm ra nguyên nhân của trường hợp này nếu chỉ dựa vào việc phân tích gói tin, nhưng người ta vẫn thường dùng cách này để đếm số lượt truyền lại các gói TCP.
- Sử dụng bộ đếm này giúp xác định số lượng gói tin bị mất giữa máy trạm và máy chủ. Tham khảo các thông số như lỗi Ethernet trên switch, router giữa máy trạm và máy chủ cũng có thể là nguyên nhân gây ra hiện tượng mất gói tin.
- Nếu không xuất hiện các lỗi trên, nhân viên kĩ thuật cần lưu ý khả năng mất gói tin trên hệ thống WAN do việc sử dụng vượt quá mức cho phép của nhà cung cấp dịch vụ. Ngoài ra, cũng có thể phân tích hiệu suất ứng dụng nhờ các bộ công cụ phân tích mạng chuyên nghiệp, từ đó cung cấp thông tin từ việc bắt các gói tin cùng với đó phân tích thời gian phản hồi từ các máy chủ, thời gian xử lý trên máy con và cả thời gian truyền trên hệ thống mạng, từ đó có thể đưa ra được nhận định chính xác đâu là nguyên nhân gây ra lỗi hiệu suất mạng.

2.7.3 Không thể kết nối đến máy chủ

Dấu hiệu:

- Trên máy của người dùng cảnh báo "Không thể kết nối đến máy chủ". Các cảnh báo này xuất hiện khi người dùng sử dụng những ứng dụng như CRM hoặc e-mail. Người sử dụng thường cho rằng lỗi này xuất hiện do mất mạng, tuy nhiên nguyên nhân không chỉ có vậy.

Nguyên nhân:

- Tình trạng này có thể xảy ra do nhiều nguyên nhân khác nhau. Điều nhân viên kĩ thuật cũng như người dùng cần quan tâm là lỗi này xày ra với tần suất ra sao? Thường xuyên hay chỉ thỉnh thoảng? Nếu lỗi xảy ra thường xuyên dù máy tính đã có địa chỉ IP phù hợp, nguyên nhân có thể do các vấn đề liên quan đến định tuyến trên hệ thống mạng giữa máy chủ và máy trạm, có thể kiểm tra dễ dàng bằng việc kiểm tra "ping". Nếu lỗi xảy ra không thường xuyên, có thể do máy chủ bị quá tải và không thể phản hồi tất cả các yêu cầu từ máy trạm.

Giải pháp:

- Trong trường hợp không phải từ định tuyến, nhân viên kĩ thuật hãy kiểm tra lại mức độ sử dụng cũng như tài nguyên của máy chủ. Máy chủ có thể đang quá tải do chạy song song các tác vụ khác như việc sao lưu dữ liệu không? Nếu không, hãy thử kiểm tra lưu lượng mạng giữa máy trạm và máy chủ xem có quá tải không? Phương thức tốt nhất là sử dụng công cụ SNMP để giám sát hiệu năng của các kết nối. Ngoài ra, các lỗi Ethernet (Alignment Error , FCS Error, hay Late Collision) trên router và switch cũng có thể là nguyên nhân dẫn đến mất gói tin giữa máy trạm và máy chủ.

2.7.4 Các lỗi về in ấn

Dấu hiệu:

- Hệ thống in ấn qua mạng hoạt động chập chờn, không ổn định và có thể không hoạt động tuy nhiên máy in vẫn hiển thị sẵn sàng cho việc hoạt động.

Nguyên nhân:

- Cần xác định xem tình trạng này diễn ra tại một hay nhiều máy trạm? Nếu chỉ xảy ra tại một máy, có thể do máy tính không được thiết lập phù hợp với việc kết nối tới máy in. Nếu không phải nguyên nhân này, có thể do hệ thống mạng giữa máy trạm và máy in đang có vấn đề. Mất gói tin cũng có thể là nguyên nhân gây ra hiện tượng này.

Giải pháp:

- Kiểm tra cấu hình máy trạm xem có nhận được địa chỉ IP thích hợp để truy cập đến máy in chủ (print server) hay không? Đôi khi, cập nhật trình điều khiển máy in (driver) cũng có thể giúp giải quyết hiện tượng này. Nhìn chung, hãy chắc chắn dung lượng mạng

đến và đi từ máy in phải luôn được đảm bảo một cách tốt nhất, đồng thời cập nhật các trình điều khiển cho tất cả các máy in thuộc hệ thống hệ thống.

2.7.5 Cáp kém chất lượng

Dấu hiệu:

- Chất lượng kết nối mạng kém, không được đảm bảo. Nhiều khi người dùng còn không thể truy cập mạng từ các máy trạm hoặc lúc được lúc không, ảnh hưởng đến chất lượng cũng như năng suất làm việc.

Có rất nhiều loại cáp mạng kém chất lượng, không đảm bảo được bày bán tràn lan trên thị trường

Nguyên nhân:

- Gigabit cho máy trạm hiện nay đã trở nên vô cùng thông dụng trong các hệ thống mạng. Công nghệ Gigabit cần bốn đôi dây cho một kết nối, do vậy, hệ thống cáp phải đạt tiêu chuẩn từ Cat5e trở lên. Với các tòa nhà sử dụng các hệ thống mạng cũ, lâu đời thì đây có thể nói là nguyên nhân hàng đầy dẫn đến hiện tượng chất lượng mạng kém. Ngoài ra, dây cáp bị tháo xoắn quá nhiều (khi bấm đầu hay kết nối vào thanh đấu nối) hoặc cáp không phải là loại cáp chuyên dụng nhưng vẫn phải hoạt động trong các môi trường khắc nghiệt như: ngoài trời, môi trường dễ gây nhiễu, nhiệt độ cao,…

Giải pháp:

- Trong hầu hết trường hợp, giải pháp đơn giản nhất là thay thế loại cáp đang sử dụng. Nếu lỗi là do tháo xoắn cáp quá mức, nhân viên kĩ thuật cần tiến hành bấm lại đầu kết nối và kiểm tra bằng bộ máy test cáp mạng LAN sẽ giải quyết được vấn đề này. Nếu do hệ thống cáp đã lỗi thời, không thể hỗ trợ các công nghệ mới như Gigabit hay PoE (Power over Ethernet), nên cân nhắc việc thay thế bằng hệ thống mạng sử dụng mạng Cat5e, Cat6 hoặc hơn. Trong trường hợp này, nhân viên kĩ thuật và người dùng có thể liên hệ trực tiếp với các đơn vị chuyên phân vối cáp mạng để được tư vấn tốt nhất.
- Hiện nay, Công ty Cổ phần Viễn Thông Xanh Việt Nam đang là một trong những đơn vị chuyên cung cấp các sản phẩm cáp Cat5e và Cat6 cũng như thiết bị mạng chính hãng uy tín hàng đầu Việt Nam với các thương hiệu như: AMP, Alantek, LS Vina, ADC, Goldenlink,…để người dùng có thể đa dạng trong việc lựa chọn và sử dụng theo đúng nhu cầu và mục đích của hệ thống mạng của mình.

2.7.6 Lỗi DNS

Dấu hiệu:

- Người dùng không thể kết nối Internet hoặc các ứng dụng. Hệ thống mạng hiển thị không thể kết nối.

Nguyên nhân:

- Máy trạm không thể phân giải tên của máy chủ nên không thể gửi được các yêu cầu kết nối. Nguyên nhân thường do cấu hình DNS trên máy trạm không tương thích, máy chủ không thể phân giải được các yêu cầu DNS được gửi tới (do các yêu cầu này không nằm trong cơ sở dữ liệu), hay do mất gói tin trên đường truyền. Do DNS là một giao thức loại UDP nên các gói tin bị mất không được truyền lại. Đây là nguyên nhân cơ bản dẫn đến lỗi DNS.

Giải pháp:

- Người dùng cần kiểm tra lại cấu hình DNS máy trạm. Nếu cấu hình không phú hợp, cần cấu hình lại cho máy trạm hoặc cấu hình lại máy chủ DHCP nhằm mục đích cung cấp thông tin chính xác cho máy trạm. Kiểm tra máy chủ DNS từ phía máy trạm nhiều lần để đánh giá được tình trạng phản hồi từ máy chủ, xem có xuất hiện tình trạng mất gói nào không? Nếu có, hãy xem xét kĩ các lỗi Ethernet giữa máy trạm và máy chủ. Tốt nhất, nên thiết lập một công cụ kiểm tra liên tục máy chủ DNS và tự động cảnh bảo khi có sự cố xảy ra.

2.7.7 Máy trạm không thể kết nối Wi-Fi

Dấu hiệu:

- Máy trạm có thể phát hiện AP nhưng không kết nối vào hệ thống Wi-Fi.
- Lỗi không kết nối với Wi-fi

Nguyên nhân:

- Không có thông tin về bảo mật, nhiễu hoặc điểm chết đều có thể dẫn tới vấn đề này. Vì hệ thống mạng không dây là vô hình nên rất khó trong việc xem xét và kiểm tra trừ khi có công việc cụ thể.

Giải pháp:

- Sử dụng công cụ giám sát mạng không dây để đo lường độ mạnh, yếu của tín hiệu tại vùng ảnh hưởng, nếu có thể, hãy khảo sát cả các vùng lân cận, tìm kiếm các AP không chính thức hay AP có tính mạo danh – là các AP mà người dùng mang vào sử dụng mà không có sự cho phép từ các nhà quản trị mạng. Các AP này có thể được cấu hình chồng lên các kênh Wi-Fi hiện có và gây ảnh hưởng đến chất lượng Wi-Fi. Kiểm tra các nguồn có thể gây nhiễu xung quanh các AP như từ lò vi sóng hay điện thoại không dây. Kiểm tra tiến trình kết nối đến AP của máy trạm, xác định lỗi xuất hiện ở bước nào

Kết luận

Trên đây là danh sách bảy sự cố người dùng thường gặp nhất khi sử dụng mạng hiện nay. Trong nhiều trường hợp, các sự cố doanh nghiệp gặp phải thường tập trung ở một hoặc hai nguyên nhân phổ biến, và đã được giải quyết. Tất cả các nguyên nhân trên đều được tổng hợp từ thực tế, trong giáo trình này hy vọng sẽ giúp cho người dùng hoặc các nhân viên kĩ thuật chủ động hơn trong việc khắc phục các sự cố hệ thống mạng xảy ra.

Câu hỏi ôn tập

1. Hãy nêu các bước khởi động một Cisco IOS switch;
2. Nhận dạng và đọc các lỗi đèn trên switch phản ánh điền kiện làm việc của switch;
3. Mô tả các kết qủa hiển thị của quá trình khởi độngtrên switch;
4. Đăng nhập vào Cisco IOS switch;
5. Cấu hình switch bằng CLI, kiểm tra hoạt động ban đầu của switch;
6. Quản lý bảng MAC của switch và ghi lại các địa chỉ MAC

BÀI 6. MẠNG CỤC BỘ ẢO

Giới thiệu:

VLAN là cụm từ viết tắt của *virtual local area network* (hay *virtual LAN*) hay còn được gọi là **mạng LAN ảo**. VLAN là một kỹ thuật cho phép tạo lập các mạng LAN độc lập một cách logic trên cùng một kiến trúc hạ tầng vật lý. Việc tạo lập nhiều mạng LAN ảo trong cùng một mạng cục bộ (giữa các khoa trong một trường học, giữa các cục trong một công ty,...) giúp giảm thiểu miền quảng bá (*broadcast domain*) cũng như tạo thuận lợi cho việc quản lý một mạng cục bộ rộng lớn. VLAN tương đương như mạng con (*subnet*).

1. Mục tiêu của bài

- Mô tả được chức năng của mạng ảo VLAN;
- Mô phỏng được vai trò của Switch trong VLAN;
- Trình bày được lợi ích của VLAN;
- Thiết lập được các VLAN;
- Triển khai được VTP, OSPF và EIGRP;

2. Nội dung bài

2.1 Triển khai VLANs và Trunks

2.1.1. Khái niệm

VLAN (Virtual Local Area Networks) được sử dụng để chia 1 mạng vật lý thành nhiều mạng con nhỏ tùy mục đích sử dụng.

Tiêu chuẩn mà VLAN sử dụng là IEEE 802.1q

Mỗi một VLAN được gán một id cụ thể có giá trị từ 1-4094 trong đó id bằng 1 thường được sử dụng để quản lý vì vậy không nên sử dụng id này cho các VLAN mới của bạn .

2.1.2 Cấu hình VLAN,TRUNK trên Switch Cisco

Trong giáo trình này sẽ hướng dẫn cơ bản cho các bạn cấu hình VLAN, Trunk trên đơn Switch

2.1.2.1 Cấu hình VLAN

Truy cập và kiểm tra VLAN hiện có

- Switch>enable
- Switch#show vlan

Tạo VLAN

- Switch# configure terminal
- Switch(config)# vlan 10
- Switch(config-vlan)# name vlan10
- Switch(config)# vlan 20
- Switch(config-vlan)# name vlan20
- Switch(config-vlan)# exit

Xóa VLAN

- Switch(config)# no vlan 10

Kiểm tra VLAN vừa tạo

- Switch# show vlan

Tiến hành xác định port mà Server, thiết bị cần access VLAN tiến hành cấu hình VLAN cho port đó

- Switch(config)# interface range F0/1-F0/2
- Switch(config-if-range)# switchport access vlan 10
- Switch(config)# interface F0/3
- Switch(config-if)# switchport access vlan 20

2.1.2.2 Một đường kết nối muốn sử dụng nhiều VLAN trên này thì sao? Trunking thôi chứ sao nữa?

Cấu hình trunking trên SW Cisco

- Truy cập
  + Switch>enable

Xác định port muốn cấu hình trunking

- Switch# configure terminal
- Switch(config)# interface F0/3

Thao tác cấu hình như sau

- Switch(config-if)# switchport trunk encapsulation dot1q
- Switch(config-if)# switchport mode trunk
- Switch(config-if)# exit

2.1.2.3 Switch port, VTP, InterVLAN Routing

Ở phần 2.1.2.1 và 2.1.2.2 chúng ta đã cấu hình được cơ bản về VLANs và Trunk trên đơn Switch. Thực ra đối với môi trường thực tế thì việc cấu hình còn phức tạp hơn vì nó kết nối đến nhiều SW[5], router khác nhau nữa.

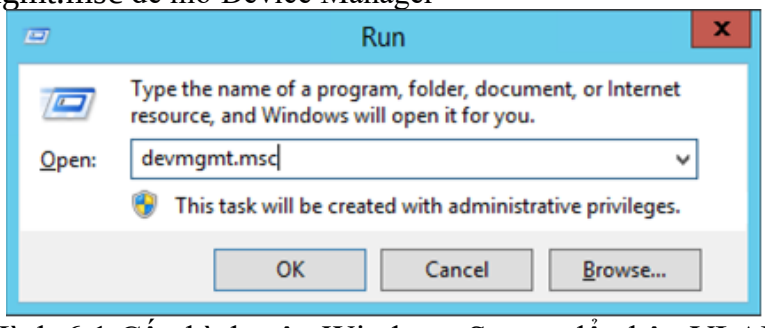
Việc đồng bộ dữ liệu VLANs được cấu hình giữa các thiết bị là cần thiết nhưng nó không nằm trong phạm vi của giáo trình này, các bạn có thể tham khảo cụ thể tại các trang mạng về Cấu hình Switch port, VLANs, Trunk, VTP, InterVLAN Routing

2.1.3. Cấu hình trên Windows Server để nhận VLAN

Đối với interface kết nối đến port trên Switch là access vlan X thì đơn giản chỉ cần đặt IP cho Server thôi, không phải thao tác gì khác.

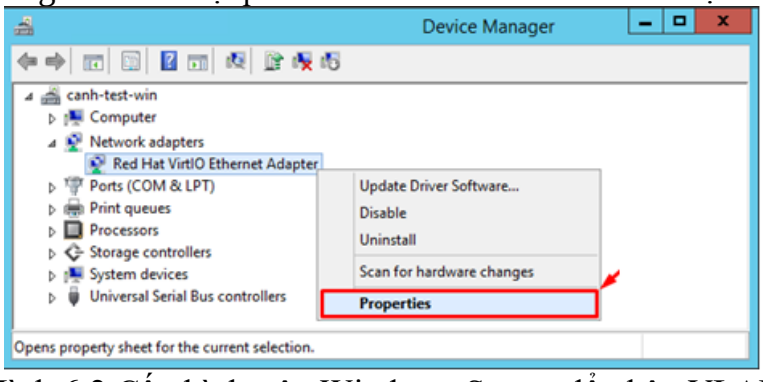
Đối với interface kết nối đến port trên Switch là mode trunk thì chúng ta phải thực hiện cấu hình như sau

Mở Run gõ devmgmt.msc để mở Device Manager



Hình 6.1 Cấu hình trên Windows Server để nhận VLAN

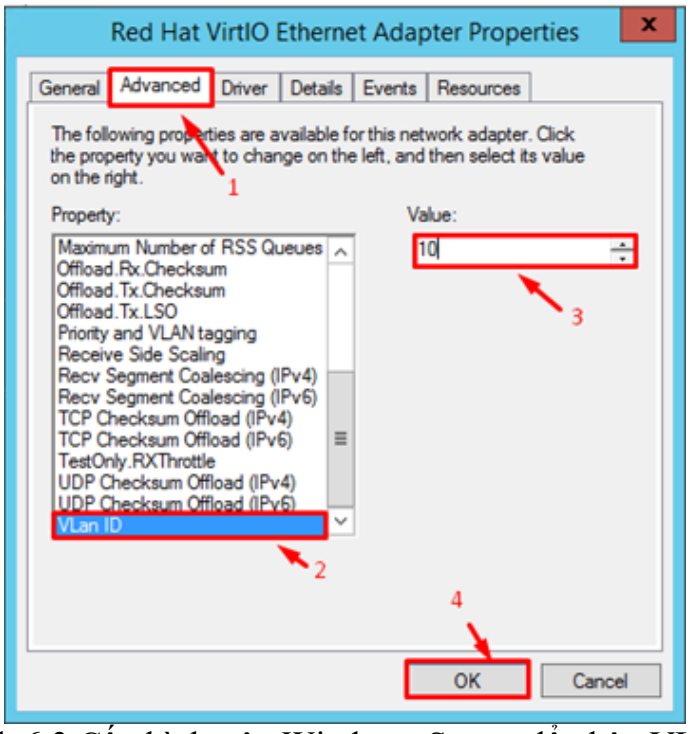
Trong Device Manager click chuột phải vào NIC kết nối đến Switch chọn Properties



Hình 6.2 Cấu hình trên Windows Server để nhận VLAN

Click vào Advanced tab kéo xuống chọn VLAN ID set giá trị ID VLAN

[5] SW: Switch



Hình 6.3 Cấu hình trên Windows Server để nhận VLAN

Hoàn tất cấu hình

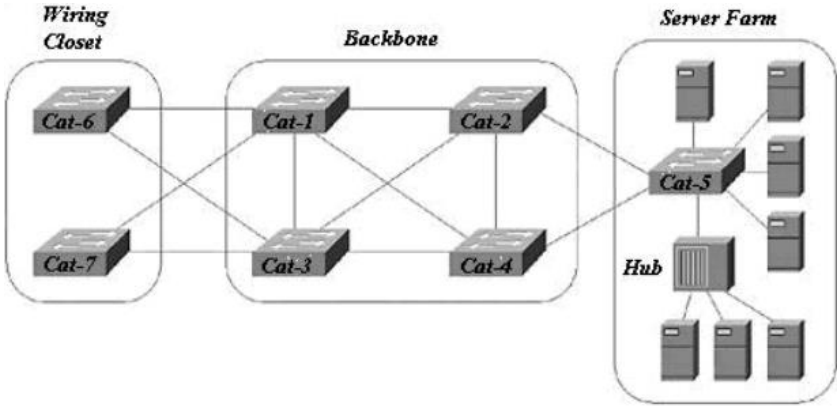
2.2 Cải tiến hiệu suất với Spanning Tree

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.

2.2.1 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.

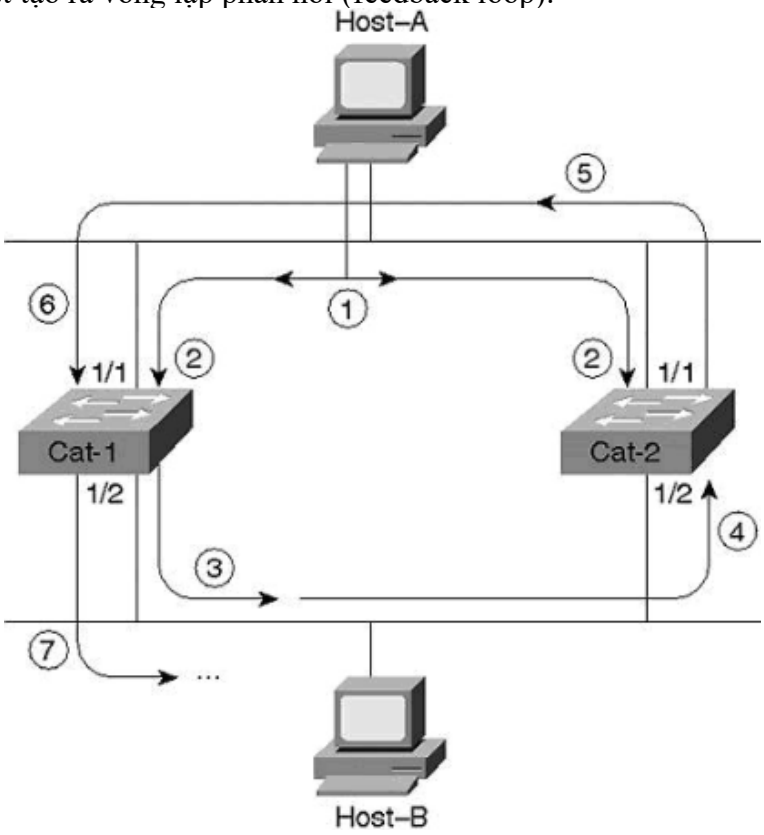
Hầu hết các nguyên nhân thôngthường là kết quả của việc cố gắng tính toán để cung cấp khả năng dự phòng, trong trườnghợp này, một liên kết hoặc switch bị hỏng, các liên kết hoặc switch khác vẫn tiếp tục hoạtđộng, tuy nhiên các vòng lặp cũng có thể xảy ra do lỗi. Hình 6.4 biểu diễn một mạngchuyển mạch với các vòng lặp cố ý được dùng để cung cấp khả năng dự phòng như thế nào.



Hình 6.4 bridging loop trong mạng

Hai nguyên nhân chính gây ra sự lặp vòng tai hại trong mạng chuyển mạch là dobroadcast 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 6.5 biểu diễn broadcast tạo ra vòng lặp phản hồi (feedback loop).



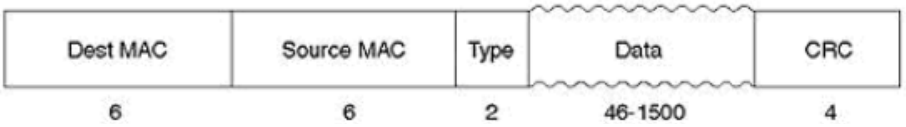
Hình 6.5 không có STP, broadcast tạo Feedback loop

Giả sử rằng, không có switch nào chạy STP:

- Bước 1: host A gửi một frame bằng địa chỉ broadcast (FF-FF-FF-FF-FF-FF).
- 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 kểcả 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 thànhmột 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 nữa trong hình 6.5 là vòng lặp bridge nguy hiểm hơn nhiều so với vòng lặp định tuyến. Hình 6.6 mô tả định dạng của một DIXv2 Ethernet frame.



Hình 6.6 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.

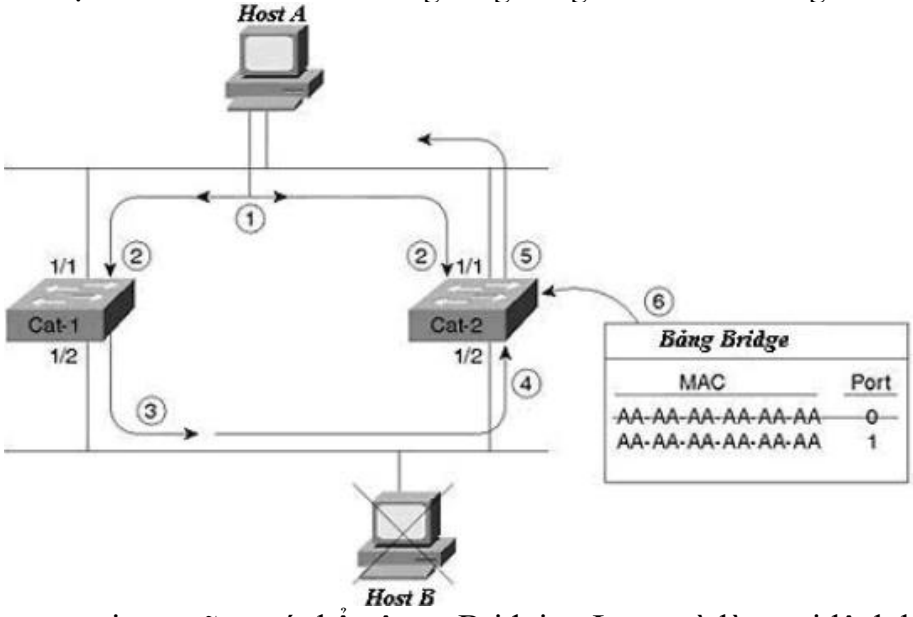
Trong một mạng phức tạp hơn mạng được mô tả trong hình 6.4, và 6.5 thì có thể gây ra vòng lặp feedback rất nhanh theo tỉ lệ số mũ. Vì cứ mỗi frame tràn qua nhiều cổng của switch, thì tổng số frame tăng nhanh rất nhiều. Ngoài ra cần phải chú ý đến cơn bão broadcast trên người dùng của host A và B trong hình 6.5. 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 sửdụng 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 6.7 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 cổng1/1 trên cả hai switch.
- Bước 3: vì host B bị down, nên Cat-1 không có địa chỉ MAC (BB-BB-BB-BB-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-BB-BB-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 chỉMAC là AA-AA-AA-AA-AA-AA. Nó thay đổi địa chỉ MAC của hostA trong bảng bridge dẫn đến sai cổng.



Hình 6.7 frame unicast cũng có thể gây ra Bridging Loop và làm sai lệnh bảng bridge

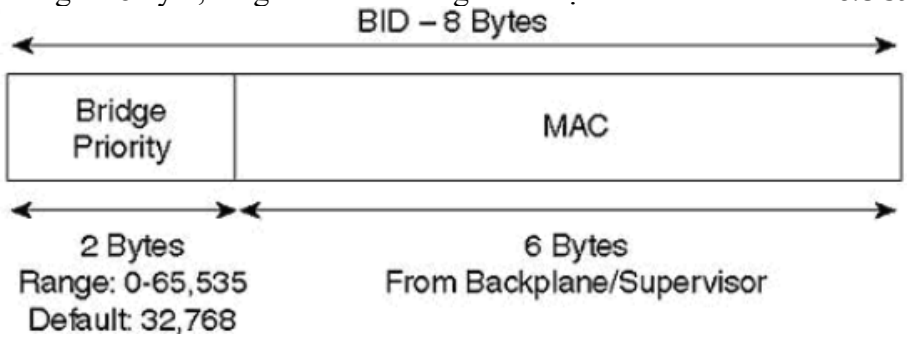
Vì frame bị lặp theo hướng ngược lại, nên ta thấy địa chỉ MAC của host A bị lẫn giữa cổng 1/1 và 1/2. Điều này không chỉ làm mạng bị tràn với các gói unicast mà còn sửa sai bảng bridge. Như vậy không chỉ có broadcast mới làm hư hại mạng.

2.2.2 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 6.8 sau:



Hình 6.8: 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 kết10BaseT 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 ngăncản 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 tínhco dãn không tuyến tính. Bảng sau cho ta một danh sách giá trị chi phí mới.

Băng thông	Chi phí STP
4 Mbps	250
10 Mbps	100
16 Mbps	624
5 Mbps	39
100 Mbps	19
155 Mbps	14
622 Mbps	6

1 Gbps	4
10 Gbps	2

Giá trị trong bảng trên 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.

2.2.3 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).

2.2.4 Sự hội tụ STP ban đầu (Initial STP Convergence)

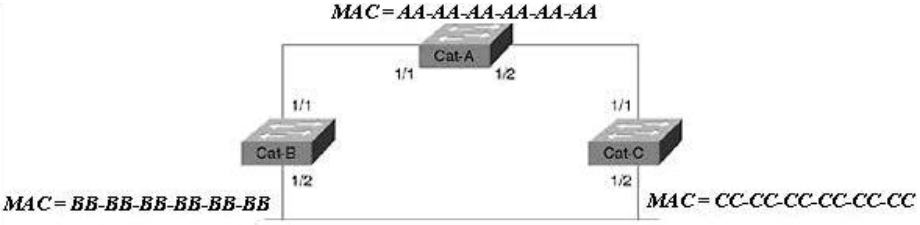
Phần này ta sẽ xem xét thuật toán mà STP sử dụng để hội tụ lần đầu tiên trên cấu trúc mạng logic chứa vòng lặp (loop-free). Mặc dù có nhiều khía cạnh STP, nhưng sự hội tụ ban đầu được phân nhỏ thành ba bước sau:

- Quyết định một bridge gốc (Root Bridge).
- Quyết định cổng gốc (Root Port).
- Quyết định cổng được chỉ định (Designated Port).

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.

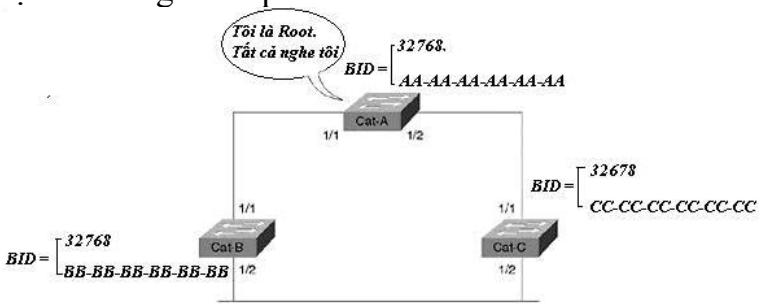
Hình 6.9 là mô hình của một mạng switch/bridge. Mạng này gồm có ba bridge kết nối thành một vòng lặp. Mỗi cầu nối được gán một địa chỉ MAC không có thật tương ứng với tên thiết bị (ví dụ như Cat-A sử dụng địa chỉ MAC là AA-AA-AA-AA-AA-AA).



Hình 6.9: mô hình mạng sử dụng STP

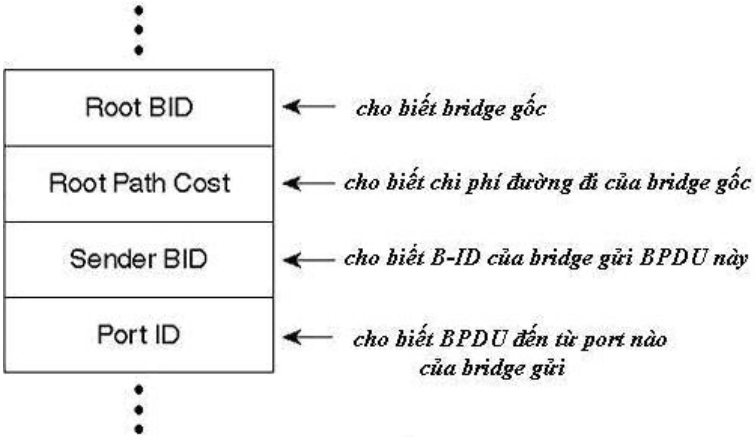
Bước 1: quyết định một bridge gốc.

- 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-AA-AA-AA-AA-AA. Cat-B là (32.768, BB-BB-BB-BB-BB-BB) và Cat-C là (32.768, CC-CC-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 6.10* mô tả quá trình này.
- ***Chú ý:*** giá trị BID cũng là thấp nhất.



Hình 6.10: chọn Bridge Root

- Nhưng làm thế nào các bridge biết được Cat-A có BID thấp nhất? Đó là do việc trao đổi các BPDU. Bridge sử dụng BPDU dành riêng để thay đổi cấu trúc mạng và thông tin Spanning Tree lẫn nhau. Các BPDU được gửi mặc định 2s một lần. Các BPDU là lưu lượng bridge-to-bridge, nó không mang lưu lượng end-to-end. *Hình 6.11* mô tả các phần cơ bản của một BPDU.

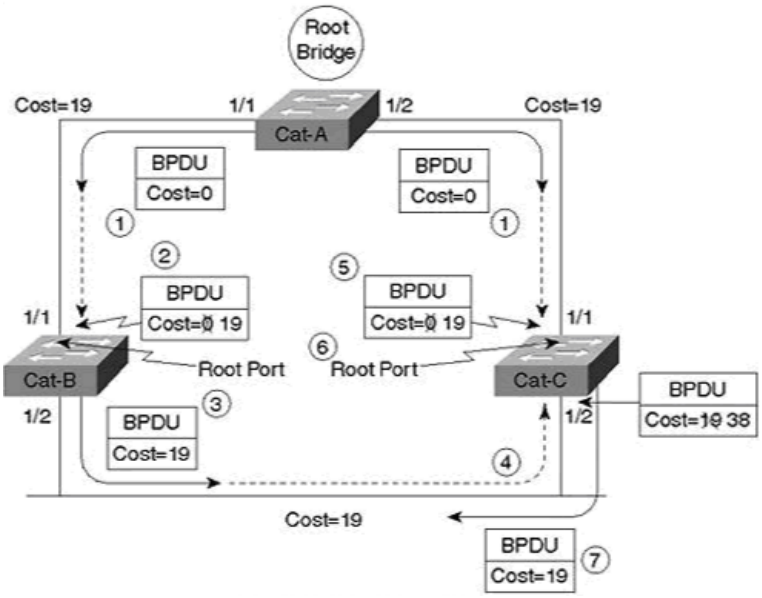


Hình 6.11: các thành phần cơ bản của BPDU

- 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 6.12* 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.



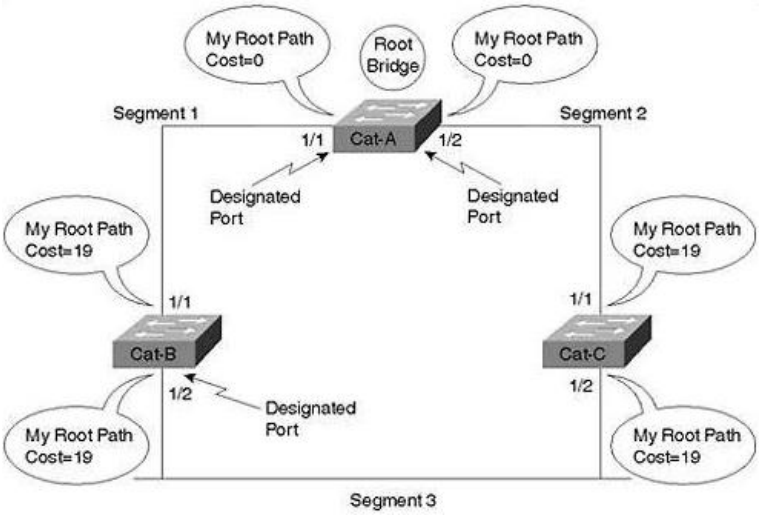
Hình 6.12 : chọn Root Port

Hình 6.12 biểu diễn Cat-B tính toán và chọn ra cổng 1/1 là cổng gốc với chi phí là 19, và chú ý là khi một cổng nhận BPDU thì chi phí sẽ tăng 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 cũng dựa trên chi phí tích lũy của đường đi gốc đến bridge gốc (*hình 6.13*).



Hình 6.13: 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 6.13*, 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.BB-BB-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

Các thành phần STP	Số
Bridge gốc	1
Cổng gốc	14
Cổng được chỉ định	146

Bảng 3.2: Các thành phần STP trong mạng có 15 switch và 146 đoạn mạng

- 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 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.

2.2.5 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	Mục đích
Chuyển tiếp (forwading)	Gửi và nhận dữ liệu người dùng
Học hỏi (learning)	Xây dựng bảng bridge

Lắng nghe (listening)	Xây dựng cấu trúc mạng "active"
Khóa (blocking)	Chỉ nhận các BPDU
Vô hiệu hóa (disable)	Các cổng bị down

Bảng 3.3: Các trạng thái của STP

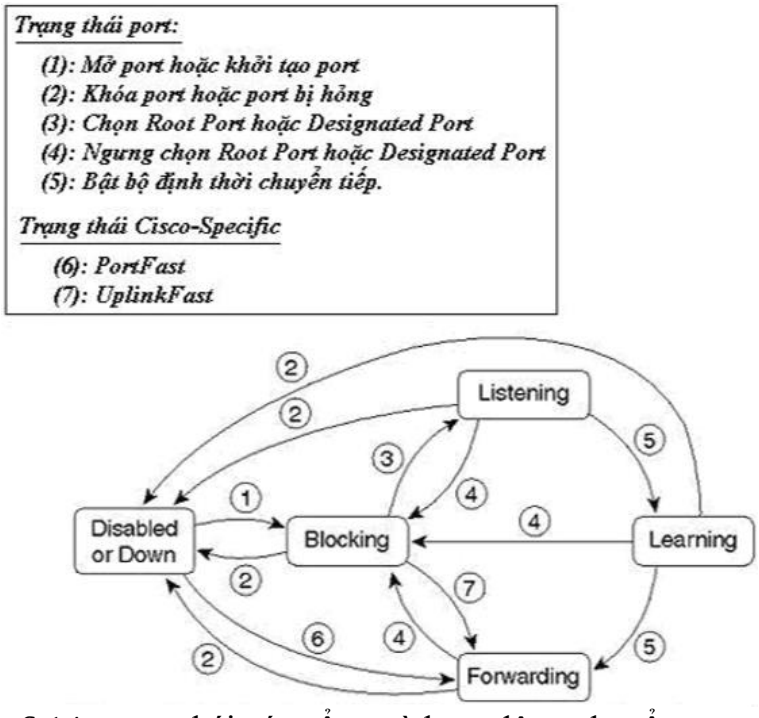
Trạng thái "disable" cho phép người quản trị mạng quản lý việc ngừng hoạt động của một cổng. Sau khi khởi tạo, các cổng bắt đầu trong trạng thái "blocking" để lắng nghe các BPDU.

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.

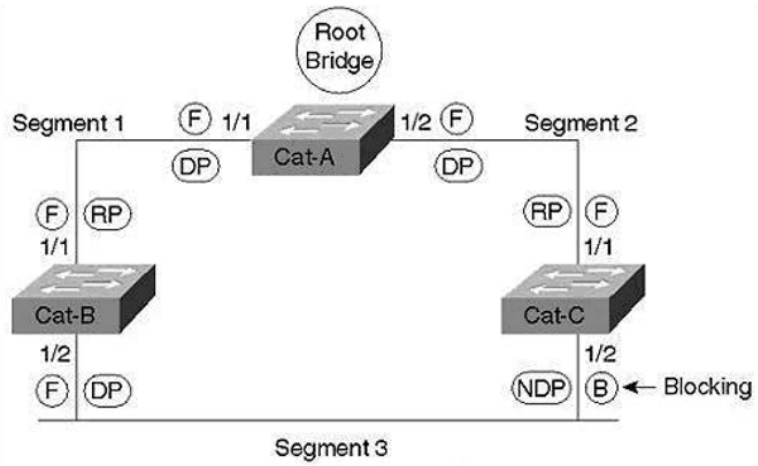
Chú ý: Trong việc lưu trữ địa chỉ MAC và thông tin cổng, các Catalyst học các thông tin như VLAN nguồn.

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 6.14* mô tả trạng thái các cổng và việc chuyển trạng thái.



Hình 6.14: trạng thái các cổng và hoạt động chuyển trạng thái

Hình 6.15 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 6.15: sơ đồ mạng với các cổng được định danh

Trạng thái/cổng	Ký hiệu
Blocking	B
Forwading	F
Cổng được chỉ định	DP
Cổng gốc	RP
Cổng không được chỉ định	NDP

Bảng 3.4 : Các trạng thái STP và các ký hiệu cổng

2.2.6 Bộ định thời gian STP

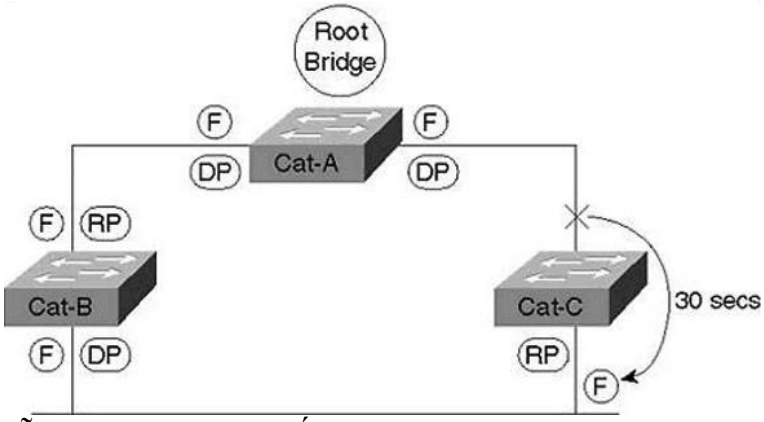
Một bridge trải qua 15s ở mỗi trạng thái "listening" và "learning". STP được điều khiển bởi ba bộ đếm thời gian (timer) như trong *bảng 3.5.*

Timer	Mục đích	Giá trị mặc định
Hello Timer	Khoảng thời gian gửi các BPDU cấu hình gửi bởi Bridge gốc	2s
Forward Delay	Thời hạn ở trạng thái Listening và Learning	15s
Max Age	Thời gian lưu trữ BPDU	20s

Bảng 3.5: STP Timer

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 6.16*.



Hình 6.16: 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 là từ 30s đến 50s.

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

Thứ nhất: không thay đổi giá trị thời gian mặc định khi không có sự cân nhắc cẩn thận.

Thứ hai: ta chỉ được sửa thời gian từ bridge gốc.

2.2.7 Hai loại BPDU

Có hai loại BPDU là :

- BPDU cấu hình.

+ BPDU thông báo 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 : c***ác trường trong BPDU cấu hình được tóm tắt trong *bảng 3.6*

Trường	Chiều dài (octet)	Ý nghĩa
Protocol ID	2	Luôn bằng 0
Version	1	Luôn bằng 0
Type	1	Cho biết kiểu BPDU BPDU cấu hình = 0
Flag	1	LSB = Cờ thay đổi cấu trúc mạng MSB = Cờ xác nhận thay đổi cấu trúc mạng
Root ID	8	BID của bridge gốc hiện tại
Root Path Cost (chi phí đường đi gốc)	4	Chi phí tích lũy đến bridge gốc

Trường	Chiều dài (octet)	Ý nghĩa
Sender BID	8	BID của bridge hiện tại
Cổng ID	2	ID của cổng gửi BPDU này
Message Age	2	Khoảng thời gian tử khi bridge gốc tạo BPDU đến khi phát BPDU đi.
Max Age	2	Khoảng thời gian lưu thông tin BPDU
Hello Time	2	Khoảng thời gian giữa các BPDU
Forward Delay	2	Thời gian trong trạng thái listening và learning
Bảng 3.6 : Các trường trong BPDU cấu hình		

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.

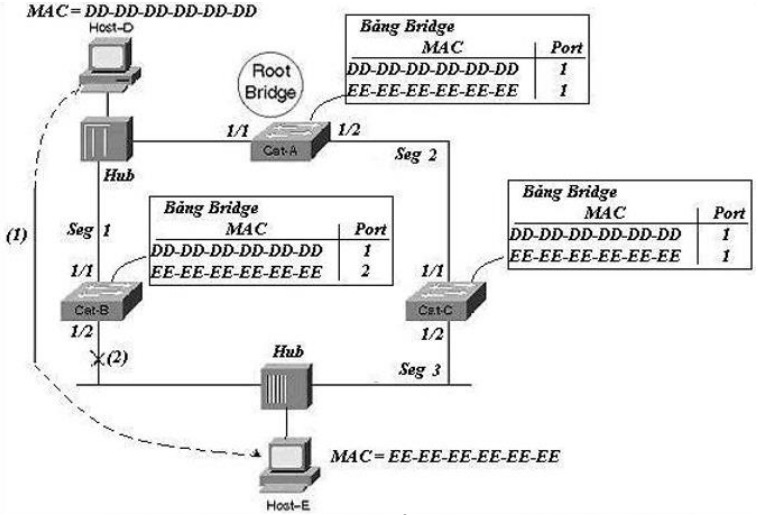
2.2.8 Quá trình thay đổi cấu trúc mạng

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 6.17*.

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.



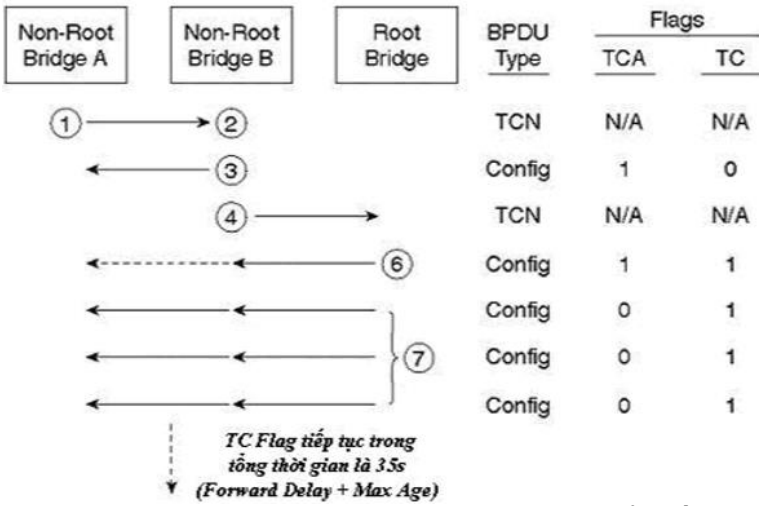
Hình 6.17: TCN BPDU được dùng để cập nhật bảng Bridge nhanh hơn

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.

Bảng Bridge	Cổng liên quan đến địa chỉ MAC của host E
Cat-A	Cổng 1/1
Cat-B	Cổng 1/2
Cat-C	Cổng 1/1

Bảng 3.7: Giá trị bảng Bridge trước khi có sự thay đổi cấu trúc mạng

- 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:
- 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.
- 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.
- 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.
- Bridge upstream sẽ truyền TCN BPDU ra cổng gốc của nó.
- Tiếp tục bước 2 đến bước 4 cho đến khi bridge gốc nhận TCN BPDU.
- 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.
- 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 6.18: trình tự các bước trong quá trình thay đổi cấu trúc mạng

Dựa vào *hình 6.18* ta có thể biết được quá trình thay đổi cấu trúc mạng cho *hình 6.17* 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 EE-EE-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.

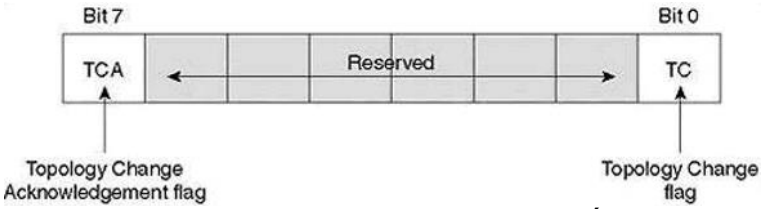
Bảng 3.8 biểu diễn toàn bộ bảng bridge cho địa chỉ MAC của E trên cả ba switch sau khi cấu trúc mạng mới hội tụ và lưu lượng lại tiếp tục.

Bảng Bridge	Cổng liên quan đến địa chỉ MAC của host E
Cat-A	Cổng 1/2
Cat-B	Cổng 1/1
Cat-C	Cổng ½

Bảng 3.8: Giá trị bảng Bridge sau khi thay đổi cấu trúc mạng

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 6.19 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.



Hình 6.19: trường cờ trong BPDU cấu hình

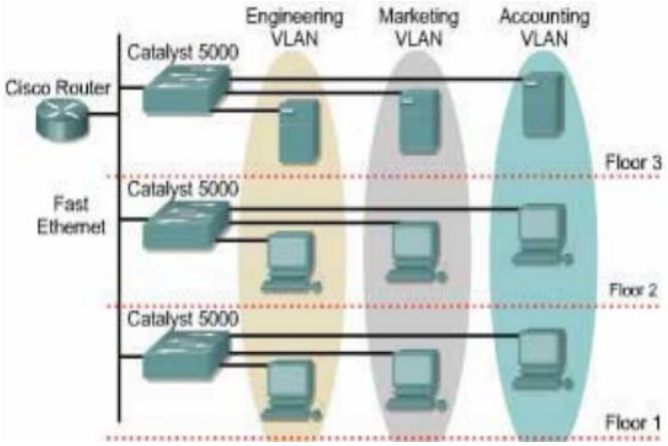
Như vậy, cờ TCN được thiết lập bởi bridge upstream để nói cho các bridge dowstream ngưng gửi TCN BPDU. Còn cờ TC được thiết lập bởi bridge gốc để giảm khoảng thời gian lỗi từ 300s xuống 15s (Forward Delay).

2.3 Định tuyến giữa các VLAN

VLAN là viết tắt của Virtual Local Area Network hay còn gọi là mạng LAN ảo. VLAN là một kỹ thuật cho phép tạo lập các mạng LAN độc lập một cách logic trên cùng một kiến trúc hạ tầng vật lý. Việc tạo lập nhiều mạng LAN ảo trong cùng một mạng cục bộ (giữa các khoa trong một trường học, giữa các cục trong một công ty,...) giúp giảm thiểu vùng quảng bá (broadcast domain) cũng như tạo thuận lợi cho việc quản lý một mạng cục bộ rộng lớn. Với mạng LAN thông thường, các máy tính trong cùng một địa điểm (cùng phòng...) có thể được kết nối với nhau thành một mạng LAN, chỉ sử dụng một thiết bị tập trung như hub hoặc switch. Có nhiều mạng LAN khác nhau cần rất nhiều bộ hub, swich. Tuy nhiên thực tế số lượng máy tính trong một LAN thường không nhiều, ngoài ra nhiều máy tính cùng một địa điểm (cùng phòng) có thể thuộc nhiều LAN khác nhau vì vậy càng tốn nhiều bộ hub, switch khác nhau. Do đó vừa tốn tài nguyên số lượng hub, switch và lãng

phí số lượng port Ethernet. Với nhu cầu tiết kiệm tài nguyên, đồng thời đáp ứng nhu cầu sử dụng nhiều LAN trong cùng một địa điểm, giải pháp đưa ra là nhóm các máy tính thuộc các LAN khác nhau vào cùng một bộ tập trung switch. Giải pháp này gọi là mạng LAN ảo hay VLAN

Hiện nay, VLAN đóng một vai trò rất quan trọng trong công nghệ mạng LAN. Để thấy rõ được lợi ích của VLAN, chúng ta hãy xét trường hợp sau : Giả sử một công ty có 3 bộ phận là: Engineering, Marketing, Accounting, mỗi bộ phận trên lại trải ra trên 3 tầng. Để kết nối các máy tính trong một bộ phận với nhau thì ta có thể lắp cho mỗi tầng một switch. Điều đó có nghĩa là mỗi tầng phải dùng 3 switch cho 3 bộ phận, nên để kết nối 3 tầng trong công ty cần phải dùng tới 9 switch. Rõ ràng cách làm trên là rất tốn kém mà lại không thể tận dụng được hết số cổng (port) vốn có của một switch. Chính vì lẽ đó, giải pháp VLAN ra đời nhằm giải quyết vấn đề trên một cách đơn giản mà vẫn tiết kiệm được tài nguyên.



Hình 6.20 Mô hình mạng của một công ty

Như hình trên ta thấy mỗi tầng của công ty chỉ cần dùng một switch, và switch này được chia VLAN. Các máy tính ở bộ phận kỹ sư (Engineering) thì sẽ được gán vào VLAN Engineering, các PC ở các bộ phận khác cũng được gán vào các VLAN tương ứng là Marketing và kế toán (Accounting). Cách làm trên giúp ta có thể tiết kiệm tối đa số switch phải sử dụng đồng thời tận dụng được hết số cổng (port) sẵn có của switch.

Có 3 loại VLAN, bao gồm:

- VLAN dựa trên cổng (port based VLAN): Mỗi cổng (Ethernet hoặc Fast Ethernet) được gắn với một VLAN xác định. Do đó mỗi máy tính/thiết bị host kết nối với một cổng của switch đều thuộc một VLAN nào đó. Đây là cách cấu hình VLAN đơn giản và phổ biến nhất.
- VLAN dựa trên địa chỉ vật lý MAC (MAC address based VLAN): Mỗi địa chỉ MAC được gán tới một VLAN nhất định. Cách cấu hình này rất phức tạp và khó khăn trong việc quản lý.
- VLAN dựa trên giao thức (protocol based VLAN): tương tự với VLAN dựa trên địa chỉ MAC nhưng sử dụng địa chỉ IP thay cho địa chỉ MAC. Cách cấu hình này không được thông dụng.

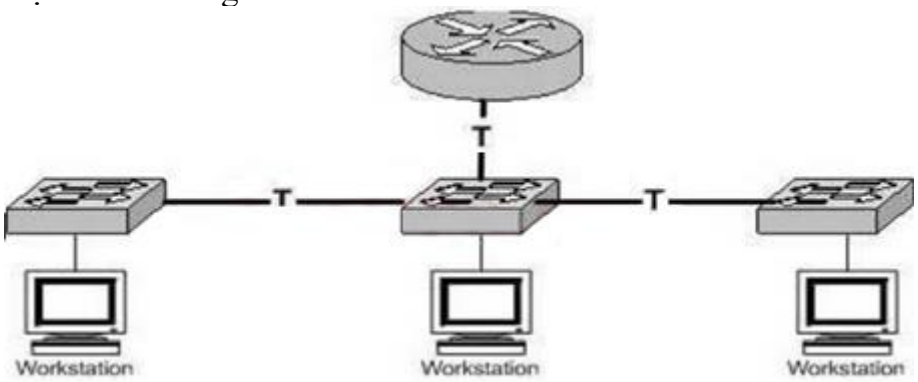
Ưu điểm của VLAN:

- Tiết kiệm băng thông của hệ thống mạng: VLAN chia mạng LAN thành nhiều đoạn (segment) nhỏ, mỗi đoạn đó là một vùng quảng bá (broadcast domain). Khi có gói tin quảng bá (broadcast), nó sẽ được truyền duy nhất trong VLAN tương ứng. Do đó việc chia VLAN giúp tiết kiệm băng thông của hệ thống mạng.

- Tăng khả năng bảo mật: Do các thiết bị ở các VLAN khác nhau không thể truy nhập vào nhau (trừ khi ta sử dụng router nối giữa các VLAN). Như trong ví dụ trên, các máy tính trong VLAN kế toán (Accounting) chỉ có thể liên lạc được với nhau. Máy ở VLAN kế toán không thể kết nối được với máy tính ở VLAN kỹ sư (Engineering).
- Dễ dàng thêm hay bớt máy tính vào VLAN: Việc thêm một máy tính vào VLAN rất đơn giản, chỉ cần cấu hình cổng cho máy đó vào VLAN mong muốn.
- Giúp mạng có tính linh động cao: VLAN có thể dễ dàng di chuyển các thiết bị. Giả sử trong ví dụ trên, sau một thời gian sử dụng công ty quyết định để mỗi bộ phận ở một tầng riêng biệt. Với VLAN, ta chỉ cần cấu hình lại các cổng switch rồi đặt chúng vào các VLAN theo yêu cầu. VLAN có thể được cấu hình tĩnh hay động. Trong cấu hình tĩnh, người quản trị mạng phải cấu hình cho từng cổng của mỗi switch. Sau đó, gán cho nó vào một VLAN nào đó. Trong cấu hình động mỗi cổng của switch có thể tự cấu hình VLAN cho mình dựa vào địa chỉ MAC của thiết bị được kết nối vào.

Cấu trúc hoạt động của VLAN:

- Cấu trúc của một mạng các VLAN gồm 3 tầng thiết bị như hình dưới.
  + Tầng 1: là Router làm nhiệm vụ định tuyến giữa các VLAN
  + Tầng 2: là các switch. Trên các cổng của mỗi switch chia thành các VLAN
  + Tầng 3: là các workstation
  + Ký hiệu T: là đường Trunk



Hình 6.21 Mô hình cấu trúc tổng thể VLAN

Cách thức tạo lập VLAN

- Mỗi một cổng trên switch có thể chia cho một VLAN. Những cổng được chia sẻ cho cùng một VLAN thì chia sẻ broadcast. Cổng nào không thuộc VLAN thì sẽ không chia sẻ broadcast. Những cải tiến của VLAN là làm giảm bớt broadcast và sự lãng phí băng thông.
- Có 2 phương thức để tạo lập VLAN:
  + VLAN tĩnh (Static VLAN)
  + VLAN động (Dynamic VLAN)

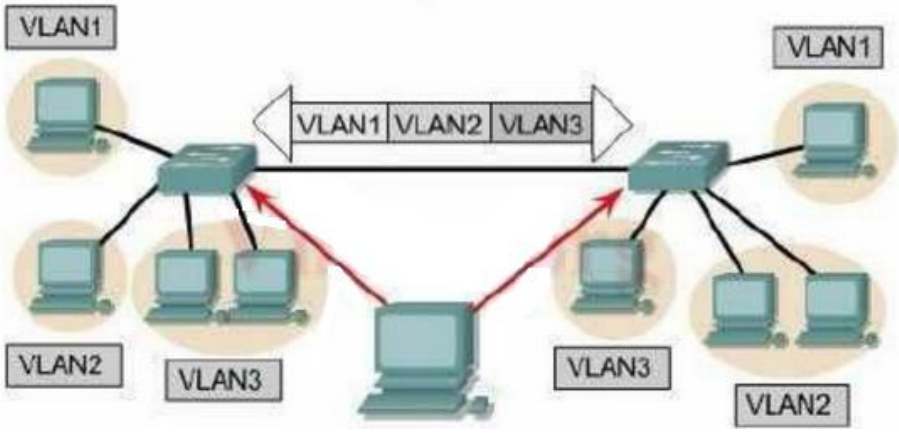
Static VLAN:

- Phương thức này được ám chỉ như là port-base membership. Việc gán các cổng switch vào một VLAN là đã tạo một static VLAN. Giống như một thiết bị được kết nối vào mạng, nó tự động thừa nhận VLAN của cổng đó. Nếu user thay đổi các cổng và cần truy cập vào cùng một VLAN, thì người quản trị mạng cần phải khai báo cổng tới VLAN cho kết nối tới.

Dynamic VLAN:

- VLAN được tạo thông qua việc sử dụng các phần mềm như Ciscowork 2000. Với một VMPS (VLAN Management Policy Server) có thể đăng ký các cổng cuả switch vào các VLAN một cách tự động dựa trên địa chỉ MAC nguồn của thiết bị được nối vào cổng. Dynamic VLAN hiện thời tính đến thành viên của nó dựa trên địa chỉ MAC của thiết bị.

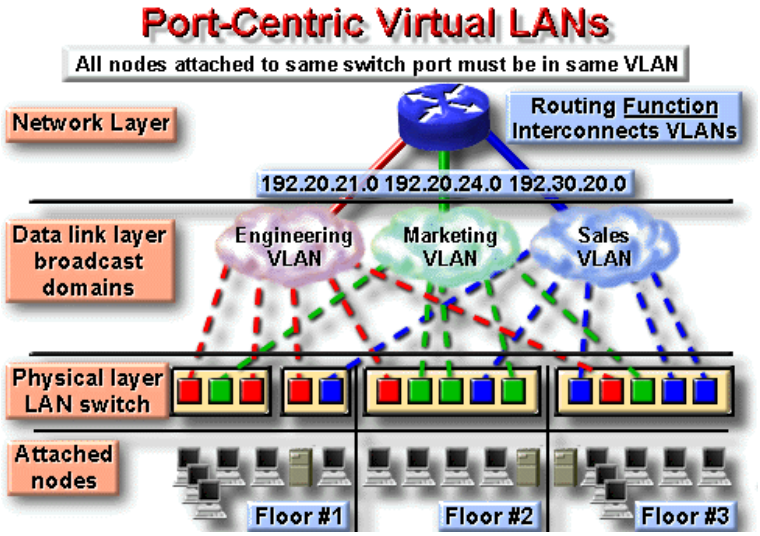
Như mộ thiết bị trong mạng, nó truy vấn một cơ sở dữ liệu trên VMPS của các VLAN thành viên



Hình 6.22 Mô hình VLAN

- Trên switch cổng được gán cho một VLAN cụ thể thì độc lập với user hoặc hệ thống gắn với cổng đó. Điều đó có nghĩa là tất cả các user nằm trên các cổng nên là thành viên của cùng một VLAN. Một workstation hay một HUB có thể kết nối vào một cổng VLAN.
- Người quản trị mạng thực hiện gán các VLAN. Cổng mà được cấu hình là Static thì không thể thay đổi một cách tự động được tới VLAN khác khi mà cấu hình lại switch. Khi các user gắn với cùng một phân đoạn mạng chia sẻ, tất cả các user đó cùng chia sẻ băng thông của phân đoạn mạng. Mỗi một user được gắn vào môi trường chia sẻ, thì sẽ có ít băng thông sẵn có cho mỗi user, bởi vì tất cả các user đầu nằn trên một miền xung đột.
- Nếu chia sẻ trở nên quá lớn, xung đột có thể sảy ra quá mức và các trình ứng dụng có thể bị mất chất lượng. Các switch làm giảm xung đột bằng cách cung cấp băng thông giữa các thiết bị sử dụng Micro segmentation (Vi phân đoạn), tuy nhiên các switch chỉ chuyển các gói tin dạng ARP (Address Resolution Protocol – Giao thức độ phân giải địa chỉ).
- VLAN đưa ra nhiều băng thông hơn cho user trong một mạng chia sẻ bằng cách hạn chế miền quảng bá cụ thể. VLAN mặc định cho tất cả các cổng trên switch là VLAN1 hoặc là management VLAN. VLAN mặc định không thể xoá, tuy nhiên các VLAN thêm vào có thể tạo ra và các cổng có thể gán lại tới các VLAN sen kẽ. Mỗi một cổng giao diện trên switch giống như cổng của bridge và switch đơn giản là một bridge nhiều cổng. Các bridge lọc tải mạng mà không cần quan tâm đến phân đoạn mạng nguồn mà chỉ cần quan tâm đến phân đoạn mạng đích. Nếu một frame cần chuyển qua bridge, và địa chỉ MAC đích là biết được, thì bridge sẽ chuyển frame tới cổng giao diện chính xác. Nếu bridge hoặc switch không biết được đích đến, nó sẽ chuyển gói tin qua tất cả các cổng trong vùng quản bá (VLAN) trừ cổng nguồn. Mỗi một VLAN nên có một địa chỉ lớp 3 duy nhất hoặc địa chỉ subnet đươc đăng ký. Điều đó giúp Router chuyển mạch gói giữa các VLAN.
- Các VLAN có thể tồn tại như các mạng End–to-end (Từ đầu cuối đến đầu cuối).

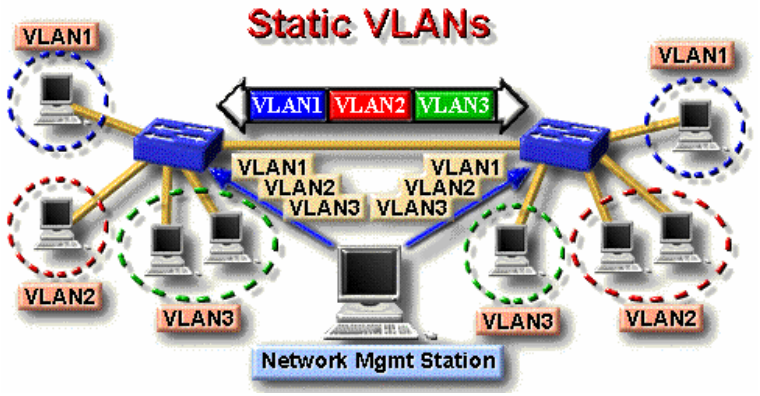
Mô hình cài đặt VLAN dựa trên cổng:



Hình 6.23 Mô hình VLAN

- Trong sơ đồ này, các nút nối cùng một cổng của switch thuộc về cùng một VLAN. Mô hình này tăng cường tối đa hiệu suất của chuyển tải thông tin bởi vì:
- Người sử dụng được gán dựa trên cổng
- VLANs được quản lý một cách dễ dàng
- Tăng cường tối đa tính an toàn của VLAN
- Các gói tin không rò rỉ sang các vùng khác
- VLANs và các thành phần được điều khiển một cách dễ dàng trên toàn mạng.

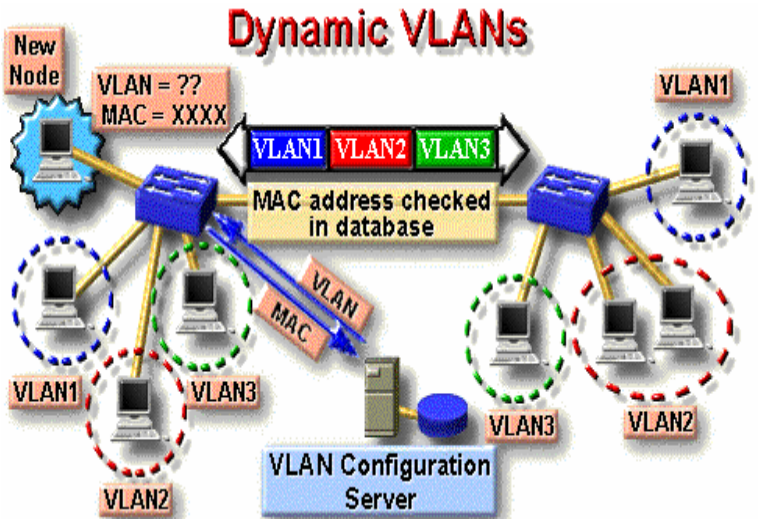
Mô hình cài đặt VLAN tĩnh:



Hình 6.24 Mô hình VLAN

- VLAN tĩnh là một nhóm cổng trên một switch mà nhà quản trị mạng gán nó vào một VLAN. Các cổng này sẽ thuộc về VLAN mà nó đã được gán cho đến khi nhà quản trị thay đổi.
- Kiểu VLAN này thường hoạt động tốt trong những mạng mà ở đó những sự di dời được điều khiển và được quản lý.

Mô hình cài đặt VLAN động :

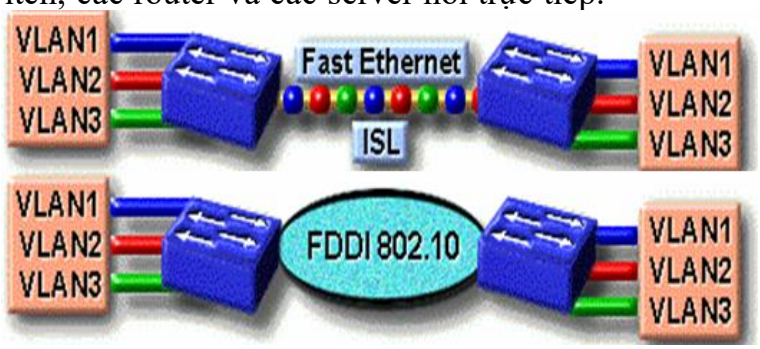


Hình 6.25 Mô hình VLAN

- VLAN động là nhóm các cổng trên một switch mà chúng có thể xác định một các tự động việc gán VLAN cho chúng. Hầu hết các nhà sản xuất switch đều sử dụng phần mềm quản lý thông minh.
- Sự vận hành của các VLAN động được dựa trên địa chỉ vật lý MAC, địa chỉ luận lý hay kiểu giao thức của gói tin.
- Khi một trạm được nối kết lần đầu tiên vào một cổng của switch, switch tương ứng sẽ kiểm tra mục từ chứa địa chỉ MAC trong cơ sở dữ liệu quản trị VLAN và tự động cấu hình cổng này vào VLAN tương ứng.
- Thông thường, cần nhiều sự quản trị trước để thiết lập cơ sở dữ liệu bằng phần mềm quản trị VLAN và duy trì một cơ sở dữ liệu chính xác về tất cả các máy tính trên toàn mạng.

Mô hình thiết kế VLAN với mạng đường trục:

- Đường trục thông thường hoạt động như là một điểm tập hợp của nhiều lượng thông tin lớn. Nó có thể mang thông tin về những người dùng cuối trong VLAN và nhận dạng giữa các switch, các router và các server nối trực tiếp.



Hình 6.26 Mô hình VLAN

Các bước cấu hình một VLAN:

- Tùy vào các SWITCH khác nhau trong một hãng hay khác hãng sản xuất mà có một cách cấu hình khác nhau. Giáo trình này đưa ra một cách khái quát các bước cấu hình một VLAN:
- Bước 1: Cấu hình Switch:
  + Vào mức cấu hình
  + Cấu hình tên Switch
  + Cấu hình password enable
  + Cấu hình Authentication

+ Cấu hình cho phép **telnet** và **console** cùng với các chính sách bảo mật cho **telne**t và **console**
+ Cấu hình VLAN cho Switch (optional)
+ Cấu hình enterface hoạt động ở trunk interface
+ Cấu hình **routing** cho VLANs (optional)
+ Cấu hình địa chỉ **IP** cho các VLAN
+ Cấu hính **SNMP** phục vụ cho nhu cầu quản trị
+ Kết thúc cấu hình

- **Bước 2:** Cấu hình VTP
- Bước 3: Cấu hình VLANs
- Bước 4: Định tuyến giữa các VLAN
  + Ngoài ra còn có thể cấu hình tham khảo như:
  + Cấu hình Port Security
  + Cấu hình **PortFast**
  + Cấu hình UplinkFast
  + Cấu hình BackboneFast

2.4 Triển khai VTP

2.4.1 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.

2.4.2 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 dóng gói trong một chi\uẩn CISCO là giao thức ISL hoặc IEEE 802.1q và sau đó đi qua các liên kết Trunk tới thiết bị khác.

2.4.3 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 thống 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

2.4.4 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. Đóng gói TVP với ISL Frame:

[IMG]file:///C:/DOCUME%7E1/TRANMY%7E1.000/LOCALS%7E1/Temp/msohtml1/01/clip_image002.jpg[/IMG]

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

2.4.5 Các chế độ VTP

Hoạt động chuyển mạch VTP hoạt động trên một trong ba chế độ sau: Server, Client, Transparent

2.4.5.1 VTP Server (Chế độ mặc định)

- 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.

2.4.5.2 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.

2.4.5.3 Chế độ VTP trong suốt (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.

2.4.6 Cấu hình VTP

Cấu hình phiên bản VTP

- Switch_A# vlan database
- Switch_A(vlan)# vtp v2-mode

Cấu hình VTP domain

- Switch_A(vlan)# vtp domain Cisco

Cấu hình chế độ VTP

- Switch_A(vlan)# vtp [client|server|transparent]

Lệnh xem cấu hình VTP

- Switch_A# show vtp status

2.5 Triển khai OSPF

Giao thức Open Shortest Path First (OSPF) được định nghĩa trong RFC 2328, là một giao thức định tuyến trong (IGP) được sử dụng để phân phối thông tin định tuyến trong một AS (Autonomous System). Bài viết này xem xét cách OSPF hoạt động và cách nó có thể được sử dụng để thiết kế và xây dựng đường đi lớn và phức tạp.

Giao thức OSPF được phát triển do nhu cầu trong cộng đồng Internet. Cuộc thảo luận về việc tạo ra một IGP tương thích chung cho Internet bắt đầu từ năm 1988 và không được chính thức hóa cho đến năm 1991. Vào thời điểm đó, nhóm làm việc OSPF đã yêu cầu OSPF được xem xét để tiến tới Dự thảo Tiêu chuẩn Internet.

Giao thức OSPF dựa trên công nghệ trạng thái đường link (link-state). OSPF đã giới thiệu các khái niệm mới như xác thực các cập nhật định tuyến (routing updates), Variable Length Subnet Masks (VLSM), route summarization,...

Ưu điểm của OSPF

- Không giới hạn hop count trong hệ thống mạng
- Hỗ trợ VLSM

OSPF sử dụng gói tin multicast để gửi cập nhật trạng thái đường link. Cập nhật chỉ được gửi trong trường hợp có thay đổi định tuyến xảy ra thay vì cập nhật định kỳ. Điều này đảm bảo sử dụng băng thông tốt hơn

Bảng định tuyến hội tụ nhanh do các thay đổi định tuyến được lan truyền tức thời và không theo định kỳ

OSPF cho phép load balancing

- OSPF là link-states protocol. Chúng ta có thể nghĩ một liên kết là một interface trên Router. Trạng thái liên kết mô tả về interface đó và mối quan hệ của nó với các router lân cận. Mô tả về interface sẽ bao gồm: địa chỉ IP của interface, mask, loại mạng được kết nối, các router được kết nối với mạng đó,... Tập hợp tất cả các trạng thái liên kết này sẽ tạo thành một cơ sở dữ liệu trạng thái liên kết.

Thuật toán Shortest Path First:

- OSPF sử dụng thuật toán Shortest Path First (Dijkstra) để xây dựng và tính toán đường đi ngắn nhất tới mạng đích. Đây là thuật toán khá phức tạp, cách đơn giản để xem xét các bước khác nhau của thuật toán:

+ Khi khởi tạo hoặc do bất kỳ thay đổi nào trong thông tin định tuyến, router sẽ tạo quảng bá trạng thái liên kết. Quảng bá này đại diện cho tập hợp tất cả các trạng thái liên kết trên router đó.

+ Tất cả các router trao đổi trạng thái liên kết bằng cách lũ lụt (flooding). Mỗi Router nhận được cập nhật trạng thái liên kết nên lưu trữ một bản sao trong cơ sở dữ liệu trạng thái liên kết của nó và sau đó truyền bản cập nhật đến các router khác.

+ Sau khi cơ sở dữ liệu của mỗi router hoàn tất, nó sẽ tính toán đường dẫn ngắn nhất đến tất cả các đích. Router sử dụng thuật toán Dijkstra để tính toán đường đi ngắn nhất. Các điểm đến, chi phí liên quan và bước nhảy tiếp theo để đến các điểm đến đó tạo thành bảng định tuyến

+ Trong trường hợp không có thay đổi nào trong mạng OSPF xảy ra, chẳng hạn như chi phí của một liên kết hoặc một mạng được thêm hoặc xóa, OSPF rất yên tĩnh. Mọi thay đổi xảy ra đều được truyền đạt thông qua các trạng thái liên kết và thuật toán Dijkstra được tính toán lại để tìm ra con đường ngắn nhất.

OSPF Cost

- Cost (còn gọi là metric) của một interface trong OSPF cho thấy chi phí cần thiết để gửi các gói tin qua một interface nhất định. Cost của một interface tỷ lệ nghịch với băng thông của interface đó. Băng thông càng cao cost càng thấp. Công thức được sử dụng để tính chi phí là:
- Cost = 100 000 000/bandwith (bps)
- Theo mặc định, cost của một interface được tính dựa trên băng thông; bạn có thể điều chỉnh cost của một interface bằng lệnh **ip ospf cost**

Area và Border Routers

- Như đã đề cập trước đây, OSPF sử dụng lũ lụt để trao đổi các cập nhật trạng thái liên kết giữa các router. Mọi thay đổi trong thông tin định tuyến đều tràn vào tất cả các Router trong mạng. Các Area được giới thiệu để đặt một ranh giới về sự bùng nổ của các cập nhật trạng thái liên kết. Ngập lụt và tính toán thuật toán Dijkstra trên router bị giới hạn trong một Area. Tất cả các router trong một area có cơ sở dữ liệu trạng thái liên kết chính xác. Router có thể thuộc nhiều area và kết nối các area này với backbone area (vùng xương sống) được gọi là Router biên (Area Border Routers - ABR). Do đó, ABR phải duy trì thông tin giữa backbone area và các Area kèm theo khác.
- Mỗi interface là một area cụ thể. Một router có tất cả các interface của nó trong cùng một area được gọi là bộ định tuyến bên trong (Internal Router - IR). Một router có các interface khác nhau nằm trong nhiều area khác nhau được gọi là bộ định tuyến biên khu vực (Area Border Routers - ABR). Router đóng vai trò là gateway (redistribution) giữa OSPF và các giao thức định tuyến khác (IGRP, EIGRP, IS-IS, RIP, BGP, static route) hoặc các tiến trình khác của giao thức định tuyến OSPF được gọi là bộ định tuyến ranh giới hệ thống tự trị (ASBR). Bất kỳ router nào cũng có thể là ABR hoặc ASBR.

Cấu hình OSPF trên Router

- Làm theo 2 bước sau đây để cấu hình OSPF:
  + 1. Enable OSPF bằng câu lệnh sau: ***router ospf***
  + 2. Chỉ định các Area cho các interface trên router: **network**
- OSPF process-id là một giá trị số cục bộ cho router. Không cần phải khớp process-id trên các router kkháy. Có thể chạy nhiều tiến trình OSPF trên cùng một router, nhưng

không được khuyến khích vì nó tạo ra nhiều phiên bản cơ sở dữ liệu có thêm chi phí phụ cho router.

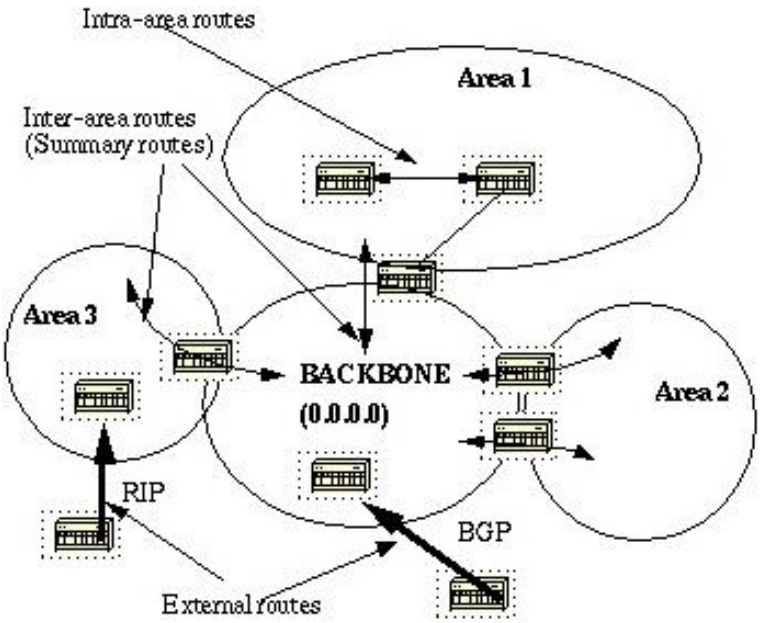
- Câu lệnh “network” dùng để gán interface cho một area nhất định. “mask” được sử dụng như một phím tắt và nó giúp đưa một danh sách các địa chỉ IP vào cùng một area. Nó chứa các bit 0 và 1 trong đó 0 là ”khớp” và 1 là bit "không quan tâm", ví dụ: 0.0.255.255 chỉ ra sự trùng khớp trong hai byte đầu tiên của mạng.
- Area-id là số vùng mà interface thuộc về. Area-id có thể là một số nguyên trong khoảng từ 0 đến 4294967295 hoặc có thể có dạng tương tự như địa chỉ IP A.B.C.D.

Xác thực OSPF

- Có thể xác thực các gói OSPF sao cho các router có thể tham gia vào các miền định tuyến dựa trên mật khẩu được xác định trước. Theo mặc định, router không sử dụng xác thực, có nghĩa là việc định tuyến trao đổi qua mạng không được xác thực. Hai phương thức xác thực khác tồn tại: Xác thực mật khẩu đơn giản (key) và xác thực Message Digest (MD-5).
- 1. Xác thực mật khẩu đơn giản (Simple password Authentication):
  + Xác thực mật khẩu đơn giản cho phép mật khẩu (key) được cấu hình cho mỗi khu vực. Router trong cùng area muốn tham gia vào miền định tuyến sẽ phải được cấu hình với cùng một khóa. Hạn chế của phương pháp này là nó dễ bị tấn công thụ động. Bất cứ ai có bộ phân tích liên kết đều có thể dễ dàng lấy mật khẩu. Để kích hoạt xác thực mật khẩu, hãy sử dụng các lệnh sau:
  + **Ip ospf authentication-key** key (cấu hình trong interface cụ thể)
  + **Area** area-id a**uthentication** (cấu hình trong “**router ospf** process-id”)
- 2. Xác thực Message Digest (MD-5):
  + Xác thực Message Digest là một xác thực mật mã. Một key (password) và key-id được cấu hình trên mỗi router. Router sử dụng thuật toán dựa trên gói OSPF, key và key-id để tạo " message digest " được gắn vào gói tin. Không giống như xác thực đơn giản, key không được trao đổi qua dây. Số thứ tự không giảm cũng được bao gồm trong mỗi gói OSPF để bảo vệ chống lại các cuộc tấn công phát lại.
- Phương pháp này cũng cho phép chuyển tiếp không bị gián đoạn giữa các phím. Điều này hữu ích cho các quản trị viên muốn thay đổi mật khẩu OSPF mà không làm gián đoạn liên lạc. Nếu một interface được cấu hình với một key mới, router sẽ gửi nhiều bản sao của cùng một gói tin, mỗi bản được xác thực bởi các khóa khác nhau. Router sẽ ngừng gửi các gói trùng lặp một khi nó phát hiện ra rằng tất cả các router neighbors đã chấp nhận key mới. Sau đây là các lệnh được sử dụng để xác thực:
  + **Ip ospf message-digest-key** key-id **md5** password (cấu hình trong interface cụ thể)
  + Area area-id authentication message-digest (cấu hình trong “router ospf process-id”)

Area backbone (area 0)

- OSPF có những hạn chế đặc biệt. Nếu có nhiều hơn một area được cấu hình, một trong những area này phải là area 0 hay còn gọi là backbone area (vùng xương sống). Khi thiết kế một hệ thống mạng, nên bắt đầu với area 0 và sau đó mở rộng sang các area khác. Backbone area phải là trung tâm của tất cả các area khác, tức là tất cả các area phải được kết nối vật lý với backbone area. Tất cả các area sẽ đưa thông tin định tuyến vào vùng backbone và tại đây nó sẽ phổ biến thông tin đó sang các area khác. Sơ đồ sau đây sẽ minh họa luồng thông tin trong mạng OSPF:



Hình 6.27 Triển khải OSPF

Trong sơ đồ trên, tất cả các area được kết nối trực tiếp với backbone. Trong một số tình huống khi một area mới được tạo ra mà không thể có kết nối vật lý trực tiếp vào backbone, một liên kết ảo (virtual link) sẽ phải được cấu hình. Các tuyến đường được tạo từ một area (đích đến thuộc area) được gọi là các tuyến nội bộ (intra-area). Các tuyến này thường được biểu thị bằng chữ **O** trong bảng định tuyến. Các tuyến có nguồn gốc từ các area khác được gọi là các tuyến liên vùng (inter-area) hoặc summary routers. Ký hiệu cho các tuyến này là **O IA** trong bảng định tuyến. Các tuyến đường bắt nguồn từ các giao thức định tuyến khác (hoặc các tiến trình OSPF khác nhau) và được đưa vào OSPF thông qua redistribution lại được gọi là các tuyến bên ngoài (external routes). Các tuyến này được biểu thị bằng **O E1** hoặc **O E2** trong bảng định tuyến. Nhiều tuyến đường đến cùng một đích được ưu tiên theo thứ tự sau: intra-area, inter-area, external E1, external E2.

2.6 Chẩn đoán và xử lý lỗi OSPF

Xử lý khi OSPF Neighbor bị mắc kẹt EXSTART/EXCHANGE

Các nguyên nhân phổ biến nhất có thể của vấn đề này như sau:

- Không phù hợp interface MTU
- Bản sao ID bộ định tuyến hàng xóm
- Không có khả năng ping qua với hơn một số kích thước MTU
- Bị phá vỡ kết nối unicast vì những điều sau đây:
  + Sai VC/DLCI lập bản đồ trong Frame Relay/ATM switch
  + Danh sách truy cập chặn unicast
  + NAT chuyển đổi unicast
  + Loại mạng lưới point-to-point giữa PRI and BRI/dialer
- Ví dụ: Show cấu hình
  + R2#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
131.108.2.1	1	EXSTART/-	00:00:33	131.108.1.1	Serial0

2.6.1. Không phù hợp interface MTU

Ví dụ: Khi cấu hình

```
R1#show ip interface serial 0.1
   Serial0.1 is up, line protocol is up
   Internet address is 131.108.1.1/24
```

Broadcast address is 255.255.255.255
MTU is 1400 bytes
R2#show ip interface serial 0.1
Serial0.1 is up, line protocol is up
Internet address is 131.108.1.2/24
Broadcast address is 255.255.255.255
MTU is 1500 bytes

Debug

Cấu hình :

R1#debug ip ospf adj

OSPF: Retransmitting DBD to 131.108.1.2 on Serial0.1

OSPF: Send DBD to 131.108.1.2 on Serial0.1 seq 0x1E55 opt 0x2 flag 0x7 len 32

OSPF: Rcv DBD from 131.108.1.2 on Serial0.1 seq 0x22AB opt 0x2 flag 0x7 len 32 mtu 1500 state EXSTART

OSPF: Nbr 131.108.1.2 has larger interface MTU

Giải pháp:

Để khắc phục vấn đề này, hãy chắc chắn rằng MTU được thiết lập với giá trị như nhau trên cả hai bên.

R1# interface Serial0.1 multipoint
ip address 141.108.10.3 255.255.255.248
mtu 1500

2.6.2 Các Route có cùng ID

Khi OSPF gửi một gói tin DBD để bầu một master và một slave ,các bộ định tuyến với các router ID cao nhất sẽ trở thành master. Điều này xảy ra trong quá trình EXSTART. Nếu có bất kỳ vấn đề với cuộc bầu cử, các bộ định tuyến sẽ bị mắc kẹt trong tình trạng EXSTART / EXCHANGE.

Ví dụ: Khi show cấu hình

R2#show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface 131.108.2.1 1 EXSTART/- 00:00:33 131.108.1.1 Serial0 Debug:

R2#debug ip ospf adj OSPF: Retransmitting DBD to 131.108.2.1 on Serial0

OSPF: Send DBD to 131.108.2.1 on Serial0 seq 0x793 opt 0x2 flag 0x7 len 32

OSPF: Rcv DBD from 131.108.2.1 on Serial0 seq 0x25F7 opt 0x2 flag 0x7 len 32

mtu 0

state EXSTART

OSPF: First DBD and we are not SLAVE

- Ta thấy R2 được gửi một gói tin DBD với một cờ là 7, nói rằng, "Tôi là master." R2 cũng nhận được một DBD từ R1 nói, "Tôi là master." R2 so sánh R1 của router ID và thấy rằng nó không phải là cao hơn so với riêng của mình, do đó nó sẽ gửi các gói tin DBD để R1 nói, "Tôi là master." Vì vậy, cả hai thiết bị định tuyến tiếp tục gửi và nhận tình trạng tổng thể và các router bị mắc kẹt trong tình trạng EXSTART.

Giải pháp:

Để giải quyết vấn đề này, xem xét cẩn thận những người hàng xóm Router ID và địa phương Router ID để xem họ là chính xác như nhau. Nếu vậy, bạn phải thay đổi router ID với một trong các router và khởi động lại quá trình OSPF để nó có thể có hiệu lực.

2.6.3 Không có khả năng ping qua vì kích thước MTU lớn

- Khi OSPF bắt đầu hình thành một kề với hàng xóm của mình, nó đi qua một số tiểu bang. Trong trạng thái EXSTART, OSPF sẽ xác định đó sẽ là master và đó sẽ là slave. Sau khi các bộ định tuyến quyết định này, họ bắt đầu trao đổi tiêu đề LSA trong các hình thức gói tin DBD. Nếu cơ sở dữ liệu là rất lớn, OSPF sử dụng interface MTU và cố gắng để gửi dữ liệu càng nhiều càng tốt lên đến giới hạn của interface MTU. Nếu có một vấn đề với lớp 2 chấp nhận các gói tin lớn có trong phạm vi interface MTU, kề OSPF sẽ bị mắc kẹt trong tình trạng EXCHANGE.
- *Ví dụ:* Khi show cấu hình

R2#show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface
131.108.2.1 1 EXCHANGE/- 00:00:46 131.108.1.2 Serial0/0 Ping)

R1#ping 131.108.1.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 131.108.1.2, timeout is 2 seconds:

! ! ! ! !

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R1#

R1#ping ip

Target IP address: 131.108.1.2

Repeat count [5]:

Datagram size [100]: 1200

Timeout in seconds [2]:

Extended commands [n]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 1200-byte ICMP Echos to 131.108.1.2, timeout is 2 seconds:

. . . . .

Success rate is 0 percent (0/5)

R1#

- Ta thấy Khi R1 ping R2 với MTU bằng hoặc lớn hơn 1200, ping không bao giờ đạt đến phía bên kia. Điều này cho thấy một vấn đề ở lớp 2

Giải pháp: Vấn đề là thực sự với lớp 2.

- R1 có thể ping R2 khi sử dụng một gói 100-byte, nhưng ping bắt đầu thất bại khi datagram kích thước lớn hơn 1200 byte. Để giải quyết vấn đề này, khắc phục vấn đề lớp 2. Một cách để thu hẹp vấn đề này là để kết nối hai thiết bị trực tiếp thay vì đi qua chuyển mạch và vv, để xem liệu vấn đề là với các thiết bị lớp 2 hoặc router. Nếu kết nối với bộ định tuyến trở lại trở lại không sửa chữa vấn đề, có một khả năng của phần cứng xấu. Hầu hết thời gian, nó quay ra là một vấn đề ở giữa, ví dụ, một chuyển đổi mạng LAN hoặc một WAN cloud.
- Tùy thuộc vào phương tiện truyền thông, có một số kiến nghị: Trong trường hợp của một phương tiện mạng LAN
- Kiểm tra kích thước MTU được xác định trong cấu hình chuyển đổi cho phương tiện này.
- Hãy thử sử dụng một cổng khác nhau. Trong trường hợp của một phương tiện WAN

- Nếu bạn là nhà cung cấp điện toán đám mây WAN, kiểm tra hop.
- Nếu bạn đang nhận được một mạch từ một công ty viễn thông, yêu cầu rằng các WAN cloud ở giữa đã được kiểm tra để xem nơi nó không thành công.

2.6.4. Bị phá vỡ kết nối unicast

Khi OSPF router bắt đầu trao đổi thông tin cơ sở dữ liệu với nhau, họ gửi một gói tin unicast với nhau trong trạng thái EXSTART / TRAO ĐỔI. Điều này chỉ xảy ra nếu các loại mạng không phải là một kết nối point-to-point. Trong trường hợp kết nối point-to-point, OSPF sẽ gửi tất cả các gói tin multicast. Nếu kết nối unicast bị hỏng, hàng xóm OSPF vẫn còn trong trạng thái EXSTART.

2.6.5. Sai VC / DLCI mapping trong Frame Relay/ATM switch

Trong trường hợp Frame Relay hoặc ATM, đây là một vấn đề rất phổ biến. Các gói tin sẽ bị mất trong Frame Relay hoặc ATM cloud. Tiếp tục xác minh rằng đây là trường hợp, debug chi tiết gói tin IP với danh sách truy cập trên cả hai router.

```
R1#show access-list 100
Extended IP access list 100
permit ip 131.108.1.0 0.0.0.255 131.108.1.0 0.0.0.255 (10 matches)
R1#debug ip packet detail 100
R1#ping 131.108.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 131.108.1.2, timeout is 2 seconds: .....
Success rate is 0 percent (0/5)
IP: s=131.108.1.1 (local), d=131.108.1.2 (Serial0), len 100, sending
ICMP type=8, code=0
IP: s=131.108.1.1 (local), d=131.108.1.2 (Serial0), len 100, sending
ICMP type=8, code=0
IP: s=131.108.1.1 (local), d=131.108.1.2 (Serial0), len 100, sending
ICMP type=8, code=0
IP: s=131.108.1.1 (local), d=131.108.1.2 (Serial0), len 100, sending
ICMP type=8, code=0
IP: s=131.108.1.1 (local), d=131.108.1.2 (Serial0), len 100, sending
ICMP type=8, code=0
R1#
R2#show access-list 100
Extended IP access list 100
permit ip 131.108.1.0 0.0.0.255 131.108.1.0 0.0.0.255 (10 matches)
R2#debug ip packet detail 100
R2#ping 131.108.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 131.108.1.1, timeout is 2 seconds: ……
Success rate is 0 percent (0/5)
IP: s=131.108.1.2 (local), d=131.108.1.1 (Serial0), len 100, sending
ICMP type=8, code=0
IP: s=131.108.1.2 (local), d=131.108.1.1 (Serial0), len 100, sending
```

ICMP type=8, code=0
IP: s=131.108.1.2 (local), d=131.108.1.1 (Serial0), len 100, sending
ICMP type=8, code=0
IP: s=131.108.1.2 (local), d=131.108.1.1 (Serial0), len 100, sending
ICMP type=8, code=0
IP: s=131.108.1.2 (local), d=131.108.1.1 (Serial0), len 100, sending
ICMP type=8, code=0
R2#

2.6.6. Danh sách truy cập chặn unicast

Nếu một danh sách truy cập được cấu hình trên một bộ định tuyến, hãy chắc chắn rằng nó không ngăn chặn các gói tin unicast.

Ví dụ:

R1#show access-list 100
Extended IP access list 100
permit ip 131.108.1.0 0.0.0.255 131.108.1.0 0.0.0.255
R1#show access-list 101
Extended IP access list 101
permit ip 141.108.10.0 0.0.0.255 any
permit ip 141.108.20.0 0.0.0.255 any
permit ip 141.108.30.0 0.0.0.255 any
permit ip 131.108.1.0 0.0.0.255 host 224.0.0.5
R1#debug ip packet 100 detail
IP packet debugging is on (detailed) for access list 100
R1#
IP: s=131.108.1.2 (Serial0.2), d=131.108.1.1, len 100, access denied
ICMP type=8, code=0
IP: s=131.108.1.1 (local), d=131.108.1.2 (Serial0.2), len 56, sending
ICMP type=3, code=13
R1#
IP: s=131.108.1.2 (Serial0.2), d=131.108.1.1, len 100, access denied
ICMP type=8, code=0
IP: s=131.108.1.1 (local), d=131.108.1.2 (Serial0.2), len 56, sending
ICMP type=3, code=13
R1#
IP: s=131.108.1.2 (Serial0.2), d=131.108.1.1, len 100, access denied
ICMP type=8, code=0
IP: s=131.108.1.1 (local), d=131.108.1.2 (Serial0.2), len 56, sending
ICMP type=3, code=13

Ta thấy danh sách truy cập 101 cho thấy chỉ có các gói multicast OSPF được phép và rằng các gói unicast từ địa chỉ 131.108.1.0 bị từ chối bởi vì có một tiềm ẩn từ chối vào cuối mỗi danh sách truy cập.

Giải pháp:

- Để giải quyết vấn đề này, sửa đổi danh sách truy cập 101 do đó, nó cho phép các gói tin unicast.

R1#show access-list 101
Extended IP access list 101
permit ip 141.108.10.0 0.0.0.255 any
permit ip 141.108.20.0 0.0.0.255 any
permit ip 141.108.30.0 0.0.0.255 any
permit ip 131.108.1.0 0.0.0.255 host 224.0.0.5
permit ip 131.108.1.0 0.0.0.255 131.108.1.0 0.0.0.255

2.6.7. NAT chuyển đổi unicast

Đây là một vấn đề phổ biến xảy ra khi NAT được cấu hình trên router. Nếu NAT là sai, nó sẽ bắt đầu dịch các gói tin unicast tiến về phía nó, sẽ phá vỡ các kết nối unicast.

```
R1# interface Ethernet 0
    ip nat outside
    ip nat inside
    source list 1 interface Serial0.2 overload
    access-list 1 permit any
```

Ta thấy R1 được cấu hình với NAT. Bên ngoài interface của R1 là Serial0.2, kết nối đến R2. Khi R2 gửi một gói tin unicast đến R1, R1 sẽ cố gắng để chuyển gói tin và R2 không bao giờ nhận được câu trả lời ping. Điều chính để xem cho là danh sách truy cập trong NAT. Nếu danh sách truy cập được cho phép tất cả mọi thứ, vấn đề này sẽ xảy ra.

- Giải pháp: Để giải quyết vấn đề này, thay đổi danh sách truy cập 1 và chỉ cho phép những địa chỉ IP mà cần dịch. Danh sách truy cập có thể là khác nhau từ mạng này sang mạng. Toàn bộ ý tưởng là lệnh giấy phép danh sách truy cập không nên bao gồm địa chỉ IP của người hàng xóm, chỉ có mạng lưới bên trong 10.0.0.0 / 8 được cho phép. Điều này có nghĩa rằng R1 sẽ không còn dịch các gói tin thuộc mạng 131.108.1.0. Cấu hình như sau:

```
R1# interface Ethernet 0
    ip address 131.108.1.1 255.255.255.0
    ip nat outside
    ip nat inside
    source list 1 interface Serial0.2 overload
    access-list 1 permit 10.0.0.0 0.255.255.255
```

2.6.8. Loại mạng lưới point-to-point giữa PRI and BRI/dialer

Các loại mạng trên một giao diện PRI là point-to-point. Điều này làm cho OSPF gửi các gói tin multicast ngay cả sau khi trạng thái 2-WAY . Nếu chỉ có một BRI đến như là một người hàng xóm OSPF, nó sẽ làm việc tốt. Tuy nhiên, khi nhiều Bris cố gắng để tạo thành một kề với PRI, PRI sẽ phàn nàn vì loại mạng của nó là point-to-point. Bởi vì tất cả các gói tin OSPF được gửi dưới dạng multicast vào một liên kết point-to-point, PRI nhận được gói tin DBD từ nhiều route láng giềng BRI, và điều này gây ra tất cả những người hàng xóm để có được vào tình trạng EXSTART / EXCHANGE.

+ Ví dụ: Show cấu hình

R1#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface

131.108.1.2 1 EXSTART/- 00:00:38 131.108.1.2 Serial0/0:23
131.108.1.3 1 EXSTART/- 00:00:32 131.108.1.3 Serial0/0:23
R2#show ip ospf interface bri0
BRI0 is up, line protocol is up (spoofing)
Internet Address 131.108.1.2/24, Area 2
Process ID 1, Router ID 131.108.1.2, Network Type POINT_TO_POINT, Cost: 1562
Transmit Delay is 1 sec, State POINT_TO_POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:06
index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

Giải pháp: Để giải quyết vấn đề này, thay đổi kiểu mạng của PRI và BRI point-to-multipoin.

R2#
interface BRI0
ip ospf network point-to-multipoint

2.7 Triển khai EIGRP

Định nghĩa: EIGRP – Enhance Interio Gateway Routing Protocol là giao thức định tuyến mở rộng của IGRP, IGRP là giao thức dạng Classfull, còn EIGRP là giao thức dạng Classless, nghĩa là có mang theo subnetmask trong các lần cập nhật EIGRP là giao thức định tuyến lai (Hybrid Routing), là sự kết hợp của Distance Vector và Link States. EIGRP là một giao thức định tuyến theo vector khoảng cách nâng cao nhưng khi cập nhật và bảo trì thông tin láng giềng và thông tin định tuyến thì nó làm việc giống như một giao thức định tuyến theo trạng thái đường liên kết.

Một số ưu điểm của EIGRP so với các giao thức định tuyến véc tơ khoảng cách:

- Khả năng hội tụ nhanh: vì chúng sử dụng DUAL. DUAL bảo đảm hoạt động không bị lặp vòng khi tính toán đường đi, cho phép mọi Router trong hệ thống mạng thực hiện đồng bộ cùng lúc khi có sự thay đổi xảy ra.
- Bảo tồn băng thông và sử dụng băng thông một cách hiệu quả: vì nó chỉ gửi thông tin cập nhật một phần và giới hạn chứ không gửi toàn bộ bảng định tuyến. Nhờ vậy nó chỉ tốn một lượng băng thông tối thiểu khi hệ thống mạng đã ổn định. Điều này tương tự như hoạt động cập nhật của OSPF, Router EIGRP chỉ gửi thông tin cập nhật một phần cho Router nào cần thông tin đó mà thôi chứ không gửi mọi Router khác trong vùng như OSPF. Chính vì hoạt động cập nhật theo chu kỳ, các Router EIGRP giữ liên lạc với nhau bằng các gói hello rất nhỏ. Việc trao đổi các gói hello theo định kỳ không chiếm nhiều băng thông đường truyền.
- Hỗ trợ VLSM (Veriable Length Subnet Mask) và CIDA (Classles Inter Domain Routing). Không giống như IGRP,EIGRP có thể trao đổi thông tin ở các IP khác lớp mạng
- Hỗ trợ IP, IPX, Apple talk: vì Talk nhờ có cấu trúc từng phần theo giao thức (PDMs – Protocok dependent modules). EIGRP có thể phân phối thông tin của IPX,RIP để cải tiến

hoạt động toàn diện. Trên thực tế, EIGRP có thể điều khiển giao thức này. Router EIGRP nhận thông tin định tuyến và dịch vụ, chỉ cập nhật cho các Router khác khi thông tin trong bảng định tuyến thay đổi.

- Chạy trực tiếp trên IP và protocol number là 88
- Load balancing trên tất cả các cost không bằng nhau
- Hỗ trợ tất cả các giao thức và cấu trúc dữ liệu ở layer 2
- Không dùng broadcast và dùng Multicast hoặc Unicast trong từng trường hợp cụ thể.
- Hỗ trợ việc chứng thực
- Manual Summary trên bất kỳ interface nào

Nhược điểm:

- EIGRP là một giao thức với rất nhiều ưu điểm và có thể được sử dụng trong những mô hình mạng vừa và lớn tuy nhiên vì đây là giao thức độc quyền của Cisco nên nó chỉ chạy trên thiết bị của cisco, trong khi đó không phải một tổ chức nào cũng có thể dùng toàn đồ Cisco mà còn các dòng sản phẩm khác nữa. Chính vì vậy, đây là một bất lợi của giao thức định tuyến EIGRP.

Nguyên lý hoạt động

- EIGRP Router lưu giữ các thông tin về đường đi và cấu trúc mạng trên RAM, nhờ đó chúng đáp ứng nhanh chóng theo sự thay đổi. Giống như OSPF, EIGRP cũng lưu những thông tin này thành từng bảng và từng cơ sở dữ liệu khác nhau. EIGRP lưu các con đường mà nó học được theo một cách đặc biệt. Mỗi con đường có trạng thái riêng và có đánh dấu để cung cấp thêm nhiều thông tin hữu dụng khác.
- Topology exchange: Những Router neighbor sẽ trao đổi thông tin lẫn nhau, cập nhật đầy đủ cấu trúc liên kết, topology mạng. Khi topoly mạng thay đổi nó sẽ cập nhật phần thay đổi.
- Choosing routes: Mỗi Router sẽ tiến hành phân tích bảng EIGRP topology table, chọn ra con đường định tuyến có metric tốt để đến các subnet. Sau khi thực hiện 3 bước ở trên, hệ điều hành IOS sẽ lưu 3 bảng EIGRP Tables quan trọng:
  + Bảng láng giềng (Neighbor table): Bảng láng giềng là bảng quan trọng nhất của EIGRP, trong đó có danh sách các router thân mật với nó. Đối với mỗi giao thức mà EIGRP hỗ trợ thì nó sẽ có 1 bảng láng giềng tương ứng. Khi phát hiện một láng giềng mới, router sẽ ghi lại thông tin về địa chỉ, cổng kết nối.
  + Bảng cấu trúc mạng (Topology table): Là bảng cung cấp dữ liệu để xây dựng nên bảng định tuyến của EIGRP. Thuật toán DUAL sẽ lấy thông tin từ bảng láng giềng và bảng cấu trúc để chọn đường có chi phí thấp nhất cho từng mạch đích. Mỗi EIGRP Router lưu một bảng cấu trúc mạng riêng tương ứng với từng loại giao thức mạng khác nhau. Bảng cấu trúc mạng chứa thông tin về tất cả các con đường mà Router học được. Nhờ những thông tin này mà Router có thể xác định đường đi khác để thay thế nhanh chóng khi cần thiết. Thuật toán DUAL chọn ra đường tốt nhất đến mạng đích gọi là đường kính (successor Router).

Những thông tin chứa trong bảng cấu trúc

- Feasible Distance (FD): Là thông tin định tuyến nhỏ nhất mà EIGRP tính được cho từng mạch đích
- Router Sourch: Là nguồn phát khởi thông tin về một nguồn nào đó, phần thông tin này chỉ có đối với những kết nối ngoài mạng EIGRP
- Reported Distance (RD): Là thông số định tuyến đến 1 Router láng giềng được thông báo qua
- Thông tin về cổng giao tiếp mà Router sử dụng để đi đến mạch đích

- Trạng thái đường đi: Trạng thái không tác động (P-Passive) là trạng thái ổn định, sẵn sàng sử dụng được, trạng thái tác động(A-active) là trạng thái đang trong tiến trình tính toán lại của DUAL.
- Bảng định tuyến (Routing table): Bảng định tuyến EIGRP lưu giữ danh sách các đường tốt nhất đến các mạng đích. Những thông tin trong bảng định tuyến được rút ra từ bảng cấu trúc mạng.

Router EIGRP có bảng định tuyến riêng cho từng giao thức mạng khác nhau. Con đường được chọn làm đường chính đến mạng đích gọi là successor. Từ thông tin trong bảng láng giềng và bảng cấu trúc mạng, DUAL chọn ra một đường chính và đưa lên mạng định tuyến. Đến một mạng đích có thể có đến 4 successor. Những đường này có chi phí bằng nhau hoặc không bằng nhau.

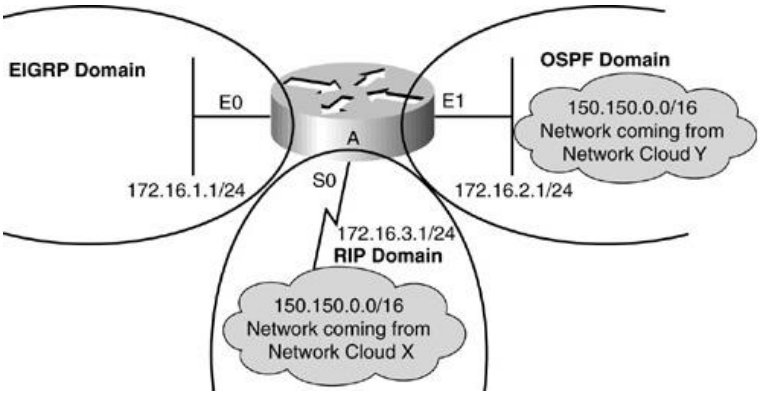
Thông tin về successor cũng được đặt trong bảng cấu trúc mạng. Đường Feasible successor (FS) là đường dự phòng cho đường successor. Đường này cũng được chọn ra cùng với đường successor nhưng chúng chỉ được lưu trong bảng cấu trúc mạng nhưng điều này không bắt buộc. Router xem hop kế tiếp của đường Feasible successor dưới nó gần mạng đích hơn nó. Do đó, chi phí của Feasbile successor được tính bằng chi phí của chính nó cộng với chi phí vào Router láng giềng thông báo qua.

Trong trường hợp này successor bị sự cố thì Router sẽ tìm Feasible successor để thay thế. Một đường Feasible successor bắt buộc phải có chi phí mà Router láng giềng thông báo qua thấp hơn chi phí của đường successor hiện tại. Nếu trong bảng cấu trúc mạng không có sẵn đường Feasible successor thì con đường đến mạng đích tương ứng được đưa vào trạng thái Active và Router bắt đầu gửi các gói yêu cầu đến tất cả láng giềng để tính toán lại cấu trúc mạng. Sau đó với thông tin mới nhận được, Router có thể sẽ chọn ra được successor mới hoặc Feasible successor mới. Đường mới được chọn xong sẽ có trạng thái là Passive

2.8 Xử lý sự cố EIGRP

2.8.1 Xử lý sự cố EIGRP Redistribution

Ta có mô hình:



Hình 6.28 Mô hình EIGRP

Cấu hình như sau:

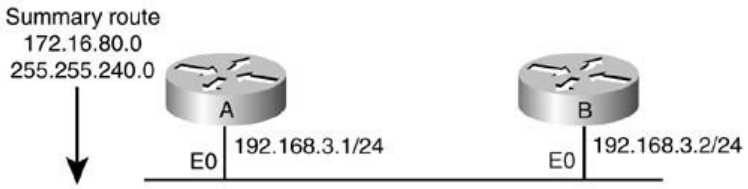
```
Router A# interface ethernet 0
ip address 172.16.1.1 255.255.255.0
interface ethernet 1
ip address 172.16.2.1 255.255.255.0
interface serial 0
ip address 172.16.3.1 255.255.255.0
```

router ospf 1
network 172.16.0.0 0.0.255.255 area 0
router rip
network 172.16.0.0
passive-interface ethernet 1
router eigrp 1
network 172.16.0.0
redistribute rip default-metric 10000 100 255 1 1500
Router A# show ip eigrp topology
150.150.0.0 255.255.0.0
% Route not in topology table
Router A# show ip route 150.150.0.0 255.255.0.0
Routing entry for 150.150.0.0/16 Known via "OSPF 1", distance 110, metric 186 Redistributing via OSPF 1 Last update from 172.16.2.2 on Ethernet 1 Routing Descriptor Blocks: * 172.16.2.2, from 172.16.2.2, 00:10:23 ago, via Ethernet 1 Route metric is 186, traffic share count is 1
Cho thấy các tuyến đường 150.150.0.0/16 được hiển thị như là một tuyến đường OSPF, không phải là một tuyến đường RIP. Đây là lý do tại sao các tuyến đường là không nhận được phân phối vào EIGRP. Trước khi tuyến RIP được phân phối vào EIGRP, các router sẽ ở bảng định tuyến và tái phân phối tất cả các tuyến RIP vào EIGRP. Các bộ định tuyến nghe các bản cập nhật cho các tuyến đường 150.150.0.0/16 từ cả OSPF và RIP. Các bộ định tuyến cài đặt các tuyến đường OSPF vì OSPF có AS thấp hơn so với RIP. Do đó, nếu các tuyến đường được hiển thị như là một tuyến đường OSPF, router sẽ không phát hành lại tuyến đường này vào EIGRP. Nói cách khác, các router sẽ phân phối lại chỉ RIP tuyến đường được hiển thị trong bảng định tuyến vào miền EIGRP.
Giải pháp: Các giải quyết vấn đề này, bạn phải làm cho Router A cài đặt các tuyến đường RIP thay vì các tuyến đường OSPF. Một cách để làm điều này là để cấu hình một danh sách phân phối theo OSPF để không cài đặt các tuyến đường 150.150.0.0/16. Cấu hình như sau:
router OSPF 1
network 172.16.0.0 0.0.255.255 area 0 distribute-list 1 out access-list 1 deny 150.150.0.0 0.0.255.255 access-list 1 permit any

2.8.2 Xử lý sự cố EIGRP Summarization

Tóm tắt mạng con không tồn tại trong bảng định tuyến

Ta có mô hình:



Hình 6.29 Mô hình EIGRP

Cấu hình như sau:
Router_A#interface ethernet 0
ip address 192.168.3.1 255.255.255.0
ip summary-address EIGRP 1 172.16.80.0 255.255.240.0
interface Serial 0
ip address 192.168.1.2 255.255.255.0
interface Serial 1
ip address 192.168.2.2 255.255.255.0
router EIGRP 1
  network 192.168.1.0
  network 192.168.2.0
  network 192.168.3.0
Router A# show ip route

C 192.168.1.0/24 is directly connected, Serial 0
C 192.168.2.0/24 is directly connected, Serial 1
C 192.168.3.0/24 is directly connected, Ethernet 0
D 172.16.99.0/24 [90/409600] via 192.168.1.1, Serial 0
D 172.16.97.0/24 [90/409600] via 192.168.1.1, Serial 0
D 172.16.79.0/24 [90/409600] via 192.168.1.1, Serial 0
D 172.16.70.0/24 [90/409600] via 192.168.1.1, Serial 0
D 172.16.103.0/24 [90/409600] via 192.168.1.1, Serial 0
D 172.16.76.0/24 [90/409600] via 192.168.1.1, Serial 0
D 172.16.98.0/24 [90/409600] via 192.168.1.1, Serial 0

Các tuyến đường tóm tắt được cấu hình để được 172.16.80.0 255.255.240.0 bằng cách sử dụng lệnh ip tóm tắt địa chỉ EIGRP 1 172.16.80.0 255.255.240.0. Tuyến đường tóm tắt này bao gồm các mạng dải địa chỉ từ 172.16.80.0 đến 172.16.95.255. Từ bảng định tuyến ta nhận thấy rằng không phù hợp với các tuyến đường giữa khoảng 172.16.80.0 đến 172.16.95.255.

Do đó, nếu không có mạng con của tuyến đường tóm tắt cấu hình có mặt trong các bảng định tuyến, các bộ định tuyến không tạo ra các tuyến đường tóm tắt.

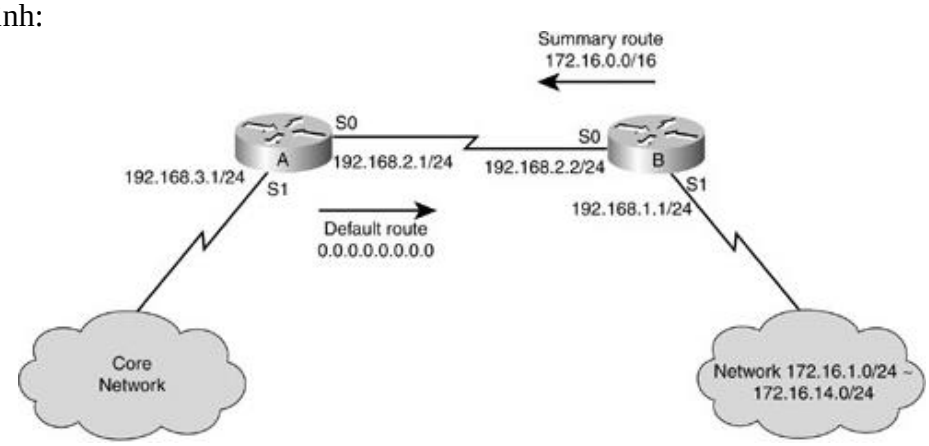
Giải pháp:

Giải pháp cho vấn đề này là để cấu hình một giao diện mà rơi vào trong mạng 172.16.80.0 255.255.240.0. Bạn có thể cấu hình một giao diện loopback với địa chỉ 172.16.81.1 255.255.255.0 để tạo ra các tuyến đường tóm tắt cấu hình trên
Ethernet 0.

Router_A#interface loopback 0
ip address 172.16.81.1 255.255.255.0
interface Ethernet 0
ip address 192.168.3.1 255.255.255.0
ip Summary-address EIGRP 1 172.16.80.0 255.255.240.0
interface Serial 0
ip address 192.168.1.2 255.255.255.0
Interface Serial 1
ip address 192.168.2.2 255.255.255.0
router EIGRP 1
  network 172.16.0.0
  network 192.168.1.0
  network 192.168.2.0
  network 192.168.3.0

Quá nhiều Summarization

Ta có mô hình:



Hình 6.30 Mô hình EIGRP

Show cấu hình:

Router A# show ip route 172.16.40.0
Routing entry for 172.16.0.0/16

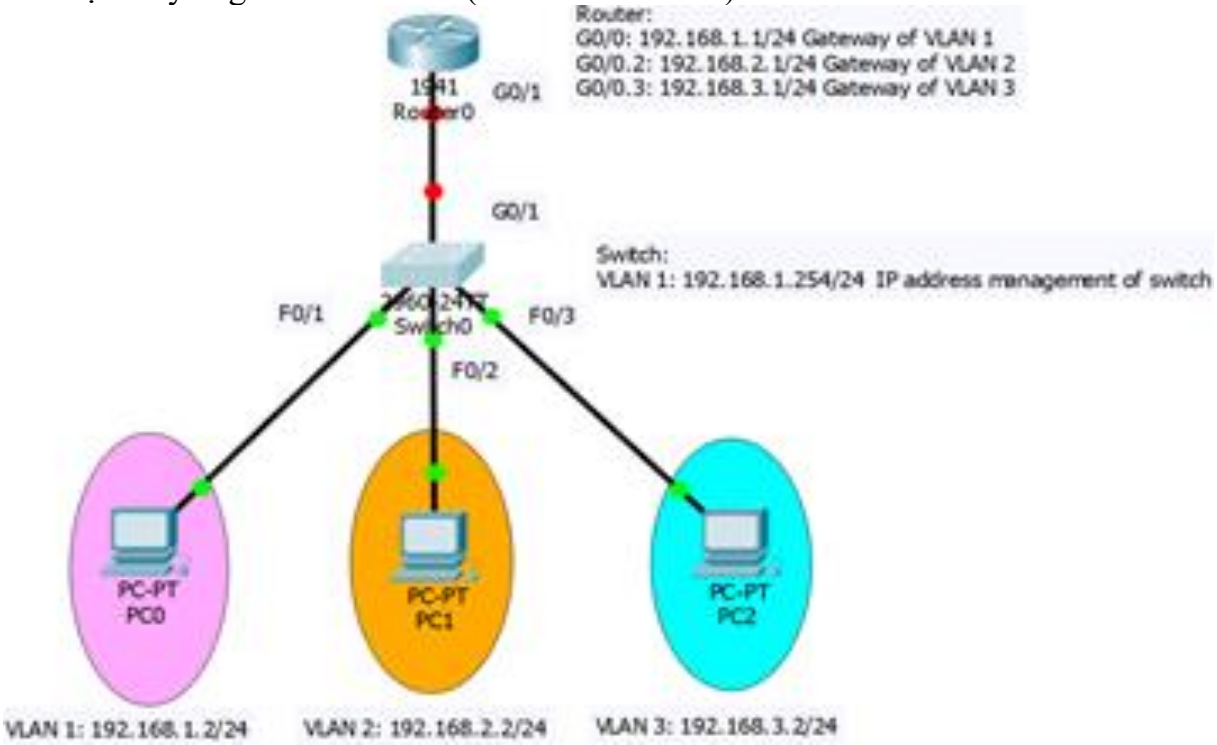
Known via "EIGRP 1", distance 90, metric 409600, type internal
Last update from 192.168.2.2 on Serial0 , 00:20:25 ago
Routing Descriptor Blocks:
* 192.168.2.2 from192.168.2.2, 00:20:25 ago, via Serial 0 Route metric is 409600,traffic share count is 1
Total delay is 6000 microseconds, minimum bandwidth is 10000 Kbit Reliability 255/255, minimum MTU 1500 bytes Loading 1/255, Hops
Mục định tuyến trong Router A cho thấy các tuyến đường tóm tắt 172.16.0.0/16 đến từ Router B. Do đó, Router A chuyển tiếp gói tin đến Router B.
Tuy nhiên, Router B gửi gói tin trở lại đúng với Router A vì Router B thì không có lộ trình cho 172.16.40.0, nó chỉ có các tuyến đường mặc định chỉ trở lại Router A. Điều này làm cho vòng lặp định tuyến giữa các Router A và Router B cho bất kỳ mạng không tồn tại trong phạm vi 172.16.0.0/16.

Giải pháp:

Vấn đề chính là tuyến đường tóm tắt của Router B là quá rộng và bao gồm các mạng con không tồn tại. Ngoài ra, Router A gửi một tuyến đường tóm tắt tổng quát hơn để đến Router B. Các giải pháp là phải có Router B gửi chỉ có tuyến đường tóm tắt bao gồm các 172.16.1.0 thông qua mạng 172.16.15.0. Nói cách khác, thay vì gửi các tuyến đường tóm tắt 172.16.0.0/16, Router B có thể gửi tuyến đường tóm tắt 172.16.0.0 255.255.240.0 đến Router A.

Câu hỏi ôn tập

- Nêu chức năng của mạng ảo VLAN;
- Mô phỏng vai trò của Switch trong VLAN, trình bày lợi ích của VLAN;
- Thiết lập được các VLAN, triển khai được VTP, OSPF và EIGRP;
- Định tuyến giữa các VLAN (Router on a Stick)



Yêu cầu:

- Thực hiện đấu nối các thiết bị, các cấu hình cơ bản: hostname, password, địa chỉ IP quản lý cho Switch…
- Cấu hình thông tin VLAN, gán port cho VLAN, cấu hình đường Trunk nối giữa Switch và Router.
- Cấu hình định tuyến giữa VLAN.
- Kiểm tra kết nối giữa các VLAN.

BÀI 7. XÂY DỰNG MẠNG LAN

Giới thiệu:

Kiến trúc Dịch vụ (Service-Oriented Architecture - SOA).

Đây là kiến trúc khung (architectural framework) mang tính định hướng sự phát triển, mở rộng có mục đích đối với các hệ thống mạng lớn và là một cuộc cách mạng trong nhận thức về nền tảng mạng truyền thông hướng tới môi trường mạng thông tin thông minh (Intelligent information network) giúp cho việc tăng nhanh các khả năng ứng dụng, dịch vụ, mở rộng tiến trình kinh doanh và tất nhiên, kèm theo đó là lợi nhuận.

Lớp cơ sở hạ tầng mạng (networked infrasstructure layer): là lớp mạng liên kết các khối chức năng theo kiến trúc phân tầng, có trật tự.

Lớp dịch vụ tương tác (Interactive services layer): bao gồm sự kết hợp một số kiến trúc mạng đầy đủ với nhau tạo thành các chức năng cho phép nhiều ứng dụng có thể sử dụng trên mạng.

Lớp ứng dụng (Application layer): Bao gồm các loại ứng dụng cộng tác và nghiệp vụ. Các ứng dụng này kết hợp với các dịch vụ tương tác cung cấp ở lớp dưới sẽ giúp triển khai nhanh và hiệu quả

1. Mục tiêu của bài

- Mô tả được quy trình thiết kế một hệ thống mạng;
- Xác định được cách đấu cáp cho các thiết bị phần cứng;
- Đọc được bảng vẽ thi công mạng;
- Cài đặt được hệ điều hành mạng;
- Cài đặt, cấu hình được các dịch vụ mạng;
- Cấu hình được các giao thức mạng;
- Xây dựng được các phương án bảo mật mạng;
- Lập được nhật kí thi công mạng;
- Thực hiện các thao tác an toàn với máy tính;

2. Nội dung bài

2.1 Các chi tiết cơ bản trên bảng vẽ thi công mạng (sử dụng microsoft visio)

2.1.1. Mục tiêu thiết kế

Thiết kế, xây dựng hạ tầng truyền thông cho các đơn vị, tổ chức tạo điều kiện triển khai các ứng dụng nghiệp vụ và các dịch vụ gia tăng của đơn vị, tổ chức đó.

Mục tiêu chung được thể hiện qua các điểm cụ thể sau:

- Xây dựng hạ tầng truyền thông thống nhất, tốc độ cao đồng bộ.
- Quản trị hệ thống tập trung.
- Phát triển các dịch vụ gia tăng trên mạng như Video conferencing, VoIP.
- Xây dựng hạ tầng cơ sở đảm bảo môi trường tiêu chuẩn cho trung tâm dữ liệu.

2.1.2 Nội dung thiết kế

- Xây dựng thiết kế mạng LAN, WAN cho các đơn vị, tổ chức.
- Xây dựng mạng trục WAN backbone.
- Xây dựng hệ thống an ninh mạng theo chiều sâu, nhiều lớp và sử dụng nhiều công nghệ khác nhau.
- Xây dựng hệ thống quản trị cấu hình trang thiết bị và giám sát kênh truyền thông.
- Xây dựng hạ tầng cơ sở trung tâm dữ liệu chính.
- Xây dựng thiết kế mạng cho trung tâm dữ liệu dự phòng.
- Xây dựng các dịch vụ mạng gia tăng như IP Telephony và Video Conferencing

2.1.3 Tổng quan về thiết kế

2.1.3.1 Định hướng kiến trúc

Trong phần này, chúng tôi xin giới thiệu sơ lược về một định hướng kiến trúc tiêu biểu được áp dụng trong việc xây dựng hạ tầng Công nghệ Thông tin cho các tổ chức và doanh nghiệp lớn. Đó là Định hướng Kiến trúc Dịch vụ (Service-Oriented Architecture-SOA).

Đây là kiến trúc khung (architectural framework) mang tính định hướng sự phát triển, mở rộng có mục đích đối với các hệ thống mạng lớn và là một cuộc cách mạng trong nhận thức về nền tảng mạng truyền thông hướng tới môi trường mạng thông tin thông minh (Intelligent information network) giúp cho việc tăng nhanh các khả năng ứng dụng, dịch vụ, mở rộng tiến trình kinh doanh và tất nhiên, kèm theo đó là lợi nhuận.

- **Lớp cơ sở hạ tầng mạng** (networked infrasstructure layer): là lớp mạng liên kết các khối chức năng theo kiến trúc phân tầng, có trật tự.

  + **Lớp dịch vụ tương tác** (Interactive services layer): bao gồm sự kết hợp một số kiến trúc mạng đầy đủ với nhau tạo thành các chức năng cho phép nhiều ứng dụng có thể sử dụng trên mạng.

  + **Lớp ứng dụng** (Application layer): Bao gồm các loại ứng dụng cộng tác và nghiệp vụ. Các ứng dụng này kết hợp với các dịch vụ tương tác cung cấp ở lớp dưới sẽ giúp triển khai nhanh và hiệu quả

2.1.3.2 Các phương thức thiết kế

Trong phần này, chúng tôi xin giới thiệu sơ lược về các phương thức thiết kế mạng và bảo mật được sử dụng trong việc thiết kế các hệ thống mạng lớn và hiện đại của các tổ chức và doanh nghiệp lớn. Tương ứng với kiến trúc SOA là thuộc lớp Cơ sở hạ tầng mạng.

2.1.3.2.1 Phương thức thiết kế phân lớp - Hierarchical

Phương thức thiết kế phân lớp (Hierarchical) ra đời và trở thành một kiến trúc phổ biến trong gần chục năm gần đây, được áp dụng để thiết kế các hệ thống mạng với qui mô trung bình cho đến qui mô lớn. Phương thức thiết kế này sử dụng các lớp (layer) để đơn giản hóa các công việc trong thiết kế mạng. Mỗi lớp có thể tập trung vào các chức năng cụ thể, cho phép người thiết kế lựa chọn đúng các hệ thống và các tính năng cho mỗi lớp.

Phương thức thiết kế Hierarchical gồm 3 lớp:

- **Lớp Core**: Có nhiệm vụ chuyển tiếp lưu thông với tốc độ cao nhất
- **Lớp Distribution**: Cung cấp các chính sách liên quan đến các hoạt động kết nối
- **Lớp Access**: Cung cấp truy cập cho các User/Workgroup vào mạng

2.1.3.2.2 Phương thức thiết kế theo mô đun - Modular

Phương thức thiết kế theo mô đun (Modular) được xem như là phương thức bổ xung cho phương thức thiết kế Hierarchical. Trong một hệ thống mạng qui mô lớn, nói chung sẽ bao gồm nhiều vùng mạng phục vụ các hoạt động và chức năng khác nhau. Việc thiết kế theo mô đun cho một hạ tầng mạng lớn bằng việc tách biệt các vùng mạng với chức năng khác nhau, cũng đang là một phương pháp thiết kế được sử dụng rộng rãi trong thiết kế hạ tầng mạng cho các doanh nghiệp, các công ty, và các tổ chức lớn (gọi tắt là Enterprise).

Phương thức thiết kế Modular có thể được chia làm ba vùng chính, mỗi vùng được tạo bởi các mô đun mạng nhỏ hơn:

- **Enterprise campus**: Bao gồm các module được yêu cầu để xây dựng một mạng campus đòi hỏi tính sẵn sàng cao, tính mềm dẻo và linh hoạt.

- **Enterprise edge**: Hội tụ các kết nối từ các thành phần khác nhau tại phía rìa mạng của Enterprise. Vùng chức năng này sẽ lọc lưu thông từ các module trong Enterprise edge và gửi chúng vào trong vùng Enterprise campus. Enterprise edge bao gồm tất cả các thành phần thiết bị để đảm bảo truyền thông hiệu quả và bảo mật giữa Enterprise campus với các hệ thống bên ngoài, các đối tác, mobile users, và mạng Internet.
- **Service provider edge**: Các module trong vùng này được triển khai bởi các nhà cung cấp dịch vụ, chứ không thuộc về Enterprise. Các module trong Service provider edge cho phép truyền thông với các mạng khác sử dụng các công nghệ WAN và các ISPs khác nhau.

2.1.3.2.3 Phương thức thiết kế bảo mật cho hệ thống mạng

Phương thức thiết kế bảo mật cho hệ thống mạng được sử dụng là Kiến trúc an ninh cho các Doanh nghiệp – SAFE (Security Architecture for Enterprise Networks), được xây dựng dựa trên nền tảng các công nghệ an ninh mạng tiên tiến nhất để bảo vệ các cuộc tấn công từ bên ngoài và bên trong của hệ thống mạng các doanh nghiệp. SAFE đem lại sự linh hoạt và khả năng mở rộng cao bao gồm khả năng dự phòng vật lý và cấu hình thiết bị khi có sự cố hay bị kẻ xấu tấn công vào hệ thống mạng. Khái niệm Module được sử dụng trong SAFE giúp cho việc tổ chức hệ thống an ninh được chặt chẽ và cho phép công việc thiết kế triển khai hệ thống an ninh mạng một cách linh hoạt theo từng Module một (Module by Module), trong khi vẫn đảm bảo được yêu cầu theo chính sách an ninh đặt ra cho từng giai đoạn.

Kiến trúc SAFE bao gồm các module sau:

- **Corporate Internet Module:** Corporate Internet Module tập trung chủ yếu các kết nối của người dùng bên trong hệ thống mạng (Internal user) truy cập Internet và các kết nối từ người dùng bên ngoài (Internet user) truy cập vào hệ thống các máy chủ Public Servers của doanh nghiệp như HTTP, FTP, SMTP và DNS. Ngoài ra trong Module này còn cung cấp dịch vụ truy cập từ xa bằng công nghệ VPN hay quay số truyền thống dial-up.

+ **Campus Module: Campus** Module chủ yếu tập trung các máy trạm làm việc, hệ thống máy chủ và kiến trúc chuyển mạch lớp 2 và lớp 3. Campus Module bao gồm nhiều thành phần hợp nhất thành một Module thống nhất được mô tả bằng mô hình kết nối tổng quát sau:

- Campus Module có cấu trúc thiết kế tương tự mô hình mạng Campus truyền thống và cũng được chia theo 3 lớp là Core, Distribution và Access Layer. Tuy nhiên ở lớp Access thì Campus Module được phân làm 3 Module bảo vệ gồm Building Module (users), Management Module và Server Module. Với sự phân cấp bảo vệ trong Campus Module giúp cho việc thiết lập hệ thống an ninh mạng được linh động và độc lập giữa các Module, nhờ vậy công việc tổ chức và quản trị trở nên dễ dàng hơn và giúp cho doanh nghiệp có thể mở rộng, gia cố và khắc phục các vấn đề an toàn cho hệ thống mạng khi có sự cố xảy ra.

+ **WAN Module**: WAN Module chỉ có một kết nối duy nhất đến các mạng khác cách xa nhau về mặt địa lý thông qua các đường truyền thuê bao riêng. Các khả năng có thể bảo vệ các cuộc tấn công vào WAN Module gồm:

- IP *spoofing*-IP spoofing có thể được ngăn chặn thông qua Layer 3 filtering
- *Unauthorized* access—Tránh các truy cập trái phép bằng việc giới hạn và kiểm soát các kiểu giao thức sử dụng từ chi nhánh kết nối về Trung tâm thông qua Router

2.1.3.2.4 Nguyên lý thiết kế hệ thống bảo mật

An ninh mạng phải được thiết lập dựa trên các nguyên tắc sau:

- Bảo vệ có chiều sâu (defense in depth): Hệ thống phải được bảo vệ theo chiều sâu, phân thành nhiều tầng và tách thành nhiều lớp khác nhau. Mỗi tầng và lớp đó sẽ được thực

hiện các chính sách bảo mật hay ngăn chặn khác nhau. Mặt khác cũng là để phòng ngừa khi một tầng hay một lớp nào đó bị xâm nhập thì xâm nhập trái phép đó chỉ bó hẹp trong tầng hoặc lớp đó thôi và không thể ảnh hưởng sang các tầng hay lớp khác.

- Sử dụng nhiều công nghệ khác nhau: Không nên tin cậy vào chỉ một công nghệ hay sản phẩm công nghệ bảo đảm an ninh cho mạng của một hãng nào đó. Bởi nếu như sản phẩm của hãng đó bị hacker tìm ra lỗ hổng thì dễ dàng các sản phẩm tương tự của hãng đó trong mạng cũng sẽ bị xuyên qua và việc phân tầng, phân lớp trong chính sách phòng vệ là vô nghĩa. Vì vậy khi tiến hành phân tầng, tách lớp, nên sử dụng nhiều sản phẩm công nghệ của nhiều hãng khác nhau để hạn chế nhược điểm trên. Đồng thời sử dụng nhiều cộng nghệ và giải pháp bảo mật kết hợp để tăng cường sức mạnh hệ thống phòng vệ như phối hợp Firewall làm công cụ ngăn chặn trực tiếp, IDS làm công cụ "đánh hơi", phản ứng phòng vệ chủ động, Anti-virus để lọc virus...v.v
- Các tiêu chuẩn đáp ứng: Các sản phẩm bảo mật phải đáp ứng một số chứng nhận tiêu chuẩn như Common Criteria, ISO/IEC 15408:2005 và ISO/IEC 18405:2005 EAL4, ICSA Firewall và VPN, FIPS-140

2.2 Giám sát thi công mạng

Điều kiện thi công: Trước khi thi công, tư vấn giám sát thi công tiến hành:

- Kiểm tra đảm bảo có mặt bằng thi công đối với xây lắp mạng, lắp đặt vật tư, thiết bị công nghệ thông tin, phụ kiện và phần mềm thương mại.
- Kiểm tra đảm bảo có hợp đồng giao nhận thầu.
- Kiểm tra đảm bảo có hồ sơ thiết kế thi công đã được phê duyệt.
- Kiểm tra có kế hoạch thi công chi tiết của đơn vị thi công lập.
- Kiểm tra biện pháp đảm bảo an toàn phòng, chống cháy, nổ, an toàn vận hành, vệ sinh công nghiệp tại hiện trường đối với xây lắp mạng, lắp đặt vật tư, thiết bị công nghệ thông tin và phụ kiện.

Sự phù hợp về năng lực của nhà thầu thi công đối với hồ sơ dự thầu và hợp đồng: Trước khi thi công, tư vấn giám sát thi công tiến hành.

- Kiểm tra nhân lực nhà thầu tham gia thi công.
- Kiểm tra điều kiện năng lực của chỉ huy thi công tại hiện trường theo quy định tại Điều 70 Nghị định số 102/2009/NĐ-CP đối với thi công xây lắp mạng, lắp đặt vật tư, thiết bị công nghệ thông tin và phụ kiện.
- Kiểm tra thiết bị thi công của nhà thầu. Đối với phần mềm nội bộ, cơ sở dữ liệu phải kiểm tra công cụ phát triển phần mềm và các công cụ khác.
- Kiểm tra quy trình đảm bảo chất lượng của nhà thầu trong trường hợp chủ đầu tư yêu cầu.
- Kiểm tra phòng thí nghiệm và các cơ sở sản xuất vật tư, thiết bị công nghệ thông tin phục vụ thi công của nhà thầu thi công (nếu có nêu trong hồ sơ dự thầu, hợp đồng).
- Kiểm tra việc ứng vốn của nhà thầu để thực hiện hợp đồng theo cam kết của nhà thầu (nếu có nêu trong hồ sơ dự thầu, hợp đồng).

Chất lượng vật tư, thiết bị công nghệ thông tin trước khi lắp đặt: Trước khi thi công, tư vấn giám sát thi công tiến hành.

- Kiểm tra giấy chứng nhận chất lượng của nhà sản xuất, kiểm tra chứng nhận hợp quy, kết quả kiểm định thiết bị của các tổ chức được cơ quan nhà nước có thẩm quyền công nhận đối với vật tư, thiết bị công nghệ thông tin lắp đặt trong dự án được nêu trong hồ sơ dự thầu trước khi đưa vào thi công.
- Kiểm tra các thông số kỹ thuật của các vật tư, thiết bị công nghệ thông tin so với các thông số kỹ thuật ghi trong hợp đồng và hồ sơ thiết kế thi công trước khi đưa vào thi công.

- Vật tư, thiết bị công nghệ thông tin trước khi lắp đặt phải được kiểm tra chất lượng. Khi nghi ngờ các kết quả kiểm tra, kiểm định, đơn vị tư vấn giám sát thi công phải kết hợp với chủ đầu tư thực hiện kiểm tra trực tiếp vật tư, thiết bị công nghệ thông tin lắp đặt trong dự án. Trường hợp các vật tư, thiết bị công nghệ thông tin không phù hợp với công nghệ, không đúng tính năng sử dụng so với thiết kế thi công được duyệt, hồ sơ dự thầu phải được đưa khỏi khu vực thi công.
- Biên bản nghiệm thu vật tư, thiết bị công nghệ thông tin lập theo mẫu.

Giám sát trong quá trình thi công: Trong quá trình thi công, tư vấn giám sát thi công tiến hành:

- Lập và ghi nhật ký giám sát thi công. Nội dung nhật ký giám sát thi công quy định chi tiết.
- Đối với xây lắp mạng, lắp đặt vật tư, thiết bị công nghệ thông tin, phụ kiện và phần mềm thương mại:

+ Kiểm tra và giám sát thường xuyên, liên tục, có hệ thống quá trình nhà thầu thi công triển khai các công việc tại hiện trường. Kết quả kiểm tra đều phải được ghi vào nhật ký giám sát thi công;

+ Kiểm tra biện pháp thi công của nhà thầu (đối với trường hợp thi công phức tạp);

+ Kiểm tra số lượng, hình thức bên ngoài, bên trong của các thiết bị công nghệ thông tin;

+ Kiểm tra bản quyền của phần mềm thương mại (tính hợp pháp, số lượng);

+ Tham gia công tác nghiệm thu vận hành thử. Khi quá trình vận hành thử đạt yêu cầu, tư vấn giám sát thi công và các bên tham gia tiến hành lập biên bản nghiệm thu vận hành thử thiết bị công nghệ thông tin theo mẫu;

+ Tham gia công tác nghiệm thu lắp đặt thiết bị công nghệ thông tin. Khi quá trình lắp đặt thiết bị đạt yêu cầu chất lượng, tư vấn giám sát thi công và các bên tham gia tiến hành lập biên bản nghiệm thu lắp đặt thiết bị công nghệ thông tin theo mẫu.

- Đối với phần mềm nội bộ, cơ sở dữ liệu:

+ Kiểm tra và giám sát quá trình nhà thầu triển khai các công việc tại hiện trường theo tiến độ thi công chi tiết. Kết quả kiểm tra đều phải được ghi vào nhật ký giám sát thi công;

+ Giám sát quá trình kiểm thử, vận hành thử: Tư vấn giám sát thi công có trách nhiệm tổng hợp kết quả kiểm thử, vận hành thử vào Báo cáo kết quả giám sát thi công. Việc kiểm thử, vận hành thử theo hướng dẫn tại Điều 46 Nghị định số 102/2009/NĐ-CP. Tư vấn giám sát thi công và các bên tham gia tiến hành lập biên bản nghiệm thu kiểm thử, vận hành thử theo mẫu.

+ Tham gia công tác nghiệm thu, bàn giao sản phẩm của dự án hoặc hạng mục dự án. Khi công tác nghiệm thu đạt yêu cầu chất lượng, tiến hành lập biên bản nghiệm thu bàn giao sản phẩm dự án ứng dụng công nghệ thông tin theo mẫu.

+ Phối hợp với các bên liên quan giải quyết những vướng mắc, phát sinh trong quá trình thi công.

+ Phát hiện sai sót, bất hợp lý về thiết kế thi công để điều chỉnh hoặc yêu cầu nhà thầu thiết kế điều chỉnh.

+ Xác nhận hồ sơ hoàn công: trong quá trình triển khai thực hiện dự án đơn vị giám sát thi công ký xác nhận vào các bản vẽ thực tế triển khai thi công.

+ Tổng hợp các biên bản, lập hồ sơ báo cáo giám sát thi công trình chủ đầu tư, đồng thời đề nghị chủ đầu tư tiến hành công tác tổng nghiệm thu bàn giao toàn bộ các sản phẩm của dự án. Biên bản tổng nghiệm thu bàn giao toàn bộ các sản phẩm của dự án lập theo mẫu. Nội dung báo cáo kết quả giám sát thi công quy định

Giám sát khối lượng thi công: Trong quá trình giám sát thi công dự án, tư vấn giám sát thi công thực hiện:

- Giám sát thi công theo khối lượng của thiết kế thi công được phê duyệt.
- Tính toán và xác nhận khối lượng thi công do nhà thầu thi công đã hoàn thành theo thời gian hoặc giai đoạn thi công và đối chiếu với thiết kế thi công được duyệt. Nếu có phát sinh khối lượng, phần phát sinh đó phải được chủ đầu tư phê duyệt. Kết quả phê duyệt phần khối lượng phát sinh đó là cơ sở để thanh toán, quyết toán dự án.

Giám sát tiến độ thi công: Trong quá trình giám sát thi công dự án, tư vấn giám sát thi công thực hiện:

- Kiểm tra việc nhà thầu thi công lập tiến độ thi công trước khi triển khai thi công. Tiến độ thi công phải phù hợp với tổng tiến độ của dự án đã được phê duyệt.
- Kiểm tra việc lập tiến độ thi công cho từng giai đoạn, tháng, quý, năm đối với dự án có quy mô lớn và thời gian thi công kéo dài.
- Kiểm tra việc nhà thầu thi công lập tiến độ thi công chi tiết, bố trí xen kẽ kết hợp các công việc cần thực hiện.
- Theo dõi, giám sát tiến độ thi công.
- Đề xuất với chủ đầu tư, nhà thầu thi công và các bên liên quan điều chỉnh tiến độ thi công trong trường hợp tiến độ thi công ở một số giai đoạn bị kéo dài. Trường hợp xét thấy tiến độ tổng thể của dự án bị kéo dài, chủ đầu tư phải báo cáo người quyết định đầu tư để quyết định việc điều chỉnh tổng tiến độ dự án.
- Đề xuất chủ đầu tư phạt vi phạm và yêu cầu nhà thầu thi công bồi thường thiệt hại khi kéo dài tiến độ thi công gây thiệt hại cho chủ đầu tư.

Bảo đảm an toàn phòng, chống cháy, nổ, an toàn vận hành và vệ sinh công nghiệp tại hiện trường trong quá trình thi công: Trong quá trình giám sát thi công dự án, tư vấn giám sát thi công thực hiện:

- Kiểm tra việc nhà thầu thi công lập các biện pháp đảm bảo an toàn cho người tham gia thi công.
- Yêu cầu các bên thỏa thuận biện pháp đảm bảo an toàn phòng, chống cháy, nổ, an toàn vận hành khi liên quan đến nhiều bên.
- Yêu cầu nhà thầu thi công phải thể hiện công khai các biện pháp an toàn phòng, chống cháy, nổ, nội quy về an toàn vận hành để mọi người biết và chấp hành.
- Cùng nhà thầu thi công và các bên có liên quan xử lý và báo cáo cơ quan quản lý nhà nước về an toàn lao động theo quy định pháp luật khi có sự cố về an toàn lao động.
- Kiểm tra việc nhà thầu thi công thực hiện các biện pháp đảm bảo vệ sinh công nghiệp theo các quy định hiện hành của Nhà nước.
- Kiểm tra việc bảo vệ hạ tầng kỹ thuật, trang thiết bị được lắp đặt trong vùng, khu vực, địa điểm thi công của dự án (nếu có). Trong trường hợp gây hư hại, hỏng hóc, ảnh hưởng tới vùng, khu vực, địa điểm thi công, tư vấn giám sát thi công phối hợp với nhà thầu thi công, chủ đầu tư tiến hành lập biên bản hiện trường đồng thời đề xuất chủ đầu tư yêu cầu nhà thầu thi công phải bồi thường thiệt hại.

Quản lý thay đổi trong thi công:

- Trong quá trình thi công, trường hợp phát hiện những yếu tố bất hợp lý hoặc xuất hiện yếu tố mới nếu không thay đổi thiết kế thi công sẽ ảnh hưởng đến chất lượng đầu tư của dự án, tiến độ thi công, biện pháp thi công và hiệu quả đầu tư của dự án, tư vấn giám sát thi công báo cáo chủ đầu tư đồng thời lập biên bản hiện trường theo mẫu.

Nhật ký giám sát thi công

- Đối với giám sát thi công xây lắp mạng, lắp đặt vật tư, thiết bị công nghệ thông tin, phụ kiện và phần mềm thương mại.

- Việc ghi nhật ký phải thường xuyên, kể cả những ngày nghỉ. Nội dung nhật ký giám sát thi công gồm:
  + Mô tả tóm tắt quá trình thi công;
  + Diễn biến tình hình thi công hàng ngày;
  + Tình trạng thực tế của vật tư, vật liệu, thiết bị sử dụng;
  + Những sai lệch so với hồ sơ thiết kế thi công, ghi rõ nguyên nhân, kèm theo biện pháp sửa chữa (nếu có).
  + Đối với giám sát thi công phát triển, nâng cấp, chỉnh sửa phần mềm nội bộ, cơ sở dữ liệu.
- Việc ghi nhật ký theo mốc thời gian. Nội dung nhật ký giám sát thi công gồm:
  + Xác nhận khối lượng công việc hoàn thành theo kế hoạch, tiến độ thi công chi tiết do nhà thầu thi công lập;
  + Xác nhận kết quả kiểm thử, vận hành thử đối với công việc được hoàn thành;
  + Những sai lệch so với hồ sơ thiết kế thi công, ghi rõ nguyên nhân, kèm theo biện pháp sửa chữa (nếu có).

Báo cáo kết quả giám sát thi công:

- Báo cáo kết quả giám sát thi công là cơ sở để chủ đầu tư tổ chức nghiệm thu bàn giao. Nội dung Báo cáo kết quả giám sát thi công gồm:
- Thông tin chung của dự án:
  + Tên dự án;
  + Tên hạng mục;
  + Địa điểm;
  + Tên chủ đầu tư;
  + Tên tổ chức thi công;
  + Tên tổ chức tư vấn thiết kế thi công;
  + Tên tổ chức tư vấn giám sát thi công.
- Nội dung giám sát:
  + Điều kiện thi công;
  + Sự phù hợp về năng lực của nhà thầu thi công đối với hồ sơ dự thầu và hợp đồng;
  + Chất lượng vật tư, thiết bị công nghệ thông tin trước khi lắp đặt;
  + Chất lượng thi công;
  + Khối lượng thi công;
  + Tiến độ thi công;
  + An toàn lao động và bảo vệ môi trường;
  + Thay đổi trong thi công.
  + Kết luận và kiến nghị.
  + Các phụ lục:
- Nhật ký giám sát thi công;
- Các biên bản.

2.3 Các kỹ thuật thi công công trình mạng

Để thi công hệ thống mạng hoàn chỉnh và hoạt động tối ưu, người thi công mạng bắt buộc phải tuân thủ một số nguyên tắc kỹ thuật thi công nhằm tránh rủi ro và dễ dàng quản trị sau này.

- Tuân thủ các nguyên tắc an toàn trong thi công cáp và lắp đặt thiết bị
- Lắp đặt được hệ thống cáp UTP, F-O và các phụ kiện
- Lắp đặt được thiết bị mạng Hub/Switch

Trong lúc lắp đặt thi công hệ thống cáp mạng chúng ta cần tuân thủ nghiêm ngặt các nguyên tắc sau: an toàn về điện, an toàn lắp đặt cáp

An toàn về điện:

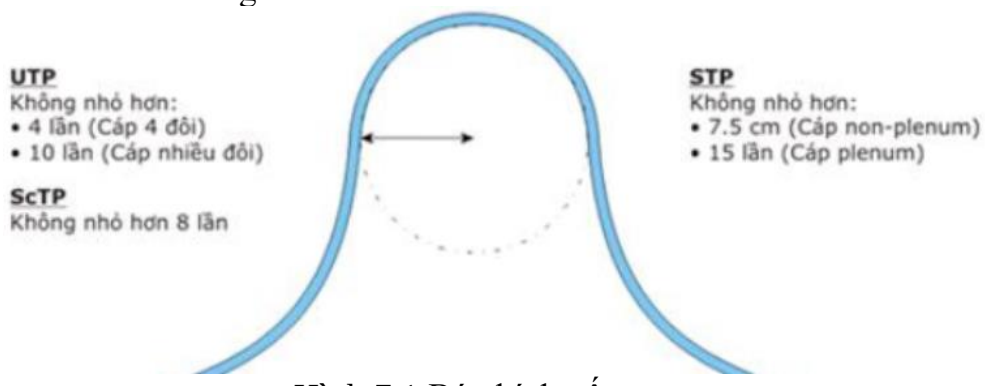
- Đường ống cáp điện không được lắp đặt chung với đường ống cáp mạng.
- Hai đường ống này phải đặt cách xa nhau một khoảng cách nhất định

An toàn lắp đặt cáp và thiết bị mạng:

- Trang bị đủ đồ bảo hộ lao động: quần áo, kính, găng, giày...
- Xác định các đường cáp có sẵn, bảo đảm trong tình trạng không hoạt động
- Dùng đúng dụng cụ
- Đặt bảng chú ý tại khu vực làm việc, tránh gây hại cho khách hàng hoặc công nhân

Thi công hệ thống cáp:

- Tiêu chuẩn lắp đặt cáp:
- Độ căng lực kéo:
  + Lực kéo tối đa khi thi công cáp 100/120 Ω UTP không vượt quá 25 lbs/ft
  + Lời khuyên: Không kéo cáp trong ống một lúc qua hơn hai góc 90°
  + Không kéo cáp trong ống qua chiều dài hơn 30 m
  + Đỡ cáp mỗi 1.2 -1.5 m
  + Tránh các vật hoặc góc nhọn, sắc bén
  + Dùng ròng rọc hoặc người đỡ tại các góc, cua
  + Không cố kéo khi cáp bị kẹt, Kéo cáp đi vòng tránh các vật cản.
  + Bán kính uốn cong:



Hình 7.1 Bán kính uốn cong

- Sức ép lên cáp:
  + Tránh dẫm/đạp lên cáp
  + Không đi cáp giữa các tường giả
  + Tránh bó cáp quá chặt

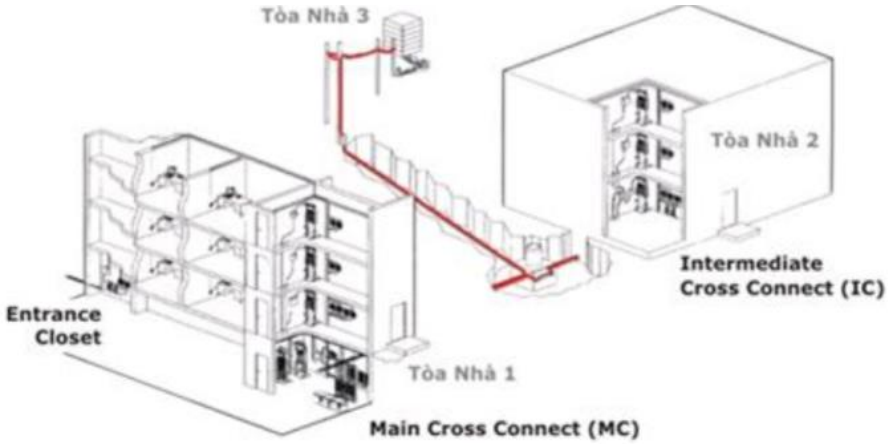
Bó đúng:

Bó sai:

- Chú ý trọng lượng của bó cáp trong máng.
  + EMI (Nhiễu sóng điện từ)/RFI:
- Tránh đặt cáp gần các nguồn nhiễu như dây điện, motor điện, đèn huỳnh quang,...
- Đi cáp trong ống - máng kim loại có thể giúp giảm ảnh hưởng của EMI
- Nếu đi cáp trần hoặc trong ống phi kim, phải giữ khoảng cách tối thiểu 120mm khỏi nguồn nhiễu. Các yêu cầu về khoảng cách tối thiểu có thể tìm trong:
  + TIA/EIA-569, NEC (National Electrical Code) Phần 800-52
  + Lắp đặt phụ kiện bảo vệ và hỗ trợ hạ tầng cáp mạng: Face plate, và Outlet
  + Lắp đặt: Cáp ngang, trục chính, Patchpanel
- Cáp ngang

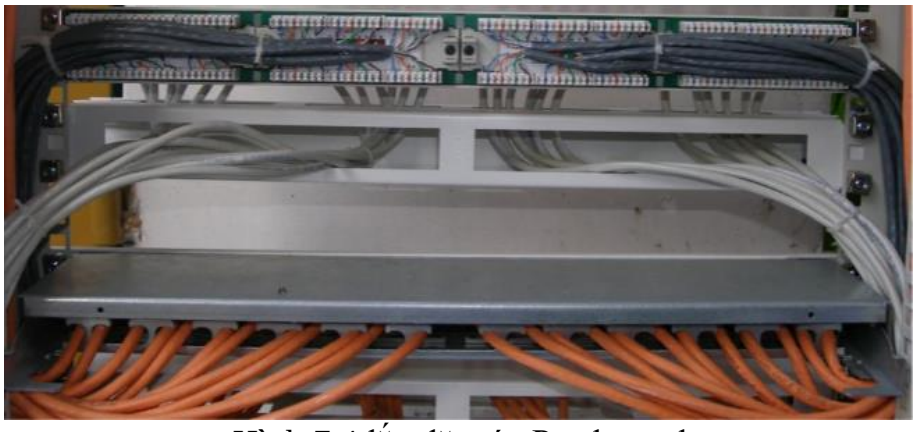
Hình 7.2 lắp đặt cáp ngang

- Trục chính



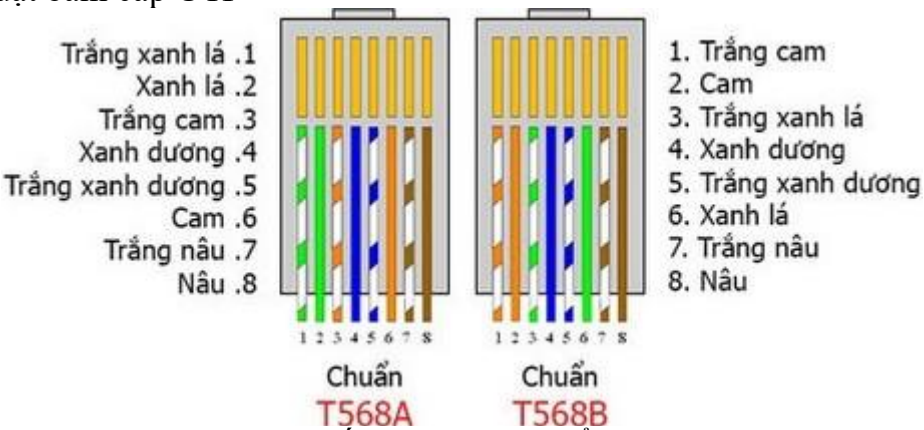
Hình 7.3 lắp đặt cáp trục chính

- Patchpanel



Hình 7.4 lắp đặt cáp Patchpanel

- Kỹ thuật bấm cáp UTP



Hình 7.5 Kỹ thuật bấm cáp UTP chuẩn T568A và T568B

2.4 Các kỹ thuật đấu nối

2.4.1 Bấm dây mạng

Là một trong những kỹ thuật bắt buộc người học kỹ thuật máy tính phải biết, bơi vì trong nhiều trường hợp đột xuất như dây mạng bị đứt, bị lỏng phải dùng dây mới, cũng như phải cắt bỏ đoạn bị đứt để nối lại ...

Nếu như dùng laptop, chúng ta có thể nối mạng internet bằng cách bắt wifi, tuy nhiên, nhiều trường hợp latop bị lỗi không bắt được wifi, hoặc bị đổi mật khẩu wifi và bạn không nhớ, lúc này bạn phải sử dụng tới dây mạng.

Bạn đã biết cách bấm dây mạng, cáp mạng cho máy tính chưa? Trong giáo trình này sẽ giúp các bạn cách bấm dây mạng có thể kết nối mạng internet cho máy tính.

Chuẩn bị:

- 01 kìm bấm cáp.
- 01 hộp đầu cáp RJ45.
- Đoạn dây cáp mạng (độ dài tùy theo nhu cầu sử dụng của bạn)
- Hiện nay có hai chuẩn bấm cáp là **T568A** nối 2 máy vi tính với nhau và **T568B** nối máy vi tính với hub hai chuẩn bấm cáp này gồm :
- ***Bấm thẳng*:** Kiểu này dùng để nối 2 thiết bị khác loại lại với nhau. VD: PC + Switch, Switch + Router

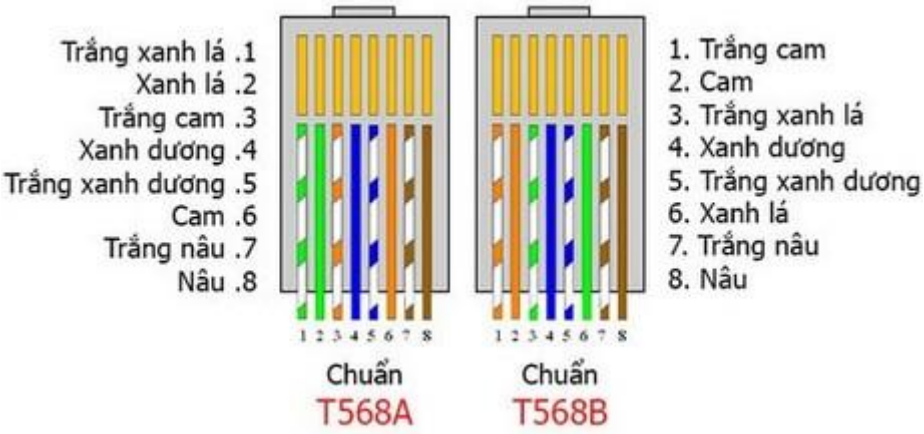
RJ-45 JACK TIA/EIA 568A STANDARD được gọi là chuẩn A.

T568A: **1. Trắng xanh lá 2. Xanh lá 3. Trắng cam 4. Xanh dương 5. Trắng xanh dương 6. Cam 7. Trắng nâu 8. Nâu**

- ***Bấm chéo*:** Kiểu này dùng để nối 2 thiết bị cùng loại lại với nhau. VD: PC-PC, PC-Router ...

RJ-45 JACK TIA/EIA 568B STANDARD được gọi là chuẩn B.

T568B: **1. Trắng cam 2. Cam 3. Trắng xanh lá 4. Xanh dương 5. Trắng xanh dương 6. Xanh lá 7. Trắng nâu 8. Nâu.**



Hình 7.6 chuẩn T568A và T568B

Một số bạn thắc mắc: Khi bấm dây giữ nguyên thức tự sau khi cắt dây (không đảo vị trí dây) với thiết bị đồng đẳng như PC-Router mà mạng vẫn dùng được. Điều này không sai, nếu bạn bấm thẳng có thể vẫn nhận nhưng chất lượng đường truyền đôi khi không được tốt, **do thiếu khả năng khử nhiễu điện từ** (có được khi điều chỉnh vị trí cặp dây)

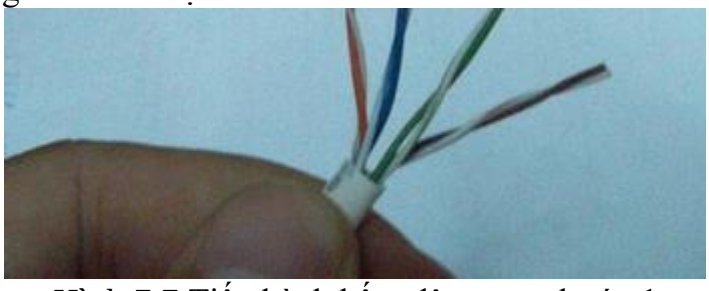
Trong một dây cáp đạt chuẩn qui định bao gồm tám sợi dây đồng trong đó mỗi hai sợi xoắn với nhau thành từng cặp theo qui định nâu - trắng nâu, cam - trắng cam - xanh lá - trắng xanh lá, xanh dương - trắng xanh dương và 1 sợi dây kẽm. Sợi dây kẽm này chỉ có

chức năng làm cho sợi dây cáp chắc chắn hơn. Sợi dây cáp này sẽ được nối với một đầu RJ45 để bấm dây mạng thì phải bấm tám sợi dây đồng vào các điểm tiếp xúc bằng đồng trong đầu RJ45.

Tiến hành bấm dây mạng

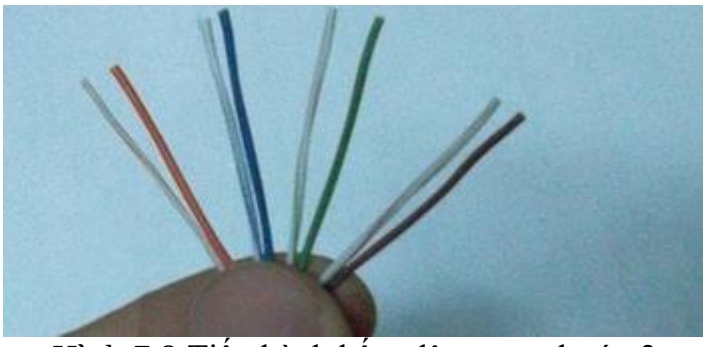
- ***Cách bấm cáp chéo***

+ ***Bước 1:*** Các bạn dùng kìm hoặc kéo cắt vỏ đầu cáp cứ cắt dài thêm chút tý xếp màu cho dễ khoảng 4 cm là được .



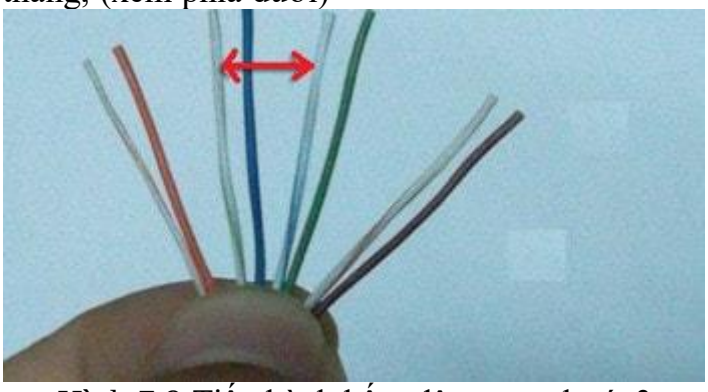
Hình 7.7 Tiến hành bấm dây mạng bước 1

+ Bước 2: Gỡ các đầu xoắn và xếp theo thứ tự: Màu trắng xếp trước - Cam - Xanh da trời - Xanh lá - Nâu.



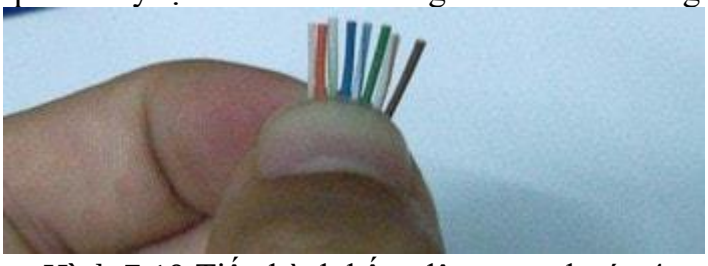
Hình 7.8 Tiến hành bấm dây mạng bước 2

+ Bước 3: Đổi chỗ màu trắng của xanh lá cây và màu trắng của xanh da trời cho nhau, **Lưu ý** ở bước này nếu bạn **có thể không cần đổi vị trí** cho dễ thì dây mạng sẽ được kết nối theo chuẩn thẳng, (xem phía dưới)



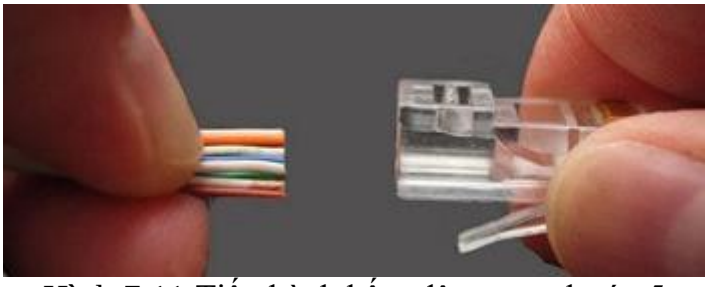
Hình 7.9 Tiến hành bấm dây mạng bước3

+ ***Bước 4:*** Xếp các dây lại sát nhau và dùng kìm cắt cho bằng.



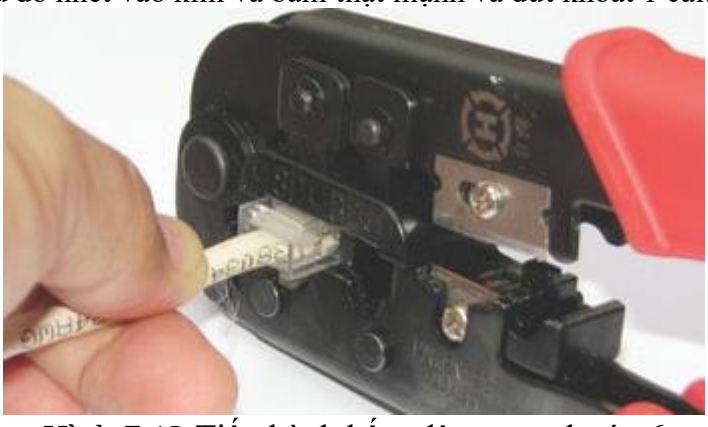
Hình 7.10 Tiến hành bấm dây mạng bước 4

+ ***Bước 5:*** Các bạn tiến hành đút dây vào đầu cáp thật sâu để các đầu dây chạm lõi đồng.



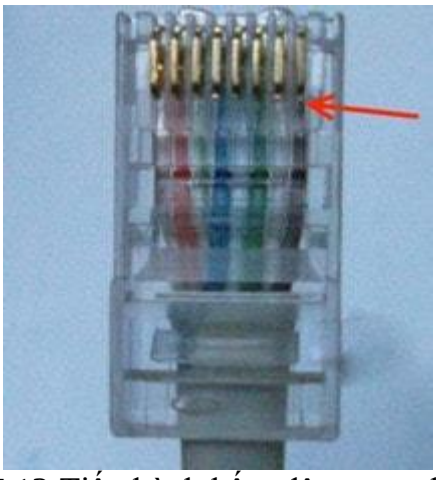
Hình 7.11 Tiến hành bấm dây mạng bước 5

+ ***Bước 6:*** Sau đó nhét vào kìm và bấm thật mạnh và đứt khoát 1 cái.



Hình 7.12 Tiến hành bấm dây mạng bước 6

+ ***Bước 7:*** Quan sát xem các dây đồng của dây và lá đồng trong đâu RJ 45 đã kít chưa.



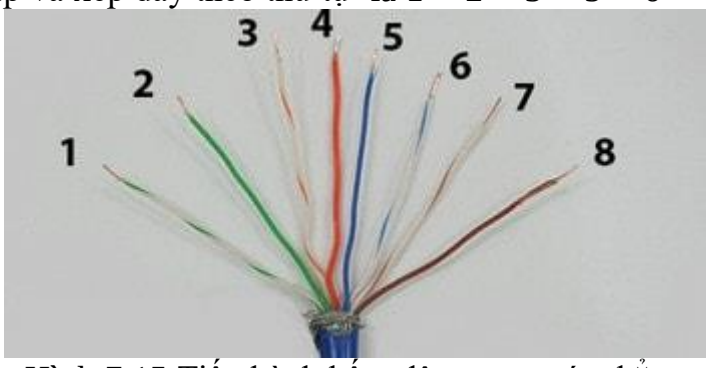
Hình 7.13 Tiến hành bấm dây mạng bước 7

+ ***Bước 8:*** Cuối cùng cắm 1 đâu vừa làm xong vào máy tính. Còn đầu kia thì tiến hành làm tương tự.

Hình 7.14 Tiến hành bấm dây mạng bước 8

Cách bấm cáp thẳng

- Cắt vỏ dây cáp và xếp dây theo thứ tự là 1-->2-->3-->5-->6-->4-->7-->8.



Hình 7.15 Tiến hành bấm dây mạng cáp thẳng

- Xếp sát lại và cắt cho bằng lại chừa lại 1 đoạn vừa đủ với đầu RJ45.

Hình 7.16 Tiến hành bấm dây mạng cáp thẳng

- Sau đó các bước còn lại làm tương tự như bấm cáp chéo.

2.4.2 Bấm dây mạng âm tường sử dụng AMP

Việc bấm mạng âm tường vì nó khác so với bấm mạng cáp 5e nhiều lần. Trong giáo trình này sẽ hướng dẫn bạn cách bấm mạng LAN cáp 5e âm tường sử dụng AMP.

- Đầu tiên các bạn cần chuẩn bị các vật liệu sau:
  + Ổ LAN âm tường - AMP
  + Kìm bấm mạng cáp 5e.
  + 1 đoạn dây LAN 2 đầu bấm sẵn.

Hình 7.17 ổ LAN âm tường - AMP

Hình ảnh mặt cổng internet LAN âm tường thông qua ổ mạng AMP thường có bán ở các tiệm điện với giá chỉ từ 60.000đ - 100.000đ tùy theo chất lượng

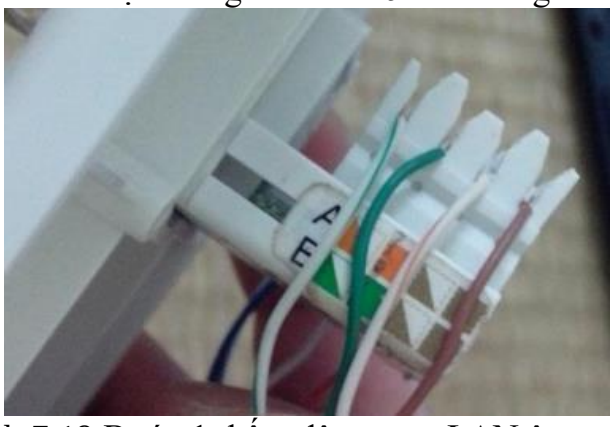
Hình 7.18 ảnh chi tiết Jack cấm AMP âm tường

Hình ảnh chi tiết Jack cấm AMP âm tường bao gồm 1 cổng LAN ra và cổng còn lại gồm 8 sợi mạng tín hiệu âm tường bên trong

Trong giáo trình này hướng dẫn cho các bạn cách bấm dây mạng LAN âm tường sử dụng AMP bằng vài thao tác đơn giản như sau:

Tháo ổ AMP ra và ta sẽ có thấy có 2 bên:

- 1 Bên bạn bấm theo thứ tự: Trắng Cam - Cam - Trắng Xanh Đậm - Xanh Đậm.
- 1 Bên bạn bấm theo thứ tự: Trắng Xanh - Xanh - Trắng Nâu - Nâu.



Hình 7.19 Bước 1: bấm dây mạng LAN âm tường

- Cắm dây vào modem và test xem có tín hiệu sáng cổng Internet là thành công.

2.5 Các bước tiến hành thi công

Chắc hẳn sẽ có rất nhiều bạn đọc còn chưa nắm được quy trình lắp đặt mạng Lan thường qua những bước nào để có hệ thống mạng hoàn chỉnh nhất. Trong giáo trình này xin đưa ra một quy trình lắp mạng Lan đơn giản để quý bạn đọc tham khảo.

Các bước tiến hành triển khai lắp đặt hệ thống mạng lan:

- **Bước 1**: Khảo sát và thiết kế hệ thống mạng

+ Sau khi tiếp nhận thông tin kỹ thuật sẽ đến khảo sát theo các tiêu chí: mục đích sử dụng của khách hàng và yêu cầu sử dụng thiết bị, khảo sát mặt bằng, kết cấu toà nhà và vị trí lắp đặt thiết bị, điều kiện thi công và chất lượng vật liệu thi công (cable, ống, nẹp….) Các điều kiện có thể ảnh hưởng đến hệ thống (điện, môi trường…)

+ Thiết kế chi tiết: Vẽ kỹ thuật chi tiết hệ thống loại thiết bị được dùng (biểu giá, tính năng kỹ thuật, thời hạn bảo hành) bao gồm: Sơ đồ logic, sơ đồ lắp đặt… số lượng vật tư và các linh kiện đi kèm; thống nhất hời gian thi công.

- **Bước 2:** Lắp đặt hệ thống

+ Thi công hệ thống cáp mạng
+ Triển khai thiết bị dẫn (ống nhựa, nẹp, dây dẫn …)
+ Triển khai hệ thống cáp mạng theo đúng sơ đồ thiết kế
+ Đánh dấu dây cáp và kết nối vào bộ tập trung (Swich, Router, Firewall…)
+ Gắn máy tính vào hệ thống mạng
+ Gắn các thiết bị ngoại vi vào hệ thống mạng
+ Cài đặt hệ thống mạng
+ Phân chia nhóm người dùng theo VLAN (chia system thành các mạng con)
+ Cấu hình Router, các giao thức định tuyến, load-balancing…
+ Cấu hình tường lửa, tạo DMZ cho Server
+ Cài đặt hệ điều hành cho server
+ Cài đặt giao thức và các dịch vụ mạng
+ Tạo nhóm người dùng
+ Thiết lập tài khoản của người dùng
+ Phân quyền người dùng
+ Cài đặt chương trình ứng dụng mạng

+ Cài đăt giao thức các máy Client
+ Tạo tài khoản máy Client
+ Chia sẻ tài nguyên máy Cliet

- **Bước 3**: Chuyển giao hệ thống
+ Nghiệm thu hệ thống và chuyển giao
+ Kiểm tra sự tương thích và tính ổn định của hệ thống
+ Nghiệm thu hệ thống chuyển giao hồ sơ thiết bị (phiếu bảo hành, hoá đơn thanh toán…)
+ Chuyển giao hợp đồng thiết kế và lắp đặt, sơ đồ mạng
+ Hướng dẫn sử dụng hệ thống và đào tạo nhân sự.

Trên đây là các bước chi tiết cơ bản khi bạn muốn thi công lắp đặt mạng lan, cũng tùy thuộc vào địa hình, quy mô văn phòng, vị trí lắp đặt mà bạn lựa chọn cách thì công cho phù hợp. Thiết kế sao cho có thể thêm bớt thiết bị trong hệ thống dễ dàng để có thể thay đổi về sau.

2.6 Đấu nối và cấu hình phần cứng

Thiết lập mạng:

- **Lắp card mạng:** Ban đầu bạn phải lắp card mạng vào máy tính bằng cách: tắt máy tính, tháo vỏ của máy tính, sau đó bạn tìm khe (slot) trống để cắm card mạng vào. Vặn ốc lại. Sau đó đóng vỏ máy lại.
- **Cài driver cho card mạng:** Sau khi bạn đã lắp card mạng vào trong máy, khi khởi động máy tính lên, nó sẽ tự nhận biết có thiết bị mới và yêu cầu bạn cung cấp driver, lúc đó bạn chỉ việc đưa đĩa driver vào và chỉ đúng đường dẫn nơi lưu chứa driver (bạn có thể làm theo tờ hướng dẫn cài đặt kèm theo khi bạn mua card mạng). Sau khi cài đặt hoàn tất bạn có thể tiến hành thiết lập nối dây cáp mạng.
- **Nối kết cáp mạng:** Trong mô hình này bạn dùng cáp xoắn để nối kết. Yêu cầu trước tiên là bạn phải đo khoảng cách từ nút (từ máy tính) muốn kết nối vào mạng tới thiết bị trung tâm (có thể Hub hay Switch). Sau đó bạn cắt một đoạn cáp xoắn theo kích thước mới đo, rồi bạn bấm hai đầu cáp với chuẩn RJ_45. Khi đã hoàn tất bạn chỉ việc cắm một đầu cáp mạng này vào card mạng, và đầu kia vào một port của thiết bị trung tâm (Hub hay Switch). Sau khi nối kết cáp mạng nếu bạn thấy đèn ngay port (Hub hay Switch) mới cắm sáng lên tức là về liên kết vật lý giữa thiết bị trung tâm và nút là tốt. Nếu không thì bạn phải kiểm tra lại cáp mạng đã bấm tốt chưa, hay card mạng đã cài tốt chưa.

Định cấu hình mạng:

- Sau khi đã thiết lập mạng, hay nói cách khác là đã thiết lập nối kết về phần cứng giữa thiết bị trung tâm và nút thì các nút vẫn chưa thể thông tin với nhau được. Để giữa các nút có thể thông tin với nhau được thì yêu cầu bạn phải thiết lập các nút (các máy tính) trong LAN theo một chuẩn nhất định. Chuẩn là một giao thức (Protocol) nhằm để trao đổi thông tin giữa hai hệ thống máy tính, hay hai thiết bị máy tính. Giao thức (Protocol) còn được gọi là nghi thức hay định ước của mạng máy tính. Trong một mạng ngang hàng (Peer to Peer) các máy tính sử dụng hệ điều hành của Microsoft thông thường sử dụng giao thức TCP/IP (Transmission control protocol/ internet protocol).
- **Gán IP cho mạng:** Khi định cấu hình và gán IP cho mạng có hai kiểu chính: Gán IP theo dạng động (Dynamic): Thông thường sau khi bạn đã nối kết vật lý thành công, và gán TCP/IP trên mỗi nút (máy tính) thì các máy đã có thể liên lạc được với nhau, bạn không cần phải quan tâm gán IP nữa. Gán IP theo dạng tĩnh (Static): Nếu bạn có nhu cầu là thiết lập mạng để chia sẻ tài nguyên trên mạng như, máy in, file, cài đặt mail offline, hay bạn sẽ cài share internet trên một máy bất kỳ, sau đó định cấu hình cho các máy khác đều kết nối ra được internet thì bạn nên thiết lập gán IP theo dạng tĩnh.

Windows 7 trở lên, bạn chuột phải vào biểu tượng mạng trên khay hệ thống > **Open Network and Sharing Center** > **Change adapter Settings** > chuột phải lên tên mạng, chọn **Properties** > kéo xuống chọn **TCP/IPv4** > **Properties.** Rồi chọn Dynamic hoặc Static.

Lưu ý: Việc đặt địa chỉ TCP/IP tĩnh là điều bắt buộc trong các mạng ngang hàng dùng giao thức TCP/IP. Nhưng với mạng cục bộ chạy trên nền Windows NT theo mô hình Client/Server bạn cũng nên đặt địa chỉ tĩnh để dễ dàng quản lý và phát hiện lỗi. Các máy tính trong mạng phải có địa chỉ IP không trùng nhau và phải cùng một Subnet Mask. Sau khi đã hoàn tất các bước trên thì các nút, các máy tính trong mạng LAN của bạn đã có thể trao đổi thông tin cho nhau, chia sẻ tài nguyên giữa các máy.

2.7 Nhật kí thi công

NHẬT KÝ THI CÔNG CÔNG TRÌNH

QUYỂN SỐ: …/NKCT

TÊN CÔNG TRÌNH: .....

ĐỊA ĐIỂM XÂY DỰNG: .....

CHỦ ĐẦU TƯ: .....

ĐƠN VỊ THI CÔNG: DỊCH VỤ VI TÍNH KIM TÀI COMPUTER

Hotline : 0919005366

NHẬT KÝ THI CÔNG CÔNG TRÌNH

QUYỂN SỐ: …/NKCT-NV

1. Tên công trình (hạng mục công trình): .....
2. Địa điểm xây dựng:.....
3. Chủ đầu tư: .....

Điện thoại: .....

4. Nhà thầu tư vấn giám sát thi công công trình:.....

Họ và tên kỹ sư giám sát: .....

Điện thoại: .....

5. Nhà thầu thi công công trình: .....

DỊCH VỤ VI TÍNH KIM TÀI COMPUTER

Họ và tên chỉ huy trưởng công trình: .....

Điện thoại: .....

6. Tên nhà thầu thiết kế kỹ thuật, thiết kế bản vẽ thi công: .....

Họ và tên kiến trúc sư chủ trì:.....

Họ và tên kỹ sư chủ trì:.....

Khởi công theo hợp đồng ngày..... Thực tế.....

Bàn giao theo hợp đồng ngày ..... Thực tế.....

Sổ này gồm: 03 trang, đánh số thứ tự từ 01 đến số 03 đóng dấu giáp lai và chữ ký của ông:

.....

Họ tên, chữ ký người phụ trách thi công công trình và quản lý quyển nhật ký :

Họ tên: .....

Chữ ký: .....

Họ tên, chữ ký người phụ trách giám sát thi công của Chủ đầu tư:

Họ tên: .....

Chữ ký: .....

Củ chi, Ngày ..... tháng ..... năm .....

DỊCH VỤ VI TÍNH KIM TÀI COMPUTER

Giám đốc

DANH SÁCH CB CHỈ HUY VÀ CB KỸ THUẬT CỦA CÔNG TRÌNH

Họ và tên	Chức danh	Nhiệm vụ	Điện thoại	Ghi chú

Ngày ..... tháng ..... năm .....

1. Thời tiết

   □ *Bình thường* □ *Mưa* □ *Nắng*

2. Công việc thực hiện

   2.1 Thiết bị:

   .....

   .....

   2.2 Nhân công:

   .....

   .....

3. Nhận xét đánh giá của phụ trách giám sát hoặc chủ đầu tư:

   3.1 Công tác vệ sinh môi trường

   □ Tốt □ Bình thường □ kém

   3.2 Công tác an toàn lao động

   □ Tốt □ Bình thường □ kém

   3.3 Ý kiến khác:

   .....

   .....

4. Ý kiến tiếp thu của nhà thầu:

   .....

   .....

CÁN BỘ GIÁM SÁT
hoặc CHỦ ĐẦU TƯ
(Ký, ghi rõ họ tên)

CÁN BỘ PHỤ TRÁCH THI CÔNG
(Ký, ghi rõ họ tên)

Câu hỏi ôn tập

1. Mô tả quy trình thiết kế một hệ thống mạng;
2. Xác định cách đấu cáp cho các thiết bị phần cứng;
3. Cài đặt, cấu hình các dịch vụ mạng; Cấu hình các giao thức mạng;
4. Xây dựng các phương án bảo mật mạng;
5. Lập nhật kí thi công mạng;

TÀI LIỆU THAM KHẢO

- [1]. KS. Nguyễn Công Sơn, *Hướng Dẫn Quản Trị Mạng Microsoft Windows Server 2003*, nhà xuất bản: Tổng Hợp TP. Hồ Chí Minh, năm 2005.
- [2]. Th.s Ngô Bá Hùng, Giáo trình thiết kế và cài đặt mạng, năm 2002.
- [3]. Giáo trình *Thiết kế và xây dựng mạng LAN và WAN*; Trung tâm Điện toán và Truyền số liệu KV1.
- [4].Website: https://vnpro.vn, https://quantrimang.com, https://cuongquach.com, và một số trang mạng khác.

PHỤ LỤC BÀI TẬP

Câu hỏi ôn tập bài 4:

Hướng dẫn

1. Kết nối cáp cho các thiết bị như sơ đồ bên trên

2. Xóa cấu hình cho các thiết bị và reload

3. Cấu hình các thông số cơ bản cho các router

4. Cấu hình địa chỉ ip cho các thiết bị

Trên router R1:

Đặt địa chỉ và kích hoạt interface fastethernet 0/0

Code:

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 172.16.3.1 255.255.255.0
R1(config-if)#no shutdown
*Mar 1 01:16:08.212: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 01:16:09.214: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,changed state to up
R1(config-if)#
```

Đặt địa chỉ và kích hoạt interface serial 0/0/0

Code:

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface Serial 0/0/0
R1(config-if)#ip address 172.16.2.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#clock rate 64000
```

Trên router R2:

Đặt địa chỉ và kích hoạt interface fastethernet 0/0

Code:

```
R2(config)#interface fastethernet 0/0
R2(config-if)#ip address 172.16.1.1 255.255.255.0
R2(config-if)#no shutdown
*Mar 1 01:16:08.212: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 01:16:09.214: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R2(config-if)#
```

Đặt địa chỉ và kích hoạt interface serial 0/0/0

Code:

```
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface Serial 0/0/0
R2(config-if)#ip address 172.16.2.2 255.255.255.0
R2(config-if)#no shutdown
```

Đặt địa chỉ và kích hoạt interface serial 0/0/1

Code:

```
R2(config)#interface Serial 0/0/1
```

R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#clock rate 64000
R2(config-if)#no shutdown
Trên router R3:
Đặt địa chỉ và kích hoạt interface fastethernet 0/0
Code:
R3(config)#interface fastethernet 0/0
R3(config-if)#ip address 192.168.2.1 255.255.255.0
R3(config-if)#no shutdown
*Mar 1 01:16:08.212: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 01:16:09.214: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R3(config-if)#
Đặt địa chỉ và kích hoạt interface serial 0/0/1
Code:
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface Serial 0/0/1
R3(config-if)#ip address 192.168.1.1 255.255.255.0
R3(config-if)#no shutdown
Trên PC1:
Ip address: 172.16.3.10
Subnet mask: 255.255.255.0
Default gateway: 172.16.3.1
Trên PC2:
Ip address: 172.16.1.10
Subnet mask: 255.255.255.0
Default gateway: 172.16.1.1
Trên PC3:
Ip address: 192.168.2.10
Subnet mask: 255.255.255.0
Default gateway: 192.168.2.1

5. Kiểm tra cấu hình ban đầu

Kiểm tra trạng thái của các interface
Router R1
Code:
R1#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 172.16.3.1 YES manual up up
FastEthernet0/1 unassigned YES unset administratively down down
Serial0/0/0 172.16.2.1 YES manual up up
Serial0/0/1 unassigned YES manual up up
Vlan1 unassigned YES manual administratively down down
Router R2
Code:
R2#show ip interface brief
Interface IP-Address OK? Method Status Protocol

FastEthernet0/0 172.16.1.1 YES manual up up
FastEthernet0/1 unassigned YES unset administratively down down
Serial0/0/0 172.16.2.2 YES manual up up
Serial0/0/1 192.168.1.2 YES manual up up
Vlan1 unassigned YES manual administratively down down

Router R3

Code:

R3#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 192.168.2.1 YES manual up up
FastEthernet0/1 unassigned YES unset administratively down down
Serial0/0/0 unassigned YES manual up up
Serial0/0/1 192.168.1.1 YES manual up up
Vlan1 unassigned YES manual administratively down down

Kiểm tra bảng định tuyến của 3 router

Router R1

Code:

R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
172.16.0.0/24 is subnetted, 2 subnets
C 172.16.2.0 is directly connected, Serial0/0/0
C 172.16.3.0 is directly connected, FastEthernet0/0

Router R2

Code:

R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
U - per-user static route, o – ODR
Gateway of last resort is not set
172.16.0.0/24 is subnetted, 2 subnets
C 172.16.1.0 is directly connected, FastEthernet0/0
C 172.16.2.0 is directly connected, Serial0/0/0
C 192.168.1.0/24 is directly connected, Serial0/0/1

Router R3

Code:

R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
U - per-user static route, o – ODR
Gateway of last resort is not set
C 192.168.1.0/24 is directly connected, Serial0/0/1
C 192.168.2.0/24 is directly connected, FastEthernet0/0

6. Test kết nối

Trên PC1: ping đến địa chỉ IP trên interface fastethernet 0/0 của router R1: thành công
Trên router R1: ping đến địa chỉ IP trên interface serial 0/0/0 của router R2: thành công
Trên PC2: ping đến địa chỉ IP trên interface fastethernet 0/0 của router R2: thành công
Trên router R2: ping đến địa chỉ IP trên interface serial 0/0/1 của router R3: thành công
Trên PC3: ping đến địa chỉ IP trên interface fastethernet 0/0 của router R3: thành công

7. Cấu hình static routing trên các router

Command cấu hình static route sử dụng ip next hop:

Code:

Router(config)# ip route network-address subnet-mask ip-address

Cấu hình trên router R1:

Code:

R1(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.2
R1(config)#ip route 192.168.1.0 255.255.255.0 172.16.2.2
R1(config)#ip route 192.168.2.0 255.255.255.0 172.16.2.2

Cấu hình trên router R2:

Code:

R2(config)#ip route 172.16.3.0 255.255.255.0 172.16.2.1
R2(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.1

Cấu hình trên router R3:

Code:

R3(config)#ip route 172.16.3.0 255.255.255.0 192.168.1.2
R3(config)#ip route 172.16.1.0 255.255.255.0 192.168.1.2
R3(config)#ip route 172.16.2.0 255.255.255.0 192.168.1.2

Kiểm tra kết quả định tuyến

Code:

R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
U - per-user static route, o – ODR
Gateway of last resort is not set
172.16.0.0/24 is subnetted, 3 subnets
C 172.16.3.0 is directly connected, FastEthernet0/0
C 172.16.2.0 is directly connected, Serial0/0/0
S 172.16.1.0 [1/0] via 172.16.2.2
S 192.168.1.0/24 [1/0] via 172.16.2.2
S 192.168.2.0/24 [2/0] via 172.16.2.2
R1#

_____

Code:

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
U - per-user static route, o – ODR
Gateway of last resort is not set
172.16.0.0/24 is subnetted, 3 subnets
C 172.16.1.0 is directly connected, FastEthernet0/0
C 172.16.2.0 is directly connected, Serial0/0/0
S 172.16.3.0 [1/0] via 172.16.2.1
C 192.168.1.0/24 is directly connected, Serial0/0/1
S 192.168.2.0/24 [1/0] via 192.168.1.1
R2#
```

_____

Code:

```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
U - per-user static route, o – ODR
Gateway of last resort is not set
172.16.0.0/24 is subnetted, 3 subnets
S 172.16.1.0 [1/0] via 192.168.1.2
S 172.16.2.0 [1/0] via 192.168.1.2
S
172.16.3.0 [2/0] via 192.168.1.2
C 192.168.1.0/24 is directly connected, Serial0/0/1
C 192.168.2.0/24 is directly connected, FastEthernet0/0
R3#Command cấu hình static route sử dụng exit interface:
```

Code:

```
Router(config)# ip route network-address subnet-mask exit-interface
```

Xóa cấu hình định tuyến trên router R3

Code:

```
R3(config)#no ip route 172.16.3.0 255.255.255.0 192.168.1.2
R3(config)#no ip route 172.16.1.0 255.255.255.0 192.168.1.2
R3(config)#no ip route 172.16.2.0 255.255.255.0 192.168.1.2
```

Cấu hình định tuyến lại cho R3 sử dụng exit interface

Code:

```
R3(config)#ip route 172.16.3.0 255.255.255.0 serial 0/0/1
R3(config)#ip route 172.16.1.0 255.255.255.0 serial 0/0/1
R3(config)#ip route 172.16.2.0 255.255.255.0 serial 0/0/1
```

Kiểm tra kết quả định tuyến

Code:
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
U - per-user static route, o – ODR
Gateway of last resort is not set
172.16.0.0/24 is subnetted, 3 subnets
S 172.16.1.0 is directly connected, Serial0/0/1
S 172.16.2.0 is directly connected, Serial0/0/1
S 172.16.3.0 is directly connected, Serial0/0/1
C 192.168.1.0/24 is directly connected, Serial0/0/1
C 192.168.2.0/24 is directly connected, FastEthernet0/0
R3#

8.Cấu hình static default route cho các router

Command cấu hình static default route:
Code:
Router(config)#ip route 0.0.0.0 0.0.0.0 { ip-address | interface }
Cấu hình cho router R1:
Code:
R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2
Cấu hình cho rouer R2:
Code:
R2(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
Cấu hình cho router R3:
Code:
R3(config)#ip route 0.0.0.0 0.0.0.0 Fastethernet0/1
Kiểm tra bảng định tuyến của các router
Code:
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
U - per-user static route, o – ODR
Gateway of last resort is 172.16.2.2 to network 0.0.0.0
172.16.0.0/24 is subnetted, 3 subnets
C 172.16.3.0 is directly connected, FastEthernet0/0
C 172.16.2.0 is directly connected, Serial0/0/0
S 172.16.1.0 [1/0] via 172.16.2.2
S 192.168.1.0/24 [1/0] via 172.16.2.2
S 192.168.2.0/24 [2/0] via 172.16.2.2
S* 0.0.0.0/0 [1/0] via 172.16.2.2
R1#

Code:
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
U - per-user static route, o – ODR
Gateway of last resort is 192.168.1.1 to network 0.0.0.0
172.16.0.0/24 is subnetted, 3 subnets
C 172.16.1.0 is directly connected, FastEthernet0/0
C 172.16.2.0 is directly connected, Serial0/0/0
S 172.16.3.0 [1/0] via 172.16.2.1
C 192.168.1.0/24 is directly connected, Serial0/0/1
S 192.168.2.0/24 [1/0] via 192.168.1.1
S* 0.0.0.0/0 [1/0] via 192.168.1.1
R2#

Code:
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
U - per-user static route, o – ODR
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
172.16.0.0/24 is subnetted, 3 subnets
S 172.16.1.0 [1/0] via 192.168.1.2
S 172.16.2.0 [1/0] via 192.168.1.2
S 172.16.3.0 [2/0] via 192.168.1.2
C 192.168.1.0/24 is directly connected, Serial0/0/1
C 192.168.2.0/24 is directly connected, FastEthernet0/0
S* 0.0.0.0/0 is directly connected, FastEthernet0/1
R3#

9. Cấu hình summary route

Tiến hành summary ba đường mạng bằng tay
172.16.1.0 10101100.00010000.00000001.00000000
172.16.2.0 10101100.00010000.00000010.00000000
172.16.3.0 10101100.00010000.00000011.00000000
=> Đường mạng summary được là: 172.16.0.0/22
Cấu hình static summary route cho router R3
Xóa cấu hình định tuyến đang có trên router R3
Code:
R3(config)#no ip route 172.16.3.0 255.255.255.0 192.168.1.2
R3(config)#no ip route 172.16.1.0 255.255.255.0 192.168.1.2
R3(config)#no ip route 172.16.2.0 255.255.255.0 192.168.1.2
Cấu hình một đường static summary route trên router R3

Code:
R3(config)#ip route 172.16.0.0 255.255.252.0 192.168.1.2
Kiểm tra bảng định tuyến của router R3
Code:
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
U - per-user static route, o – ODR
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
172.16.0.0/22 is subnetted, 1 subnets
S 172.16.0.0 [1/0] via 192.168.1.2
C 192.168.1.0/24 is directly connected, Serial0/0/1
C 192.168.2.0/24 is directly connected, FastEthernet0/0
S* 0.0.0.0/0 is directly connected, FastEthernet0/1
R3#
Test kết nối:
Ping từ PC3 đến PC1: thành công
Ping từ PC3 đến PC2: thành công
10. Dùng lệnh show running-config để kiểm tra cấu hình các router.
Code:
R1#show running-config
R2#show running-config
R3#show running-config

Câu hỏi ôn tập bài 6:

Thực hiện

- Bước 1: Thực hiện kết nối và cấu hình cơ bản
  + Cấu hình IP để quản lý Switch từ xa:
  + *Switch(config)#interface vlan 1*
  + *Switch(config-if)#ip address 192.168.1.254 255.255.255.0*
  + *Switch(config-if)#no shutdown*
- Bước 2: Cấu hình thông tin VLAN, gán port cho VLAN, cấu hình đường Trunk nối giữa Switch và Router.
- Cấu hình thông tin VLAN:
  + *Switch(config)#vlan 2*
  + *Switch(config-vlan)#exit*
  + *Switch(config)#vlan 3*
  + *Switch(config-vlan)#exit*
- Cấu hình gán Port cho VLAN :
  + *Switch(config)#interface F0/2*
  + *Switch(config-if)#switchport access vlan 2*
  + *Switch(config-if)#exit*
  + *Switch(config)#interface F0/3*
  + *Switch(config-if)#switchport access vlan 3*
  + *Switch(config-if)#exit*
- Cấu hình đường Trunk giữa Switch và Router:
  + *Switch(config)#interface G0/1*
  + *Switch(config-if)#switchport mode trunk*
- Bước 3: Cấu hình định tuyến giữa các VLAN
  + Cấu hình các sub-interface tương ứng với các VLAN:
- *R1(config)#interface G0/1*
- *R1(config-if)#ip address 192.168.1.1 255.255.255.0*
- *R1(config-if)#no shutdown*
- *R1(config)#interface G0/1.2 ß sub-interface cho VLAN 2*
- *R1(config-subif)#encapsulation dot1Q 2 ß đóng gói giao thức dot1.q cho VLAN 2*
- *R1(config-subif)#ip address 192.168.2.1 255.255.255.0*
- *R1(config)#interface G0/1.3 ß sub-interface cho VLAN 3*
- *R1(config-subif)#encapsulation dot1Q 3 ß đóng gói giao thức dot1.q cho VLAN 3*
- *R1(config-subif)#ip address 192.168.3.1 255.255.255.0*
- Kiểm tra địa chỉ IP của cổng trên Router:

```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  administratively down down
GigabitEthernet0/1     192.168.1.1     YES manual up                    up
GigabitEthernet0/1.2   192.168.2.1     YES manual up                    up
GigabitEthernet0/1.3   192.168.3.1     YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
R1#
```

- Kiểm tra bảng định tuyến trên Router:
  + R1#show ip route
  + …
  + C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
  + C 192.168.2.0/24 is directly connected, GigabitEthernet0/1.2
  + C 192.168.3.0/24 is directly connected, GigabitEthernet0/1.3
- Bước 4: Kiểm tra kết nối giữa các PC

- Ping từ PC1 đến PC3

```
C:\>ping 192.168.3.2
Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time<1ms TTL=127
Reply from 192.168.3.2: bytes=32 time=10ms TTL=127
Reply from 192.168.3.2: bytes=32 time<1ms TTL=127
Reply from 192.168.3.2: bytes=32 time=3ms TTL=127
```

- Ping từ PC1 đến PC2

```
C:\>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time=1ms TTL=127
Reply from 192.168.2.2: bytes=32 time=11ms TTL=127
```

- Chúc các em học tốt !